

**ПАРЛАМЕНТАРНА СКУПШТИНА
БОСНЕ И ХЕРЦЕГОВИНЕ**

170

На основу члана IV 4. а) Устава Босне и Херцеговине, Парламентарна скупштина Босне и Херцеговине, на 16. хитној сједници Представничког дома, одржаној 23. јануара 2025. године, и на 8. хитној сједници Дома народа, одржаној 30. јануара 2025. године, усвојила је

ЗАКОН

О ЗАШТИТИ ЛИЧНИХ ПОДАТАКА

ДИО ПРВИ – ОПШТЕ ОДРЕДБЕ

Члан 1.
(Предмет)

- (1) Овим законом прописују се:
- правила у вези са заштитом физичких лица у вези с обрадом личних података и правила повезана са слободним кретањем личних података;
 - надлежности Агенције за заштиту личних података у Босни и Херцеговини (у даљем тексту: Агенција), организација и управљање, као и друга питања значајна за њен рад и законито функционисање;
 - заштита физичких лица у вези с обрадом личних података од надлежних органа у сврхе спречавања, истраге и откривања кривичних дјела или гоњења починилаца кривичних дјела, извршавање кривичних санкција, укључујући заштиту од пријетњи јавној безбједности и њихово спречавање.
- (2) Овим законом врши се усклађивање с одредбама Уредбе (ЕУ) 2016/679 Европског парламента и Савјета од 27. априла 2016. године о заштити појединаца у

вези с обрадом личних података и о слободном кретању таквих података, те о стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података) и одредбама Директиве (ЕУ) 2016/680 Европског парламента и Савјета о заштити појединаца у вези с обрадом личних података од надлежних органа с циљем спречавања, истраге и откривања кривичних дјела или гоњења починилаца кривичних дјела или извршавање кривичних санкција и о слободном кретању таквих података, те о стављању ван снаге Оквирне одлуке Савјета 2008/977/ПУП.

- (3) Навођење одредаба Уредбе и Директиве из става (2) овог члана обавља се искључиво с циљем праћења и информисања о преузимању правне тековине Европске уније у законодавству Босне и Херцеговине.

Члан 2.

(Циљ Закона)

Овим законом штите се основна права и слободе физичких лица у Босни и Херцеговини без обзира на њихово држављанство и пребивалиште, а посебно њихово право на заштиту личних података.

Члан 3.

(Употреба мушког или женског рода)

Изрази који су ради прегледности дати у само једном граматичком роду у овом закону без дискриминације се односе и на мушки и женски род.

Члан 4.

(Дефиниције)

Поједини изрази употребљени у овом закону имају следећа значења:

- "лични податак" је сваки податак који се односи на физичко лице чији је идентитет утврђен или се може утврдити;
- "носилац података" је физичко лице чији је идентитет утврђен или чији се идентитет може

- увердити, посредно или непосредно, посебно помоћу идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог лица;
- ц) "обрада" је сваки поступак или скуп поступака који се обавља на личним подацима или на скуповима личних података, аутоматизованим или неаутоматизованим средствима, као што су прикупљање, евидентирање, организација, структурирање, чување, прилагођавање или измјена, проналажење, остваривање увида, употреба, откривање преносом, ширењем или стављањем на располагање на други начин, усклађивање или комбиновање, ограничење, брисање или уништавање;
- д) "ограничење обраде" је обиљежавање чуваног личног податка с циљем ограничења његове обраде у будућности;
- е) "израда профила" је сваки облик аутоматске обраде личног податка који се састоји од коришћења личног податка за процјену одређених личних аспеката у вези са физичким лицем, посебно за анализу или предвиђање аспеката у вези са радним резултатом, економским стањем, здрављем, личним склоностима, интересима, поузданошћу, понашањем, локацијом или кретањем тог физичког лица;
- ф) "псеудонимизација" је обрада личног податка тако да се лични податак више не може приписати одређеном носиоцу података без коришћења додатних информација, уз услов да се такве додатне информације држе одвојено те да подлијежу техничким и организационим мјерама како би се обезбиједило да се лични податак не може приписати појединцу чији је идентитет утврђен или се може утврдити;
- г) "збирка личних података" је сваки структурирани скуп личних података који су доступни у складу са посебним критеријумима, без обзира на то да ли су централизовани, децентрализовани или распрострањени на функционалној или географској основи;
- х) "контролор података" је физичко или правно лице, јавни орган или надлежни орган који самостално или са другим одређује сврхе и средства обраде личних података. Када су сврхе и средства такве обраде утврђени законом, контролор података или посебни критеријуми за његово именовање прописују се законом;
- и) "јавни орган" је сваки законодавни, извршни и судски орган на свим нивоима власти у Босни и Херцеговини;
- ј) "надлежни орган" је орган који је надлежан за спречавање, истрагу и откривање кривичних дјела, гоњење починилаца кривичних дјела или извршење кривичних санкција, укључујући и заштиту и спречавање пријетњи јавној безбједности, као и правна лица ако су законом овлашћена за обављање тих послова, као посебна категорија контролора података;
- к) "обрађивач" је физичко или правно лице, јавни орган који обрађује личне податке у име контролора података;
- л) "прималац" је физичко или правно лице, јавни орган којем се откривају лични подаци, независно од тога да ли је у питању трећа страна. Јавни органи који могу примити личне податке у оквиру одређене истраге у складу са законом не сматрају се примаоцима, али обрада тих података мора бити у складу са важећим правилима о заштити података према сврхама обраде;
- м) "трећа страна" значи физичко или правно лице, јавни орган, Агенција или други орган који није носилац података, контролор података, обрађивач ни лица која су овлашћена за обраду личних података под непосредном надлежношћу контролора података или обрађивача;
- н) "сагласност" носиоца података је свако добровољно, посебно, информисано и недвосмислено изражавање воље носиоца података када он изјавом или јасном потврдом радњом даје пристанак за обраду личних података који се на њега односе;
- о) "повреда личног податка" је кршење безбједности које доводи до случајног или незаконитог уништења, губитка, измјене, неовлашћеног откривања или приступа личним подацима који су пренесени, чувани или на други начин обрађивани;
- п) "генетски податак" је лични податак који се односи на наслијеђена или стечена генетска обиљежја физичког лица која дају јединствене информације о физиологији или здрављу тог физичког лица и који су добијени посебном анализом биолошког узорка тог физичког лица;
- р) "биометријски податак" је лични податак добијен посебном техничком обрадом у вези са физичким особинама, физиолошким обиљежјима или обиљежјима понашања физичког лица која омогућавају или потврђују јединствену идентификацију тог физичког лица, као што су фотографије лица или дактилоскопски подаци;
- с) "податак који се односи на здравље" је лични податак у вези са физичким или менталним здрављем физичког лица, укључујући пружање здравствених услуга, који даје информације о његовом здравственом стању;
- т) "представник" је физичко или правно лице са пребивалиштем или боравиштем, односно сједиштем или пословним настаном у Босни и Херцеговини које је контролор података или обрађивач писаним путем именовао у складу са чланом 29. овог закона;
- у) "привредни субјекат" је физичко или правно лице које обавља привредну дјелатност, без обзира на правни облик те дјелатности;
- в) "група привредних субјеката" је привредни субјекат који остварује контролу и привредни субјекти који су под његовом контролом;
- з) "обавезујуће пословно правило" су политике заштите личних података којих се контролор података и обрађивач са сједиштем или пословним настаном у Босни и Херцеговини придржава приликом преноса или скупова преноса личних података контролору података или обрађивачу у једној или више других држава

- у оквиру групе привредних субјеката или групе привредних субјеката који се баве заједничком привредном дјелатношћу;
- аа) "услуга информационог друштва" јесте свака услуга која се обично пружа уз накнаду, на даљину, електронским средствима те на лични захтјев примаоца услуга, гдје:
- 1) "на даљину" значи да се услуга пружа а да при томе стране нису истовремено присутне;
 - 2) "електронским средствима" значи да се услуга на почетку шаље и прима на одредишту помоћу електронске опреме за обраду (укључујући дигиталну компресију) и похрану података те у потпуности шаље, преноси и прима телеграфски, радио-везом, оптичким средствима или осталим електромагнетним средствима;
 - 3) "на лични захтјев примаоца услуга" значи да се услуга пружа преносом података на лични захтјев.
- бб) "међународна организација" је организација са својим органима уређена међународним јавним правом или било који други орган који су споразумом или на основу споразума основале двије земље или више земаља;
- цц) "пословни настан" је дјелотворно и стварно обављање дјелатности путем стабилних аранжмана;
- дд) "видео-надзор" је информационо-комуникациони систем који има могућност прикупљања и даље обраде личних података, који обухвата стварање снимка који чини или је намијењен да чини дио система складиштења.

Члан 5.

(Главна област примјене)

- (1) Овај закон се примјењује на обраду личног податка која се у потпуности обавља аутоматизовано те на неаутоматизовану обраду личног податка који чини дио збирке личних података или је намијењен да буде дио збирке личних података.
- (2) Овај закон не примјењује се на обраду личног податка коју обавља физичко лице искључиво у сврху личних активности или активности домаћинства.
- (3) На обраду личног податка од надлежног органа у сврху заштите физичких лица у вези с обрадом личних података у сврху спречавања, истраге и откривања кривичних дјела или гоњења починилаца кривичних дјела, извршења кривичних санкција, укључујући и заштиту од пријетњи јавној безбједности и њихово спречавање, не примјењује се ДИО ДРУГИ овог закона.

Члан 6.

(Територијално подручје примјене)

- (1) Овај закон примјењује се на обраду личног податка коју обавља контролор података или обрађивач који има сједиште или пословни настан, пребивалиште или боравиште у Босни и Херцеговини, независно од тога обавља ли се обрада у Босни и Херцеговини или не.
- (2) Овај закон примјењује се на обраду личног податка носиоца података у Босни и Херцеговини коју обавља контролор података или обрађивач који нема сједиште или пословни настан, пребивалиште или боравиште у Босни и Херцеговини, ако је активност обраде повезана са:

- а) нуђењем робе или услуга тим носиоцима података у Босни и Херцеговини, независно од тога да ли носилац података треба да изврши плаћање, или
 - б) праћењем понашања носилаца података, уз услов да се њихово понашање одвија унутар Босне и Херцеговине.
- (3) Овај закон примјењује се на обраду личног податка коју обавља контролор података или обрађивач који нема сједиште или пословни настан у Босни и Херцеговини већ у мјесту гдје се право Босне и Херцеговине примјењује на основу међународног права.
 - (4) На обраду личног податка од надлежног органа у сврху заштите физичког лица у вези с обрадом личног податка у сврху спречавања, истраге и откривања кривичних дјела или гоњења починилаца кривичних дјела, извршења кривичних санкција, укључујући и заштиту од пријетњи јавној безбједности и њихово спречавање, не примјењује се овај члан.

ДИО ДРУГИ – ОБРАДА ЛИЧНОГ ПОДАТКА ОД СТРАНЕ ФИЗИЧКОГ ЛИЦА, ПРАВНОГ ЛИЦА ИЛИ ЈАВНОГ ОРГАНА КАО КОНТРОЛОРА ПОДАТАКА

ГЛАВА I - ПРИНЦИПИ ОБРАДЕ ЛИЧНОГ ПОДАТКА

Члан 7.

(Принципи обраде личног податка)

- (1) Принципи обраде личног податка су:
 - а) законитост, правичност и транспарентност, у односу на носиоца података;
 - б) ограничење сврхе – подаци морају бити прикупљени у посебне, изричите и законите сврхе те се даље не смију обрађивати на начин који није у складу с тим сврхама. Даља обрада у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, у складу са чланом 56. ставом (1) овог закона, не сматра се неусклађеном са првобитним сврхама;
 - ц) смањење обима података – подаци морају бити примјерени, релевантни и ограничени на оно што је неопходно у односу на сврхе за које се обрађују;
 - д) тачност – подаци морају бити тачни и по потреби ажурирани. Морају се предузети све разумне мјере како би се обезбиједило да лични подаци који нису тачни, имајући у виду сврхе у које се обрађују, буду без одгађања избрисани или исправљени;
 - е) ограничење чувања – подаци морају бити чувани у форми која омогућава идентификацију носиоца података и то не дуже него што је потребно у сврхе у које се лични подаци обрађују. Лични подаци се могу чувати на дужи период ако ће се лични подаци обрађивати искључиво у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, у складу са чланом 56. ставом (1) овог закона, што подлијеже спровођењу примјерених техничких и организационих мјера прописаних овим законом ради заштите права и слобода носиоца података;
 - ф) цијеловитост и повјерљивост – подаци морају бити обрађивани тако да се осигура одговарајућа безбједност личних података, укључујући и заштиту од неовлашћене или незаконите обраде

и од случајног губитка, уништења или оштећења примјеном одговарајућих техничких или организационих мјера.

- (2) Принцип поузданости – контролор података одговоран је за усклађеност обраде личног податка са ставом (1) овог члана и мора бити у могућности да докаже ту усклађеност.

Члан 8.

(Законитост обраде личног податка)

- (1) Обрада личног податка је законита само ако је испуњен најмање један од следећих услова:
- а) ако је носилац података дао сагласност за обраду својих личних података у једну или више посебних сврха;
 - б) ако је обрада неопходна ради извршења уговора у којем је носилац података уговорна страна или ради предузимања радњи на захтјев носиоца података прије закључења уговора;
 - ц) ако је обрада неопходна ради поштовања правних обавеза контролора података;
 - д) обрада је неопходна ради заштите кључних интереса носиоца података или другог физичког лица;
 - е) ако је обрада неопходна за извршење задатка који се обавља у јавном интересу или у оквиру извршавања службених овлашћења контролора података;
 - ф) ако је обрада неопходна због легитимних интереса контролора података или треће стране, осим када пад тим интересима претежу интереси или основна права и слобода носиоца података, а који захтијевају заштиту личних података, посебно ако је носилац података дијете. Ова тачка се не примјењује на обраду коју врше јавни органи при обављању својих послова.
- (2) Правни основ за обраду личног податка из става (1) тач. ц) и е) овог члана утврђује се законима институција БиХ, ентитета и кантона у складу са надлежностима, тако да се прецизније пропишу посебни услови за обраду те друге мјере за обезбјеђивање законите и правичне обраде, између осталог и за друге посебне обраде како је то предвиђено у Глави V овог закона.
- (3) Посебним законом за обраду податка из става (1) тач. ц) и е) овог члана институција БиХ, ентитета и кантона, у складу са надлежностима, прописује се сврха обраде, која у вези с обрадом из става (1) тачке е) овог члана мора бити неопходна за извршење задатка који се обавља у јавном интересу или у оквиру извршавања службених овлашћења контролора података. Тим законом прописују се: општи услови којима се уређује законитост обраде коју обавља контролор података, врсте података који се обрађују, категорије носилаца података, субјекти којима се лични подаци могу открити и сврхе у које се подаци могу открити, ограничење сврхе, рокови чувања те радње обраде и поступци обраде, укључујући и мјере за обезбјеђивање законите и правичне обраде, као и за друге посебне обраде како је наведено у Глави V овог закона. Тим законом мора се остварити циљ од јавног интереса и обрада мора да буде пропорционална законитом циљу којем се тежи.
- (4) Ако се обрада обавља у сврху која је различита од сврхе у коју су лични подаци прикупљени и не заснива се на сагласности носилаца података или посебном закону који представља неопходну и

пропорционалну мјеру у демократском друштву за заштиту циљева из члана 25. става (1) овог закона, контролор података, с циљем утврђивања да ли је обрада у другу сврху у складу са сврхом у коју су лични подаци првобитно прикупљени, узима у обзир, између осталог:

- а) сваку везу између сврха у које су лични подаци прикупљени и сврха намјераване даље обраде;
 - б) контекст у којем су лични подаци прикупљени, посебно у вези с односом између носиоца података и контролора података;
 - ц) природу личних података, посебно чињеницу да ли се обрађују посебне категорије личних података у складу са чланом 11. овог закона или лични подаци који се односе на кривичну осуђиваност и кривична дјела у складу са чланом 12. овог закона;
 - д) могуће последице намјераване даље обраде за носиоце података;
 - е) постојање одговарајућих мјера заштите, које могу укључивати енкрипцију или псеудонимизацију.
- (5) Јавни и надлежни органи ентитета и Брчко Дистрикта БиХ дужни су да, уз поштовање одредаба овог закона, уступе личне податке из својих евиденција овлашћеном контролору података, у сврху претходног изјашњавања грађана који имају бирачко право о питањима за које је посебним прописима омогућено то право.

Члан 9.

(Сагласност)

- (1) Када је обрада заснована на сагласности, контролор података мора да докаже да је носилац података дао сагласност за обраду својих личних података.
- (2) Ако носилац података даје сагласност у писаној изјави која се односи и на друга питања, захтјев за сагласност мора да буде представљен тако да се јасно разликује од других питања, у разумљивој и лако доступној форми, уз употребу јасног и једноставног језика. Део сагласности који представља кршење овог закона се не примјењује.
- (3) Носилац података има право да у било којем тренутку повуче своју сагласност. Повлачење сагласности не утиче на законитост обраде података на основу сагласности прије њеног повлачења. Прије давања сагласности носилац података се о томе обавјештава. Повлачење сагласности мора да буде једнако једноставно као и њено давање.
- (4) Када се процјењује да ли је сагласност дата добровољно, у највећој могућој мјери се узима у обзир да ли је, између осталог, извршење уговора, укључујући и пружање услуге, условљено сагласношћу за обраду личних података која није неопходна за извршење тог уговора.

Члан 10.

- (Услови који се примјењују на сагласност дјетета у вези са услугом информационог друштва)
- (1) Када се примјењује члан 8. став (1) тачка а) овог закона у вези са непосредним нуђењем услуге информационог друштва дјетету, обрада личног податка дјетета законита је ако дијете има најмање 16 година. Ако је дијете млађе од 16 година, таква обрада је законита само ако и у мјери у којој је сагласност дао или одобрио родитељ, усвојилац, старатељ дјетета или други заступник дјетета.

- (2) Контролор података мора да уложи разумне напоре приликом провјере да ли је сагласност у тим случајевима дао или одобрио родитељ, усвојилац, односно старатељ дјетета, узимајући у обзир доступну технологију.
- (3) Став (1) овог члана не утиче на општа правила облигационог права која се тичу важења, закључења или учинка уговора у вези са дјететом.

Члан 11.

(Обрада посебних категорија личних података)

- (1) Обрада личних података који откривају расно или етничко поријекло, политичка мишљења, вјерска или филозофска увјерења или припадност синдикату, као и обрада генетских података, биометријских података у сврху јединствене идентификације лица, података о здрављу или података о полном животу или сексуалној оријентацији лица је забрањена.
- (2) Изузетно од одредбе става (1) овог члана, обрада посебне категорије личних података допуштена је ако је испуњен један од следећих услова:
- а) ако је носилац података дао изричиту сагласност за обраду тих личних података за једну или више конкретних сврха, осим када је посебним законом прописано да се обрада тих података не може обављати на основу сагласности;
 - б) ако је обрада неопходна ради извршавања обавеза и остваривања посебних права контролора података или носиоца података у области радног права и права социјалног осигурања и социјалне заштите, у мјери у којој је то прописано законом или колективним уговором у складу са посебним законом којим се прописују одговарајуће мјере заштите основних права и интереса носиоца података;
 - ц) ако је обрада неопходна ради заштите кључних интереса носиоца података или другог физичког лица ако носилац података физички или правно не може дати сагласност;
 - д) ако се обрада обавља у оквиру легитимних активности, уз одговарајуће заштитне мјере, фондације, удружења или било које друге непрофитне организације са политичким, филозофским, вјерским или синдикалним циљем, и то уз услов да се обрада односи искључиво на чланове или бивше чланове те организације или на физичка лица која имају редован контакт с њом, а у вези с њеним сврхама, и да се лични подаци не откривају ван те организације без сагласности носиоца података;
 - е) ако се обрада односи на личне податке за које је очигледно да их је објавио носилац података;
 - ф) ако је обрада неопходна за успостављање, остваривање или одбрану правних захтјева или кад судови поступају у судском својству;
 - г) ако је обрада неопходна за потребе значајног јавног интереса, на основу закона који је пропорционалан легитимном циљу и којим се поштује суштина права на заштиту личних података и обезбјеђују примјерене и посебне мјере за заштиту основних права и интереса носиоца података;
 - х) ако је обрада неопходна за потребе превентивне медицине или медицине рада због процјене радне способности запослених, медицинске дијагнозе, пружања здравствене или социјалне заштите или третмана или управљања системима

и услугама здравствене или социјалне заштите на основу посебног закона или у складу с уговором са здравственим радником и уз услове и мјере заштите из става (3) овог члана;

- и) ако је обрада неопходна из разлога јавног интереса у области јавног здравља, као што је заштита од озбиљних прекограничних пријетњи за здравље или обезбјеђивање високих стандарда квалитета и безбједности здравствене заштите и лијекова и медицинских средстава, на основу посебног закона којим се прописују одговарајуће и посебне мјере за заштиту права и слобода носиоца података, а посебно чување професионалне тајне;
 - ј) ако је обрада неопходна за потребе архивирања у јавном интересу, потребе научног или историјског истраживања или статистичке потребе у складу са чланом 56. ставом (1) овог закона, а на основу посебног закона, који је пропорционалан легитимном циљу и којим се поштује суштина права на заштиту података и обезбјеђују примјерене и посебне мјере за заштиту основних права и интереса носиоца података.
- (3) Лични подаци из става (1) овог члана могу се обрађивати у сврхе наведене у ставу (2) тачки х) овог члана када те податке обрађује стручно лице или се подаци обрађују под одговорношћу стручног лица на које се примјењује обавеза чувања професионалне тајне у складу са посебним законом или правилима која су утврдили надлежни јавни органи или друга лица на које се примјењује обавеза чувања тајне у складу са посебним законом или правилима која су утврдили надлежни јавни органи.
- (4) Посебним законима могу се задржати или увести додатни услови, укључујући и ограничења у односу на обраду генетских података, биометријских података или података о здрављу.

Члан 12.

(Обрада личних података који се односе на кривичну осуђиваност и кривична дјела)

Обрада личних података који се односе на кривичну осуђиваност и кривична дјела или повезане мјере безбједности на основу члана 8. става (1) овог закона може се обављати само под надзором јавног органа или када је обрада прописана посебним законом којим се прописују одговарајуће заштитне мјере за права и слободу носиоца података. Регистар кривичних пресуда води се искључиво под надзором јавног органа.

Члан 13.

(Обрада за коју није потребна идентификација)

- (1) Ако контролор података обрађује личне податке за чију сврху обраде не захтијева или више не захтијева идентификавање носиоца података, контролор података није дужан да чува, прибавља или обрађује додатне информације ради идентификације носиоца података само за потребе поштовања овог закона.
- (2) Ако у случајевима из става (1) овог члана контролор података може да докаже да не може да идентификује носиоца података, контролор података о томе, на одговарајући начин, обавјештава носиоца података, ако је могуће. У тим случајевима се не примјењују чл. од 17. до 22. овог закона, осим у случају да носилац података у сврху остваривања својих права из тих

чланова пружи додатне информације које омогућавају његову идентификацију.

ГЛАВА II - ПРАВА НОСИОЦА ПОДАТАКА

Члан 14.

(Транспарентна информација, комуникација и начин остваривања права носиоца података)

- (1) Контролор података предузима одговарајуће мјере како би се носиоцу података пружиле све информације из чл. 15. и 16. овог закона и сви видови комуникације за остваривање права из чл. од 17. до 24. овог закона и члана 36. овог закона у вези с обрадом података, и то у сажетој, транспарентној, разумљивој и лако доступној форми, уз употребу јасног и једноставног језика, што се посебно односи на све информације које су изричито намијењене дјетету. Информације се пружају у писаној форми или на друге начине, укључујући и електронску форму када је примјерено. Ако носиоца података захтијева, информације се могу пружити усмено, уз услов да је идентитет носиоца података утврђен другим средствима.
- (2) Контролор података олакшава остваривање права носиоца података из чл. од 17. до 24. овог закона. У случајевима из члана 13. става (1) овог закона контролор података не смије да одбије да поступи по захтјеву носиоца података за остваривање његових права из чл. од 17. до 24. овог закона, осим ако контролор података докаже да не може да утврди идентитет носиоца података.
- (3) Контролор података носиоцу података на његов захтјев пружа информације о предузетим радњама из чл. од 17. до 24. овог закона без непотребног одгађања и у сваком случају у року од 30 дана од дана запримања захтјева. Тај се рок може, према потреби, продужити за 60 дана, узимајући у обзир сложеност и број запримљених захтјева. Контролор података обавјештава носиоца података о сваком таквом продужењу у року од 30 дана од дана запримања захтјева, при чему наводи разлоге за одгађање. Ако носиоца података поднесе захтјев електронским путем, информације се пружају електронским путем ако је то могуће, осим у случају када носиоца података захтијева другачије.
- (4) Ако контролор података не поступи по захтјеву носиоца података, дужан је да без одгађања, а најкасније 30 дана од дана запримања захтјева, обавјести носиоца података о разлозима због којих није поступио по захтјеву и о могућности подношења приговора Агенцији или тужбе надлежном суду и другим правним средствима.
- (5) Информације пружене у складу са чл. 15. и 16. овог закона и сва комуникација и дјеловања из чл. од 17. до 24. овог закона и члана 36. овог закона пружају се без накнаде. Ако су захтјеви носиоца података очигледно неосновани или претјерани, посебно због учесталог понављања, контролор података може:
 - а) наплатити накнаду стварних административних трошкова, као што су трошкови умножавања скенирања или трошкови носача података, као и накнаду трошкова достављања или поступања по захтјеву, или
 - б) одбити да поступи по захтјеву.
- (6) Терет доказивања очигледне неоснованости или претјераности захтјева је на контролору података.

- (7) Ако контролор података има оправдане сумње у вези с идентитетом физичког лица које подноси захтјев из чл. од 17. до 23. овог закона, он може, не доводећи у питање члан 13. овог закона, затражити додатне информације неопходне за потврђивање идентитета носиоца података.
- (8) Информације које морају да буду пружене носиоцима података, у складу са чл. 15. и 16. овог закона, могу се пружити у комбинацији са стандардизованим симболима, како би се на лако видљив, разумљив и јасно читљив начин пружило логичан преглед намјераване обраде. Ако су симболи приказани електронски, морају да буду машински читљиви.
- (9) Агенција је овлашћена да донесе прописе у сврху одређивања информација које се приказују симболима и поступке за утврђивање стандардизованих симбола.

Члан 15.

(Информације које треба доставити ако се лични податак прикупља од носиоца података)

- (1) Ако се лични податак прикупља од носиоца података, контролор података у тренутку прикупљања личног податка носиоцу података пружа сљедеће информације:
 - а) идентитет и контактне податке контролора података и контактне податке представника контролора података, ако је примјениво;
 - б) контактне податке службеника за заштиту података, ако је примјениво;
 - ц) правни основ за обраду, те сврху обраде личног податка;
 - д) легитимни интерес контролора података или трећег лица, ако је обрада заснована на члану 8. ставу (1) тачки ф) овог закона;
 - е) о примаоцу или категорији примаоца личних података, ако их има;
 - ф) чињеницу да контролор података намјерава да пренесе личне податке у другу државу или међународну организацију и постојању или непостојању одлуке Савјета министара Босне и Херцеговине о адекватности, односно, у случају преношења из члана 48. или 49. овог закона или члана 51. става (2) овог закона, упућивање на примјерене или одговарајуће заштитне мјере и начине добијања њихове копије или мјесто на којем су стављене на располагање, ако је примјениво.
- (2) Осим информација из става (1) овог члана, контролор података у тренутку прикупљања личног податка пружа носиоцу података сљедеће додатне информације, ако је то неопходно да би се обезбиједила правична и транспарентна обрада:
 - а) о року у којем ће се лични податак чувати или, ако то није могуће, критеријумима који се користе за одређивање тог рока;
 - б) о праву да се од контролора података затражи приступ личног податку, исправка или брисање личног податка или ограничење обраде у вези са носиоцем података или права на улагање приговора на обраду таквог податка те права на преносивост податка;
 - ц) о праву да се сагласност повуче у било којем тренутку, без утицаја на законитост обраде која се заснивала на сагласности прије њеног повлачења, ако је обрада заснована на члану 8. ставу (1) тачки а) овог закона или члану 11. ставу (2) тачки а) овог закона;

- д) о праву на подношење приговора Агенцији или тужбе надлежном суду;
- е) информације о томе да ли је давање личног податка законска или уговорна обавеза или неопходан услов за закључење уговора, као и има ли носилац података обавезу да да лични податак и које су могуће последице ако се такав податак не пружи;
- ф) о постојању аутоматизованог доношења одлука, укључујући и израду профила из чл. 24. ст. (1) и (4) овог закона, при чему је минимално дужан да да информације о начину рада, као и значају и предвиђеним последицама такве обраде за носиоца података.
- (3) Ако контролор података намјерава додатно да обрађује личне податке у сврху која се разликује од сврхе за коју су подаци прикупљени, он прије те додатне обраде носиоцу података пружа информације о тој другој сврси и све додатне релевантне информације из става (2) овог члана.
- (4) Контролор података није дужан да пружи информације носиоцу података из ст. (1), (2) и (3) овог члана у оној мјери у којој носилац података већ располаже тим информацијама.
- Члан 16.
- (Информације које се пружају ако лични податак није добијен од носиоца података)
- (1) Ако лични податак није добијен од носиоца података, контролор података пружа носиоцу података сљедеће информације о:
- а) идентитету и контактним подацима контролора података и представника контролора података, ако је примјениво;
- б) контактним подацима службеника за заштиту података, ако је примјениво;
- ц) правном основу за обраду и за сврхе обраде којој су намињени лични подаци;
- д) категоријама личних података који се обрађују;
- е) примаоцу или категоријама прималаца личних података, према потреби;
- ф) чињеницама да контролор података намјерава да пренесе личне податке примаоцу у другој држави или међународној организацији и постојању или непостојању одлуке Савјета министара Босне и Херцеговине о адекватности из члана 47. става (3) овог закона или у случају преношења личних података из члана 48. или 49. овог закона или члана 51. става (2) овог закона, упућивање на примјерене или одговарајуће заштитне мјере и начине добијања њихове копије или мјеста на којем су стављене на располагање, ако је примјениво.
- (2) Осим информација из става (1) овог члана, контролор података пружа носиоцу података сљедеће информације ако је то неопходно да би се обезбједила правична и транспарентна обрада у односу на носиоца података:
- а) о року у којем ће се лични податак чувати или, ако то није могуће, критеријуме који се користе за одређивање тог рока;
- б) о легитимним интересима контролора података или трећег лица ако је обрада заснована на члану 8. ставу (1) тачки ф) овог закона;
- ц) о праву да се од контролора података затражи приступ личним подацима, исправка или брисање личних података или ограничење обраде у вези са носиоцем података и праву на приговор на обраду, као и праву на преносивост података;
- д) о праву да се сагласност повуче у било којем тренутку, без утицаја на законитост обраде засноване на сагласности прије повлачења, ако је обрада заснована на члану 8. ставу (1) тачки а) овог закона или члану 11. ставу (2) тачки а) овог закона;
- е) о праву на подношење приговора Агенцији или тужбе надлежном суду;
- ф) о извору личних података и, према потреби, да ли долазе из јавно доступних извора;
- г) о постојању аутоматизованог доношења одлука, укључујући и израду профила из члана 24. ст. (1) и (4) овог закона те, најмање у тим случајевима, разумне информације о критеријуму који се користи, као и значају и предвиђеним последицама такве обраде за носиоца података.
- (3) Контролор података пружа информације из ст. (1) и (2) овог члана:
- а) у разумном року након добијања личних података, а најкасније у року од 30 дана, узимајући у обзир посебне околности обраде личног податка;
- б) ако се лични податак користи за комуникацију са носиоцем података, најкасније приликом прве комуникације, или
- ц) ако је предвиђено откривање података другом примаоцу, најкасније у тренутку када је лични податак први пут откривен.
- (4) Ако контролор података намјерава додатно да обрађује лични податак у сврху која се разликује од сврхе за коју су подаци прикупљени, он прије те додатне обраде пружа носиоцу података информације о тој другој сврси и све додатне релевантне информације из става (2) овог члана.
- (5) Ставови од (1) до (4) овог члана не примјењују се ако и у мјери у којој:
- а) носилац података већ посједује информације;
- б) пружање таквих информација је немогуће или би захтијевало непропорционалне напоре, посебно за обраде у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе, у складу са условима и мјерама заштите из члана 56. става (1) овог закона или у мјери у којој је вјероватно да се обавезом из става (1) овог члана може онемогућити или озбиљно угрозити остваривање циљева те обраде. У таквим случајевима, контролор података предузима одговарајуће мјере за заштиту права и слобода и легитимних интереса носиоца података, између осталог и стављањем информација на располагање јавности;
- ц) добијање или откривање података је изричито прописано посебним законом који се примјењује на носиоца података, а који предвиђа одговарајуће мјере за заштиту легитимних интереса носиоца података, или
- д) лични податак мора да остане повјерљив у складу с обавезом чувања професионалне тајне коју прописује посебни закон, укључујући и друге законске обавезе чувања тајне.

Члан 17.

(Право носиоца података на приступ личном податку)

- (1) Носилац података има право да добије потврду од контролора података о томе обрађују ли се његови лични подаци и, ако се обрађују, приступ личним подацима и сљедећим информацијама:
 - а) сврси обраде;
 - б) категорији личног податка који се обрађује;
 - ц) примаоцу или категоријама прималаца којима је лични податак откривен или ће им бити откривен, а посебно примаоцу у другој држави или међународној организацији;
 - д) предвиђеном року у којем се лични подаци чувају или, ако то није могуће, критеријумима коришћеним за одређивање тог рока;
 - е) право да се од контролора података затражи исправка или брисање личног податка или ограничавање обраде личног податка који се односи на носиоца података или право на приговор на такву обраду;
 - ф) право на подношење приговора Агенцији или тужбе надлежном суду;
 - г) ако се лични податак не прикупља од носиоца података, свакој доступној информацији о његовом извору;
 - х) постојању аутоматизованог доношења одлука, укључујући и профилисање из члана 24. ст. (1) и (4) овог закона те, најмање у тим случајевима, разумне информације о критеријуму који се користи, као и значају и предвиђеним последицама такве обраде за носиоца података.
- (2) Ако се лични податак преноси у другу државу или међународну организацију, носилац података има право да буде информисан о одговарајућим мјерама заштите у складу са чланом 48. овог закона које се односе на преношење података.
- (3) Контролор података обезбјеђује копију личног податка који се обрађује. За све додатне копије које затражи носилац података, контролор података може наплатити оправдану накнаду на основу административних трошкова. Ако носилац података поднесе захтјев електронским путем, осим ако носилац података не захтијева другачије, информације се пружају у уобичајеној електронској форми.
- (4) Право на добијање копије из става (3) овог члана не смије негативно утицати на права и слободе других.

Члан 18.

(Право на исправку)

- (1) Носилац података има право да му контролор података омогући исправку нетачног личног податка, без непотребног одгађања.
- (2) Узимајући у обзир сврху обраде, носилац података има право да допуни непотпун лични податак, између осталог и давањем додатне изјаве.

Члан 19.

(Право на брисање)

- (1) Носилац података има право да му контролор података омогући брисање личног податка који се на њега односи, а контролор података има обавезу да обрише лични податак, без непотребног одгађања, ако је испуњен један од сљедећих услова:
 - а) лични податак више није неопходан за сврхе у које је прикупљен или на други начин обрађен;
 - б) носилац података повукао је сагласност на којој је обрада заснована у складу са чланом 8. ставом

(1) тачком а) овог закона или чланом 11. ставом

(2) тачком а) овог закона и ако не постоји други правни основ за обраду;

- ц) носилац података уложио је приговор на обраду у складу са чланом 23. ставом (1) овог закона и не постоје законски разлози за обраду или је носилац података уложио приговор на обраду у складу са чланом 23. ставом (2) овог закона;
 - д) лични податак је незаконито обрађен;
 - е) лични податак мора бити обрисан ради поступања у складу са законском обавезом којој подлијеже контролор података;
 - ф) лични податак је прикупљен у вези са понудом услуга информационог друштва из члана 10. става (1) овог закона.
- (2) Ако је контролор података јавно објавио лични податак, а дужан је да у складу са ставом (1) овог члана тај лични податак брише, узимајући у обзир доступну технологију и трошкове спровођења, контролор података предузима разумне мјере, укључујући и техничке мјере, да би обавијестио контролоре података који обрађују лични податак да је носилац података затражио од тих контролора података да бришу све повезнице до њега или копију или реконструкцију тог личног податка.
 - (3) Ставови (1) и (2) овог члана не примјењују се у мјери у којој је обрада неопходна:
 - а) ради остваривања права на слободу изражавања и информисања;
 - б) ради поштовања законске обавезе којом се захтијева обрада прописана посебним законом, а која се примјењује на контролора података или ради извршења задатка који се обавља у јавном интересу или у оквиру извршавања службених овлашћења додијељених контролору података;
 - ц) ради јавног интереса у области јавног здравља у складу са чланом 11. ставом (2) тач. х) и и) овог члана, као и чланом 11. ставом (3) овог закона;
 - д) у сврхе архивирања у јавном интересу, у сврхе научног или историјског истраживања или у статистичке сврхе у складу са чланом 56. ставом (1) овог закона у мјери у којој је вјероватно да се правом из става (1) овог члана може онемогућити или озбиљно угрозити остваривање циљева те обраде или
 - е) ради постављања, остваривања или одбране правних захтјева.

Члан 20.

(Право на ограничење обраде)

- (1) Носилац података има право на ограничење обраде података ако је испуњен један од сљедећих услова:
 - а) носилац података оспорава тачност личног податка, у року у којем се контролору података омогућава да провери тачност личног податка;
 - б) обрада је незаконита, а носилац података се противи брисању личног податка и умјесто тога тражи ограничење његове обраде;
 - ц) контролору података више није потребан лични податак за потребе обраде, али га носилац података захтијева ради постављања, остваривања или одбране правних захтјева;
 - д) носилац података уложио је приговор на обраду у складу са чланом 23. ставом (1) овог закона и очекује потврду о томе да ли превладавају његови разлози над легитимним разлозима контролора података.

- (2) Ако је обрада ограничена у складу са ставом (1) овог члана, тај лични податак смије се обрађивати само уз сагласност носиоца података, изузев чувања, или за постављање, остваривање или одбрану правних захтјева или заштиту права другог физичког или правног лица или због важног јавног интереса.
- (3) Носиоца података који је остварио право на ограничење обраде, у складу са ставом (1) овог члана, контролор података обавјештава прије укидања ограничења обраде.

Члан 21.

(Обавеза обавјештавања о исправци или брисању личног податка или ограничењу обраде)

- (1) Контролор података обавјештава све примаоце којима су лични подаци откривени о свакој исправци или брисању личног податка или ограничењу обраде извршеном у складу са чланом 18, чланом 19. ставом (1) и чланом 20. овог закона, осим у случају када је то немогуће или ако то захтијева непропорционалан напор.
- (2) Контролор података обавјештава носиоца података о тим примаоцима, ако носилац података то захтијева.

Члан 22.

(Право на преносивост личног податка)

- (1) Носилац података има право да преузме лични податак, који се односи на њега а који је дао контролору података, у структурираном, уобичајено употребљаваном и машински читљивом формату, те има право да преноси тај податак другом контролору података без ометања од контролора података којем је лични податак дат, ако се:
- а) обрада обавља у складу са чланом 8. ставом (1) тачком а) овог закона или чланом 11. ставом (2) тачком а) овог закона или на основу уговора у складу са чланом 8. ставом (1) тачком б) овог закона;
- б) обрада обавља аутоматски.
- (2) При остваривању свог права на преносивост податка, у складу са ставом (1) овог члана, носилац података има право на непосредни пренос од једног контролора података другом контролору података, ако је то технички изводљиво.
- (3) Остваривањем права на преносивост података из става (1) овог члана не доводи се у питање члан 19. овог закона. То право се не примјењује на обраду неопходну за извршење задатка који се обавља у јавном интересу или у оквиру службених овлашћења додијељених контролору података.
- (4) Право на преносивост податка из става (1) овог члана не смије негативно утицати на права и слободе других.

Члан 23.

(Право на приговор)

- (1) Носилац података има право да на основу своје посебне ситуације у сваком тренутку контролору података поднесе приговор на обраду његовог личног податка, у складу са чланом 8. ставом (1) тач. е) или ф) овог закона, укључујући профилисање засновано на тим одредбама. Контролор података не смије даље обрађивати лични податак, осим у случају да докаже да постоје увјерљиви легитимни разлози за обраду који превађавају над интересима, правима и слободама носиоца података или ради постављања, остваривања или одбране правних захтјева.

- (2) Ако се лични податак обрађује за потребе директног маркетинга, носилац података има право да у било којем тренутку уложи приговор на обраду личног податка који се односи на њега, за потребе таквог маркетинга, што укључује израду профила у мјери у којој је повезано са таквим директним маркетингом.
- (3) Ако се носилац података противи обради за потребе директног маркетинга, лични податак се више не смије обрађивати у те сврхе.
- (4) Најкасније у тренутку прве комуникације са носиоцем података, носилац података се изричито мора упутити на права из ст. (1) и (2) овог члана те се то мора учинити на јасан начин и одвојено од било које друге информације.
- (5) У контексту коришћења услуга информационог друштва и не узимајући у обзир прописе из области електронских комуникација, носилац података може остварити своје право на приговор аутоматизованим путем помоћу техничких спецификација.
- (6) Ако се лични податак обрађује у сврхе научног или историјског истраживања или у статистичке сврхе на основу члана 56. става (1) овог закона, носилац података на основу своје посебне ситуације има право да уложи приговор на обраду личног податка који се на њега односи, осим ако је обрада неопходна за извршење задатка који се обавља у јавном интересу.

Члан 24.

(Аутоматизовано појединачно доношење одлуке, укључујући и профилисање)

- (1) Носилац података има право да се на њега не примјењује одлука заснована искључиво на аутоматизованој обради, укључујући и профилисање, која производи правни učinak који се на њега односи или на сличан начин значајно на њега утиче.
- (2) Став (1) овог члана не примјењује се ако је одлука:
- а) потребна за закључивање или извршење уговора између носиоца података и контролора података;
- б) допуштена законом који се примјењује на контролора података и којим се прописују одговарајуће заштитне мјере за права и слободе те легитимне интересе носиоца података, или
- ц) заснована на изричитој сагласности носиоца података.
- (3) У случајевима из става (2) тач. а) и ц) овог члана, контролор података предузима одговарајуће мјере за заштиту права и слобода те легитимних интереса носиоца података, најмање права на учествовање физичког лица у доношењу одлуке, права изражавања властитог става и права на оспоравање одлуке.
- (4) Одлука из става (2) овог члана не смије бити заснована на посебним категоријама личних података из члана 11. става (1) овог закона, осим ако се примјењује члан 11. став (2) тачка а) или г) овог закона те ако су успостављене одговарајуће мјере за заштиту права и слобода и легитимних интереса носиоца података.

Члан 25.

(Ограничења)

- (1) На основу посебног закона који се примјењује на контролора података и обрађивача може се ограничити опсег права и обавеза из члана 7, чл. од 14. до 24. овог закона и члана 36. овог закона, ако одредбе тог закона одговарају правима и обавезама прописаним у чл. од 14. до 24. овог закона, ако се таквим ограничењем поштује суштина основних

права и слобода и ако оно представља неопходну и пропорционалну мјеру у демократском друштву за заштиту:

- а) државне безбједности;
 - б) одбране;
 - ц) јавне безбједности;
 - д) спречавања, истраге, откривања или гоњења кривичних дјела или извршења кривичних санкција, укључујући заштиту од пријетњи јавној безбједности и њихово спречавање;
 - е) других важних циљева од општег јавног интереса у Босни и Херцеговини, а посебно важног привредног или финансијског интереса, што укључује монетарна, буџетска и пореска питања, јавно здравство и социјалну заштиту;
 - ф) независности правосуђа и судских поступака;
 - г) спречавања, истраге, откривања и гоњења поворде етике у законски регулисаним професијама;
 - х) надзорне, инспекцијске или регулаторне функције која је, најмање повремено, повезана с извршавањем службених овлашћења у случајевима из тач. од а) до е) и тачке г) овог става;
 - и) носиоца података или права и слобода других;
 - ј) остваривања потраживања у грађанским споровима.
- (2) Посебни закон из става (1) овог члана садржи, по потреби, посебне одредбе, које садрже најмање следеће:
- а) сврху обраде или категорију обраде;
 - б) категорију личног податка;
 - ц) обим уведених ограничења;
 - д) мјере заштите за спречавање злоупотребе или незаконитог приступа или преношења;
 - е) одређивање контролора података или категорију контролора података;
 - ф) рок чувања и мјере заштите које се могу примјенити узимајући у обзир природу, обим и сврху обраде или категорије обраде;
 - г) ризик за права и слободу носиоца података;
 - х) право носиоца података да буде обавијештен о ограничењу, осим ако то може бити штетно за сврху тог ограничења.

ГЛАВА III - КОНТРОЛОР ПОДАТАКА И ОБРАЂИВАЧ

Члан 26.

(Обавеза контролора података)

- (1) Контролор података дужан је да примјени одговарајуће техничке и организационе мјере имајући у виду природу, обим, околности и сврху обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободу физичких лица, како би обезбиједио да се обрада обавља у складу с овим законом и како би то могао доказати. Те мјере се према потреби преиспитују и ажурирају.
- (2) Мјере из става (1) овог члана, ако су пропорционалне у односу на активности обраде, укључују спровођење одговарајућих политика заштите података од контролора података.
- (3) Поштовање одобрених кодекса понашања из члана 42. овог закона или одобрених механизма сертификације из члана 44. овог закона може служити као елемент за доказивање усклађености с обавезама контролора података.

Члан 27.

(Техничка и интегрисана заштита података)

- (1) Узимајући у обзир најновија достигнућа, трошкове спровођења и природу, обим, контекст и сврху обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободу физичких лица који произлазе из обраде података, контролор података, приликом одређивања средстава обраде и при самој обради, примјењује одговарајуће техничке и организационе мјере, попут псеудонимизације, за омогућавање дјелотворне примјене принципа заштите података, као што је смањење количине података те укључивање заштитних мјера у обраду како би се испунили захтјеви из овог закона и заштитила права носиоца података.
- (2) Контролор података примјењује одговарајуће техничке и организационе мјере којима се обезбеђује да интегрисаним начином буду обрађени само лични подаци који су неопходни за сваку посебну сврху обраде. Та обавеза се примјењује на све прикупљене личне податке, обим њихове обраде, рок њиховог чувања и њихову доступност. Тим се мјерама обезбеђује да лични подаци нису аутоматски, без интервенције физичког лица, доступни неограниченом броју других физичких лица.
- (3) Одобрени механизам сертификације из члана 44. овог закона може служити као елемент за доказивање усклађености са захтјевима из ст. (1) и (2) овог члана.

Члан 28.

(Заједнички контролори података)

- (1) Ако два или више контролора података заједнички одреде сврху и начине обраде, сматрају се заједничким контролорима података. Они на транспарентан начин, међусобним споразумом, одређују одговорности свакога од њих с циљем извршавања обавеза из овог закона, посебно у вези са остваривањем права носиоца података и дужностима свакога од њих у вези са пружањем информација из чл. 15. и 16. овог закона, осим у случају да су одговорности сваког од контролора података утврђене законом који се примјењује на контролоре података. Споразумом се може одредити контактна тачка за носиоца података.
- (2) Споразум из става (1) овог члана мора на одговарајући начин одражавати појединачне улоге и односе заједничких контролора података у односу на носиоце података. Суштина споразума мора бити доступна носиоцу података.
- (3) Независно од услова споразума из става (1) овог члана, носилац података може остваривати своја права из овог закона у вези са сваким контролором података и против сваког од њих.

Члан 29.

(Представник контролора података или обрађивача који нема сједиште или пословни настан у Босни и Херцеговини)

- (1) Ако се примјењује члан 6. став (2) овог закона, контролор података или обрађивач има обавезу да писаним путем именује свог представника у Босни и Херцеговини.
- (2) Обавеза из става (1) овог члана не примјењује се на:
 - а) обраду која је повремена, не подразумијева у већој мјери обраду посебних категорија података из члана 11. става (1) овог закона или обраду личних података који се односе на кривичну

осуђиваност и кривична дјела из члана 12. овог закона и за коју није вјероватно да ће проузроковати ризик за права и слободе физичких лица, узимајући у обзир природу, околности, обим и сврхе обраде или

- б) јавне органе.
- (3) Контролор података или обрађивач овлашћује представника како би се, уз обраћање контролору података или обрађивачу или умјесто обраћања њима, њему обраћали посебно Агенција и носилац података у вези са свим питањима која се односе на обраду личног податка ради обезбјеђивања усклађености обраде личног податка с овим законом.
- (4) Именоване представника контролора података или обрађивача не утиче на правне захтјеве који могу бити усмјерени против самог контролора података или обрађивача.

Члан 30. (Обрађивач)

- (1) Ако се обрада личног податка обавља у име контролора података, контролор података користи искључиво обрађивача који у довољној мјери гарантује примјену одговарајућих техничких и организационих мјера тако да обрада буде у складу са захтјевима из овог закона и да се обрадом обезбјеђује заштита права носиоца података.
- (2) Обрађивач не смије ангажовати другог обрађивача без претходног посебног или општег писаног одобрења контролора података. У случају општег писаног одобрења, обрађивач обавјештава контролора података о свим планираним измјенама у вези са додавањем или замјеном других обрађивача како би тиме контролору података омогућио да уложи приговор на те измјене.
- (3) Обрада коју обавља обрађивач уређује се уговором или другим правним актом у складу са законом који обавезује обрађивача према контролору података, у којем се наводе предмет и трајање обраде, природа и сврха обраде, врста личних података и категорија носиоца података, као и обавезе и права контролора података.
- (4) Уговором или другим правним актом из става (3) овог члана прописује се да је обрађивач дужан да:
- обрађује лични податак само према документованим упутствима контролора података, између осталог и у вези са преносом личног податка у другу државу или међународну организацију, осим ако је то прописано посебним законом који се примјењује на обрађивача, а у том случају, обрађивач обавјештава контролора података о том правном захтјеву прије обраде, осим ако се тим законом забрањује такво обавјештавање због важних разлога од јавног интереса;
 - обезбјеђује да су се лица овлашћена за обраду личног податка обавезала на поштовање повјерљивости или да их на поштовање повјерљивости обавезује одговарајући закон;
 - предузима све потребне мјере у складу са чланом 34. овог закона;
 - поштује услове из ст. (2) и (5) овог члана за ангажовање другог обрађивача;
 - узимајући у обзир природу обраде, помаже контролору података путем одговарајућих техничких и организационих мјера, колико је то могуће, да испуни обавезу контролора података да одговори на захтјеве за остваривање права носиоца података из Главе II овог закона;
 - помаже контролору података у обезбјеђивању усклађености с обавезама из чл. 34. до 38. овог закона, узимајући у обзир природу обраде и информације које су доступне обрађивачу;
 - по избору контролора података, брише или враћа контролору података све личне податке након завршетка пружања услуга у вези с обрадом и брише постојеће копије, осим у случају да је посебним законом прописана обавеза чувања личних података;
 - контролору података ставља на располагање све информације које су неопходне за доказивање поштовања обавеза из овог члана и контролору података или другом ревизору којег је овластио контролор података омогућава обављање ревизије, укључујући и инспекције, и помаже у њиховом обављању;
 - у случају из тачке х) овог става обрађивач одмах обавјештава контролора података ако, према његовом мишљењу, одређено упутство крши овај закон или друга правила о заштити података.
- (5) Ако обрађивач ангажује другог обрађивача за обављање посебних активности обраде у име контролора података, исте обавезе за заштиту података као оне које су наведене у уговору или другом правном акту између контролора података и обрађивача из става (4) овог члана намећу се том другом обрађивачу уговором или другим правним актом у складу са посебним законом, а посебно обавеза давања довољно гаранција за примјену одговарајућих техничких и организационих мјера на начин којим се обезбјеђује да обрада задовољава захтјеве из овог закона. Ако тај други обрађивач не испуњава обавезе заштите података, први обрађивач остаје у потпуности одговоран контролору података за извршавање обавеза тог другог обрађивача.
- (6) Поштовање одобрених кодекса понашања од обрађивача, из члана 42. овог закона, или одобреног механизма сертификације, из члана 44. овог закона, може служити као елемент за доказивање пружања довољно гаранција из ст. (1) и (5) овог члана.
- (7) Не доводећи у питање појединачни уговор између контролора података и обрађивача, уговор или други правни акт из ст. (3), (4) и (5) овог члана може се у цјелини или дјелимично заснивати на стандардним уговорним клаузулама из ст. (8) и (9) овог члана, укључујући између осталог и клаузуле које су дио сертификата додијељеног контролору података или обрађивачу у складу са чл. 44. и 45. овог закона.
- (8) Агенција може донијети стандардне уговорне клаузуле за питања из ст. (3), (4) и (5) овог члана с циљем досљедне примјене овог закона.
- (9) Уговор или други правни акт из ст. (3), (4) и (5) овог члана мора бити у писаној форми, што укључује и електронску форму.
- (10) Не доводећи у питање чл. 112, 113, 114. и 115. овог закона, ако обрађивач крши овај закон тиме што одређује сврху и начине обраде података, обрађивач се сматра контролором података у вези с том обрадом.

Члан 31.

(Обрада личног податка под контролом контролора података или обрађивача)

Обрађивач и лице које ради под контролом контролора података или обрађивача, а има приступ

личном податку, не смије обрађивати тај податак без налога контролора података, осим када је то прописано посебним законом.

Члан 32.

(Евиденција о обради личног податка)

- (1) Сваки контролор података и представник контролора података, ако је примјениво, води евиденцију активности обраде за које је одговоран. Евиденција садржи следеће информације:
 - а) име и контакт податке контролора података и, ако је примјениво, заједничког контролора података, представника контролора података и службеника за заштиту података;
 - б) сврхе обраде;
 - ц) опис категорија носилаца података и категорија личних података;
 - д) категорије прималаца којима су лични подаци откривени или ће им бити откривени, укључујући и примаоце у другим државама или међународним организацијама;
 - е) ако је примјениво, о преносу личних података у другу државу или међународну организацију, укључујући идентификацију друге државе или међународне организације и, у случају преноса из члана 51. става (2) овог закона, документацију о одговарајућим заштитним мјерама;
 - ф) ако је могуће, предвиђене рокове за брисање различитих категорија података;
 - г) ако је могуће, општи опис техничких и организационих безбједносних мјера из члана 34. става (1) овог закона.
- (2) Сваки обрађивач и представник обрађивача, ако је примјениво, води евиденцију о свим активностима обраде које се обављају у име контролора података, која садржи:
 - а) име и контакт податке једног или више обрађивача и сваког контролора података у чије име обрађивач дјелује те, ако је примјениво, представника контролора података или обрађивача, као и службеника за заштиту података;
 - б) врсте обраде које се обављају у име сваког контролора података;
 - ц) ако је примјениво, информације о преносу личних података у другу државу или међународну организацију, с идентификацијом те друге државе или међународне организације и у случају преноса из члана 51. става (2) овог закона, документацију о одговарајућим заштитним мјерама;
 - д) ако је могуће, општи опис техничких и организационих безбједносних мјера из члана 34. става (1) овог закона.
- (3) Евиденција из ст. (1) и (2) овог члана мора бити у писаној форми, што укључује и електронску форму.
- (4) Контролор података или обрађивач те представник контролора података или обрађивача, ако је примјениво, на захтјев Агенције омогућавају увид у евиденцију.
- (5) Обавезе из ст. (1) и (2) овог члана не примјењују се на привредни субјекат или организацију у којој је запослено мање од 250 лица, осим када постоји вјероватноћа да ће обрада коју обавља представљати висок ризик за права и слободе носиоца података, ако обрада није повремени или ако обрада обухвата посебне категорије података из члана 11. става (1)

овог закона, или су у питању лични подаци који се односе на кривичну осуђиваност и кривична дјела.

Члан 33.

(Сарадња с Агенцијом)

Контролор података и обрађивач, те ако су одређени њихови представници, дужни су, на образложен и на основу закона оправдан захтјев, да сарађују с Агенцијом у обављању њених задатака.

Члан 34.

(Безбједност обраде личног податка)

- (1) Узимајући у обзир најновија достигнућа, трошкове спровођења и природу, обим, контекст и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободе физичких лица, спроводећи поступак из члана 37. овог закона, контролор података и обрађивач примјењују одговарајуће техничке и организационе мјере како би постигли одговарајући ниво безбједности с обзиром на ризик, што према потреби подразумева:
 - а) псеудонимизацију и енкрипцију личног податка;
 - б) могућност обезбјеђивања трајне повјерљивости, цијеловитости, доступности и отпорности система и услуга обраде;
 - ц) способност благовременог поновног успостављања доступности личног податка и приступа њему у случају физичког или техничког инцидента;
 - д) поступак редовног тестирања, оцјењивања и процјене дјелотворности техничких и организационих мјера за постизање безбједности обраде.
- (2) Приликом процјене одговарајућег нивоа безбједности, у обзир се узимају прије свега ризици које представља обрада, а посебно ризици од случајног или незаконитог уништења, губитка, измјене, неовлашћеног откривања личног податка или неовлашћеног приступа личном податку који је пренесен, чуван или на други начин обрађиван.
- (3) Примјена одобреног кодекса понашања из члана 42. овог закона или одобреног механизма сертификације из члана 44. овог закона може се користити као елемент за доказивање усклађености са захтјевима из става (1) овог члана.
- (4) Контролор података и обрађивач предузимају мјере како би обезбједили да свако физичко лице које дјелује под надлежношћу контролора података или обрађивача, а које има приступ личном податку, не обрађује тај податак ако то није према упутствима контролора података, осим у случајевима када је то прописано посебним законом.

Члан 35.

(Извјештавање Агенције о повреди личног податка)

- (1) Контролор података дужан је да о повреди личног податка без непотребног одгађања и, ако је могуће, најкасније у року од 72 сата након сазнања за ту повреду обавијести Агенцију о повреди личног податка, осим у случају ако је вјероватно да та повреда неће угрозити права и слободе физичког лица. Ако извјештавање није извршено у року од 72 сата, контролор података дужан је да Агенцији наведе разлоге за кашњење.
- (2) Обрађивач је дужан да, по сазнању за повреду личног податка, без непотребног одгађања о томе обавијести контролора података.

- (3) Извјештај из става (1) овог члана садржи најмање следеће:
- а) опис природе повреде личних података и, ако је могуће, са наведеним категоријама и приближним бројем носилаца података, као и категоријама и приближним бројем евиденција личних података;
 - б) име и презиме те контакт податке службеника за заштиту података или друге контакт тачке од које се може добити још информација;
 - ц) опис могуће последице повреде личног податка;
 - д) опис мјера које је контролор података предузео или чије је предузимање предложено ради рјешавања проблема повреде личног податка, укључујући према потреби и мјере за ублажавање њених могућих штетних последица.
- (4) Ако и у мјери у којој није могуће истовремено доставити информације, информације се могу достављати у дијеловима, без непотребног даљег одгађања.
- (5) Контролор података документује сваку повреду личног податка, укључујући и чињенице у вези са повредом личног податка, њене последице и мјере предузете за отклањање штете. Документација из овог става омогућава Агенцији поступање по овом члану.

Члан 36.

(Обавјештавање носиоца података о повреди личног податка)

- (1) Контролор података дужан је да без одгађања писаним путем обавијести носиоца података о повреди личног податка, ако је вјероватно да ће повреда личног податка проузроковати висок ризик за права и слободе физичког лица.
- (2) Контролор података у обавјештењу из става (1) овог члана, јасним и једноставним језиком, описује природу повреде личног податка те се најмање наводе информације и мјере из члана 35. става (3) тач. б), ц) и д) овог закона.
- (3) Обавјештавање носиоца података из става (1) овог члана није обавезно ако је испуњен један од следећих услова:
 - а) ако је контролор података предузео одговарајуће техничке и организационе заштитне мјере и те мјере су примјењене на лични податак у вези с којим је дошло до повреде личног податка, а прије свега мјере које лични податак чине неразумљивим лицу које није овлашћено да му приступи, као што је енкрипција;
 - б) ако је контролор података предузео наплатне мјере којима се обезбјеђује да више није могуће да ће доћи до високог ризика за права и слободе носиоца података из става (1) овог члана;
 - ц) ако би то захтијевало непропорционалан напор, мора се објавити јавно саопштење или се предузима слична мјера којом се носиоци података обавјештавају на једнако дјелотворан начин.
- (4) Ако контролор података није обавијестио носиоца података о повреди личног податка, Агенција, након разматрања степена вјероватноће да ће повреда личног податка проузроковати висок ризик за права и слободе физичких лица, може од контролора података захтијевати да то учини, ако није испуњен неки од услова из става (3) овог члана.

Члан 37.

(Процјена утицаја обраде на заштиту личног податка)

- (1) Ако је вјероватно да ће нека врста обраде, посебно посредством нових технологија и узимајући у обзир природу, обим, контекст и сврхе обраде, проузроковати висок ризик за права и слободе физичких лица, контролор података прије обраде спроводи процјену утицаја предвиђених обрада на заштиту личног податка.
- (2) Приликом спровођења процјене утицаја обраде на заштиту личног податка, контролор података тражи савјет службеника за заштиту личних података, ако је именован.
- (3) Процјена утицаја обраде на заштиту личног податка из става (1) овог члана обавезна је посебно у случају:
 - а) системске и обимне процјене личних аспеката у вези са физичким лицима која се заснива на аутоматизованој обради, укључујући профилисање, и која је основа за доношење одлука које производе правни učinak у односу на физичко лице или на сличан начин значајно утичу на физичко лице;
 - б) обимне обраде посебних категорија личних података из члана 11. става (1) овог закона или података који се односе на кривичну осуђиваност и кривична дјела из члана 12. овог закона, или
 - ц) системског праћења јавно доступног подручја у великој мјери.
- (4) Агенција утврђује и јавно објављује листу врста поступака обраде на које се примјењује обавеза спровођења процјене утицаја на заштиту личних података, у складу са ставом (1) овог члана.
- (5) Агенција може да утврди и јавно објави листу врста поступака обраде за које није потребна процјена утицаја на заштиту личног податка.
- (6) Процјена утицаја обухвата најмање:
 - а) системски опис предвиђених обрада и сврха обраде, укључујући, ако је примјењиво, легитиман интерес контролора података;
 - б) процјену нужности и пропорционалности обрада повезаних с њиховим сврхама;
 - ц) процјену ризика за права и слободе носиоца података;
 - д) предвиђене мјере за рјешавање ризика, што укључује заштитне мјере, безбједносне мјере и механизме за безбједност заштите личних података и доказивање усклађености с овим законом, узимајући у обзир права и легитимне интересе носиоца података и других укључених лица.
- (7) Усклађеност кодекса понашања из члана 42. овог закона одобрених од контролора података или обрађивача узима се у обзир приликом процјене утицаја обраде које примјењују ти контролори података или обрађивачи, посебно у сврхе процјене утицаја на заштиту личних података.
- (8) Контролор података, по потреби, од носиоца података или његовог представника тражи мишљење о намјерованој обради, не доводећи у питање комерцијалне или јавне интересе или безбједност поступка обраде.
- (9) Ако обрада у складу са чланом 8. ставом (1) тач. ц) или е) овог закона има правну основу у посебном закону који се примјењује на контролора података, ако су тим законом уређене посебне обраде или скуп предметних радњи и ако је процјена утицаја на

заштиту личних података већ спроведена као дио опште процјене утицаја у контексту доношења правног основа, ст. од (1) до (6) овог члана се не примјењују, осим ако је посебним прописом утврђено да је потребно спровести такву процјену прије обраде.

(10) Контролор података, по потреби, преиспитује да ли је обрада извршена у складу са проценом утицаја на заштиту личних података и то најмање када дође до промјене у нивоу ризика који представљају поступци обраде.

Члан 38.

(Претходно савјетовање контролора података с Агенцијом)

- (1) Контролор обраде савјетује се с Агенцијом прије обраде ако је процјена утицаја на заштиту личних података из члана 37. овог закона показала да би обрада података проузроковала висок ризик за права и слободе појединаца, у случају да контролор података не донесе мјере за ублажавање ризика.
- (2) Ако Агенција утврди да би се намјераваном обрадом из става (1) овог члана кршио овај закон, посебно ако контролор података није у довољној мјери утврдио или умањio ризик за права и слободе појединаца, Агенција у року од највише 56 дана од запримања захтјева за савјетовање писаним путем савјетује контролора података, а по потреби и обрађивача, и при томе може користити овлашћења из члана 103. овог закона.
- (3) Рок из става (2) овог члана, по потреби, може се продужити за 42 дана, у зависности од сложености намјераване обраде.
- (4) Агенција у року од 30 дана од запримања захтјева обавјештава контролора података, а по потреби и обрађивача, о продужењу рока из става (3) овог члана и о разлозима одлагања.
- (5) Протичање рокова из ст. (2) и (3) овог члана може бити привремено обустављено док Агенција не добије информације које је захтијевала за потребе савјетовања.
- (6) При савјетовању контролор података Агенцији доставља:
 - а) ако је примјениво, одговарајуће одговорности контролора података, заједничких контролора података и обрађивача који учествују у обради, посебно у случају обраде унутар групе привредних субјеката;
 - б) сврху и средства намјераване обраде;
 - ц) заштитне мјере и друге мјере за заштиту права и слобода носиоца података на основу овог закона;
 - д) контактне податке службеника за заштиту података, ако је примјениво;
 - е) процјену утицаја на заштиту података како је прописано чланом 37. овог закона;
 - ф) све друге информације које Агенција затражи.
- (7) О приједлогу закона којим се регулише обрада личних података, прије његовог упућивања у парламентарну процедуру, предлагач се може претходно савјетовати с Агенцијом.
- (8) Независно од става (1) овог члана, посебним законом се може прописати обавеза контролору података да се савјетује с Агенцијом и да од ње прибави претходно одобрење у вези с обрадом коју обавља за извршење задатака у јавном интересу, укључујући и обраду у вези са социјалном и здравственом заштитом.

Члан 39.

(Именовање службеника за заштиту личних података)

- (1) Контролор података и обрађивач дужни су да именују службеника за заштиту личних података у случајевима:
 - а) ако обраду обавља јавни орган, осим судова који поступају у оквиру судске надлежности;
 - б) ако се основне дјелатности контролора података или обрађивача састоје од поступака обраде које због своје природе, обима и/или сврхе захтијевају редовно и системско праћење носиоца података у великом броју, или
 - ц) ако се основне дјелатности контролора података или обрађивача састоје од обимне обраде посебних категорија података на основу члана 11. овог закона и личних података у вези са кривичном осуђиваношћу и кривичним дјелима из члана 12. овог закона.
- (2) Група привредних субјеката може именовати једног службеника за заштиту личних података уз услов да је службеник за заштиту личних података лако доступан из сваког сједишта или пословног настана.
- (3) Ако је контролор података или обрађивач јавни орган, за више таквих органа може се именовати један службеник за заштиту личних података, узимајући у обзир њихову организациону структуру и величину.
- (4) У случајевима који нису наведени у ставу (1) овог члана, контролор података или обрађивач или удружење и други орган који представља категорију контролора података или обрађивача могу, односно у случајевима када је то прописано посебним законом, морају именовати службеника за заштиту личних података. Службеник за заштиту личних података може да обавља послове у име тих удружења и других органа који представљају контролоре података или обрађиваче.
- (5) Службеник за заштиту личних података именује се на основу његових стручних квалификација, а посебно стручног знања о праву и пракси у области заштите личних података и способности обављања задатака из члана 41. овог закона.
- (6) Службеник за заштиту личних података може бити запослен код контролора података или обрађивача или може обављати послове на основу уговора о дјелу.
- (7) Контролор података или обрађивач објављује контактне податке службеника за заштиту личних података и доставља их Агенцији.

Члан 40.

(Статус службеника за заштиту личних података)

- (1) Контролор података и обрађивач обезбјеђују да службеник за заштиту личних података буде на одговарајући начин и благовремено укључен у сва питања која се тичу заштите личних података.
- (2) Контролор података и обрађивач подржавају службеника за заштиту личних података у обављању задатака из члана 41. овог закона, пружајући му потребна средства за извршавање тих задатака и остваривање приступа личним подацима и поступцима обраде, као и за одржавање његовог стручног знања.
- (3) Контролор података и обрађивач обезбјеђују да службеник за заштиту личних података не прима никакве инструкције при обављању тих задатака. Контролор података или обрађивач не може га разријешити дужности или казнити због тога што обавља своје задатке. Службеник за заштиту личних

- података одговара непосредно највишем нивоу руководства контролора података или обрађивача.
- (4) Носилац података може се обратити службенику за заштиту личних података за сва питања која се тичу обраде његових личних података и остваривања његових права из овог закона.
- (5) Службеник за заштиту личних података, у вези с обављањем својих задатака, дужан је да све податке до којих дође у поступку обраде података чува као службену тајну у складу са законом.
- (6) Службеник за заштиту личних података може обављати друге задатке и дужности. Контролор података или обрађивач обезбјеђује да ти задаци и дужности не доведу до сукоба интереса.

Члан 41.

(Задатак службеника за заштиту личних података)

- (1) Службеник за заштиту личних података обавља следеће задатке:
- а) информисање и савјетовање контролора података или обрађивача и запослених који обављају обраду о њиховим обавезама из овог закона и других закона којима се прописује заштита личних података;
- б) праћење поштовања овог закона и других закона којима се прописује заштита личних података, као и политика контролора података или обрађивача у вези са заштитом личних података, укључујући и подјелу одговорности, подизање свијести и оспособљавање запослених који учествују у радњама обраде, као и с тим повезаним ревизијама;
- ц) пружање савјета, када је то затражено, у вези са проценом утицаја на заштиту личних података и праћење њеног извршавања у складу са чланом 37. овог закона;
- д) сарадња с Агенцијом;
- е) дјеловање као контакт тачка за Агенцију о питањима која се тичу обраде, што укључује и претходно савјетовање из члана 38. овог закона, те савјетовање, по потреби, о свим другим питањима.
- (2) Службеник за заштиту личних података приликом обављања својих задатака води рачуна о ризику повезаним са радњом обраде и узима у обзир природу, обим, контекст и сврхе обраде.

Члан 42.

(Кодекс понашања)

- (1) Агенција издаје препоруку за израду кодекса понашања с циљем правилне примјене овог закона, узимајући у обзир специфичност различитих сектора обраде и посебне потребе микро, малих и средњих привредних субјеката.
- (2) Удружење и други субјекат који представља категорије контролора података или обрађивача могу израдити кодекс понашања, односно измијенити и проширити такве кодексе понашања, ради прецизирања примјене овог закона, који се односе на:
- а) правичну и транспарентну обраду;
- б) легитимне интересе контролора података у посебним контекстима;
- ц) прикупљање личних података;
- д) псеудонимизацију личних података;
- е) информисаност јавности и носиоца података;
- ф) остваривање права носиоца података;

- г) информисаност и заштиту дјете и начин прибављања сагласности носиоца родитељског права над дјететом;
- х) мјере и поступке из чл. 26. и 27. овог закона, као и мјере за постизање безбједности обраде из члана 34. овог закона;
- и) извјештавање Агенције о повредама личних података и обавјештавање носиоца података о таквим повредама;
- ј) пренос личних података другим земљама или међународним организацијама, или
- к) вансудске поступке и друге поступке за рјешавање спорова између контролора података и носиоца података у вези с обрадом, не доводећи у питање права носиоца података на основу чл. 108. и 110. овог закона.

- (3) Кодекс понашања из става (2) овог члана обавезно садржи одредбе које правном лицу из члана 43. става (1) овог закона омогућавају да спроводи обавезно праћење усклађености контролора података или обрађивача који су се обавезали на његову примјену, не доводећи у питање надлежности Агенције.
- (4) Удружења и субјекат из става (2) овог члана који намјеравају да израде кодекс понашања или измијене и прошире постојећи кодекс понашања, нацрт кодекса понашања, односно измјене или проширење кодекса понашања достављају Агенцији.
- (5) Агенција даје мишљење о томе да ли је нацрт кодекса у складу с овим законом те одобрава нацрт кодекса ако оцијени да обезбјеђује довољно адекватне заштитне мјере.
- (6) Ако Агенција одобри нацрт кодекса понашања, односно измјене или допуне кодекса понашања, у складу са ставом (5) овог члана, Агенција региструје и објављује кодекс понашања.
- (7) Контролор података или обрађивач, на које се овај закон не примјењује у складу с чланом 6. овог закона, могу примјењивати кодекс понашања који је одобрен, у складу са ставом (5) овог члана, како би обезбједили одговарајуће заштитне мјере у оквиру преношења личних података другој држави или међународној организацији, уз услове из члана 48. става (2), тачке д) овог закона.
- (8) Контролор података или обрађивач из става (7) овог члана, путем уговорних или других правно обавезујућих инструмената, преузима обавезујуће и извршне обавезе за примјену заштитних мјера, укључујући и мјере у вези са правима носиоца података.

Члан 43.

(Праћење одобреног кодекса понашања)

- (1) Правно лице с одговарајућим степеном стручности за предмет кодекса понашања може обављати праћење усклађености са кодексом понашања, ако га је у ту сврху акредитовала Агенција.
- (2) Правно лице из става (1) овог члана може бити акредитовано за праћење усклађености са кодексом понашања ако је:
- а) Агенцији доказало своју независност и стручност за предмет кодекса понашања;
- б) успоставило поступке који му омогућавају да оцјењује квалификованост контролора података и обрађивача за примјену кодекса понашања, да прати њихове примјене одредаба кодекса понашања и да периодично преиспитује његово функционисање;

- ц) успоставило поступке и структуре за рјешавање приговора на кршења кодекса понашања или на начин на који контролор података или обрађивач примјењује или је примијенио кодекс понашања и учинио те поступке и структуре транспарентним носиоцима података и јавности, и
- д) Агенцији доказало да његови задаци и дужности не доводе до сукоба интереса.
- (3) Правно лице из става (1) овог члана, уз примјену одговарајућих заштитних мјера, предузима одговарајуће радње у случајевима кршења кодекса понашања од контролора података или обрађивача, што укључује суспендовање или искључење из кодекса понашања.
- (4) Правно лице из става (1) овог члана дужно је да обавијести Агенцију о радњама и разлозима из става (3) овог члана.
- (5) Агенција одузима акредитацију правном лицу које више не испуњава услове за акредитацију или ако правно лице крши одредбе овог закона.
- (6) Овај члан се не примјењује на обраду личних података коју обавља јавни орган.

Члан 44.

(Сертификација)

- (1) Агенција препоручује успостављање поступка сертификације заштите личних података, печата и ознака за заштиту података с циљем доказивања поштовања одредаба овог закона, посебно узимајући у обзир потребе микро, малих и средњих правних лица.
- (2) Поступак сертификације заштите личних података, печата и ознака може бити успостављен и ради доказивања постојања одговарајућих заштитних мјера које обезбјеђују контролор података и обрађивач на које се овај закон у складу са чланом 6. овог закона не односи, у оквиру преноса личних података другој држави или међународној организацији, уз услове из члана 48. става (2) тачке д) овог закона.
- (3) Контролори података или обрађивачи, из става (2) овог члана, путем уговорних или других правно обавезујућих инструмената прихватају примјену одговарајућих заштитних мјера, укључујући и мјере у вези са носиоцем података.
- (4) Сертификација је добровољна и доступна путем процеса који је транспарентан.
- (5) Сертификација, у складу с овим чланом, не умањује одговорност контролора података или обрађивача за поштовање овог закона и не доводи у питање надлежности Агенције.
- (6) Сертификацију, у складу с овим чланом, издаје сертификациони орган из члана 45. овог закона на основу критеријума које је одобрила Агенција.
- (7) Контролор података или обрађивач, у поступку сертификације, сертификационом органу пружа све информације и омогућава приступ активностима обраде које су потребне за поступак сертификације.
- (8) Сертификат се контролору података или обрађивачу издаје на највише три године и може се обновити уз исте услове.
- (9) Сертификациони орган одузима сертификат контролору или обрађивачу ако више не испуњава услове за издавање сертификата.
- (10) Агенција поступак сертификације заштите личних података, печата и ознаке уноси у евиденцију и јавно објављује.

Члан 45.

(Сертификациони орган)

- (1) Акредитацију сертификационог органа, с одговарајућим степеном стручности из области заштите личних података, обавља Агенција.
- (2) Сертификациони орган обавјештава Агенцију о одлуци о издавању и обнављању сертификата како би Агенција могла обављати овлашћења из члана 103. става (2) тачке х) овог закона.
- (3) Сертификациони орган може бити акредитован само ако:
 - а) Агенцији на задовољавајући начин докаже своју независност и стручност у предмету сертификације;
 - б) се обавезе да ће поштовати критеријуме из члана 44. става (6) овог закона;
 - ц) успостави поступке за издавање, периодично преиспитивање и повлачење сертификације, печата и ознака за заштиту података;
 - д) успостави поступке и структуре за рјешавање приговора на кршења сертификације или начин на који контролор података или обрађивач примјењује или је примијенио сертификацију и учини те поступке и структуре транспарентним носиоцима података и јавности;
 - е) Агенцији докаже да његови задаци и дужности не доводе до сукоба интереса.
- (4) Акредитација сертификационог органа спроводи се на основу критеријума које је прописала Агенција.
- (5) Акредитација се издаје на највише пет година и може се обновити уз исте услове ако сертификациони орган и даље испуњава захтјеве из овог члана.
- (6) Не доводећи у питање ДИО ЧЕТВРТИ овог закона, Агенција повлачи акредитацију сертификационог органа ако се услови из става (3) овог члана не испуне или више нису испуњени, или ако се радњама које предузима сертификациони орган крши овај закон.
- (7) Сертификациони орган одговоран је за правилну процјену која доводи до сертификације или одузимања сертификата, не доводећи у питање одговорност контролора података или обрађивача за поштовање овог закона.
- (8) Сертификациони орган у писаној форми обавјештава Агенцију о разлозима за издавање или одузимање сертификата.
- (9) Агенција јавно објављује критеријуме из члана 44. става (6) овог закона.

ГЛАВА IV - ПРЕНОС ЛИЧНОГ ПОДАТКА У ДРУГУ ДРЖАВУ ИЛИ МЕЃУНАРОДНУ ОРГАНИЗАЦИЈУ

Члан 46.

(Општи принципи преноса)

Сваки пренос личног податка чија је обрада у току или је намијењен даљој обради послје његовог преношења у другу државу или међународну организацију може се обављати само ако је такав пренос у складу с одредбама овог закона, што обухвата и даљи пренос личног податка из друге државе или међународне организације у још једну другу државу или међународну организацију.

Члан 47.

(Пренос на основу адекватности нивоа заштите личног податка)

- (1) Пренос личног податка у другу државу, на дио њене територије или у један или више сектора у тој држави или међународну организацију може се обављати ако је утврђено да та друга држава, дио њене територије

- или један или више сектора у тој држави или та међународна организација обезбјеђује адекватан ниво заштите личног податка.
- (2) Сматра се да је адекватан ниво заштите из става (1) овог члана обезбјеђен у држави, дијеловима њене територије или једном или више сектора у тој држави или међународној организацији, за које је од Европске уније утврђено да обезбјеђују адекватан ниво заштите личног податка.
- (3) Одлуку о адекватности нивоа заштите личног податка из става (1) овог члана доноси Савјет министара Босне и Херцеговине на приједлог Агенције.
- (4) Агенција припрема приједлог одлуке из става (3) овог члана, узимајући у обзир:
- принцип владавине права, поштовање људских права и основних слобода, секторско законодавство, укључујући законодавство о јавној безбједности, одбрани, државној безбједности, кривичном праву и приступу јавних органа личним подацима, као и примјену тих прописа, правила о заштити личних података, правила струке и мјере обезбјеђивања заштите личних података, укључујући правила о даљем преносу личних података у другу државу или међународну организацију, која се примјењују у пракси судова и других органа власти у другој држави или међународној организацији, као и дјелотворност остваривања права носиоца личног податка, а посебно дјелотворност управних и судских поступака заштите права носиоца личног податка;
 - постојање и ефикасност рада надзорног органа у другој држави или органа који је надлежан за међународну организацију у овој области, с овлашћењем да обезбједи примјену правила о заштити личног податка и покрене поступке заштите личног податка у случају њиховог непоштовања, пружи помоћ и савјетује носиоце личних података у остваривању њихових права, као и да сарађује са надзорним органима других држава;
 - међународне обавезе које је друга држава или међународна организација преузела, или друге обавезе које произлазе из правно обавезујућих међународних уговора или других правних инструмената, као и из чланства у мултилатералним или регионалним организацијама, а посебно у вези са заштитом личних података.
- (5) Агенција континуирано прати стање у области заштите личних података у другој држави, дијелу њене територије, једном или више сектора унутар те државе или међународној организацији и о томе по потреби извјештава Савјет министара Босне и Херцеговине.
- (6) Извјештај из става (5) овог члана укључује доступне информације и информације прикупљене од међународних организација, које су од значаја за преиспитивање постојања адекватног нивоа заштите личног податка, на основу чега Савјет министара Босне и Херцеговине доноси одлуку из става (3) овог члана.
- (7) Одлука донесена на основу става (3) овог члана не доводи у питање пренос личног податка у другу државу, на територију или у један или више одређених сектора унутар те друге државе или међународну организацију у складу са чл. 48. до 51. овог закона.
- (8) Листа држава, дио њихових територија, један или више сектора унутар државе и међународних организација, у вези с којим је Савјет министара Босне и Херцеговине донио одлуку да не обезбјеђују или да више не обезбјеђују адекватан ниво заштите личних података, објављују се у "Службеном гласнику БиХ" и на службеној интернет страници Агенције.

Члан 48.

(Пренос на који се примјењују одговарајуће заштитне мјере)

- Контролор података или обрађивач може пренијети личне податке у другу државу, на дио њене територије, један или више сектора унутар те државе или у међународну организацију за коју листом из члана 47. става (8) овог закона није утврђено постојање адекватног нивоа заштите личних података само ако је контролор података или обрађивач обезбједио одговарајуће заштитне мјере тих података и ако су носиоцу личних података обезбјеђени остваривања права и дјелотворна судска заштита.
- Одговарајуће заштитне мјере из става (1) овог члана могу се, без посебног одобрења Агенције, обезбједити:
 - правно обавезујућим актом сачињеним између јавних органа;
 - обавезујућим пословним правилима у складу са чланом 49. овог закона;
 - одобраним кодексом понашања у складу са чланом 42. овог закона с обавезујућим и извршним обавезама контролора података или обрађивача у другој држави за примјену одговарајућих заштитних мјера, између осталог и у вези са правом носиоца података, или
 - одобраним поступком сертификације у складу са чланом 44. овог закона с обавезујућим и извршним обавезама контролора података или обрађивача у другој држави за примјену одговарајућих заштитних мјера, између осталог и у вези са правима носиоца података.
- Одговарајуће заштитне мјере из става (1) овог члана могу се обезбједити стандардним уговорним клаузулама о заштити података које доноси Агенција.
- Уз услов да то одобри Агенција, одговарајуће заштитне мјере из става (1) овог члана такође могу бити обезбјеђене посебно:
 - уговором између контролора података или обрађивача и контролора података, обрађивача или примаоца личних података у другој држави или међународној организацији, или
 - одредбама које се уносе у споразуме између јавних органа и које садрже остваривања и дјелотворна права носиоца података.

Члан 49.

(Обавезујућа пословна правила)

- Обавезујућа пословна правила одређују најмање:
 - структуру и податке за контакт групе привредних субјеката који обављају заједничку привредну дјелатност и сваког од њихових чланова;
 - преносе података или скупове преноса, уз навођење категорије личних података, врсте

- обrade и њене сврхе, категорије носилаца података и одређења друге државе или држава о којима се ради;
- ц) њихову правно обавезујућу природу;
- д) примјену принципа заштите података, а посебно ограничења сврхе, смањења количине података, ограничења рока чувања, квалитета података, техничке и интегрисане заштите података, правног основа обраде, обраде посебних категорија личних података, мјера за постизање безбједности података и услова у вези са даљим преносом органима који нису обавезани обавезујућим пословним правилима;
- е) права носилаца података у вези с обрадом и начине за остварење тих права, укључујући и право да се на њих не примјењују одлуке које се заснивају искључиво на аутоматској обради, што укључује и израду профила у складу са чланом 24. овог закона, право на приговор Агенцији и право на судску заштиту, у складу са чланом 110. овог закона, а у одговарајућим случајевима и право на накнаду штете за кршење обавезујућих пословних правила;
- ф) да контролор података или обрађивач са сједиштем или пословним настаном на територији Босне и Херцеговине прихвата одговорност за сва кршења обавезујућих пословних правила од било којег члана који нема сједиште или пословни настан у Босни и Херцеговини или је контролор података или обрађивач у цјелини или дјелимично изузет од одговорности ако докаже да тај члан групе привредних субјеката није одговоран за догађај који је проузроковао штету;
- г) на који начин се носиоцима података, осим информација из чл. 15. и 16. овог закона, пружају информације о обавезујућим пословним правилима, посебно о одредбама из тач. д), е) и ф) овог става;
- х) задатке сваког службеника за заштиту података именованог у складу са чланом 39. овог закона или било којег другог лица или субјекта одговорног за праћење усклађености с обавезујућим пословним правилима у групи привредних субјеката који обављају заједничку привредну дјелатност, као и праћење оспособљености и рјешавање приговора;
- и) поступке поводом приговора;
- ј) механизме унутар групе привредних субјеката који обављају заједничку привредну дјелатност, којима се обезбјеђује провјера поштовања обавезујућих пословних правила, који укључују ревизију заштите података и методе за обезбјеђивање корективних мјера за заштиту права носиоца података. Резултате такве провјере потребно је саопштити лицу или субјекту из тачке х) овог става и управљачком органу групе привредних субјеката који обављају заједничку привредну дјелатност, а на захтјев их је потребно ставити на располагање Агенцији;
- к) механизме за извјештавање и вођење евиденције о промјенама правила и извјештавање Агенције о тим промјенама;
- л) механизам сарадње са Агенцијом ради обезбјеђивања усклађености сваког члана групе привредних субјеката који обављају заједничку привредну дјелатност, прије свега тако што се Агенцији ставе на располагање резултати провјера мјера из тачке ј) овог става;
- м) механизме за извјештавање Агенцији о било каквим правним обавезама које се односе на члана групе привредних субјеката који обављају заједничку привредну дјелатност и примјењују се у другој држави, а које би могле имати значајан негативан утицај на гаранције садржане у обавезујућим пословним правилима;
- н) одговарајуће оспособљавање из области заштите личних података за особе које има сталан или редовни приступ личним подацима.
- (2) Агенција одобрава обавезујућа пословна правила уз услов да:
- а) су правно обавезујућа и да се примјењују на сваког заинтересованог члана одређене групе привредних субјеката који обављају заједничку привредну дјелатност, што укључује и њихове запослене, те да их они извршавају;
- б) носиоцима података изричито дају остварива права у вези с обрадом њихових личних података;
- ц) испуњавају услове из става (1) овог члана.
- (3) Агенција може да одреди формат и поступке размјене информација између контролора података, обрађивача и Агенције за обавезујућа пословна правила у смислу овог члана.

Члан 50.

(Пренос или откривање података који нису допуштени)

Свака пресуда суда, трибунала или одлука управног органа друге државе којом се од контролора података или обрађивача захтијева пренос или откривање личних података може бити призната или извршена само ако се заснива на међународном споразуму, као што је споразум о узајамној правној помоћи, између друге државе која је поднијела захтјев и Босне и Херцеговине, не доводећи у питање друге разлоге за преношење у складу с овом главом.

Члан 51.

(Одступање у посебним случајевима)

- (1) Пренос или скуп преноса личних података у другу државу или међународну организацију, ако не постоји одлука о адекватности, у складу са чланом 47. ставом (3) овог закона или одговарајуће заштитне мјере у складу са чланом 48. овог закона, укључујући и обавезујућа пословна правила из члана 49. овог закона, обавља се само уз један од следећих услова:
- а) носилац података је изричито сагласан са предложеним преносом, након што је упознат са могућим ризицима таквих преноса због непостојања одлуке о адекватности и одговарајућих заштитних мјера из члана 48. овог закона;
- б) пренос је неопходан за извршење уговора између носиоца података и контролора података или спровођење предуговорних мјера на захтјев носиоца података;
- ц) пренос је неопходан ради склапања или извршења уговора склопљеног у интересу носиоца података између контролора података и другог физичког или правног лица;
- д) пренос је неопходан из важних разлога јавног интереса;

- е) пренос је неопходан за постављање, остваривање или одбрану правних захтјева;
 - ф) пренос је неопходан за заштиту кључних интереса носиоца података или других лица ако носилац података физички или правно није способан да да сагласност;
 - г) пренос се врши из регистра, који према правним прописима у Босни и Херцеговини служи за пружање информација јавности и који је доступан на увид јавности или било којем лицу које може доказати постојање легитимног интереса, али само у мјери у којој су испуњени услови прописани посебним законом за увид у том посебном случају.
- (2) Пренос или скуп преноса личних података у другу државу или међународну организацију, у случају када основ за пренос не може бити чл. 47. или 48. овог закона, укључујући и обавезујућа пословна правила из члана 49. овог закона, и када се не примјењује ниједно одступање у посебним случајевима из става (1) овог члана, може се обавити само ако се пренос не понавља, ако се односи само на ограничен број носилаца података и ако је неопходан за потребе важних, легитимних интереса контролора података над којима не превладавају интереси или права и слободу носиоца података, а контролор података је процијенио све околности преноса података и на основу те процјене је предвидио одговарајуће заштитне мјере у вези са заштитом личних података. Контролор података о преносу обавјештава Агенцију. Уз информације из чл. 15. и 16. овог закона, контролор података обавјештава носиоца података о преносу и о важним легитимним интересима.
- (3) Пренос на основу става (1) тачке г) овог члана не укључује личне податке у цијелини ни цијеле категорије личних података садржаних у регистру. Када је регистар намијењен за увид лицима која имају легитиман интерес, пренос се обавља само ако то захтијевају та лица или ако су они примаоци.
- (4) На активности које обављају јавни органи приликом извршавања својих јавних овлашћења не примјењују се став (1) тач. а), б) и ц) и став (2) овог члана.
- (5) Јавни интерес из става (1) тачке д) овог члана мора бити прописан законом који се примјењује на контролора података.
- (6) Ако није донесена одлука о адекватности, из важних разлога јавног интереса посебним прописом могу бити изричито прописана ограничења преноса одређених категорија личних података другој држави или међународној организацији.
- (7) Контролор података или обрађивач документује процјену, као и одговарајуће заштитне мјере из ст. (1) и (2) овог члана, у евиденцијама из члана 32. овог закона.

ГЛАВА V - ПОСЕБНИ СЛУЧАЈЕВИ ОБРАДЕ

Члан 52.

(Обрада личног податка и слобода изражавања и информисања)

- (1) Обрада личних података приликом коришћења права на слободу изражавања и информисања, што укључује обраду искључиво у новинарске сврхе, у сврхе академског, умјетничког или књижевног изражавања, обавља се у складу са посебним прописима.
- (2) Посебним прописима из става (1) овог члана утврђују се изузеци или одступања од примјене Главе I, Главе

II, Главе III, Главе IV, Главе V овог дијела и ДИЈЕЛА ЧЕТВРТОГ овог закона, ако су такви изузеци или одступања потребни да се усклади право на заштиту личних података са слободом изражавања и информисања.

Члан 53.

(Обрада личног податка и јавни приступ службеним документима)

- (1) Јавни орган и надлежни орган, у складу са законом који се примјењује на тај орган, могу у јавном интересу открити личне податке из службених докумената којима располажу, како би се јавни приступ службеним документима ускладио са правом на заштиту личних података у складу с овим законом.
- (2) Овај закон примјењује се приликом примјене прописа о слободи приступа информацијама у Босни и Херцеговини.

Члан 54.

(Обрада јединственог матичног броја физичког лица)

- (1) Посебни услови за обраду јединственог матичног броја физичког лица или било којег другог идентификатора опште примјене прописују се посебним законом.
- (2) Јединствени матични број физичког лица или било који други идентификатор опште примјене из става (1) овог члана обрађује се само уз примјену одговарајућих заштитних мјера у вези са правима и слободама носиоца података у складу с овим законом.

Члан 55.

(Обрада личних података у контексту запослења)

- (1) Посебним законом или колективним уговором прецизирају се правила с циљем обезбјеђивања заштите права и слобода у вези с обрадом личних података у контексту запослења, посебно за потребе запошљавања, извршења уговора о раду, укључујући и извршавање обавеза прописаних законом или колективним уговорима, за потребе управљања, планирања и организације рада, једнакости и различитости на радном мјесту, здравства и безбједности на раду, заштите имовине послодавца или клијента и за потребе индивидуалног или колективног остваривања и уживања права и погодности из радног односа, као и за потребе престанка радног односа.
- (2) Правила из става (1) овог члана укључују прикладне и посебне мјере за заштиту људског достојанства носиоца података, његових легитимних интереса и основних права, посебно у вези са транспарентношћу обраде, преносом личних података унутар групе привредних субјеката или групе привредних субјеката који обављају заједничку привредну дјелатност, као и системом праћења на радном мјесту.

Члан 56.

(Заштитне мјере и одступања у вези с обрадом личног податка у сврху архивирања у јавном интересу, у сврху научног или историјског истраживања или у статистичке сврхе)

- (1) На обраду личних података у сврху архивирања у јавном интересу, у сврху научног или историјског истраживања или у статистичке сврхе примјењују се одговарајуће заштитне мјере у складу с овим законом у погледу права и слобода носиоца података.
- (2) Заштитним мјерама из става (1) овог члана обезбјеђује се примјена техничких и организационих мјера, посебно оних којима се гарантује примјена принципа

- смањења обима података, које могу укључивати псеудонимизацију, ако се сврхе могу остварити тако.
- (3) Ако се сврхе из става (1) овог члана могу постићи даљом обрадом која не омогућава или више не омогућава идентификацију носиоца података, те сврхе се остварују на тај начин.
 - (4) Ако се лични подаци обрађују у сврху научног или историјског истраживања или у статистичке сврхе, само се посебним законом могу предвидјети одступања од права наведених у чл. 17, 18, 20. и 23. овог закона, уз примјену услова и мјера заштите из става (1) овог члана, ако је вјероватно да би та права могла спријечити или озбиљно угрожити остваривање тих посебних сврха, па су таква одступања неопходна за њихово постизање.
 - (5) Ако се лични подаци обрађују у сврху архивирања у јавном интересу, само се посебним законом могу предвидјети одступања од права наведених у чл. 17, 18, 20, 21, 22. и 23. овог закона, уз примјену услова и мјера заштите из става (1) овог члана, ако је вјероватно да би та права могла спријечити или озбиљно угрожити остваривање те посебне сврхе, па су таква одступања неопходна за њено постизање.
 - (6) Ако обрада из ст. (2) и (3) овог члана истовремено служи и другој сврси, одступања се примјењују само за обраду у сврхе које су наведене у тим ставовима.

Члан 57.

(Видео-надзор)

- (1) Праћење одређеног простора путем видео-надзора допуштено је само ако је то пуно за заштиту лица и имовине и ако не превладају интереси носиоца података.
- (2) Видео-надзором могу бити обухваћени само простори или дијелови простора чији је надзор нужан ради постизања сврхе из става (1) овог члана.
- (3) Успостављање видео-надзора јавно доступних објеката великих површина, као што су спортски објекти, забавни центри, тржни центри или паркиралишта, или возила јавног превоза, допуштено је искључиво с циљем заштите живота, здравља и слободе лица те имовине.
- (4) Контролор података који обавља видео-надзор дужан је да донесе одлуку која ће садржавати правила обраде с циљем поштовања права на заштиту приватности и личног живота носиоца података, ако видео-надзор није прописан законом.
- (5) Контролор података или обрађивач дужан је да на видном мјесту истакне ознаку о видео-надзору. Ознака о видео-надзору садржи следеће информације: да је простор под видео-надзором, податке о контролору података, односно обрађивачу и контактне податке путем којих носилац података може остварити своја права. Ознака треба бити видљива најкасније приликом уласка у видокруг снимања.
- (6) Контролор података или обрађивач дужан је да, код система видео-надзора јавно доступних објеката из става (3) овог члана, биљежи записе о употреби система и да их чува најмање 12 мјесеци. Записи омогућавају да се утврди датум и вријеме те идентитет лица које је остварило увид у систем видео-надзора.

- (7) За успостављање видео-надзора у стамбеним, односно пословно-стамбеним зградама потребна је сагласност сувласника који чине најмање 2/3 сувласничких дијелова. Видео-надзором може се обухватити само приступ уласку и изласку из стамбене зграде, те заједничке просторије у стамбеним зградама.
- (8) Праћење јавних простора путем видео-надзора у сврхе из члана 1. става (1) тачке ц) овог закона допуштено је само ако је то прописано посебним законом.

Члан 57а.

(Обрада биометријских података у сврху сигурне идентификације)

- (1) Обрада биометријских података може се спроводити само ако је прописана законом или ако је нужна за заштиту лица, имовине, класификованих података, пословних тајни или за појединачну и сигурну идентификацију корисника услуга, узимајући у обзир да не превладају интереси носиоца података који су у супротности с обрадом биометријских података из овог члана.
- (2) Правни основ за обраду биометријских података носиоца података ради сигурне идентификације корисника услуга изричита је сагласност таквог носиоца података дата у складу с одредбама овог закона.

Члан 57б.

(Обрада биометријских података у службеним просторијама)

Допуштена је обрада биометријских података запосленика у сврху евидентирања радног времена и ради уласка и изласка из службених просторија, ако је прописано законом или ако се таква обрада спроводи као алтернатива другом рјешењу за евидентирање радног времена или уласка и изласка из службених просторија, уз услов да је запосленик дао изричиту сагласност за такву обраду биометријских података у складу са одредбама овог закона.

Члан 58.

(Постојећа правила о заштити личних података цркава и вјерских заједница)

- (1) Ако цркве и вјерске заједнице примјењују свеобухватна правила у вези с обрадом личних података, та постојећа правила могу се и даље примјењивати уз услов да се ускладе с овим законом.
- (2) Цркве и вјерске заједнице које примјењују свеобухватна правила надзире Агенција, осим ако црква или вјерска заједница не образује посебан независни надзорни орган, уз услов да испуњава услове утврђене у ДИЈЕЛУ ЧЕТВРТОМ овог закона.

Члан 59.

(Обавеза чувања професионалне тајне)

- (1) Посебним прописом може се утврдити ограничење Агенције из члана 103. става (1) тач. ф) и г) у вези са контролором података или обрађивачем који, на основу посебног прописа који је донио надлежни орган, подлијежу обавези професионалне тајне и другим једнаковриједним обавезама тајности, ако је то нужно и размјерно како би се ускладило право на заштиту личних података с обавезом тајности.
- (2) Посебни пропис из става (1) овог члана примјењује се само на личне податке које је контролор података или обрађивач добио као резултат или примио током активности која је обухваћена обавезом тајности.

ДИО ТРЕЋИ – ОБРАДА ЛИЧНОГ ПОДАТКА ОД НАДЛЕЖНОГ ОРГАНА КАО КОНТРОЛОР ПОДАТАКА У СВРХУ СПРЕЧАВАЊА, ИСТРАГЕ И ОТКРИВАЊА КРИВИЧНИХ ДЈЕЛА ИЛИ ГОЋЕЊА ПОЧИНИЛАЦА КРИВИЧНИХ ДЈЕЛА, ИЗВРШАВАЊЕ КРИВИЧНИХ САНКЦИЈА, УКЉУЧУЈУЋИ ЗАШТИТУ ОД ПРИЈЕТЊИ ЈАВНОЈ БЕЗБЈЕДНОСТИ И ЊИХОВО СПРЕЧАВАЊЕ

Члан 60.

- (Принципи обраде личних података од надлежног органа)
- (1) Принципи обраде личних података од надлежног органа су:
 - а) законитост и правичност;
 - б) ограничење сврхе – подаци морају бити прикупљени у посебне, изричите и законите сврхе те се даље не смију обрађивати на начин који није у складу с тим сврхама;
 - ц) смањење опсега података – подаци морају бити примјерени, релевантни и ограничени на оно што је неопходно у сврхе у које се обрађују;
 - д) тачност – подаци морају бити тачни и према потреби ажурирани, морају се предузети све разумне мјере како би се обезбиједило да лични подаци који нису тачни, имајући у виду сврхе у које се обрађују, буду без одгађања избрисани или исправљени;
 - е) ограничење чувања – подаци морају бити чувани у форми која омогућава идентификацију носиоца података, и то не дужи него што је потребно у сврхе у које се подаци обрађују;
 - ф) цјеловитост и повјерљивост – подаци морају бити обрађивани тако да се осигура одговарајућа безбједност личних података, укључујући и заштиту од неовлашћене или незаконите обраде и од случајног губитка, уништења или оштећења примјеном одговарајућих техничких или организационих мјера.
 - (2) Обрада коју обавља исти или неки други надлежни орган у сврху из члана 1. става (1) тачке ц) овог закона различиту од оне за коју су лични подаци прикупљени допуштена је:
 - а) ако је надлежни орган овлашћен за обраду таквих личних података у такву сврху у складу са посебним прописом, или
 - б) ако је обрада неопходна и пропорционална другој законитој сврси.
 - (3) Обрада коју обавља исти или неки други надлежни орган може укључивати архивирање у јавном интересу, у научне, статистичке или историјске сврхе, за сврхе из члана 1. става (1) тачке ц) овог закона, уз предузимање одговарајућих заштитних мјера у вези са правима и слободама носиоца података.
 - (4) Надлежни орган одговоран је за усклађеност са ст. (1), (2) и (3) овог члана и мора бити у могућности да докаже ту усклађеност.

Члан 61.

(Рок за чување и брисање личног податка)

- (1) Рок за брисање личних података или за периодично преиспитивање потребе њиховог чувања прописује се посебним законом.
- (2) Надлежни органи дужни су да успоставе правила и процедуре којима се обезбјеђује поштовање рока из става (1) овог члана.

Члан 62.

(Разлика између различитих категорија носилаца података)
Надлежни орган дужан је да, према потреби и ако је то могуће, направи јасну разлику између личних података различитих категорија носилаца података, као што је:

- а) лице за које постоји основ сумње да је извршило или намјерава да изврши кривично дјело;
- б) лице осуђено за кривична дјела;
- ц) лице које је жртва кривичног дјела или лице у погледу којег постоје одређене чињенице које дају основу за сумњу да би то лице могло бити жртва кривичног дјела;
- д) лице које се доводи у везу са кривичним дјелом, као што је лице које се може позвати да свједочи у истрагама или накнадном кривичном поступку, лице које може дати информације о кривичним дјелима или лице за контакт или сарадници лица из тач. а) и б) овог става.

Члан 63.

(Разлика између личних података и провјера квалитета личних података)

- (1) Надлежни орган дужан је да утврди механизам којим ће се обезбиједити да се лични подаци засновани на чињеницама разликују, што је више могуће, од личних података заснованих на личним процјенама.
- (2) Надлежни орган дужан је да предузме све разумне мјере како би обезбиједио да се лични подаци који су нетачни, непотпуни или неажурирани не преносе нити стављају на располагање. Надлежни орган, ако је то могуће, провјерава квалитет личних података прије њиховог преношења или стављања на располагање. Приликом сваког преношења личних података, што је више могуће, достављају се неопходне информације надлежном органу, који је податке добио, омогућава се оцјена степена тачности, потпуности и поузданости личних података, као и у којој су мјери ажурирани.
- (3) Ако се утврди да су пренесени нетачни лични подаци или да су лични подаци пренесени незаконито, надлежни орган мора без одгађања о томе обавијестити примаоца. У том случају лични подаци морају се исправити или брисати или обрада ограничити у складу са чланом 72. овог закона.

Члан 64.

(Законитост обраде личног податка од надлежног органа)

- (1) Обрада личних података коју обавља надлежни орган законита је само ако је нужна и само у оној мјери у којој је нужна за обављање послова надлежног органа у сврхе из члана 1. става (1) тачке ц) овог закона и ако је прописана посебним законом.
- (2) Посебни закон из става (1) овог члана прописује најмање циљеве обраде, личне податке који се обрађују и сврхе обраде.

Члан 65.

(Посебни услови обраде)

- (1) Лични подаци које надлежни органи прикупљају за сврхе утврђене у члану 1. ставу (1) тачки ц) овог закона не смију се обрађивати у друге сврхе, осим ако је таква обрада прописана посебним законом и у том случају не примјењују се одредбе овог дијела закона.
- (2) Ако је посебним законом надлежном органу повјерено обављање послова другачијих од оних које обављају у сврхе из члана 1. става (1) тачке ц) овог закона, у том случају не примјењују се одредбе овог дијела закона, између осталог и за сврху архивирања у јавном

интересу, или у сврху научног или историјског истраживања или у статистичке сврхе.

- (3) Ако су посебним законом, који се односи на надлежни орган који преноси податке, прописани посебни услови за обраду, надлежни орган који преноси те личне податке примаоцу дужан је да га обавијести о тим условима и о захтјевима за поштовање тих услова.

Члан 66.

(Обрада посебних категорија личних података од надлежног органа)

- (1) Забрањена је обрада личних података који откривају расно или етничко поријекло, политичка мишљења, вјерска или филозофска увјерења или припадност синдикату, као и обрада генетских података, биометријских података у сврху јединствене идентификације лица или података о здрављу или података о полном животу или сексуалној оријентацији лица.
- (2) Изузетно од става (1) овог члана, обрада посебних категорија личних података је допуштена искључиво ако је то нужно, придржавајући се одговарајућих заштитних мјера у вези са правима и слободама носиоца података:
- а) ако је прописана посебним законом;
 - б) ради заштите виталних интереса носиоца података или другог појединца, или
 - ц) ако се таква обрада односи на податке за које је очигледно да их је објавио носилац података.

Члан 67.

(Аутоматизовано појединачно доношење одлуке од надлежног органа)

- (1) Надлежном органу забрањено је доношење одлуке искључиво на основу аутоматизоване обраде, укључујући и израду профила, која производи негативне правне ефекте за носиоца података или на њега значајно утиче, осим ако је одобрено посебним законом којим се прописују одговарајуће заштитне мјере за права и слободе носиоца података, најмање права на учествовање физичког лица у доношењу одлуке.
- (2) Одлука из става (1) овог члана не смије бити заснована на посебним категоријама личних података из члана 66. овог закона, осим ако су успостављене одговарајуће мјере заштите права и слобода и легитимних интереса носиоца података.
- (3) Надлежном органу забрањена је израда профила који доводи до дискриминације лица на основу посебних категорија личних података из члана 66. овог закона.

Члан 68.

(Обавјештавање и начин остваривања права носилаца података)

- (1) Надлежни орган дужан је да предузме све одговарајуће мјере како би се носиоцу података пружиле све информације из члана 69. овог закона те дала сва обавјештења у вези са чланом 67, чл. од 70. до 74. и члана 87. овог закона у вези с обрадом.
- (2) Информације из става (1) овог члана дају се у сажетој, разумљивој и лако доступној форми, уз употребу јасног и једноставног језика.
- (3) Информације из става (1) овог члана пружају се носиоцу података у облику у којем је захтјев поднесен или на начин који је истакнут у захтјеву, у року од 30 дана од дана подношења захтјева.

- (4) Надлежни орган дужан је да олакша остваривање права носиоца података из члана 67. и чл. 70. до 74. овог закона.
- (5) Надлежни орган дужан је да носиоца података писаним путем обавијести о даљим радњама у вези с његовим захтјевом, без одгађања.
- (6) Надлежни орган дужан је да, без накнаде, пружи информације, односно предузме мјере на основу члана 69. овог закона, те сва обавјештења пружена или мјере предузете на основу члана 67, чл. од 70. до 74. овог закона и члана 87. овог закона.
- (7) Ако је захтјев носиоца података очигледно неоснован или претјеран, посебно због његовог учесталог понављања, надлежни орган може:
- а) наплатити накнаду стварних административних трошкова, као што су трошкови умножавања, скенирања или трошкови носача података, као и накнаду трошкова достављања или предузимања тражених мјера, или
 - б) одбити да поступи по захтјеву.
- (8) Терет доказивања очигледне неоснованости или претјераности захтјева из става (7) овог члана је на надлежном органу.
- (9) Ако надлежни орган има оправдану сумњу у вези с идентитетом физичког лица које подноси захтјев из чл. 70. или 72. овог закона, надлежни орган може да затражи додатне информације неопходне за потврђивање идентитета носиоца података.

Члан 69.

(Информације које се стављају на располагање или уступају носиоцу података)

- (1) Надлежни орган дужан је да носиоцу података стави на располагање као минимум следеће информације:
- а) идентитет и контакт податке надлежног органа;
 - б) контакт податке службеника за заштиту личних података, ако је примјениво;
 - ц) сврху обраде личних података;
 - д) о праву на подношење приговора Агенцији и контакт подацима Агенције или тужбе надлежном суду;
 - е) о постојању права да од надлежног органа затражи приступ својим личним подацима, њихову исправку или брисање, или ограничење обраде личних података.
- (2) Осим информација из става (1) овог члана, ради остваривања његових права, надлежни орган носиоцу података даје следеће додатне информације:
- а) правни основ обраде личних података;
 - б) рок у којем ће се лични подаци чувати или, ако то није могуће, о критеријумима коришћеним за утврђивање тог рока;
 - ц) о категоријама прималаца личних података, укључујући друге државе или међународне организације, ако је примјениво;
 - д) према потреби и додатне информације ако се лични подаци прикупљају без знања носиоца података.
- (3) Посебним законом могу се прописати мјере за одгађање, ограничење или ускраћивање пружања информација из става (2) овог члана носиоцу података у оној мјери и у оном трајању у којем таква мјера представља потребну и пропорционалну мјеру у демократском друштву, уз поштовање основних права и легитимних интереса носиоца података, с циљем да се:

- а) спријечи ометање службеног и законом уређеног прикупљања информација, истрага или поступака;
 - б) избјегне ометање, спречавање истраге и откривања кривичних дјела или гоњења починилаца кривичних дјела или извршавања кривичних санкција;
 - ц) заштити јавна безбједност;
 - д) заштити државна безбједност;
 - е) заштите права и слободе других.
- (4) Посебним законом могу се прописати категорије обраде које могу у цјелини или дјелимично бити обухваћене било којом од тачака из става (3) овог члана.

Члан 70.

(Право носиоца података на приступ личном податку код надлежног органа)

- (1) Надлежни орган дужан је да у року од 30 дана од дана заступања захтјева за приступ личним подацима носиоцу података изда потврду о томе да ли обрађује његове личне податке те ако се такви лични подаци обрађују, приступ личним подацима и информацијама о:
- а) сврси обраде и правном основу обраде;
 - б) категорији личних података који се обрађују;
 - ц) примаоцу или категорији примаоца којем су лични подаци откривени, посебно примаоцу у другој држави или међународној организацији;
 - д) предвиђеном року у којем ће се лични подаци чувати, ако је то могуће, или, ако то није могуће, критеријумима коришћеним за утврђивање тог рока;
 - е) постојању права да од надлежног органа затражи исправку или брисање својих личних података или ограничење обраде личних података;
 - ф) праву на подношење приговора Агенцији и контактним подацима Агенције или тужбе надлежном суду;
 - г) личним подацима који се обрађују и о свим доступним информацијама о извору личних података.
- (2) Потврда из става (1) овог члана издаје се у складу с одредбама члана 71. овог закона.

Члан 71.

(Ограничења права приступа личном податку)

- (1) Посебним законом који се односи на надлежни орган може се носиоцу података у цјелини или дјелимично ограничити право приступа личном податку у оној мјери и у оном трајању у којем такво дјелимично или потпуно ограничење чини неопходну и пропорционалну мјеру у демократском друштву, уз поштовање основних права и легитимних интереса носиоца података, како би се:
- а) спријечило ометање службеног или законом уређеног прикупљања информација, истрага или поступака;
 - б) избјегло ометање, спречавање истраге и откривања кривичних дјела или гоњења починиоца кривичних дјела или извршавања кривичних санкција;
 - ц) заштитила јавна безбједност;
 - д) заштитила државна безбједност;
 - е) заштитила права и слободе других.

- (2) Посебним законом могу се одредити категорије обраде које могу у цјелини или дјелимично бити обухваћене било којом тачком из става (1) овог члана.
- (3) У случајевима из ст. (1) и (2) овог члана, надлежни орган дужан је да, без одгађања, писаним путем обавијести носиоца података о сваком одбијању или ограничењу приступа личним подацима те о разлозима одбијања или ограничења, осим ако би пружање таквих информација довело у питање неку од сврха из става (1) овог члана.
- (4) Надлежни орган дужан је да обавијести носиоца података о могућности подношења приговора Агенцији или тужбе надлежном суду.
- (5) Надлежни орган дужан је да документује чињеничне или правне разлоге на којима се заснива одлука.
- (6) Документација из става (5) овог члана ставља се Агенцији на располагање.

Члан 72.

(Право на исправку или брисање личног податка и ограничење обраде од надлежног органа)

- (1) Надлежни орган дужан је да:
- а) без непотребног одгађања, носиоцу података омогући исправку нетачних личних података који се на њега односе. Узимајући у обзир сврхе обраде података, носилац података има право да допуни непотпуне личне податке, између осталог и давањем додатне изјаве;
 - б) носиоцу података омогући брисање личних података, без непотребног одгађања, ако се обрадом крше одредбе чл. 60, 64. или 66. овог закона, или ако се лични подаци морају брисати ради поштовања правне обавезе из посебног закона;
 - ц) ограничи обраду ако:
 - 1) носилац података оспорава тачност личних података, а њихову тачност или нетачност није могуће утврдити, или
 - 2) лични подаци морају бити сачувани као доказ;
 - д) обавијести носиоца података прије уклањања ограничења обраде ако је обрада ограничена на основу тачке ц) алинеје 1) овог става;
 - е) писаним путем обавијести носиоца података о сваком одбијању исправке или брисања личних података или ограничења обраде те о разлозима одбијања. Посебним законом који се односи на надлежни орган може се носиоцу података потпуно или дјелимично ограничити право приступа у оној мјери и у оном трајању у којем такво потпуно или дјелимично ограничење чини неопходну и пропорционалну мјеру у демократском друштву, уз поштовање основних права и легитимних интереса носиоца података, како би се:
 - 1) избјегло ометање службеног или законом уређеног прикупљања информација, истрага или поступака;
 - 2) избјегло ометање, спречавање истраге и откривања кривичних дјела, или гоњења починиоца кривичних дјела или извршавања кривичних санкција;
 - 3) заштитила јавна безбједност;
 - 4) заштитила државна безбједност, и
 - 5) заштитила права и слободе других;

- ф) обавијести носиоца података о могућности подношења приговора Агенцији или тужбе надлежном суду;
 - г) о исправи нетачних личних података обавијести надлежни орган од којег потичу нетачни подаци.
- (2) Ако су лични подаци исправљени или брисани, или је обрада била ограничена на основу става (1) тач. а), б) или ц) овог члана, надлежни орган дужан је да обавијести примаоца, а примаоци су дужни да исправе или обришу личне податке или ограниче обраду личних података у оквиру своје одговорности.

Члан 73.

(Остваривање права носилаца података и провјера Агенције)

- (1) Надлежни орган дужан је да обавијести носиоца података о могућности остваривања права путем приговора Агенцији или тужбе надлежном суду.
- (2) Ако је носилац података незадовољан поступком надлежног органа, може да поднесе приговор Агенцији или тужбу надлежном суду, у случајевима из члана 69. става (3), члана 71. става (3) и члана 72. става (1) тачке д) овог закона.
- (3) У случају из става (1) овог члана, Агенција је дужна да обавијести носиоца података о томе да су спроведене провјере и надзор, као и о праву на правни лијек.

Члан 74.

(Права носиоца података у кривичним истрагама и поступцима)

Носилац података остварује права из чл. 69. 70. и 72. овог закона у складу са законима о кривичним поступцима, ако су лични подаци садржани у судској одлуци или евиденцији или спису предмета обрађени током кривичних истрага и поступака.

Члан 75.

(Обавеза надлежног органа)

- (1) Надлежни орган дужан је да примјени одговарајуће техничке и организационе мјере имајући у виду природу, обим, околности и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободе физичких лица, како би обезбједио да се обрада обавља у складу с овим законом и како би то могао доказати. Те мјере се по потреби преиспитују и ажурирају.
- (2) Мјере из става (1) овог члана, ако су пропорционалне у односу на активности обраде, укључују спровођење одговарајућих политика заштите података од надлежног органа.

Члан 76.

(Техничка и интегрисана заштита личног податка од надлежног органа)

- (1) Надлежни орган дужан је да, узимајући у обзир најновија достигнућа и трошак спровођења, као и природу, обим, контекст и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободе лица који произлазе из обраде података, и у вријеме одређивања средстава обраде и у вријеме саме обраде, примјени одговарајуће техничке и организационе мјере, попут псеудонимизације, за омогућавање дјелотворне примјене принципа заштите података, као што је смањење количине података те укључење заштитних мјера у обраду, како би се испунили захтјеви из овог закона и заштитила права носиоца података.

- (2) Мјере из става (1) овог члана односе се на количину прикупљених личних података, опсег њихове обраде, рок њиховог чувања и њихову доступност, чиме се обезбјеђује да лични подаци нису аутоматски, без интервенције физичког лица, доступни неограниченом броју лица.

Члан 77.

(Надлежни орган као заједнички контролор података)

- (1) Ако два или више надлежних органа одреде сврхе и начине обраде личних података, сматра се да су заједнички контролори података. Они на транспарентан начин међусобним споразумом одређују одговорности свакога од њих с циљем извршавања обавеза из овог закона, посебно у вези са остваривањем права носилаца података и дужностима свакога од њих у вези са пружањем информација из члана 69. овог закона, осим ако су одговорности надлежних органа утврђене законом који се примјењује на те надлежне органе. Споразумом се одређује контакт тачка за носиоца података. Законом се може одредити који од заједничких контролора података може дјеловати као јединствена контакт тачка за остваривање права носиоца података.
- (2) Независно од услова споразума из става (1) овог члана, носилац података може остваривати своја права из овог закона у односу на сваки надлежни орган и против сваког од њих.

Члан 78.

(Коришћење услуге обрађивача од надлежног органа)

- (1) Надлежни орган користи услугу само оног обрађивача који може у довољној мјери обезбједити спровођење одговарајућих техничких и организационих мјера прописаних овим законом.
- (2) Коришћење услуге обрађивача од надлежног органа уређује се уговором или другим правним актом којим се уређују предмет, техничке и организационе мјере прописане овим законом, трајање обраде, обим, садржај и сврха обраде, врста личних података, категорије носилаца података те обавезе и права надлежног органа, као и да обрађивач:
- а) дјелује само према упутствима надлежног органа;
 - б) обезбјеђује да су се лица овлашћена за обраду личних података обавезала на поштовање повјерљивости или да подлијежу законским одредбама о повјерљивости;
 - ц) било којим одговарајућим средством помаже надлежном органу да обезбједи усклађеност с одредбама о правима носиоца података;
 - д) према избору надлежног органа, брише или враћа надлежном органу све личне податке након завршетка пружања услуге обраде података те брише постојеће копије, осим ако према некој законској одредби не постоји обавеза чувања личних података;
 - е) надлежном органу ставља на располагање све информације потребне за придржавање одредаба овог члана;
 - ф) поштује одредбе става (3) овог члана за ангажовање другог обрађивача.
- (3) Обрађивач не може користити услугу другог обрађивача без претходног писаног одобрења надлежног органа.
- (4) По запримању одобрења обрађивач је дужан да обавијести надлежни орган о свим планираним

измјенама у вези са коришћењем услуге других обрађивача.

- (5) Надлежни орган може ускратити сагласност обрађивачу за коришћење услуге другог обрађивача.
- (6) Ако обрађивач утврђује сврхе и начине обраде кршећи одредбе овог закона, тај обрађивач се сматра надлежним органом у вези с обрадом која му је повјерена.

Члан 79.

(Обрада под контролом надлежног органа)

Лице које дјелује под контролом надлежног органа или обрађивача, а има приступ личним подацима, не смије обрађивати те податке без налога контролора података, осим када је то прописано посебним законом.

Члан 80.

(Евиденција о обради од надлежног органа)

- (1) Надлежни орган води евиденцију обраде за коју је одговоран. Та евиденција садржи следеће информације:
 - а) назив и контакт податке надлежног органа, заједничког надлежног органа и службеника за заштиту личних података;
 - б) сврху обраде;
 - ц) категорију примаоца којем су лични подаци откривени или ће му бити откривени, укључујући примаоца у другој држави или међународној организацији;
 - д) опис категорије носиоца података и категорије личних података;
 - е) употребу израде профила, ако је примјениво;
 - ф) категорију преноса личних података у другу државу или међународну организацију, ако је примјениво;
 - г) правни основ за поступак обраде, укључујући преносе, којем су лични подаци намијењени;
 - х) предвиђени рокови за брисање различитих категорија личних података, ако је могуће;
 - и) општи опис техничких и организационо-безбједносних мјера из члана 85. става (1) овог закона, ако је могуће.
- (2) Надлежни орган обезбјеђује да сваки обрађивач води евиденцију свих категорија активности обраде које се обављају у име контролора података, а која садржи:
 - а) име и контакт податке једног или више обрађивача и сваког контролора података у чије име обрађивач дјелује, те службеника за заштиту података, ако је примјениво;
 - б) категорију обраде која се спроводи за сваког контролора података;
 - ц) ако је примјениво, податке о преносу личних података у другу државу или међународну организацију, ако за то постоји изричито упутство контролора података, укључујући идентификацију те друге државе или међународне организације;
 - д) ако је могуће, општи опис техничких и организационо-безбједносних мјера из члана 85. става (1) овог закона.
- (3) Евиденција из става (1) овог члана мора бити у писаној форми, што укључује електронску форму.
- (4) Надлежни орган на захтјев Агенције, приликом надзора, ставља евиденцију на увид.

Члан 81.

(Записивање)

- (1) Надлежни орган дужан је да, код аутоматизованог система обраде личних података, успостави приступ систему који аутоматски биљежи најмање следеће информације о: прикупљању, измјени, оствареном увиду, откривању, укључујући преносе, те комбиновању и брисању. Записи о оствареном увиду и откривању омогућавају да се утврде образложење, датум и вријеме таквих поступака те, ако је то могуће, идентитет лица које је остварило увид или открило личне податке и идентитет примаоца таквих личних података.
- (2) Запис се употребљава само у сврхе провере законитости обраде, самопраћења и обезбјеђивања цјеловитости и безбједности личних података те за кривичне поступке.
- (3) Надлежни орган на захтјев Агенције, приликом надзора, ставља записе на увид.

Члан 82.

(Сарадња надлежног органа и обрађивача с Агенцијом)

Надлежни орган и обрађивач дужни су да сарађују с Агенцијом, на образложен и на основу закона оправдан захтјев, приликом извршавања њене надлежности.

Члан 83.

(Процјена утицаја на заштиту личног податка од надлежног органа)

- (1) Надлежни орган прије обраде обавља процјену утицаја предвиђених поступака обраде на заштиту личних података, ако је вјероватно да ће нека врста обраде, посебно примјеном нових технологија и узимајући у обзир природу, обим, контекст и сврхе те обраде, проузроковати високи ризик за права и слободе лица.
- (2) Процјена из става (1) овог члана мора да садржава најмање општи опис предвиђених поступака обраде, процјену ризика за права и слободе носиоца података, предвиђене мјере за ризике, заштитне и безбједносне мјере и механизме како би се обезбиједила заштита личних података и доказала усклађеност с овим законом, узимајући у обзир права и легитимне интересе носиоца података и других укључених лица.

Члан 84.

(Претходно савјетовање надлежног органа с Агенцијом)

- (1) Надлежни орган или обрађивач дужан је да се савјетује с Агенцијом прије обраде личних података који ће бити укључени у нову збирку личних података, ако:
 - а) процјена утицаја на заштиту података, како је предвиђено чланом 83. овог закона, упућује на то да би обрада могла проузроковати висок ризик ако надлежни орган не предузме мјере како би умањило ризик, или
 - б) врста обраде, посебно ако се употребљавају нове технологије, механизми или поступци, представља висок ризик за права и слободе носиоца података.
- (2) Агенција може да утврди листу поступака обраде за које је потребно обавити претходно савјетовање у складу са ставом (1) овог члана.
- (3) Надлежни орган дужан је да Агенцији достави процјену утицаја на заштиту података на основу члана 83. овог закона и да на њен захтјев пружи све остале информације помоћу којих ће Агенција моћи процјенити усклађеност обраде те посебно ризике за

заштиту личних података носиоца података и повезане заштитне мјере.

- (4) Агенција ће у року од 42 дана од запримања писаног захтјева из става (1) овог члана писаним путем дати савјет надлежном органу те може искористити било које од својих овлашћења ако сматра да би се намјераваном обрадом из става (1) овог члана кршиле одредбе овог закона, посебно ако надлежни орган није у довољној мјери утврдио или умањео ризик.
- (5) Рок из става (4) овог члана може се, по потреби, продужити за 30 дана, узимајући у обзир сложеност намјераване обраде.
- (6) Агенција у року од 30 дана од запримања захтјева обавјештава надлежни орган и, по потреби, обрађивача о сваком продужењу и разлозима одгађања.
- (7) О приједлогу закона којим се регулише обрада личних података, а прије његовог упућивања у парламентарну процедуру, предлагач се може претходно савјетовати са Агенцијом.

Члан 85.

(Безбједност обраде од надлежног органа и обрађивача)

- (1) Надлежни орган и обрађивач дужни су да, узимајући у обзир најновија достигнућа, трошкове спровођења, природу, обим, контекст и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободе физичких лица, примијене одговарајуће техничке и организационе мјере како би се постигао одговарајући ниво безбједности сходно ризику, посебно у вези с обрадом посебних категорија личних података.
- (2) У вези са аутоматизованом обрадом, надлежни орган или обрађивач, након процјене ризика, дужан је да успостави мјере које обезбјеђују да се:
 - а) онемогући неовлашћеним лицима приступ опреми која се користи за обраду;
 - б) спрјечи неовлашћено читање, умножавање, мијењање или уклањање носача података;
 - ц) спрјечи неовлашћено уношење личних података те неовлашћено прегледање, мијењање или брисање чуваних личних података;
 - д) спрјечи коришћење система за аутоматску обраду од неовлашћеног лица употребом опреме за пренос података;
 - е) лице које је овлашћено за коришћење система за аутоматску обраду има приступ само оним личним подацима на које се односи његово одобрење за приступ;
 - ф) може провјерити и утврдити коме су лични подаци пренесени, односно би могли бити пренесени или учињени доступним употребом опреме за пренос података;
 - г) може накнадно провјерити, односно утврдити који су лични подаци унесени у систем аутоматске обраде те ко их је и када унео;
 - х) спрјечи неовлашћено читање, умножавање, мијењање или брисање личних података током преноса личних података или преноса носача података;
 - и) омогући поновно успостављање инсталираних система у случају прекида њиховог рада;
 - ј) одржава исправна функција система, да се појава грешака у функционисању система пријави те да чувани лични подаци не могу бити угрожени због недостатака у функционисању система.

Члан 86.

(Обавјештавање Агенције о повреди личног податка од надлежног органа)

- (1) Надлежни орган дужан је да у случају повреде личних података, без одгађања, а најкасније 72 сата након сазнања за повреду, обавјести Агенцију о повреди личних података, осим ако повреда личних података не угрожава права и слободе физичког лица.
- (2) Обрађивач је дужан да у случају повреде личних података без одгађања обавјести надлежни орган након што сазна за повреду личних података.
- (3) Ако обавјештавање Агенције из става (1) овог члана није обављено у року од 72 сата, мора се сачинити писано образложење са навођењем разлога за кашњење.
- (4) Обавјештење из става (1) овог члана садржи најмање следеће информације:
 - а) опис повреде личних података, укључујући, ако је могуће, категорије и приближан број носилаца података, као и категорије и приближан број евиденција личних података о којима је ријеч;
 - б) име и презиме и контакт податке службеника за заштиту података или друге контакт тачке од које се може добити још информација;
 - ц) опис вјероватне посљедице повреде личних података;
 - д) опис мјера које је надлежни орган предузео или чије је предузимање предложено ради рјешавања проблема повреде личних података, укључујући према потреби и мјере за ублажавање могућих штетних посљедица.
- (5) Информације се могу достављати у дијеловима, без одгађања, ако и у мјери у којој није могуће истовремено доставити све информације.
- (6) Надлежни орган документује сваку повреду личних података из става (1) овог члана, укључујући и чињенице у вези са повредом личних података, њене посљедице и мјере предузете за поправљање ситуације.
- (7) Документација из става (4) овог члана мора бити доступна Агенцији с циљем провјере примјене овог члана.
- (8) Надлежни орган обезбјеђује да се, у случају повреде личних података која укључује личне податке које је пренио контролор података друге државе или који су пренесени њему, информације из става (4) овог члана преносе контролору података те државе без непотребног одгађања.

Члан 87.

(Обавјештавање носиоца податка о повреди личног податка)

- (1) Ако је вјероватно да ће повреда личних података проузроковати висок ризик за права и слободе физичког лица, надлежни орган, без одгађања, обавјештава носиоца података о повреди личних података.
- (2) У обавјештењу из става (1) овог члана јасним и једноставним језиком се описује природа повреде личних података те се наводе најмање информације и мјере из члана 86. става (4) тач. б), ц) и д) овог закона.
- (3) Обавјештавање носиоца података није обавезно ако је испуњен један од следећих услова:
 - а) ако је надлежни орган предузео одговарајуће техничке и организационе мјере заштите и те мјере су примијењене на личне податке у вези с којима је дошло до повреде личних података, а

- прије свега мјере које личне податке чине неразумљивим лицу које није овлашћено да им приступи, као што је енкрипција;
- б) ако је контролор података предузео накнадне мјере којима се обезбјеђује да више није вјероватно да ће доћи до високог ризика за права и слободе носиоца података;
- ц) ако би то захтијевало непропорционалан напор. У том случају се објављује јавно обавјештење или се предузима слична мјера којом се носиоци података обавјештавају на једнако дјелотворан начин.
- (4) Ако надлежни орган до тог тренутка није обавијестио носиоца података о повреди личних података, Агенција, након разматрања степена вјероватноће да ће повреда личних података проузроковати висок ризик, може од њега захтијевати да то учини или може закључити да је испуњен неки од услова из става (3) овог члана.
- (5) Обавјештавање носиоца података може се одгодити, ограничити или ускратити у складу са условима и на основу разлога из члана 69. става (3) овог закона.

Члан 88.

(Именоване службеника за заштиту личних података од надлежног органа)

- (1) Надлежни орган дужан је да именује службеника за заштиту личних података.
- (2) Судови и други независни правосудни органи, када поступају у оквиру своје правосудне надлежности, пишу дужни да именују службеника за заштиту личних података.
- (3) Службеник за заштиту личних података именује се на основу његових стручних квалификација, а посебно стручног знања о праву и пракси из области заштите личних података и способности обављања задатака из члана 90. овог закона.
- (4) Више надлежних органа може именовати једног службеника за заштиту личних података, узимајући у обзир њихову организациону структуру и величину.
- (5) Надлежни орган дужан је да објави контактне податке службеника за заштиту личних података и да их саопшти Агенцији.

Члан 89.

(Радно мјесто службеника за заштиту личних података од надлежног органа)

- (1) Надлежни орган дужан је да обезбиди да службеник за заштиту личних података буде на одговарајући начин и благовремено укључен у сва питања која се тичу заштите личних података.
- (2) Надлежни орган дужан је да подржава службеника за заштиту личних података у извршавању задатака пружајући му потребна средства за извршавање тих задатака и приступ личним подацима и поступцима обраде, као и за одржавање његовог стручног знања.

Члан 90.

(Задаци службеника за заштиту личних података од надлежног органа)

Надлежни орган службенику за заштиту личних података повјерава најмање следеће задатке:

- а) информисаност и савјетовање надлежног органа и запослених који обављају обраду о њиховим обавезама из овог закона и других закона којима се прописује заштита личних података;
- б) праћење примјене овог закона и других закона којима се прописује заштита личних података,

као и политика надлежног органа у вези са заштитом личних података, укључујући и подјелу одговорности, подизање свијести и оспособљавање запослених који учествују у радњама обраде, као и с тим повезаним ревизијама;

- ц) пружање савјета, када је то захтијевано, у вези са проценом утицаја на заштиту личних података и праћење њеног извршавања у складу са чланом 83. овог закона;
- д) сарадњу с Агенцијом;
- е) дјеловање као контактна тачка за Агенцију о питањима која се тичу обраде, што укључује и претходно савјетовање из члана 84. овог закона те савјетовање, по потреби, о свим другим питањима.

Члан 91.

(Општи принципи преноса личног податка у другу државу или међународну организацију од надлежног органа)

- (1) Надлежни орган дужан је да сваки пренос личних података који се обрађују или су намијењени за обраду након преноса у другу државу или међународну организацију, укључујући даљи пренос у још једну другу државу или међународну организацију, обавља придржавајући се одредаба овог дијела закона, само ако су испуњени следећи услови, и то:
- а) пренос је неопходан у сврхе утврђене у члану 1. става (1) тачки ц) овог закона;
- б) лични подаци преносе се надлежном органу у другој држави или међународној организацији, који представља јавни орган надлежан за потребе из члана 1. става (1) тачке ц) овог закона;
- ц) ако су лични подаци пренесени или стављени на располагање из друге државе, та је држава дала претходно одобрење за пренос у складу са својим правом;
- д) ако је Савјет министара Босне и Херцеговине, на приједлог Агенције, донио одлуку о адекватности из члана 92. става (3) овог закона или ако Савјет министара Босне и Херцеговине није донио одлуку о адекватности из члана 92. става (3) овог закона, морају бити обезбијеђене или постоје одговарајуће заштитне мјере из члана 93. овог закона или ако Савјет министара Босне и Херцеговине није донио одлуку о адекватности из члана 92. става (3) овог закона и нису обезбијеђене или не постоје одговарајуће заштитне мјере из члана 93. овог закона, примјењују се одступања за посебне ситуације из члана 94. овог закона;
- е) у случају даљег преноса у још једну другу државу или међународну организацију, надлежни орган који је обавио први пренос или други надлежни орган у Босни и Херцеговини може, након што је узео у обзир све релевантне чињенице, укључујући озбиљност кривичног дјела, сврху у коју су лични подаци прво пренесени и ниво заштите личних података у другој држави или међународној организацији, одобрити даљи пренос.
- (2) Надлежном органу допуштен је пренос, без претходног одобрења друге државе, у складу са ставом (1) тачком ц) овог члана, изузетно, ако је пренос личних података потребан за спречавање непосредне и озбиљне пријетње јавној безбједности

Босне и Херцеговине или друге државе или битним интересима Босне и Херцеговине, а претходно одобрење се не може благовремено добити.

- (3) Надлежни орган дужан је да обавијести орган у другој држави, одговоран за издавање претходног одобрења, о случају из става (2) овог члана.
- (4) Све одредбе у вези са преносом личних података у другу државу или међународну организацију примјењују се како би се обезбедило да се не угрози ниво заштите физичких лица који је загарантован овим дијелом закона.

Члан 92.

(Пренос од надлежног органа на основу одлуке о адекватности)

- (1) Пренос личних података у другу државу или међународну организацију може се обављати ако Савјет министара Босне и Херцеговине одлучи да друга држава, територија или један или више конкретних сектора унутар те друге државе, или међународна организација обезбјеђује адекватан ниво заштите, и у том случају такав пренос не захтијева посебно одобрење.
- (2) Сматра се да је адекватан ниво заштите из става (1) овог члана обезбјеђен у држави, дијеловима њене територије или једном или више сектора у тој држави, међународној организацији, за које је од Европске уније утврђено да обезбјеђују адекватан ниво заштите личних података.
- (3) Одлуку о адекватности нивоа заштите личних података из става (1) овог члана доноси Савјет министара Босне и Херцеговине на приједлог Агенције.
- (4) Агенција припрема приједлог одлуке из става (3) овог члана узимајући у обзир:
- а) владавину права, поштовање људских права и основних слобода, релевантно опште и секторско законодавство, што укључује законодавство о јавној безбједности, одбрани, државној безбједности, кривично право и приступ јавних органа личним подацима, као и примјену тог законодавства, правила о заштити личних података, правила струке и мјере безбједности, што укључује правила за даљи пренос личних података у још једну другу државу или међународну организацију, која се поштују у тој другој држави или међународној организацији, судску праксу, као и постојање дјелотворних и остваривих права носилаца података и ефикасну управну и судску заштиту носилаца података;
 - б) постојање и ефикасно функционисање једног или више независних надзорних органа у другој држави или органа којем подлијеже међународна организација, одговорних за обезбјеђивање и спровођење правила о заштити података, што укључује адекватна извршна овлашћења за пружање помоћи носиоцима података у остваривању њихових права, као и за сарадњу са Агенцијом;
 - ц) међународне обавезе које је друга држава или међународна организација преузела или друге обавезе које произлазе из правно обавезујућих конвенција или инструмената, као и из њеног учествовања у мултилатералним или регионалним организацијама, посебно у вези са заштитом личних података.

- (5) Агенција континуирано прати стање у области заштите личних података у другој држави, дијелу њене територије, једном или више сектора унутар те државе или међународној организацији и о томе по потреби извјештава Савјет министара Босне и Херцеговине.
- (6) Извјештај из става (5) овог члана укључује доступне информације и информације прикупљене од међународних организација, које су од значаја за преиспитивање постојања адекватног нивоа заштите личних података, на основу чега Савјет министара Босне и Херцеговине доноси одлуку из става (3) овог члана.
- (7) Одлука донесена на основу става (3) овог члана не доводи у питање пренос личних података у другу државу, на територији или у један или више одређених сектора унутар те друге државе или међународну организацију, у складу са чл. 93. и 94. овог закона.
- (8) Листа држава, дијела њихових територија, један или више сектора унутар тих држава и међународних организација у вези с којим је Савјет министара Босне и Херцеговине донио одлуку да не обезбјеђују или да више не обезбјеђују адекватан ниво заштите личних података објављује се у "Службеном гласнику БиХ" и на службеној интернет страници Агенције.

Члан 93.

(Пренос од надлежног органа на који се примјењују одговарајуће заштитне мјере)

- (1) Надлежни орган може да обави пренос личних података у другу државу или међународну организацију ако није донесена одлука на основу члана 92. става (3) овог закона, уз сљедеће услове:
- а) ако су одговарајуће заштитне мјере у вези са заштитом личних података предвиђене у правно обавезујућем инструменту, или
 - б) ако је надлежни орган процијенио све околности у вези са преносом личних података и закључио да постоје одговарајуће заштитне мјере у вези са заштитом личних података.
- (2) Надлежни орган дужан је да обавијести Агенцију о категоријама преноса у складу са ставом (1) тачком б) овог члана.
- (3) Када се пренос личних података заснива на ставу (1) тачки б) овог члана, надлежни орган дужан је да такав пренос документује, а документацију, на захтјев, стави на располагање Агенцији, укључујући датум и вријеме преноса, информације о надлежном органу који је добио податке, образложење преноса и који су лични подаци пренесени.

Члан 94.

(Одступање у посебним случајевима преноса личног податка од надлежног органа)

- (1) Ако не постоји одлука о адекватности из члана 92. става (3) овог закона или одговарајуће заштитне мјере из члана 93. овог закона, пренос или скуп преноса личних података у другу државу или међународну организацију обавља се само ако је пренос неопходан и ако испуњава један од сљедећих услова:
- а) како би се заштитили кључни интереси носиоца података или другог лица;
 - б) како би се заштитили легитимни интереси носиоца података, ако је то предвиђено посебним законом;

- ц) како би се спријечила непосредна и озбиљна пријетња јавној безбједности на територији Босне и Херцеговине или друге државе;
- д) у појединачним случајевима у сврхе наведене у члану 1. ставу (1) тачки ц) овог закона или
- е) у појединачном случају ради постављања, остваривања или одбране правних захтјева у вези са сврхама наведеним у члану 1. ставу (1) тачки ц) овог закона.
- (2) Лични подаци не смију се преносити ако надлежни орган који обавља пренос утврди да основна права и слободе односног носиоца података имају предност пред јавним интересом у вези са преносом из става (1) тач. д) и е) овог члана.
- (3) Ако се пренос обавља на основу става (1) овог члана, надлежни орган дужан је да такав пренос документује и документацију, на захтјев, стави на располагање Агенцији, укључујући датум и вријеме преноса, информације о надлежном органу који је добио податке, образложење преноса и који су лични подаци пренесени.
- Члан 95.
- (Пренос личног податка примаоца са сједиштем или пословним настаном у другој држави)
- (1) Надлежни орган може у складу са посебним законом, одступајући од члана 91. става (1) тачке б) овог закона и не доводећи у питање ниједан међународни споразум из става (2) овог члана, у појединачним и посебним случајевима, пренијети личне податке директно примаоцима са сједиштем или пословним настаном у другој држави само ако се придржавају одредаба овог дијела закона и ако су испуњени следећи услови:
- а) ако је пренос искључиво неопходан за обављање задатка надлежног органа који обавља пренос како је предвиђено посебним законом у сврхе наведене у члану 1. ставу (1) тачки ц) овог закона;
- б) ако надлежни орган који обавља пренос утврди да основна права и слободе дотичног носиоца података немају предност над јавним интересом који изискује пренос у предметном случају;
- ц) ако надлежни орган који обавља пренос сматра да је пренос органу надлежном за поступање у сврху из члана 1. става (1) тачке ц) овог закона у другу државу недјелотворан или непримјерен, посебно зато што се пренос не може благовремено остварити;
- д) ако орган који је у другој држави надлежан за поступање у сврху из члана 1. става (1) тачке ц) овог закона обавијештен је без одгађања, осим ако је то недјелотворно или непримјерено;
- е) ако надлежни орган који обавља пренос обавијести примаоца о одређеној сврси или сврхама у које тај прималац искључиво може обрађивати личне податке, само ако је таква обрада неопходна.
- (2) Међународни споразум из става (1) овог члана је сваки билатерални или мултилатерални међународни споразум на снази између Босне и Херцеговине и друге државе у области правосудне сарадње у кривичним стварима и полицијске сарадње.
- (3) Надлежни орган који обавља пренос дужан је да обавијести Агенцију о преносима у складу с овим чланом.
- (4) Надлежни орган који обавља пренос личних података на основу става (1) овог члана дужан је да такав пренос документује.
- ДИО ЧЕТВРТИ – АГЕНЦИЈА ЗА ЗАШТИТУ ЛИЧНИХ ПОДАТАКА У БОСНИ И ХЕРЦЕГОВИНИ**
- Члан 96.
(Агенција)
- (1) Агенција је независан надзорни орган за праћење примјене овог закона, с циљем заштите основних права и слобода физичких лица у вези с обрадом личних података у Босни и Херцеговини.
- (2) Сједиште Агенције је у Сарајеву.
- (3) На сва питања организације и управљања те друга питања значајна за функционисање Агенције примјењују се прописи којима се регулише организација рада органа управе, осим ако није другачије прописано овим законом.
- Члан 97.
(Независност Агенције)
- (1) Агенција дјелује потпуно независно при обављању својих надлежности у складу с овим законом.
- (2) Директор, замјеник директора и запослени у Агенцији, при обављању својих дужности и овлашћења у складу с овим законом, не смију бити изложени непосредном или посредном спољном утицају и не смију ни од кога тражити или примати инструкције.
- (3) Директор, замјеник директора и запослени у Агенцији морају се уздржавати од свих радњи које нису у складу са њиховим дужностима и током свог мандата и запослења не смију се бавити неспојивом дјелатношћу, без обзира на то да ли је она плаћена или не.
- (4) Агенција мора имати људске, техничке и финансијске ресурсе, просторије и инфраструктуру потребне за ефикасно обављање својих надлежности, укључујући и овлашћења која се односе на међународну узајамну помоћ и сарадњу.
- (5) Запослени у Агенцији су државни службеници и запосленици и на њих се примјењују Закон о државној служби у институцијама Босне и Херцеговине и Закон о раду у институцијама Босне и Херцеговине.
- (6) Правилник о унутрашњој организацији Агенције, на приједлог директора Агенције, одобрава Парламентарна скупштина Босне и Херцеговине.
- (7) Агенција, у складу са одредбама Закона о финансирању институција Босне и Херцеговине, припрема нацрт годишњег буџета и доставља га парламентарној комисији на одобравање. Агенција, након добијања одобрења парламентарне комисије, у складу са роковима прописаним одредбама Закона о финансирању институција Босне и Херцеговине, доставља Министарству финансија и трезора Босне и Херцеговине нацрт буџета ради уврштавања у буџет институција Босне и Херцеговине и међународних обавеза Босне и Херцеговине. Министарство финансија и трезора Босне и Херцеговине, Савјет министара Босне и Херцеговине и Предсједништво Босне и Херцеговине могу дати мишљење о нацрту буџета Агенције, без могућности измјене нацрта буџета који је претходно одобрила парламентарна комисија.
- (8) Агенција подлијеже финансијској контроли у складу са прописима о финансијској контроли.

Члан 98.

(Руковођење Агенцијом)

- (1) Агенцијом руководи директор.
- (2) Директор има једног замјеника.
- (3) Замјеник директора замјењује директора у обављању послова ако директор није у могућности да обавља послове у складу са својим овлашћењима и обавезама.
- (4) Директор је одговоран за законит рад Агенције.

Члан 99.

(Услови за именовање, привремена суспензија и разрјешење директора и замјеника директора)

- (1) Директора и замјеника директора именује Парламентарна скупштина Босне и Херцеговине (у даљем тексту: Парламентарна скупштина) на основу јавног конкурса.
- (2) Директор и замјеник директора именују се на период од шест година уз могућност још једног поновног именовања.
- (3) Услови за именовање директора и замјеника директора су:
 - а) да је старији од 18 година;
 - б) да је држављанин Босне и Херцеговине (сви држављанин Федерације БиХ, Републике Српске и Брчко Дистрикта БиХ су држављани БиХ);
 - ц) да није осуђиван и да се против њега не води кривични поступак;
 - д) да није обухваћен одредбом члана IX1. Устава Босне и Херцеговине;
 - е) да је здравствено способан;
 - ф) да има завршен факултет друштвеног смјера, ВСС/VII степен, или високо образовање болесног система студирања са најмање 240 ECTS бодова;
 - г) да има најмање 10 година радног искуства у струци, од чега најмање пет година радног искуства на пословима руковођења;
 - х) да има стручна знања и искуства из области заштите личних података;
 - и) да није члан политичке странке.
- (4) Парламентарна скупштина може привремено суспендовати директора и замјеника директора ако се открије тешка повреда службене дужности. Привремена суспензија траје док се тешка повреда службене дужности не утврди коначном одлуком.
- (5) Парламентарна скупштина може да разријешити директора и замјеника директора прије истека мандата:
 - а) на његов захтјев;
 - б) ако се утврди тешка повреда службене дужности;
 - ц) када наврши 65 година живота и најмање 20 година стажа осигурања или 40 година стажа осигурања, независно од година живота;
 - д) ако више не испуњава услове потребне за именовање.

Члан 100.

(Нespoјивост функције и обавеза чувања професионалне тајне)

- (1) Директору и замјенику директора, као и запосленима у Агенцији, забрањени су дјеловање, пословање и погодности који нису у складу са принципима независности и непристраности за вријеме трајања мандата, односно радног односа, и једну годину након његовог престанка.
- (2) Директор, замјеник директора и запослени у Агенцији, за вријеме трајања мандата односно радног

односа и након престанка мандата односно радног односа, дужни су да чувају професионалну тајну која се односи на све повјерљиве информације које сазнају приликом обављања својих дужности или овлашћења, у складу са прописима у Босни и Херцеговини. Током трајања њиховог мандата, дужност чувања професионалне тајне се посебно односи на пријаве физичких лица о кршењима овог закона.

Члан 101.

(Надлежности Агенције)

- (1) Агенција је надлежна за:
 - а) обављање задатака и овлашћења додијелиених овим законом;
 - б) надзор над поступцима обраде личних података које обављају контролори података и обрађивачи.
- (2) Агенција није надлежна за надзор над поступцима обраде личних података које спроводе судови када обављају судску функцију.

Члан 102.

(Задаци Агенције)

- (1) Агенција обавља следеће задатке:
 - а) прати и примјењује овај закон;
 - б) промовише јавну свијест о ризицима, правилима, заштитним мјерама и правима у вези с обрадом личних података те њихово разумијевање, а посебну пажњу посвећује активностима које су изричито намијењене дјети;
 - ц) савјетује, у складу с овим законом, јавне органе и друге институције и органе о законодавним и управним мјерама у вези са заштитом права и слобода физичких лица у вези с обрадом;
 - д) подиже свијест контролора података и обрађивача о њиховим обавезама из овог закона;
 - е) на захтјев сваког носиоца података пружа информације у вези са остваривањем његових права из овог закона;
 - ф) разматра приговор носиоца података или органа, организације или удружења у складу са чланом 111. овог закона и у року од 90 дана доноси рјешење по приговору, о чему обавјештава подносиоца притужбе;
 - г) спроводи провјере у вези са примјеном овог закона, између осталог, и на основу информација примљених од јавних органа;
 - х) прати битна кретања, у мјери у којој утичу на заштиту личних података, а посебно развој информационих и комуникационих технологија и комерцијалних пракси;
 - и) доноси стандардне уговорне клаузуле из члана 30. става (8) и члана 48. става (3) овог закона;
 - ј) утврђује и води списак обрада у вези с обавезом обављања процјене утицаја на заштиту података у складу са чланом 37. ставом (4) овог закона;
 - к) даје савјете о поступку обраде личних података из члана 38. става (2) овог закона и члана 84. става (4) овог закона;
 - л) подстиче израду кодекса понашања и даје мишљење и одобрава такве кодексе понашања који пружају довољне заштитне мјере у складу са чланом 42. ставом (5) овог закона;
 - м) подстиче успостављање механизма сертификације заштите података, као и печата и ознака за заштиту података у складу са чланом 44. ставом (1) овог закона и одобрава

- критеријуме сертификације у складу са чланом 44. ставом (6) овог закона;
- н) у одређеним случајевима врши периодично преиспитивање издатих сертификата у складу са чланом 44. ст. (8) и (9) овог закона;
- о) сачињава и објављује критеријуме за акредитацију органа за праћење кодекса понашања у складу са чланом 43. овог закона и акредитацију сертификационог органа у складу са чланом 45. овог закона;
- п) акредитује органе за праћење кодекса понашања у складу са чланом 43. овог закона и акредитује сертификациони орган у складу са чланом 45. овог закона;
- р) одобрава одговарајуће заштитне мјере из члана 48. став (4) овог закона;
- с) одобрава обавезујућа пословна правила у складу са чланом 49. овог закона;
- т) води интерну евиденцију о кршењима овог закона и мјерама које су предузете у складу са чланом 103. ставом (2) овог закона;
- у) даје мишљење на приједлог закона институцијама на нивоу Босне и Херцеговине који се односи на обраду личних података;
- в) извршава све остале задатке у вези са заштитом личних података.
- (2) Агенција прописује изглед и садржај обрасца за подношење приговора.
- (3) Агенција обавља задатке бесплатно за носиоце података и, ако је то примјењиво, и за службенике за заштиту личних података.
- (4) Агенција обавља задатке бесплатно за носиоце података и за службенике за заштиту личних података из ДИЈЕЛА ТРЕЋЕГ овог закона.
- (5) Ако су захтјеви носилаца података очигледно неосновани или претјерани, посебно због учесталог понављања, Агенција може да наплати накнаду стварних административних трошкова или да одбије да поступи по захтјеву, при чему Агенција сноси терет доказивања очигледне неоснованости или претјераности захтјева.
- (6) Агенција наплаћује накнаду за издавање акредитације сертификационом органу.
- (7) Агенција наплаћује накнаду за давање мишљења и других услуга пословним субјектима у сврху обављања њихове редовне дјелатности.
- (8) Критеријуме за одређивање висине накнаде из ст. (5), (6) и (7) овог члана утврђује Агенција уз претходну сагласност Савјета министара Босне и Херцеговине и они се објављују у "Службеном гласнику БиХ".
- (9) Накнада се уплаћује на Јединствени рачун трезора институција Босне и Херцеговине.
- Члан 103.
(Овлашћења Агенције)
- (1) Агенција има следећа овлашћења:
- а) да обавља преиспитивање сертификата издатих у складу са чланом 44. ст. (8) и (9) овог закона;
- б) да обавља инспекцијске надзоре;
- ц) да обавља ревизију заштите података;
- д) да наложи контролору података и обрађивачу, а према потреби и представнику контролора података или обрађивача, достављање свих информација потребних за обављање њених задатака;
- е) да обавијести контролора података или обрађивача о наводном кршењу овог закона;
- ф) да оствари приступ свим личним подацима и свим информацијама у посједу контролора података и обрађивача, које су потребне за обављање њених задатака;
- г) да оствари приступ свим просторијама контролора података и обрађивача у којима се обрађују лични подаци, укључујући сву опрему и средства за обраду података.
- (2) Агенција има следећа корективна овлашћења:
- а) да изрекне упозорење контролору података или обрађивачу да би намјераване обраде могле лако представљати кршење овог закона;
- б) да изрекне опомену контролору података или обрађивачу ако се обрадом крши овај закон;
- ц) да наложи контролору података или обрађивачу да поступи по захтјеву носиоца података за остваривање његових права у складу с овим законом;
- д) да наложи контролору података или обрађивачу да обраде, ако је потребно, усклади с одредбама овог закона на тачно одређен начин и у тачно задатом року;
- е) да наложи контролору података да носиоца података обавијести о повреди личних података;
- ф) да привремено или трајно ограничи или забрани обраду;
- г) да наложи исправљање или брисање личних података или ограничење обраде и обавјештавање о таквим радњама прималаца којима су лични подаци откривени;
- х) да одузме сертификат издат у складу са чл. 44. и 45. овог закона или да сертификационом органу наложи да не изда сертификат ако захтјеви за сертификацију нису испуњени или да повуче сертификат ако захтјеви више нису испуњени;
- и) да изда прекршајни налог у оквиру прекршајног поступка или поднесе захтјев за покретање прекршајног поступка у складу са овим законом;
- ј) да наложи привремено обустављање преноса података примаоцу у другој држави или међународној организацији.
- (3) Агенција има следећа овлашћења у вези с одобравањем и савјетовањем:
- а) да савјетује контролора података у складу са поступком претходног савјетовања из чл. 38. и 84. овог закона;
- б) да даје мишљења о свим питањима која се тичу заштите личних података, на сопствену иницијативу или на захтјев законодавних органа, влада или, у случајевима када је то посебним законом прописано, другим институцијама и органима, као и јавности;
- ц) да одобри обраду из члана 38. става (8) овог закона ако је посебним законом прописано такво претходно одобрење;
- д) да даје мишљења и одобрава нацрте кодекса понашања у складу са чланом 42. ставом (5) овог закона;
- е) да акредитује сертификационе органе у складу са чланом 45. овог закона;
- ф) да одобрава критеријуме сертификације у складу са чланом 44. ставом (6) овог закона;
- г) да усваја стандардне клаузуле о заштити података из члана 30. става (8) и члана 48. става (3) овог закона;

- х) да одобри одговарајуће заштитне мјере из члана 48. става (4) тачке а) овог закона;
 - и) да одобри одговарајуће заштитне мјере из члана 48. става (4) тачке б) овог закона;
 - ј) да одобри обавезујућа пословна правила у складу са чланом 49. овог закона.
- (4) Одлука Агенције је коначна у управном поступку и против ње није допуштена жалба, али се може покренути управни спор пред Судом Босне и Херцеговине.
- (5) Агенција у поступку одлучивања примјењује правила управног поступка, осим ако овим законом није другачије прописано.
- (6) Агенција је овлашћена да по потреби обавијести надлежне истражне органе о повредама овог закона или покрене правне поступке, или у тим поступцима на други начин учествује како би се применио овај закон.
- (7) Свака обрада личних података који имају одређен степен тајности на основу посебног закона спроводи се у складу са законом којим се уређује заштита тајних података.
- (8) Обраду личних података из става (7) овог члана спроводе службеници Агенције који имају дозволу за приступ тајним подацима, у складу са законом којим се уређује заштита тајних података.

Члан 104.

- (Међународна сарадња ради заштите личних података)
- Агенција предузима одговарајуће мјере у вези са другим државама и међународним организацијама ради:
- а) развоја механизма међународне сарадње за олакшавање ефикасне примјене законодавства о заштити личних података;
 - б) обезбјеђивања узајамне међународне помоћи у примјени законодавства о заштити личних података, што подразумијева обавјештавање, упућивање приговора, пружање помоћи у истрагама и размјену информација, у складу с одговарајућим мјерама за заштиту личних података и другим основним правима и слободама;
 - ц) укључивања релевантних интересних група у расправу и активности чији је циљ унапређење међународне сарадње у примјени законодавства о заштити личних података;
 - д) промовисања размјене и документовања законодавства и праксе у вези са заштитом личних података, укључујући и спорове око надлежности са другим државама.

Члан 105.

- (Повјерљиво пријављивање повреда закона)
- (1) Надлежни орган који обрађује личне податке у сврхе из члана 1. става (1) тачке ц) овог закона дужан је да обезбједи примјену ефикасних механизма за повјерљиво пријављивање случајева повреде овог закона.
- (2) Механизми који се примјењују у складу са ставом (1) овог члана морају да обезбједе да се повреда може пријавити надлежном органу или Агенцији.
- (3) Ови механизми укључују подизање свијести о заштити личних података и мјере о заштити лица која пријављују повреде.

Члан 106.

(Извјештаји Агенције)

- (1) Агенција подноси Парламентарној скупштини годишњи извјештај о заштити личних података за протеклу годину најкасније до краја јуна текуће године и чини га доступним јавности.
- (2) Годишњи извјештај о заштити личних података из става (1) овог члана садржи податке о:
- а) свим активностима Агенције, а посебно о врстама повреда личних података и мјерама које су предузете;
 - б) стању заштите личних података у Босни и Херцеговини;
 - ц) кључним питањима из области заштите личних података;
 - д) капацитетима Агенције.

Члан 107.

(Инспекцијски надзор)

- (1) Инспекцијски надзор над спровођењем овог закона обавља инспектор Агенције.
- (2) Инспектор свој идентитет, својство и овлашћење доказује легитимацијом инспектора.
- (3) Инспекцијским надзором остварује се непосредан увид у законитост рада и поступање контролора података и обрађивача с циљем провере усклађености његовог рада са овим законом и другим прописима који се односе на заштиту личних података.
- (4) Инспекцијски надзор може бити редовни, ванредни и ревизијски.
- (5) Редовни инспекцијски надзор се спроводи на основу годишњег и мјесечног плана инспекцијског надзора, који се доноси на нивоу Агенције.
- (6) Решење из редовног инспекцијског надзора доноси инспектор, против којег је дозвољена жалба директору Агенције у року од 15 дана од дана пријема рјешења.
- (7) Ванредни инспекцијски надзор се спроводи на основу приговора или поступања по службеној дужности када је, у односу на конкретни случај, потребно извршити инспекцијски надзор.
- (8) Записник из ванредног инспекцијског надзора је доказно средство у поступку по приговору или по службеној дужности, који спроводи и рјешава Агенција.
- (9) Ревизијски инспекцијски надзор се спроводи након редовног или ванредног инспекцијског надзора с циљем провере извршења наложених управних мјера.
- (10) Решење у поступку након извршеног ванредног и ревизијског инспекцијског надзора доноси директор Агенције и оно је коначно у управном поступку.
- (11) Након спроведеног инспекцијског надзора, инспектор саставља записник о утврђеном чињеничном стању, који потписују инспектор и овлашћено лице контролора података или обрађивача.
- (12) Инспектор има право да прегледа све пословне просторије и објекте у којима се обрађују лични подаци, процес рада, уређаје, исправе и документацију, као и да обавља друге радње у вези са сврхом инспекцијског надзора, у складу са чланом 103. ставом (1) тач. ф) и г) и чланом 103. ст. (7) и (8) овог закона.
- (13) Контролор података и обрађивач дужни су да инспектору омогуће несметано спровођење инспекцијског надзора.
- (14) Ако се инспектору у току инспекцијског надзора онемогућава обављање надзора или пружи физички

отпор или ако се тај отпор основано очекује, инспектор може затражити помоћ полиције.

- (15) О обављеном инспекцијском надзору инспектор води евиденцију.

ДИО ПЕТИ – ПРАВНА СРЕДСТВА, ОДГОВОРНОСТ И КАЗНЕ

Члан 108.

(Право на приговор Агенцији)

- (1) Носилац података има право да поднесе приговор Агенцији ако сматра да се обрадом личних података у вези с њим крши овај закон, не доводећи у питање друга управна или судска правна средства.
- (2) Агенција обавјештава подносиоца приговора о напретку и исходу поступка, укључујући и могућност примјене правног средства на основу члана 109. овог закона и пружа додатну помоћ на захтјев подносиоца приговора.

Члан 109.

(Право на дјелотворно правно средство против одлука Агенције)

- (1) Физичко лице, контролор података или обрађивач има право да покрене управни спор против одлуке Агенције пред Судом Босне и Херцеговине у року од 60 дана од дана пријема одлуке, не доводећи у питање друга управна или вансудска правна средства.
- (2) Носилац података има право да покрене управни спор пред Судом Босне и Херцеговине ако Агенција, у року од 90 дана, не ријеша приговор или не обавијести носиоца података о напретку или исходу поступка по приговору не доводећи у питање друга управна или вансудска правна средства.

Члан 110.

(Право на дјелотворно правно средство против контролора података или обрађивача)

- (1) Носилац података има право на судску заштиту против контролора података или обрађивача ако сматра да су због обраде личних података прекршена његова права из овог закона, не доводећи у питање друга управна или вансудска правна средства, укључујући право на подношење приговора Агенцији из члана 108. став (1) овог закона.
- (2) Поступак судске заштите из става (1) овог члана води се у складу са законима којима се уређује парнични поступак.

Члан 111.

(Заступање носилаца података)

Носилац података има право да дâ овлашћење непрофитном органу, организацији или удружењу основаном у складу са законом, чија сврха оснивања је остваривање циљева од јавног интереса и које је активно у области заштите права и слобода носиоца података у вези са заштитом личних података, да у његово име остварују права из чл. 108, 109. и 110. овог закона, као и да у његово име и за његов рачун остварују право на накнаду штете.

Члан 112.

(Право на накнаду штете и одговорност)

- (1) Свако лице које је претрпијело материјалну или нематеријалну штету због кршења овог закона има право на накнаду за претрпијену штету од контролора података или обрађивача.
- (2) Сваки контролор података одговоран је за штету проузроковану обрадом којом се крши овај закон. Обрађивач је одговоран за штету проузроковану обрадом само ако није поштовао обавезе из овог

закона које су посебно прописане за обрађиваче или ако је прекорачио законите инструкције контролора података или је поступио противно њима.

- (3) Контролор података или обрађивач изузет је од одговорности ако докаже да није ни на који начин одговоран за догађај који је проузроковао штету.
- (4) Ако је у исту обраду укључено више од једног контролора података или обрађивача или су у исту обраду укључени и контролор података и обрађивач и ако су одговорни за штету проузроковану обрадом, сваки контролор података или обрађивач одговоран је за cjелокупну штету.
- (5) Ако је контролор података или обрађивач платио пуну одштету у складу са ставом (4) овог члана, тај контролор података или обрађивач има право од других контролора података или обрађивача који су укључени у исту обраду да захтијева поврат дијела одштете који одговара њиховом удјелу у одговорности за штету.
- (6) Право на накнаду штете остварује се у судском поступку, а мјесна надлежност утврђује се у складу са чланом 110. ставом (2) овог закона.

Члан 113.

(Општи услови за изрицање новчане казни)

- (1) Агенција обезбјеђује да је изрицање новчане казне, у складу с овим чланом и у вези са повредама овог закона, у сваком појединачном случају дјелотворно, размјерно и одвраћајуће.
- (2) Агенција издаје прекршајни налог или подноси захтјев за покретање прекршајног поступка надлежном суду, поред мјера из члана 103. става (2) тач. од а) до х) и тачке ј) овог закона, у зависности од околности сваког појединачног случаја. Приликом одлучивања о новчаној казни и износу казне у сваком појединачном случају у обзир се узима посебно:
 - а) природа, тежина и трајање повреде, имајући у виду природу, обим и сврху предметне обраде, као и број носилаца података и степен штете коју су претрпијели;
 - б) да ли повреда има обиљежје намјере или непажње;
 - ц) свака радња коју је контролор података или обрађивач предузео како би ублажио штету коју су претрпијели носиоци података;
 - д) степен одговорности контролора података или обрађивача, при чему се узимају у обзир техничке и организационе мјере које су примијенили, у складу са чл. 27. и 34. овог закона;
 - е) све утврђене претходне повреде од контролора података или обрађивача;
 - ф) степен сарадње са Агенцијом на отклањању повреде и ублажавању могућих штетних посљедица повреде;
 - г) категорија личних података на које повреда утиче;
 - х) начин на који је Агенција сазнала за повреду, а посебно да ли је и у којем обиму контролор података или обрађивач обавијестио о повреди;
 - и) ако су против контролора података или обрађивача у вези са истим предметом претходно изречене мјере из члана 103. става (2) овог закона и поштовање тих мјера;
 - ј) поштовање одобрених кодекса понашања, у складу са чланом 42. овог закона или одобрених

- механизма сертификације, у складу са чланом 44. овог закона;
- к) све остале отежавајуће или олакшавајуће околности, као што су финансијска добит остварена кршењем или избјегнути губици, директно или индиректно, тим кршењем.
- (3) Ако контролор података или обрађивач за исту или повезане обраде намјерно или из непажње прекрши више одредаба овог закона, укупан износ новчане казне не смије бити већи од износа утврђеног за најтежу повреду.
- (4) Новчаном казном у износу од 10.000 КМ до 20.000.000 КМ, или у случају предузетника до 2% укупног годишњег промета на свјетском нивоу за претходну финансијску годину, зависно од тога који је износ виши, кажњава се:
- а) контролор података и обрађивач за обраду личних података извршену супротно чл. 10. и 13. чл. од 27. до 41, те чл. 44. и 45. овог закона;
- б) сертификациони орган који поступи супротно чл. 44. и 45. овог закона;
- ц) орган за праћење одобрених кодекса понашања ако поступи супротно члану 43. ставу (3) овог закона.
- (5) Новчаном казном у износу од 20.000 КМ до 40.000.000 КМ, или у случају предузетника до 4% укупног годишњег промета на свјетском нивоу за претходну финансијску годину, зависно од тога који је износ виши казниће се:
- а) ко обрађује личне податке супротно чл. 7, 8, 9. и 11. овог закона;
- б) ко крши права носилаца података из чл. од 14. до 24. овог закона;
- ц) ко пренесе личне податке примаоцу у другу државу или међународну организацију супротно чл. од 46. до 51. овог закона;
- д) ко поступи супротно обавезама из посебних закона донесених на основу ДИЈЕЛА ДРУГОГ Главе V овог закона;
- е) ко не поступи по налогу Агенције или привременом или трајном ограничењу обраде или привременом обустављању преноса података у складу са чланом 103. ставом (2) овог закона или ускрати приступ супротно члану 103. ставу (1) овог закона.
- (6) За непоступање по налогу Агенције из члана 103. става (2) овог закона, у складу са ставом (2) овог члана, изриче се новчана казна у износу од 20.000 КМ до 40.000.000 КМ, или у случају предузетника до 4% укупног годишњег промета на свјетском нивоу за претходну финансијску годину, зависно од тога који је износ виши.
- (7) За повреду из ст. (4), (5) и (6) овог члана новчаном казном у износу од 5.000 КМ до 70.000 КМ казниће се одговорно лице, а новчаном казном у износу од 500 КМ до 5.000 КМ казниће се запослено лице код контролора података или обрађивача.
- (8) Новчаном казном у износу од 5.000 КМ до 70.000 КМ казниће се одговорно лице, а новчаном казном у износу од 500 КМ до 5.000 КМ казниће се запослено лице у јавном и надлежном органу за прекршај:
- а) из чл. од 7. до 11, члана 13, чл. од 14. до 24, чл. од 27. до 41, чл. 44. и 45, чл. од 52. до 59, члана 60, члана 64, члана 66, чл. од 67. до 73, чл. 76. и 77. и чл. од 79. до 90. овог закона;

- б) ко пренесе личне податке примаоцу у другу државу или међународну организацију супротно чл. од 46. до 51, те чл. од 91. до 95. овог закона;
- ц) ко не поступи по налогу Агенције или привременом или трајном ограничењу обраде или привременом обустављању преноса података у складу са чланом 103. ставом (2) овог закона или ускрати приступ супротно члану 103. ставу (1) овог закона.
- (9) Застаријевање изрицања новчане казне наступа након протекла периода од пет година од дана када је повреда извршена.
- (10) Не доводећи у питање надлежности и овлашћења Агенције, новчане казне не могу се изрећи јавном и надлежном органу за повреду овог закона, осим одговорном и запосленим лицу из става (8) овог члана.
- (11) На поступак изрицања новчане казне из овог члана примјењују се одредбе Закона о прекршајима Босне и Херцеговине, а износи новчаних казни прописани су овим законом.
- (12) Изузетно од одредбе става (11) овог члана, приход остварен на основу наплате новчаних казни дијели се на начин прописан чланом 114. овог закона.

Члан 114.

(Извршење и наплата новчане казне)

Новчана казна уплаћује се на Јединствени рачун трезора институција Босне и Херцеговине и дијели се како слиједи:

- а) ако је сједиште или пословни настап правног лица или пребивалиште физичког лица у Босни и Херцеговини, средства са Јединственог рачуна трезора институција Босне и Херцеговине уплаћују се на рачун ентитета или Брчко Дистрикта Босне и Херцеговине, зависно од сједишта или пословног настана правног лица или пребивалишта физичког лица;
- б) ако је сједиште или пословни настап правног лица или пребивалиште физичког лица ван Босне и Херцеговине, средства са Јединственог рачуна трезора институција Босне и Херцеговине распоређују се према одлуци о утврђивању привремених коефицијената за расподелу средстава са Јединственог рачуна. У Федерацији Босне и Херцеговине средства се распоређују између кантона и општина у складу са законом о припадности јавних прихода у Федерацији Босне и Херцеговине.

Члан 115.

(Казне)

Кривичним законима прописују се казне за кривично дјело противзаконите обраде личних података, у случају грубог кршења одредаба овог закона.

ДИО ШЕСТИ – ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 116.

(Мјере у прелазном периоду)

- (1) Одредбе других закона које се односе на обраду личних података ускладиће се с овим законом у року од двије године од његовог ступања на снагу.
- (2) Контролори података и обрађивачи који су започели обраду личних података дужни су да те обраде ускладе с овим законом у року од двије године од његовог ступања на снагу.
- (3) Одлуке донесене на основу члана 18. става (4) Закона о заштити личних података ("Службени гласник БиХ",

бр. 49/06, 76/11 и 89/11) остају на снази док се не измијене, замијене или ставе ван снаге одлуком Агенције.

- (4) Директор и замјеник директора Агенције који су именовани у складу са Законом о заштити личних података ("Службени гласник БиХ", бр. 49/06, 76/11 и 89/11), настављају да обављају дужност до истека мандата на који су именовани.
- (5) Агенција наставља свој рад у прелазном периоду.

Члан 117.

(Подзаконски акти)

Сви подзаконски акти прописани овим законом биће донесени у року од 210 дана од дана ступања на снагу овог закона.

Члан 118.

(Однос са претходно склопљеним споразумима)

Међународни споразуми који укључују пренос личних података другим државама или међународним организацијама које је Босна и Херцеговина склопила прије доношења овог закона, а који су у складу са Законом о заштити личних података ("Службени гласник БиХ", бр. 49/06, 76/11 и 89/11), остају на снази док се не измијене, замијене или ставе ван снаге.

Члан 119.

(Престанак важења)

- (1) Почетком примјене овог закона престаје да важи Закон о заштити личних података ("Службени гласник БиХ", бр. 49/06, 76/11 и 89/11).
- (2) Почетком примјене овог закона престају да важе подзаконски акти донесени на основу закона из става (1) овог члана: Правилник о поступку по приговору носиоца личних података у Агенцији за заштиту личних података у Босни и Херцеговини ("Службени гласник БиХ", број 51/09), Правилник о инспекцијском надзору у области заштите личних података ("Службени гласник БиХ", број 51/09), Инструкција о начину провјере обраде личних података прије успостављања збирке личних података ("Службени гласник БиХ", број 51/09), Правилник о начину вођења и обрасцу евиденције о збиркама личних података ("Службени гласник БиХ", број 52/09) и Правилник о начину чувања и посебним мјерама техничке заштите личних података ("Службени гласник БиХ", број 67/09).

Члан 120.

(Ступање на снагу)

Овај закон ступа на снагу осмог дана од дана објављивања у "Службеном гласнику БиХ", а примјењује се након истека 210 дана од дана ступања на снагу.

Број 01.02-02-1-2548/24

30. јануара 2025. године

Сарајево

Предсједавајући
Представничког дома
Парламентарне скупштине
БиХ

Др Денис Звиздић, с. р.

Предсједавајући
Дома народа

Парламентарне скупштине
БиХ

Др Драган Човић, с. р.

На основу члана IV. 4. а) Устава Босне и Херцеговине, Парламентарна скупштина Босне и Херцеговине, на 16. hitnoj sjednici Predstavničkog doma, održanoj 23. januara 2025. godine, i на 8. hitnoj sjednici Doma naroda, održanoj 30. januara 2025. godine, usvojila је

ZAKON O ZAŠTITI LIČNIH PODATAKA

DIO PRVI – OPĆE ODREDBE

Члан 1.

(Предмет)

- (1) Ovim zakonom propisuju se:
- pravila u vezi sa zaštitom fizičkih lica u vezi s obradom ličnih podataka i pravila povezana sa slobodnim kretanjem ličnih podataka;
 - nadležnosti Agencije za zaštitu ličnih podataka u Bosni i Hercegovini (u daljnjem tekstu: Agencija), organizacija i upravljanje, kao i druga pitanja značajna za njen rad i zakonito funkcioniranje;
 - zaštita fizičkih lica u vezi s obradom ličnih podataka od nadležnih organa u svrhe sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinilaca krivičnih djela, izvršavanje krivičnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.
- (2) Ovim zakonom vrši se usklađivanje s odredbama Uredbe (EU) 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju van snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i odredbama Direktive (EU) 2016/680 Evropskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom ličnih podataka od nadležnih organa s ciljem sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinilaca krivičnih djela ili izvršavanje krivičnih sankcija i o slobodnom kretanju takvih podataka, te o stavljanju van snage Okvirne odluke Vijeća 2008/977/PUP.
- (3) Navođenje odredbi Uredbe i Direktive iz stava (2) ovog člana obavlja se isključivo s ciljem praćenja i informiranja o preuzimanju pravne tečevine Evropske unije u zakonodavstvu Bosne i Hercegovine.

Члан 2.

(Cilj zakona)

Ovim zakonom štite se osnovna prava i slobode fizičkih lica u Bosni i Hercegovini bez obzira na njihovo državljanstvo i prebivalište, a posebno njihovo pravo na zaštitu ličnih podataka.

Члан 3.

(Upotreba muškog ili ženskog roda)

Izrazi koji su radi preglednosti dati samo u jednom gramatičkom rodu u ovom zakonu bez diskriminacije se odnose i на muški и ženski rod.

Члан 4.

(Definicije)

Pojedini izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

- "lični podatak" je svaki podatak koji se odnosi на fizičko lice čiji je identitet utvrđen ili se može utvrditi;
- "nosilac podataka" je fizičko lice čiji je identitet utvrđen ili čiji se identitet može utvrditi, posredno ili neposredno, posebno pomoću identifikatora kao što su ime, identifikacioni broj, podaci о lokaciji, mrežni identifikator ili pomoću jednog ili više faktora svojstvenih за fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog lica;
- "obrada" je svaki postupak ili skup postupaka koji se obavlja на ličnim podacima ili на skupovima ličnih

- podataka, automatiziranim ili neautomatiziranim sredstvima, kao što su: prikupljanje, evidentiranje, organizacija, strukturiranje, čuvanje, prilagođavanje ili izmjena, pronalaženje, ostvarivanje uvida, upotreba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, uskladjivanje ili kombiniranje, ograničenje, brisanje ili uništavanje;
- d) "ograničenje obrade" je obilježavanje čuvanog ličnog podataka s ciljem ograničenja njegove obrade u budućnosti;
- e) "izrada profila" je svaki oblik automatske obrade ličnog podataka koji se sastoji od korištenja ličnog podataka za procjenu određenih ličnih aspekata u vezi s fizičkim licem, posebno za analizu ili predviđanje aspekata u vezi s radnim rezultatom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog fizičkog lica;
- f) "pseudonimizacija" je obrada ličnog podataka tako da se lični podatak više ne može pripisati određenom nosiocu podataka bez korištenja dodatnih informacija, uz uslov da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacionim mjerama kako bi se osiguralo da se lični podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;
- g) "zbirka ličnih podataka" je svaki strukturirani skup ličnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to da li su centralizirani, decentralizirani ili rasprostranjeni na funkcionalnoj ili geografskoj osnovi;
- h) "kontrolor podataka" je fizičko ili pravno lice, javni organ ili nadležni organ koji samostalno ili s drugim određuje svrhe i sredstva obrade ličnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriteriji za njegovo imenovanje propisuju se zakonom;
- i) "javni organ" je svaki zakonodavni, izvršni i sudski organ na svim nivoima vlasti u Bosni i Hercegovini;
- j) "nadležni organ" je organ koji je nadležan za sprečavanje, istragu i otkrivanje krivičnih djela, gonjenje učinilaca krivičnih djela ili izvršenje krivičnih sankcija, uključujući i zaštitu i sprečavanje prijetnji javnoj sigurnosti, kao i pravna lica ako su zakonom ovlaštena za obavljanje tih poslova, kao posebna kategorija kontrolora podataka;
- k) "obrađivač" je fizičko ili pravno lice, javni organ koji obrađuje lične podatke u ime kontrolora podataka;
- l) "primaoca" je fizičko ili pravno lice, javni organ kome se otkrivaju lični podaci, nezavisno od toga da li je u pitanju treća strana. Javni organi koji mogu primiti lične podatke u okviru određene istrage u skladu sa zakonom ne smatraju se primaocima, ali obrada tih podataka mora biti u skladu s važećim pravilima o zaštiti podataka prema svrhama obrade;
- m) "treća strana" znači fizičko ili pravno lice, javni organ, Agencija ili drugo tijelo koje nije nosilac podataka, kontrolor podataka, obrađivač ni lica koja su ovlaštena za obradu ličnih podataka pod neposrednom nadležnošću kontrolora podataka ili obrađivača;
- n) "saglasnost" nosioca podataka je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje nosioca podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu ličnih podataka koji se na njega odnose;
- o) "povreda ličnog podataka" je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa ličnim podacima koji su preneseni, čuvani ili na drugi način obrađivani;
- p) "genetski podatak" je lični podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičkog lica koja daju jedinstvene informacije o fiziologiji ili zdravlju tog fizičkog lica i koji su dobiveni posebnom analizom biološkog uzorka tog fizičkog lica;
- r) "biometrijski podatak" je lični podatak dobiven posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičkog lica koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica, kao što su fotografije lica ili daktiloskopski podaci;
- s) "podatak koji se odnosi na zdravlje" je lični podatak u vezi s fizičkim ili mentalnim zdravljem fizičkog lica, uključujući pružanje zdravstvenih usluga, koji daje informacije o njegovom zdravstvenom stanju;
- t) "predstavnik" je fizičko ili pravno lice s prebivalištem ili boravištem, odnosno sjedištem ili poslovnim nastanom u Bosni i Hercegovini koje je kontrolor podataka ili obrađivač pisanim putem imenovao u skladu s članom 29. ovog zakona;
- u) "privredni subjekt" je fizičko ili pravno lice koje obavlja privrednu djelatnost, bez obzira na pravni oblik te djelatnosti;
- v) "grupa privrednih subjekata" je privredni subjekt koji ostvaruje kontrolu i privredni subjekti koji su pod njegovom kontrolom;
- z) "obavezujuće poslovno pravilo" su politike zaštite ličnih podataka kojih se kontrolor podataka i obrađivač sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini pridržava prilikom prijenosa ili skupova prijenosa ličnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih država u okviru grupe privrednih subjekata ili grupe privrednih subjekata koji se bave zajedničkom privrednom djelatnošću;
- aa) "usluga informacionog društva" jeste svaka usluga koja se obično pruža uz naknadu, na daljinu, elektronskim sredstvima te na lični zahtjev primaoca usluga, gdje:
- 1) "na daljinu" znači da se usluga pruža a da pri tome strane nisu istovremeno prisutne;
 - 2) "elektronskim sredstvima" znači da se usluga na početku šalje i prima na određitu pomoću elektronske opreme za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radiovezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima;
 - 3) "na lični zahtjev primaoca usluga" znači da se usluga pruža prijenosom podataka na lični zahtjev;
- bb) "međunarodna organizacija" je organizacija sa svojim organima uređena međunarodnim javnim pravom ili bilo koji drugi organ koji su sporazumom ili na osnovu sporazuma osnovale dvije zemlje ili više zemalja;

- cc) "poslovni nastan" je djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana;
- dd) "videonadzor" je informaciono-komunikacioni sistem koji ima mogućnost prikupljanja i daljnje obrade ličnih podataka, koji obuhvata stvaranje snimka koji čini ili je namijenjen da čini dio sistema skladištenja.

Član 5.

(Glavna oblast primjene)

- (1) Ovaj zakon primjenjuje se na obradu ličnog podatka koja se u potpunosti obavlja automatizirano te na neautomatiziranu obradu ličnog podatka koji čini dio zbirke ličnih podataka ili je namijenjen da bude dio zbirke ličnih podataka.
- (2) Ovaj zakon ne primjenjuje se na obradu ličnog podatka koju obavlja fizičko lice isključivo u svrhu ličnih aktivnosti ili aktivnosti domaćinstva.
- (3) Na obradu ličnog podatka od nadležnog organa u svrhu zaštite fizičkih lica u vezi s obradom ličnih podataka u svrhu sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca krivičnih djela, izvršenja krivičnih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, ne primjenjuje se DIO DRUGI ovog zakona.

Član 6.

(Teritorijalno područje primjene)

- (1) Ovaj zakon primjenjuje se na obradu ličnog podatka koju obavlja kontrolor podataka ili obrađivač koji ima sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, nezavisno od toga obavlja li se obrada u Bosni i Hercegovini ili ne.
- (2) Ovaj zakon primjenjuje se na obradu ličnog podatka nosioca podataka u Bosni i Hercegovini koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, ako je aktivnost obrade povezana s:
 - a) nuđenjem roba ili usluga tim nosiocima podataka u Bosni i Hercegovini, nezavisno od toga treba li nosilac podataka izvršiti plaćanje ili
 - b) praćenjem ponašanja nosilaca podataka, uz uslov da se njihovo ponašanje očituje unutar Bosne i Hercegovine.
- (3) Ovaj zakon primjenjuje se na obradu ličnog podatka koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan u Bosni i Hercegovini, već u mjestu gdje se pravo Bosne i Hercegovine primjenjuje na osnovu međunarodnog prava.
- (4) Na obradu ličnog podatka od nadležnog organa u svrhu zaštite fizičkog lica u vezi s obradom ličnog podatka u svrhu sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja učinilaca krivičnih djela, izvršenja krivičnih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, ne primjenjuje se ovaj član.

DIO DRUGI – OBRADA LIČNOG PODATKA OD STRANE FIZIČKOG LICA, PRAVNOG LICA ILI JAVNOG ORGANA KAO KONTROLORA PODATAKA POGLAVLJE I. PRINCIPI OBRADE LIČNOG PODATKA

Član 7.

(Principi obrade ličnog podatka)

- (1) Principi obrade ličnog podatka su:
 - a) zakonitost, pravičnost i transparentnost u odnosu na nosioca podataka;
 - b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju

obrađivati na način koji nije u skladu s tim svrhama. Daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu s članom 56. stav (1) ovog zakona ne smatra se neusklađenom s prvobitnim svrhama;

- c) smanjenje obima podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhe za koje se obrađuju;
 - d) tačnost – podaci moraju biti tačni i prema potrebi ažurirani. Moraju se preduzeti sve razumne mjere kako bi se osiguralo da lični podaci, koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni;
 - e) ograničenje čuvanja – podaci moraju biti čuvani u formi koja omogućava identifikaciju nosioca podataka i to ne duže nego što je potrebno u svrhe u koje se lični podaci obrađuju. Lični podaci mogu se čuvati na duži period ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu s članom 56. stav (1) ovog zakona, što podliježe provođenju primjerenih tehničkih i organizacionih mjera propisanih ovim zakonom radi zaštite prava i sloboda nosioca podataka;
 - f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigurava odgovarajuća sigurnost ličnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera.
- (2) Princip pouzdanosti – kontrolor podataka odgovoran je za usklađenost obrade ličnog podatka sa stavom (1) ovog člana i mora biti u mogućnosti dokazati tu usklađenost.

Član 8.

(Zakonitost obrade ličnog podatka)

- (1) Obrada ličnog podatka je zakonita samo ako je ispunjen najmanje jedan od sljedećih uslova:
 - a) ako je nosilac podataka dao saglasnost za obradu svojih ličnih podataka u jednu ili više posebnih svrha;
 - b) ako je obrada neophodna radi izvršenja ugovora u kojem je nosilac podataka ugovorna strana ili radi preduzimanja radnji na zahtjev nosioca podataka prije zaključenja ugovora;
 - c) ako je obrada neophodna radi poštovanja pravnih obaveza kontrolora podataka;
 - d) ako je obrada neophodna radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica;
 - e) ako je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka;
 - f) ako je obrada neophodna zbog legitimnih interesa kontrolora podataka ili treće strane, osim kada nad tim interesima pretežu interesi ili osnovna prava i slobode nosioca podataka, a koji zahtijevaju zaštitu ličnih podataka, posebno ako je nosilac podataka dijete. Ova tačka se ne primjenjuje na obradu koju rade javni organi pri obavljanju svojih poslova.
- (2) Pravni osnov za obradu ličnog podatka iz stava (1) tač. c) i e) ovog člana utvrđuje se zakonima institucija BiH, entiteta i kantona u skladu s nadležnostima, tako da se preciznije propišu posebni uslovi za obradu te druge mjere za osiguravanje zakonite i pravične obrade, između

ostalog i za druge posebne obrade kako je to predviđeno u Poglavlju V. ovog zakona.

- (3) Posebnim zakonom, za obradu podataka iz stava (1) tač. c) i e) ovog člana institucija BiH, entiteta i kantona u skladu s nadležnostima propisuje se svrha obrade, koja u vezi s obradom iz stava (1) tačke e) ovog člana mora biti neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka. Tim zakonom propisuju se: opći uslovi kojima se uređuje zakonitost obrade koju obavlja kontrolor podataka, vrste podataka koji se obrađuju, kategorije nosilaca podataka, subjekti kojima se lični podaci mogu otkriti i svrhe u koje se podaci mogu otkriti, ograničenje svrhe, rokovi čuvanja te radnje obrade i postupci obrade, uključujući i mjere za osiguranje zakonite i pravične obrade, kao i za druge posebne obrade kako je navedeno u Poglavlju V. ovog zakona. Tim zakonom mora se ostvariti cilj od javnog interesa i obrada mora biti proporcionalna zakonitom cilju kojem se teži.
- (4) Ako se obrada vrši u svrhu koja je različita od svrhe u koju su lični podaci prikupljeni i ne zasniva se na saglasnosti nosilaca podataka ili posebnom zakonu koji predstavlja neophodnu i proporcionalnu mjeru u demokratskom društvu za zaštitu ciljeva iz člana 25. stav (1) ovog zakona, kontrolor podataka, s ciljem utvrđivanja da li je obrada u drugu svrhu u skladu sa svrhom u koju su lični podaci prvobitno prikupljeni, uzima u obzir, između ostalog:
 - a) svaku vezu između svrha u koje su lični podaci prikupljeni i svrha namjeravane daljnje obrade;
 - b) kontekst u kojem su lični podaci prikupljeni, posebno u vezi s odnosom između nosioca podataka i kontrolora podataka;
 - c) prirodu ličnih podataka, posebno činjenicu da li se obrađuju posebne kategorije ličnih podataka u skladu s članom 11. ovog zakona ili lični podaci koji se odnose na krivičnu osuđivanost i krivična djela u skladu s članom 12. ovog zakona;
 - d) moguće posljedice namjeravane daljnje obrade za nosioce podataka;
 - e) postojanje odgovarajućih mjera zaštite, koje mogu uključivati enkripciju ili pseudonimizaciju.
- (5) Javni i nadležni organi entiteta i Brčko Distrikta BiH dužni su, uz poštivanje odredbi ovog zakona, ustupiti lične podatke iz svojih evidencija ovlaštenom kontroloru podataka, u svrhu prethodnog izjašnjavanja građana koji imaju biračko pravo o pitanjima za koje je posebnim propisima omogućeno to pravo.

Član 9. (Saglasnost)

- (1) Kada je obrada zasnovana na saglasnosti, kontrolor podataka mora dokazati da je nosilac podataka dao saglasnost za obradu svojih ličnih podataka.
- (2) Ako nosilac podataka daje saglasnost u pisanoj izjavi koja se odnosi i na druga pitanja, zahtjev za saglasnost mora biti predstavljen tako da se jasno razlikuje od drugih pitanja, u razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika. Dio saglasnosti koji predstavlja kršenje ovog zakona se ne primjenjuje.
- (3) Nosilac podataka ima pravo u bilo kojem trenutku povući svoju saglasnost. Povlačenje saglasnosti ne utiče na zakonitost obrade podataka na osnovu saglasnosti prije njenog povlačenja. Prije davanja saglasnosti nosilac podataka se o tome obavještava. Povlačenje saglasnosti mora biti jednako jednostavno kao i njeno davanje.

- (4) Kada se procjenjuje da li je saglasnost data dobrovoljno, u najvećoj mogućoj mjeri se uzima u obzir da li je, između ostalog, izvršenje ugovora, uključujući i pružanje usluge, uslovljeno saglasnošću za obradu ličnih podataka koja nije neophodna za izvršenje tog ugovora.

Član 10.

(Uslovi koji se primjenjuju na saglasnost djeteta u vezi sa uslugom informacionog društva)

- (1) Kada se primjenjuje član 8. stav (1) tačka a) ovog zakona u vezi s neposrednim nudičenjem usluge informacionog društva djetetu, obrada ličnog podatka djeteta zakonita je ako dijete ima najmanje 16 godina. Ako je dijete mlađe od 16 godina, takva obrada je zakonita samo ako i u mjeri u kojoj je saglasnost dao ili odobrio roditelj, usvojilac, staratelj djeteta ili drugi zastupnik djeteta.
- (2) Kontrolor podataka mora uložiti razumne napore prilikom provjere da li je saglasnost u tim slučajevima dao ili odobrio roditelj, usvojilac, odnosno staratelj djeteta, uzimajući u obzir dostupnu tehnologiju.
- (3) Stav (1) ovog člana ne utiče na opća pravila obligacionog prava koja se tiču važenja, zaključenja ili učinka ugovora u vezi s djetetom.

Član 11.

(Obrada posebnih kategorija ličnih podataka)

- (1) Obrada ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije lica, podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji lica je zabranjena.
- (2) Izuzetno od odredbe stava (1) ovog člana, obrada posebne kategorije ličnih podataka dopuštena je ako je ispunjen jedan od sljedećih uslova:
 - a) ako je nosilac podataka dao izričitu saglasnost za obradu tih ličnih podataka za jednu ili više konkretnih svrha, osim kada je posebnim zakonom propisano da se obrada tih podataka ne može obavljati na osnovu saglasnosti;
 - b) ako je obrada neophodna radi izvršavanja obaveza i ostvarivanja posebnih prava kontrolora podataka ili nosioca podataka u oblasti radnog prava i prava socijalnog osiguranja i socijalne zaštite, u mjeri u kojoj je to propisano zakonom ili kolektivnim ugovorom u skladu s posebnim zakonom kojim se propisuju odgovarajuće mjere zaštite osnovnih prava i interesa nosioca podataka;
 - c) ako je obrada neophodna radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica ako nosilac podataka fizički ili pravno ne može dati saglasnost;
 - d) ako se obrada obavlja u okviru legitimnih aktivnosti, uz odgovarajuće zaštitne mjere, fondacije, udruženja ili bilo koje druge neprofitne organizacije s političkim, filozofskim, vjerskim ili sindikalnim ciljem i to uz uslov da se obrada odnosi isključivo na članove ili bivše članove te organizacije ili na fizička lica koja imaju redovan kontakt s njom, a u vezi s njenim svrhama i da se lični podaci ne otkrivaju van te organizacije bez saglasnosti nosioca podataka;
 - e) ako se obrada odnosi na lične podatke za koje je očito da ih je objavio nosilac podataka;

- f) ako je obrada neophodna za uspostavljanje, ostvarivanje ili odbranu pravnih zahtjeva ili kad sudovi postupaju u sudskom svojstvu;
 - g) ako je obrada neophodna za potrebe značajnog javnog interesa, na osnovu zakona koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu ličnih podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka;
 - h) ako je obrada neophodna za potrebe preventivne medicine ili medicine rada zbog procjene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili socijalne zaštite ili tretmana ili upravljanja sistemima i uslugama zdravstvene ili socijalne zaštite na osnovu posebnog zakona ili u skladu s ugovorom sa zdravstvenim radnikom i uz uslove i mjere zaštite iz stava (3) ovog člana;
 - i) ako je obrada neophodna iz razloga javnog interesa u oblasti javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih prijetnji za zdravlje ili osiguranje visokih standarda kvaliteta i sigurnosti zdravstvene zaštite i lijekova i medicinskih sredstava, na osnovu posebnog zakona kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda nosioca podataka, a posebno čuvanje profesionalne tajne;
 - j) ako je obrada neophodna za potrebe arhiviranja u javnom interesu, potrebe naučnog ili historijskog istraživanja ili statističke potrebe u skladu s članom 56. stav (1) ovog zakona, a na osnovu posebnog zakona, koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka.
- (3) Lični podaci iz stava (1) ovog člana mogu se obrađivati u svrhe navedene u stavu (2) tačka h) ovog člana kada te podatke obrađuje stručno lice ili se podaci obrađuju pod odgovornošću stručnog lica na koje se primjenjuje obaveza čuvanja profesionalne tajne u skladu s posebnim zakonom ili pravilima koja su utvrdili nadležni javni organi ili druga lica na koje se primjenjuje obaveza čuvanja tajne u skladu s posebnim zakonom ili pravilima koja su utvrdili nadležni javni organi.
- (4) Posebnim zakonima mogu se zadržati ili uvesti dodatni uslovi, uključujući i ograničenja u odnosu na obradu genetskih podataka, biometrijskih podataka ili podataka o zdravlju.

Član 12.

(Obrada ličnih podataka koji se odnose na krivičnu osuđivanost i krivična djela)

Obrada ličnih podataka koji se odnose na krivičnu osuđivanost i krivična djela ili povezane mjere sigurnosti na osnovu člana 8. stav (1) ovog zakona može se obavljati samo pod nadzorom javnog organa ili kada je obrada propisana posebnim zakonom kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode nosioca podataka. Registar krivičnih presuda vodi se isključivo pod nadzorom javnog organa.

Član 13.

(Obrada za koju nije potrebna identifikacija)

- (1) Ako kontrolor podataka obrađuje lične podatke za čiju svrhu obrade ne zahtijeva ili više ne zahtijeva identifikiranje nosioca podataka, kontrolor podataka nije dužan čuvati, pribavljati ili obrađivati dodatne informacije radi identifikacije nosioca podataka samo za potrebe poštivanja ovog zakona.

- (2) Ako u slučajevima iz stava (1) ovog člana kontrolor podataka može dokazati da ne može identifikirati nosioca podataka, kontrolor podataka o tome, na odgovarajući način, obavještava nosioca podataka, ako je moguće. U tim slučajevima se ne primjenjuju čl. 17. do 22. ovog zakona, osim u slučaju da nosilac podataka u svrhu ostvarivanja svojih prava iz tih članova pruži dodatne informacije koje omogućavaju njegovu identifikaciju.

POGLAVLJE II. PRAVA NOSIOCA PODATAKA

Član 14.

(Transparentna informacija, komunikacija i način ostvarivanja prava nosioca podataka)

- (1) Kontrolor podataka preduzima odgovarajuće mjere kako bi se nosiocu podataka pružile sve informacije iz čl. 15. i 16. ovog zakona i svi vidovi komunikacije za ostvarivanje prava iz čl. 17. do 24. ovog zakona i člana 36. ovog zakona u vezi s obradom podataka, i to u sažetoj, transparentnoj, razumljivoj i lako dostupnoj formi, uz upotrebu jasnog i jednostavnog jezika, što se posebno odnosi na sve informacije koje su izričito namijenjene djetetu. Informacije se pružaju u pisanoj formi ili na druge načine, uključujući i elektronsku formu kada je primjereno. Ako nosilac podataka zahtijeva, informacije se mogu pružiti usmeno, uz uslov da je identitet nosioca podataka utvrđen drugim sredstvima.
- (2) Kontrolor podataka olakšava ostvarivanje prava nosioca podataka iz čl. 17. do 24. ovog zakona. U slučajevima iz člana 13. stav (1) ovog zakona kontrolor podataka ne smije odbiti da postupi po zahtjevu nosioca podataka za ostvarivanje njegovih prava iz čl. 17. do 24. ovog zakona, osim ako kontrolor podataka dokaže da ne može utvrditi identitet nosioca podataka.
- (3) Kontrolor podataka nosiocu podataka na njegov zahtjev pruža informacije o preduzetim radnjama iz čl. 17. do 24. ovog zakona bez nepotrebnog odgađanja i u svakom slučaju u roku od 30 dana od dana zaprimanja zahtjeva. Taj se rok može, prema potrebi, produžiti za 60 dana, uzimajući u obzir složenost i broj zaprimljenih zahtjeva. Kontrolor podataka obavještava nosioca podataka o svakom takvom produženju u roku od 30 dana od dana zaprimanja zahtjeva, pri čemu navodi razloge za odgađanje. Ako nosilac podataka podnese zahtjev elektronskim putem, informacije se pružaju elektronskim putem ako je to moguće, osim u slučaju kada nosilac podataka zahtijeva drugačije.
- (4) Ako kontrolor podataka ne postupi po zahtjevu nosioca podataka, dužan je bez odgađanja, a najkasnije 30 dana od dana zaprimanja zahtjeva, obavijestiti nosioca podataka o razlozima zbog kojih nije postupio po zahtjevu i o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu i drugim pravnim sredstvima.
- (5) Informacije pružene u skladu s čl. 15. i 16. ovog zakona i sva komunikacija i djelovanja iz čl. 17. do 24. ovog zakona i člana 36. ovog zakona pružaju se bez naknade. Ako su zahtjevi nosioca podataka očito neosnovani ili pretjerani, posebno zbog učestalog ponavljanja, kontrolor podataka može:
- a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnožavanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili postupanja po zahtjevu, ili
 - b) odbiti postupiti po zahtjevu.
- (6) Teret dokazivanja očite neosnovanosti ili pretjeranosti zahtjeva je na kontroloru podataka.

- (7) Ako kontrolor podataka ima opravdane sumnje u vezi s identitetom fizičkog lica koje podnosi zahtjev iz čl. 17. do 23. ovog zakona, on može, ne dovodeći u pitanje član 13. ovog zakona, zatražiti dodatne informacije neophodne za potvrđivanje identiteta nosioca podataka.
- (8) Informacije koje moraju biti pružene nosiocima podataka, u skladu s čl. 15. i 16. ovog zakona, mogu se pružiti u kombinaciji sa standardiziranim simbolima, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio logičan pregled namjeravane obrade. Ako su simboli prikazani elektronski, moraju biti mašinski čitljivi.
- (9) Agencija je ovlaštena da donese propise u svrhu određivanja informacija koje se prikazuju simbolima i postupke za utvrđivanje standardiziranih simbola.

Član 15.

(Informacije koje treba dostaviti ako se lični podatak prikuplja od nosioca podataka)

- (1) Ako se lični podatak prikuplja od nosioca podataka, kontrolor podataka u trenutku prikupljanja ličnog podatka nosiocu podataka pruža sljedeće informacije:
- identitet i kontaktne podatke kontrolora podataka, ako je primjenjivo;
 - kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
 - pravni osnov za obradu, te svrhu obrade ličnog podatka;
 - legitimni interes kontrolora podataka ili trećeg lica, ako je obrada zasnovana na članu 8. stav (1) tačka f) ovog zakona;
 - o primaocu ili kategoriji primaoca ličnih podataka, ako ih ima;
 - činjenicu da kontrolor podataka namjerava prenijeti lične podatke u drugu državu ili međunarodnu organizaciju i postojanju ili nepostojanju odluke Vijeća ministara Bosne i Hercegovine o adekvatnosti, odnosno u slučaju prijenosa iz čl. 48. ili 49. ovog zakona ili člana 51. stav (2) ovog zakona, upućivanje na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove kopije ili mjesto na kojem su stavljene na raspolaganje, ako je primjenjivo.
- (2) Osim informacija iz stava (1) ovog člana, kontrolor podataka u trenutku prikupljanja ličnog podatka pruža nosiocu podataka sljedeće dodatne informacije, ako je to neophodno da bi se osigurala pravična i transparentna obrada:
- o roku u kojem će se lični podatak čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog roka;
 - o pravu da se od kontrolora podataka zatraži pristup ličnom podatku, ispravka ili brisanje ličnog podatka ili ograničenje obrade u vezi s nosiocem podataka ili prava na ulaganje prigovora na obradu takvog podatka te prava na prenosivost podatka;
 - o pravu da se saglasnost povuče u bilo kojem trenutku, bez uticaja na zakonitost obrade koja se zasnivala na saglasnosti prije njenog povlačenja, ako je obrada zasnovana na članu 8. stav (1) tačka a) ovog zakona ili članu 11. stav (2) tačka a) ovog zakona;
 - o pravu na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;
 - informacije o tome da li je davanje ličnog podatka zakonska ili ugovorna obaveza ili neophodan uslov za zaključenje ugovora, kao i ima li nosilac podataka

obavezu dati lični podatak i koje su moguće posljedice ako se takav podatak ne pruži;

- o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz člana 24. st. (1) i (4) ovog zakona, pri čemu je minimalno dužan dati informacije o načinu rada, kao i značaju i predviđenim posljedicama takve obrade za nosioca podataka.
- (3) Ako kontrolor podataka namjerava dodatno obrađivati lične podatke u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade nosiocu podataka pruža informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stava (2) ovog člana.
- (4) Kontrolor podataka nije dužan pružiti informacije nosiocu podataka iz st. (1), (2) i (3) ovog člana u onoj mjeri u kojoj nosilac podataka već raspolaze tim informacijama.

Član 16.

(Informacije koje se pružaju ako lični podatak nije dobiven od nosioca podataka)

- (1) Ako lični podatak nije dobiven od nosioca podataka, kontrolor podataka pruža nosiocu podataka sljedeće informacije:
- o identitetu i kontaktnim podacima kontrolora podataka i predstavnika kontrolora podataka, ako je primjenjivo;
 - o kontaktnim podacima službenika za zaštitu podataka, ako je primjenjivo;
 - o pravnom osnovu za obradu i za svrhe obrade kojih su namijenjeni lični podaci;
 - o kategorijama ličnih podataka koji se obrađuju;
 - o primaocu ili kategorijama primalaca ličnih podataka, prema potrebi;
 - o činjenicama da kontrolor podataka namjerava lične podatke prenijeti primaocu u drugoj državi ili međunarodnoj organizaciji i postojanju ili nepostojanju odluke Vijeća ministara Bosne i Hercegovine o adekvatnosti iz člana 47. stav (3) ovog zakona ili u slučaju prijenosa ličnih podataka iz čl. 48. ili 49. ovog zakona ili člana 51. stav (2) ovog zakona, upućivanje na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove kopije ili mjesta na kojem su stavljene na raspolaganje, ako je primjenjivo.
- (2) Osim informacija iz stava (1) ovog člana, kontrolor podataka pruža nosiocu podataka sljedeće informacije ako je to neophodno da bi se osigurala pravična i transparentna obrada u odnosu na nosioca podataka:
- o roku u kojem će se lični podatak čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog roka;
 - o legitimnim interesima kontrolora podataka ili trećeg lica ako je obrada zasnovana na članu 8. stav (1) tačka f) ovog zakona;
 - o pravu da se od kontrolora podataka zatraži pristup ličnim podacima, ispravka ili brisanje ličnih podataka ili ograničenje obrade u vezi s nosiocem podataka i pravu na prigovor na obradu, kao i pravu na prenosivost podataka;
 - o pravu da se saglasnost povuče u bilo kojem trenutku, bez uticaja na zakonitost obrade zasnovane na saglasnosti prije povlačenja, ako je obrada zasnovana na članu 8. stav (1) tačka a) ovog zakona ili članu 11. stav (2) tačka a) ovog zakona;
 - o pravu na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;

- f) o izvoru ličnih podataka i, prema potrebi, da li dolaze iz javno dostupnih izvora;
- g) o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz člana 24. st. (1) i (4) ovog zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nosioca podataka.
- (3) Kontrolor podataka pruža informacije iz st. (1) i (2) ovog člana:
- a) u razumnom roku nakon dobivanja ličnih podataka, a najkasnije u roku od 30 dana i uzimajući u obzir posebne okolnosti obrade ličnog podatka;
- b) ako se lični podatak koristi za komunikaciju s nosiocem podataka, najkasnije prilikom prve komunikacije ili
- c) ako je predviđeno otkrivanje podataka drugom primaocu, najkasnije u trenutku kada je lični podatak prvi put otkriven.
- (4) Ako kontrolor podataka namjerava dodatno obrađivati lični podatak u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade pruža nosiocu podataka informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stava (2) ovog člana.
- (5) St. (1) do (4) ovog člana ne primjenjuju se ako i u mjeri u kojoj:
- a) nosilac podataka već posjeduje informacije;
- b) pružanje takvih informacija je nemoguće ili bi zahtijevalo neproporcionalne napore, posebno za obradu u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu sa uslovima i mjerama zaštite iz člana 56. stav (1) ovog zakona ili u mjeri u kojoj je vjerovatno da se obavezom iz stava (1) ovog člana može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade. U takvim slučajevima, kontrolor podataka preduzima odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nosioca podataka, između ostalog i stavljanjem informacija na raspolaganje javnosti;
- c) dobivanje ili otkrivanje podataka je izričito propisano posebnim zakonom koji se primjenjuje na nosioca podataka, a kojim se predviđaju odgovarajuće mjere za zaštitu legitimnih interesa nosioca podataka ili
- d) lični podatak mora ostati povjerljiv u skladu s obavezom čuvanja profesionalne tajne koja je propisana posebnim zakonom, uključujući i druge zakonske obaveze čuvanja tajne.
- Član 17.
(Pravo nosioca podataka na pristup ličnom podatku)
- (1) Nosilac podataka ima pravo da dobije potvrdu od kontrolora podataka o tome da li se obrađuju njegovi lični podaci i, ako se obrađuju, pristup ličnim podacima i sljedećim informacijama:
- a) svrsi obrade;
- b) kategoriji ličnog podatka koji se obrađuje;
- c) primaocu ili kategorijama primalaca kojima je lični podatak otkriven ili će im biti otkriven, a posebno primaocu u drugoj državi ili međunarodnoj organizaciji;
- d) predviđenom roku u kojem se lični podaci čuvaju, ili ako to nije moguće, kriterijima korištenim za određivanje tog roka;
- e) pravo da se od kontrolora podataka zatraži ispravka ili brisanje ličnog podatka ili ograničavanje obrade ličnog podatka koji se odnosi na nosioca podataka ili pravo na prigovor na takvu obradu;
- f) pravo na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;
- g) ako se lični podatak ne prikuplja od nosioca podataka, svakoj dostupnoj informaciji o njegovom izvoru;
- h) postojanju automatiziranog donošenja odluka, uključujući i profiliranje iz člana 24. st. (1) i (4) ovog zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nosioca podataka.
- (2) Ako se lični podatak prenosi u drugu državu ili međunarodnu organizaciju, nosilac podataka ima pravo da bude informiran o odgovarajućim mjerama zaštite u skladu s članom 48. ovog zakona koje se odnose na prijenos podataka.
- (3) Kontrolor podataka osigurava kopiju ličnog podatka koji se obrađuje. Za sve dodatne kopije koje zatraži nosilac podataka, kontrolor podataka može naplatiti opravdanu naknadu na osnovu administrativnih troškova. Ako nosilac podataka podnese zahtjev elektronskim putem, osim ako nosilac podataka ne zahtijeva drugačije, informacije se pružaju u uobičajenoj elektronskoj formi.
- (4) Pravo na dobivanje kopije iz stava (3) ovog člana ne smije negativno uticati na prava i slobode drugih.
- Član 18.
(Pravo na ispravku)
- (1) Nosilac podataka ima pravo da mu kontrolor podataka omogući ispravku netačnog ličnog podatka, bez nepotrebnog odgađanja.
- (2) Uzimajući u obzir svrhu obrade, nosilac podataka ima pravo dopuniti nepotpun lični podatak, između ostalog i davanjem dodatne izjave.
- Član 19.
(Pravo na brisanje)
- (1) Nosilac podataka ima pravo da mu kontrolor podataka omogući brisanje ličnog podatka koji se na njega odnosi, a kontrolor podataka ima obavezu obrisati lični podatak, bez nepotrebnog odgađanja, ako je ispunjen jedan od sljedećih uslova:
- a) lični podatak više nije neophodan za svrhe u koje je prikupljen ili na drugi način obrađen;
- b) nosilac podataka povukao je saglasnost na kojoj je obrada zasnovana u skladu s članom 8. stav (1) tačka a) ovog zakona ili članom 11. stav (2) tačka a) ovog zakona i ako ne postoji drugi pravni osnov za obradu;
- c) nosilac podataka uložio je prigovor na obradu u skladu s članom 23. stav (1) ovog zakona i ne postoje zakonski razlozi za obradu ili je nosilac podataka uložio prigovor na obradu u skladu s članom 23. stav (2) ovog zakona;
- d) lični podatak je nezakonito obrađen;
- e) lični podatak mora biti obrisani radi postupanja u skladu sa zakonskom obavezom kojoj podliježe kontrolor podataka;
- f) lični podatak je prikupljen u vezi s ponudom usluga informacionog društva iz člana 10. stav (1) ovog zakona.
- (2) Ako je kontrolor podataka javno objavio lični podatak, a dužan je u skladu sa stavom (1) ovog člana taj lični podatak brisati, uzimajući u obzir dostupnu tehnologiju i troškove provođenja, kontrolor podataka preduzima

razumne mjere, uključujući i tehničke mjere, da bi obavijestio kontrolore podataka koji obrađuju lični podatak da je nosilac podataka zatražio od tih kontrolora podataka da brišu sve poveznice do njega ili kopiju ili rekonstrukciju tog ličnog podatka.

- (3) St. (1) i (2) ovog člana ne primjenjuju se u mjeri u kojoj je obrada neophodna:
- a) radi ostvarivanja prava na slobodu izražavanja i informiranja;
 - b) radi poštivanja zakonske obaveze kojom se zahtijeva obrada propisana posebnim zakonom, a koja se primjenjuje na kontrolora podataka ili radi izvršenja zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja dodijeljenih kontroloru podataka;
 - c) radi javnog interesa u oblasti javnog zdravlja u skladu s članom 11. stav (2) tač. h) i i) ovog člana, kao i članom 11. stav (3) ovog zakona;
 - d) u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe u skladu s članom 56. stav (1) ovog zakona u mjeri u kojoj je vjerovatno da se pravom iz stava (1) ovog člana može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade ili
 - e) radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

Član 20.

(Pravo na ograničenje obrade)

- (1) Nosilac podataka ima pravo na ograničenje obrade podataka ako je ispunjen jedan od sljedećih uslova:
 - a) nosilac podataka osporava tačnost ličnog podatka, u roku u kojem se kontroloru podataka omogućava da provjeri tačnost ličnog podatka;
 - b) obrada je nezakonita, a nosilac podataka se protivi brisanju ličnog podatka i umjesto toga traži ograničenje njegove obrade;
 - c) kontroloru podataka više nije potreban lični podatak za potrebe obrade, ali ga nosilac podataka zahtijeva radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva;
 - d) nosilac podataka uložio je prigovor na obradu u skladu s članom 23. stav (1) ovog zakona i očekuje potvrdu da li njegovi razlozi prevladavaju nad legitimnim razlozima kontrolora podataka.
- (2) Ako je obrada ograničena u skladu sa stavom (1) ovog člana, taj lični podatak smije se obrađivati samo uz saglasnost nosioca podataka, izuzev čuvanja, ili za postavljanje, ostvarivanje ili odbranu pravnih zahtjeva ili zaštitu prava drugog fizičkog ili pravnog lica ili zbog važnog javnog interesa.
- (3) Nosioca podataka koji je ostvario pravo na ograničenje obrade, u skladu sa stavom (1) ovog člana, kontrolor podataka obavještava prije ukidanja ograničenja obrade.

Član 21.

(Obaveza obavještanja o ispravci ili brisanju ličnog podatka ili ograničenju obrade)

- (1) Kontrolor podataka obavještava sve primaocima kojima su lični podaci otkriveni o svakoj ispravci ili brisanju ličnog podatka ili ograničenju obrade izvršenom u skladu s članom 18, članom 19. stav (1) i članom 20. ovog zakona, osim u slučaju kada je to nemoguće ili ako to zahtijeva neproporcionalan napor.
- (2) Kontrolor podataka obavještava nosioca podataka o tim primaocima ako nosilac podataka to zahtijeva.

Član 22.

(Pravo na prenosivost ličnog podatka)

- (1) Nosilac podataka ima pravo preuzeti lični podatak, koji se odnosi na njega a koji je dao kontroloru podataka, u strukturiranom, uobičajeno upotrebljavanom i mašinski čitljivom formatu, te ima pravo prenositi taj podatak drugom kontroloru podataka bez ometanja od kontrolora podataka kojem je lični podatak dat, ako se:
 - a) obrada obavlja u skladu s članom 8. stav (1) tačka a) ovog zakona ili članom 11. stav (2) tačka a) ovog zakona ili na osnovu ugovora u skladu s članom 8. stav (1) tačka b) ovog zakona;
 - b) obrada obavlja automatski.
- (2) Pri ostvarivanju svog prava na prenosivost podatka, u skladu sa stavom (1) ovog člana, nosilac podataka ima pravo na neposredni prijenos od jednog kontrolora podataka drugom kontroloru podataka, ako je to tehnički izvodljivo.
- (3) Ostvarivanjem prava na prenosivost podataka iz stava (1) ovog člana ne dovodi se u pitanje član 19. ovog zakona. To pravo se ne primjenjuje na obradu neophodnu za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru službenih ovlaštenja dodijeljenih kontroloru podataka.
- (4) Pravo na prenosivost podatka iz stava (1) ovog člana ne smije negativno uticati na prava i slobode drugih.

Član 23.

(Pravo na prigovor)

- (1) Nosilac podataka ima pravo na osnovu svoje posebne situacije u svakom trenutku kontroloru podataka podnijeti prigovor na obradu njegovog ličnog podatka, u skladu s članom 8. stav (1) tač. e) ili f) ovog zakona, uključujući profiliranje zasnovano na tim odredbama. Kontrolor podataka ne smije dalje obrađivati lični podatak, osim u slučaju da dokaže da postoje uvjerljivi legitimni razlozi za obradu koji prevladavaju nad interesima, pravima i slobodama nosioca podataka ili radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.
- (2) Ako se lični podatak obrađuje za potrebe direktnog marketinga, nosilac podataka ima pravo u bilo kojem trenutku uložiti prigovor na obradu ličnog podatka koji se odnosi na njega, za potrebe takvog marketinga, što uključuje izradu profila u mjeri u kojoj je povezano s takvim direktnim marketingom.
- (3) Ako se nosilac podataka protivi obradi za potrebe direktnog marketinga, lični podatak više se ne smije obrađivati u te svrhe.
- (4) Najkasnije u trenutku prve komunikacije s nosiocem podataka, nosilac podataka se izričito mora uputiti na prava iz st. (1) i (2) ovog člana te se to mora učiniti na jasan način i odvojeno od bilo koje druge informacije.
- (5) U kontekstu korištenja usluga informacionog društva i ne uzimajući u obzir propise iz oblasti elektronskih komunikacija, nosilac podataka može ostvariti svoje pravo na prigovor automatiziranim putem pomoću tehničkih specifikacija.
- (6) Ako se lični podatak obrađuje u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe na osnovu člana 56. stav (1) ovog zakona, nosilac podataka na osnovu svoje posebne situacije ima pravo uložiti prigovor na obradu ličnog podatka koji se na njega odnosi, osim ako je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu.

Član 24.

(Automatizirano pojedinačno donošenje odluke, uključujući i profiliranje)

- (1) Nosilac podataka ima pravo da se na njega ne primjenjuje odluka zasnovana isključivo na automatiziranoj obradi, uključujući i profiliranje, koja proizvodi pravni učinak koji se na njega odnosi ili na sličan način značajno na njega utiče.
- (2) Stav (1) ovog člana ne primjenjuje se ako je odluka:
 - a) potrebna za zaključivanje ili izvršenje ugovora između nosioca podataka i kontrolora podataka;
 - b) dopuštena zakonom koji se primjenjuje na kontrolora podataka i kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode te legitimne interese nosioca podataka ili
 - c) zasnovana na izričitoj saglasnosti nosioca podataka.
- (3) U slučajevima iz stava (2) tač. a) i c) ovog člana, kontrolor podataka preduzima odgovarajuće mjere za zaštitu prava i sloboda te legitimnih interesa nosioca podataka, najmanje prava na učešće fizičkog lica u donošenju odluke, prava izražavanja vlastitog stava i prava na osporavanje odluke.
- (4) Odluka iz stava (2) ovog člana ne smije biti zasnovana na posebnim kategorijama ličnih podataka iz člana 11. stav (1) ovog zakona, osim ako se primjenjuje član 11. stav (2) tač. a) ili g) ovog zakona te ako su uspostavljene odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nosioca podataka.

Član 25.

(Ograničenja)

- (1) Na osnovu posebnog zakona koji se primjenjuje na kontrolora podataka i obrađivača, može se ograničiti obim prava i obaveza iz člana 7, čl. 14. do 24. ovog zakona i člana 36. ovog zakona, ako odredbe tog zakona odgovaraju pravima i obavezama propisanim u čl. 14. do 24. ovog zakona, ako se takvim ograničenjem poštuje suština osnovnih prava i sloboda i ako ono predstavlja neophodnu i proporcionalnu mjeru u demokratskom društvu za zaštitu:
 - a) državne sigurnosti;
 - b) odbrane;
 - c) javne sigurnosti;
 - d) sprečavanja, istrage, otkrivanja ili gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
 - e) drugih važnih ciljeva od općeg javnog interesa u Bosni i Hercegovini, a posebno važnog privrednog ili finansijskog interesa, što uključuje monetarnu, budžetsku i poresku pitanja, javno zdravstvo i socijalnu zaštitu;
 - f) nezavisnosti pravosuđa i sudskih postupaka;
 - g) sprečavanja, istrage, otkrivanja i gonjenja povrede etike u zakonski reguliranim profesijama;
 - h) nadzorne, inspeksijske ili regulatorne funkcije koja je, najmanje povremeno, povezana sa izvršavanjem službenih ovlaštenja u slučajevima iz tač. a) do e) i tačke g) ovog stava;
 - i) nosioca podataka ili prava i sloboda drugih;
 - j) ostvarivanja potraživanja u građanskim sporovima.
- (2) Posebni zakon iz stava (1) ovog člana sadrži, po potrebi, posebne odredbe, koje sadrže najmanje sljedeće:
 - a) svrhu obrade ili kategoriju obrade;
 - b) kategoriju ličnog podatka;
 - c) obim uvedenih ograničenja;

- d) mjere zaštite za sprečavanje zloupotrebe ili nezakonitog pristupa ili prijenosa;
- e) određivanje kontrolora podataka ili kategoriju kontrolora podataka;
- f) rok čuvanja i mjere zaštite koje se mogu primijeniti uzimajući u obzir prirodu, obim i svrhe obrade ili kategorije obrade;
- g) rizik za prava i slobode nosioca podataka;
- h) pravo nosioca podataka da bude obaviješten o ograničenju, osim ako to može biti štetno za svrhu tog ograničenja.

POGLAVLJE III. KONTROLOR PODATAKA I OBRADIVAČ

Član 26.

(Obaveza kontrolora podataka)

- (1) Kontrolor podataka dužan je primijeniti odgovarajuće tehničke i organizacione mjere imajući u vidu prirodu, obim, okolnosti i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica, kako bi osigurao da se obrada obavlja u skladu s ovim zakonom i kako bi to mogao dokazati. Te mjere se prema potrebi preispituju i ažuriraju.
- (2) Mjere iz stava (1) ovog člana, ako su proporcionalne u odnosu na aktivnosti obrade, uključuju provođenje odgovarajućih politika zaštite podataka od kontrolora podataka.
- (3) Poštivanje odobrenih kodeksa ponašanja iz člana 42. ovog zakona ili odobrenih mehanizama certifikacije iz člana 44. ovog zakona može služiti kao elemenat za dokazivanje usklađenosti s obavezama kontrolora podataka.

Član 27.

(Tehnička i integrirana zaštita podataka)

- (1) Uzimajući u obzir najnovija dostignuća, troškove provođenja i prirodu, obim, kontekst i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica koji proizlaze iz obrade podataka, kontrolor podataka, prilikom određivanja sredstava obrade i pri samoj obradi, primjenjuje odgovarajuće tehničke i organizacione mjere, poput pseudonimizacije, za omogućavanje djelotvorne primjene principa zaštite podataka, kao što je smanjenje količine podataka te uključivanje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ovog zakona i zaštitila prava nosioca podataka.
- (2) Kontrolor podataka primjenjuje odgovarajuće tehničke i organizacione mjere kojima se osigurava da integriranim načinom budu obrađeni samo lični podaci koji su neophodni za svaku posebnu svrhu obrade. Ta obaveza primjenjuje se na sve prikupljene lične podatke, obim njihove obrade, rok njihovog čuvanja i njihovu dostupnost. Tim mjerama osigurava se da lični podaci nisu automatski, bez intervencije fizičkog lica, dostupni neograničenom broju drugih fizičkih lica.
- (3) Odobreni mehanizam certifikacije iz člana 44. ovog zakona može služiti kao elemenat za dokazivanje usklađenosti sa zahtjevima iz st. (1) i (2) ovog člana.

Član 28.

(Zajednički kontrolori podataka)

- (1) Ako dva ili više kontrolora podataka zajednički odrede svrhe i načine obrade, smatraju se zajedničkim kontrolorima podataka. Oni na transparentan način, međusobnim sporazumom, određuju odgovornosti svakoga od njih s ciljem izvršavanja obaveza iz ovog zakona, posebno u vezi sa ostvarivanjem prava nosioca podataka i dužnostima svakoga od njih u vezi s pružanjem informacija iz čl. 15. i 16. ovog zakona, osim u slučaju da

su odgovornosti svakog od kontrolora podataka utvrđene zakonom koji se primjenjuje na kontrolore podataka. Sporazumom se može odrediti kontakt-tačka za nosioca podataka.

- (2) Sporazum iz stava (1) ovog člana mora na odgovarajući način odražavati pojedinačne uloge i odnose zajedničkih kontrolora podataka u odnosu na nosioce podataka. Suština sporazuma mora biti dostupna nosiocu podataka.
- (3) Nezavisno od uslova sporazuma iz stava (1) ovog člana, nosilac podataka može ostvarivati svoja prava iz ovog zakona u vezi sa svakim kontrolorom podataka i protiv svakog od njih.

Član 29.

(Predstavnik kontrolora podataka ili obrađivača koji nema sjedište ili poslovni nastan u Bosni i Hercegovini)

- (1) Ako se primjenjuje član 6. stav (2) ovog zakona, kontrolor podataka ili obrađivač ima obavezu pisanim putem imenovati svog predstavnika u Bosni i Hercegovini.
- (2) Obaveza iz stava (1) ovog člana ne primjenjuje se na:
 - a) obradu koja je povremena, ne podrazumijeva u većoj mjeri obradu posebnih kategorija podataka iz člana 11. stav (1) ovog zakona ili obradu ličnih podataka koji se odnose na krivičnu osuđivanost i krivična djela iz člana 12. ovog zakona i za koju nije vjerovatno da će uzrokovati rizik za prava i slobode fizičkih lica, uzimajući u obzir prirodu, okolnosti, obim i svrhe obrade ili
 - b) javne organe.
- (3) Kontrolor podataka ili obrađivač ovlašćuje predstavnika kako bi se, uz obraćanje kontroloru podataka ili obrađivaču ili umjesto obraćanja njima, njemu obraćali posebno Agencija i nosilac podataka u vezi sa svim pitanjima koja se odnose na obradu ličnog podatka radi osiguranja usklađenosti obrade ličnog podatka s ovim zakonom.
- (4) Imenovanje predstavnika kontrolora podataka ili obrađivača ne utiče na pravne zahtjeve koji mogu biti usmjereni protiv samog kontrolora podataka ili obrađivača.

Član 30.

(Обрађивач)

- (1) Ako se obrada ličnog podatka obavlja u ime kontrolora podataka, kontrolor podataka koristi isključivo obrađivača koji u dovoljnoj mjeri garantira primjenu odgovarajućih tehničkih i organizacionih mjera tako da obrada bude u skladu sa zahtjevima iz ovog zakona i da se obradom osigurava zaštita prava nosioca podataka.
- (2) Обрађивач не смеје ангажирати другог обрађивача без претходног посебног или опћег писаног одобрења контролора података. У случају опћег писаног одобрења, обрађивач обавјештава контролора података о свим планираним измјенaма у вези с додaвањем или зaмјеном других обрађивача како би тиме контролору података омогућио да уложи приговор на те измјене.
- (3) Обрада коју обавља обрађивач уређује се уговором или другим правним актом у складу са законом који обавезује обрађивача према контролору података, у којем се наводе предмет и трајање обраде, природа и сврха обраде, врста лиčnih података и категорија носioca података, као и обавезе и права контролора података.
- (4) Уговором или другим правним актом из става (3) овог члана прописује се да је обрађивач дужан да:
 - a) обрађује лични податак само према документираним упутствима контролора података, између осталог и у вези с пријеносом личног податка у другу државу или

међународну организацију, осим ако је то прописано посебним законом који се примјенује на обрађивача, а у том случају обрађивач обавјештава контролора података о том правном заhtјеву прије обраде, осим ако се тим законом забрањује такво обавјештавање због важних разлога од јавног интереса;

- b) осигурава да су се лица овлашћена за обраду личног податка обавезала на поштовање повjerљивости или да их на поштовање повjerљивости обавезује одговарајући закон;
 - c) предузима све потребне мјере у складу с чланом 34. овог закона;
 - d) поштује услове из ст. (2) и (5) овог члана за ангажирање другог обрађивача;
 - e) узимајући у обзир природу обраде, помаже контролору података путем одговарајућих техничких и организационих мјера, колико је то могуће, да испуни обавезу контролора података да одговори на заhtјеве за остваривање права носioca података из Поглавља II. овог закона;
 - f) помаже контролору података у осигуравању усклађености с обавезама из чл. 34. до 38. овог закона, узимајући у обзир природу обраде и информације које су доступне обрађивачу;
 - g) по избору контролора података, брише или враћа контролору података све личне податке након завршетка пружања услуга у вези с обрадом и брише постојеће копије, осим у случају да је посебним законом прописана обавеза чувања личних података;
 - h) контролору података ставља на располагање све информације које су неопходне за доказивање поштовања обавеза из овог члана и контролору података или другом ревизору којег је овластио контролор података омогућава обављање ревизије, укључујући и инспекције, и помаже у njihovom обављању;
 - i) у случају из тачке h) овог става обрађивач одмах обавјештава контролора података ако се, према njegovom мишљењу, одређеним упутством крши овај закон или друга правила о заштити података.
- (5) Ако обрађивач ангажира другог обрађивача за обављање посебних активности обраде у име контролора података, исте обавезе за заштиту података као оне које су наведене у уговору или другом правном акту између контролора података и обрађивача из става (4) овог члана намећу се том другом обрађивачу уговором или другим правним актом у складу с посебним законом, а посебно обавеза давања довољно гаранција за примјenu одговарајућих техничких и организационих мјера на начин којим се осигурава да обрада задовољава заhtјеве из овог закона. Ако тај други обрађивач не испуњава обавезе заштите података, први обрађивач остаје у потпуности одговоран контролору података за извршавање обавеза тог другог обрађивача.
 - (6) Поштовање одобрених кодекса понашања од обрађивача, из члана 42. овог закона, или одобреног механизма сертификације, из члана 44. овог закона, може служити као елемент за доказивање пружања довољно гаранција из ст. (1) и (5) овог члана.
 - (7) Не доводећи у питање појединачни уговор између контролора података и обрађивача, уговор или други правни акт из ст. (3), (4) и (5) овог члана може се у cjелини или djelimično заснивати на standardnim уговорним клаузулама из ст. (8) и (9) овог члана, укључујући између

- ostalog i klauzule koje su dio certifikata dodijeljenog kontroloru podataka ili obrađivaču u skladu s čl. 44. i 45. ovog zakona.
- (8) Agencija može donijeti standardne ugovorne klauzule za pitanja iz st. (3), (4) i (5) ovog člana s ciljem dosljedne primjene ovog zakona.
- (9) Ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog člana mora biti u pisanoj formi, što uključuje i elektronsku formu.
- (10) Ne dovodeći u pitanje čl. 112, 113, 114. i 115. ovog zakona, ako obrađivač krši ovaj zakon time što određuje svrhu i načine obrade podataka, obrađivač se smatra kontrolorom podataka u vezi s tom obradom.

Član 31.

(Obrada ličnog podatka pod kontrolom kontrolora podataka ili obrađivača)

Obrađivač i lice koje radi pod kontrolom kontrolora podataka ili obrađivača, a ima pristup ličnom podatku, ne smije obrađivati taj podatak bez naloga kontrolora podataka, osim kada je to propisano posebnim zakonom.

Član 32.

(Evidencija o obradi ličnog podatka)

- (1) Svaki kontrolor podataka i predstavnik kontrolora podataka, ako je primjenjivo, vodi evidenciju aktivnosti obrade za koje je odgovoran. Evidencija sadrži sljedeće informacije:
- ime i kontakt-podatke kontrolora podataka i, ako je primjenjivo, zajedničkog kontrolora podataka, predstavnika kontrolora podataka i službenika za zaštitu podataka;
 - svrhe obrade;
 - opis kategorija nosilaca podataka i kategorija ličnih podataka;
 - kategorije primalaca kojima su lični podaci otkriveni ili će im biti otkriveni, uključujući i primaocce u drugim državama ili međunarodnim organizacijama;
 - ako je primjenjivo, o prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, uključujući identifikaciju druge države ili međunarodne organizacije i, u slučaju prijenosa iz člana 51. stav (2) ovog zakona, dokumentaciju o odgovarajućim zaštitnim mjerama;
 - ako je moguće, predviđene rokove za brisanje različitih kategorija podataka;
 - ako je moguće, opći opis tehničkih i organizacionih sigurnosnih mjera iz člana 34. stav (1) ovog zakona.
- (2) Svaki obrađivač i predstavnik obrađivača, ako je primjenjivo, vodi evidenciju o svim aktivnostima obrade koje se obavljaju u ime kontrolora podataka, koja sadrži:
- ime i kontaktne podatke jednog ili više obrađivača i svakog kontrolora podataka u čije ime obrađivač djeluje te ako je primjenjivo, predstavnika kontrolora podataka ili obrađivača kao i službenika za zaštitu podataka;
 - vrste obrade koje se vrše u ime svakog kontrolora podataka;
 - ako je primjenjivo, informacije o prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, s identifikacijom te druge države ili međunarodne organizacije i u slučaju prijenosa iz člana 51. stav (2) ovog zakona, dokumentaciju o odgovarajućim zaštitnim mjerama;
 - ako je moguće, opći opis tehničkih i organizacionih sigurnosnih mjera iz člana 34. stav (1) ovog zakona.

- (3) Evidencija iz st. (1) i (2) ovog člana mora biti u pisanoj formi, što uključuje i elektronsku formu.
- (4) Kontrolor podataka ili obrađivač te predstavnik kontrolora podataka ili obrađivača, ako je primjenjivo, na zahtjev Agencije omogućavaju uvid u evidenciju.
- (5) Obaveze iz st. (1) i (2) ovog člana ne primjenjuju se na privredni subjekat ili organizaciju u kojoj je zaposleno manje od 250 lica, osim kada postoji vjerovatnoća da će obrada koju obavlja predstavljati visok rizik za prava i slobode nosioca podataka, ako obrada nije povremena ili ako obrada obuhvata posebne kategorije podataka iz člana 11. stav (1) ovog zakona, ili su u pitanju lični podaci koji se odnose na krivičnu osuđivanost i krivična djela.

Član 33.

(Saradnja s Agencijom)

Kontrolor podataka i obrađivač, te ako su određeni njihovi predstavnici, dužni su, na obrazložen i na osnovu zakona opravdan zahtjev, sarađivati s Agencijom u obavljanju njenih zadataka.

Član 34.

(Sigurnost obrade ličnog podatka)

- (1) Uzimajući u obzir najnovija dostignuća, troškove provođenja i prirodu, obim, kontekst i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica, provodeći postupak iz člana 37. ovog zakona, kontrolor podataka i obrađivač primjenjuju odgovarajuće tehničke i organizacione mjere kako bi postigli odgovarajući nivo sigurnosti s obzirom na rizik, što prema potrebi podrazumijeva:
- pseudonimizaciju i enkripciju ličnog podatka;
 - mogućnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sistema i usluga obrade;
 - sposobnost pravovremenog ponovnog uspostavljanja dostupnosti ličnog podatka i pristupa njemu u slučaju fizičkog ili tehničkog incidenta;
 - postupak redovnog testiranja, ocjenjivanja i procjene djelotvornosti tehničkih i organizacionih mjera za postizanje sigurnosti obrade.
- (2) Pri procjeni odgovarajućeg nivoa sigurnosti, u obzir se uzimaju prije svega rizici koje predstavlja obrada, a posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ličnog podatka ili neovlaštenog pristupa ličnom podatku koji je prenesen, čuvan ili na drugi način obrađivan.
- (3) Primjena odobrenog kodeksa ponašanja iz člana 42. ovog zakona ili odobrenog mehanizma certifikacije iz člana 44. ovog zakona može se koristiti kao elemenat za dokazivanje usklađenosti sa zahtjevima iz stava (1) ovog člana.
- (4) Kontrolor podataka i obrađivač preduzimaju mjere kako bi osigurali da svako fizičko lice koje djeluje pod nadležnošću kontrolora podataka ili obrađivača, a koje ima pristup ličnom podatku, ne obrađuje taj podatak ako to nije prema uputstvima kontrolora podataka, osim u slučajevima kada je to propisano posebnim zakonom.

Član 35.

(Izvršavanje Agencije o povredi ličnog podatka)

- (1) Kontrolor podataka dužan je o povredi ličnog podatka bez nepotrebnog odgađanja i, ako je moguće, a najkasnije u roku od 72 sata nakon saznanja za tu povredu, obavijestiti Agenciju o povredi ličnog podatka, osim u slučaju ako je vjerovatno da ta povreda neće ugroziti prava i slobode fizičkog lica. Ako izvršavanje nije izvršeno u roku od 72

- sata, kontrolor podataka dužan je Agenciji navesti razloge za kašnjenje.
- (2) Obradivač je dužan, po saznanju za povredu ličnog podatka, bez nepotrebnog odgađanja o tome obavijestiti kontrolora podataka.
- (3) Izvještaj iz stava (1) ovog člana sadrži najmanje sljedeće:
- opis prirode povrede ličnih podataka, i ako je moguće, s navedenim kategorijama i približnim brojem nosilaca podataka, kao i kategorijama i približnim brojem evidencija ličnih podataka;
 - ime i prezime te kontakt-podatke službenika za zaštitu podataka ili druge kontaktne tačke od koje se može dobiti još informacija;
 - opis moguće posljedice povrede ličnog podatka;
 - opis mjera koje je kontrolor podataka preduzeo ili čije je preduzimanje predložio radi rješavanja problema povrede ličnog podatka, uključujući prema potrebi i mjere za ublažavanje njenih mogućih štetnih posljedica.
- (4) Ako i u mjeri u kojoj ih nije moguće istovremeno dostaviti, informacije se mogu dostavljati u dijelovima, bez nepotrebnog daljnjeg odgađanja.
- (5) Kontrolor podataka dokumentira svaku povredu ličnog podatka, uključujući i činjenice u vezi s povredom ličnog podatka, njene posljedice i mjere preduzete za otklanjanje štete. Dokumentacija iz ovog stava omogućava Agenciji postupanje po ovom članu.

Član 36.

(Obavješćavanje nosioca podataka o povredi ličnog podatka)

- (1) Kontrolor podataka dužan je bez odgađanja pisanim putem obavijestiti nosioca podataka o povredi ličnog podatka, ako je vjerovatno da će povreda ličnog podatka uzrokovati visok rizik za prava i slobode fizičkog lica.
- (2) Kontrolor podataka u obavještenju iz stava (1) ovog člana, jasnim i jednostavnim jezikom, opisuje prirodu povrede ličnog podatka te se najmanje navode informacije i mjere iz člana 35. stav (3) tač. b), c) i d) ovog zakona.
- (3) Obavješćavanje nosioca podataka iz stava (1) ovog člana nije obavezno ako je ispunjen jedan od sljedećih uslova:
- ako je kontrolor podataka preduzeo odgovarajuće tehničke i organizacione zaštitne mjere i te mjere su primijenjene na lični podatak u vezi s kojim je došlo do povrede ličnog podatka, a prije svega mjere koje lični podatak čine nerazumljivim licu koje nije ovlašteno da mu pristupi, kao što je enkripcija;
 - ako je kontrolor podataka preduzeo naknadne mjere kojima se osigurava da više nije moguće da će doći do visokog rizika za prava i slobode nosioca podataka iz stava (1) ovog člana;
 - ako bi to zahtijevalo neproporcionalan napor, mora se objaviti javno saopćenje ili se preduzima slična mjera kojom se nosioci podataka obavješćavaju na jednako djelotvoran način.
- (4) Ako kontrolor podataka nije obavijestio nosioca podataka o povredi ličnog podatka, Agencija, nakon razmatranja stepena vjerovatnoće da će povreda ličnog podatka uzrokovati visok rizik za prava i slobode fizičkih lica, može od kontrolora podataka zahtijevati da to učini, ako nije ispunjen neki od uslova iz stava (3) ovog člana.

Član 37.

(Procjena uticaja obrade na zaštitu ličnog podatka)

- (1) Ako je vjerovatno da će neka vrsta obrade, posebno posredstvom novih tehnologija i uzimajući u obzir prirodu, obim, kontekst i svrhe obrade, uzrokovati visok rizik za prava i slobode fizičkih lica, kontrolor podataka

prije obrade provodi procjenu uticaja predviđenih obrada na zaštitu ličnog podatka.

- (2) Pri provođenju procjene uticaja obrade na zaštitu ličnog podatka, kontrolor podataka traži savjet od službenika za zaštitu ličnih podataka, ako je imenovan.
- (3) Procjena uticaja obrade na zaštitu ličnog podatka iz stava (1) ovog člana obavezna je posebno u slučaju:
- sistemске i obimne procjene ličnih aspekata u vezi s fizičkim licima koja se zasniva na automatiziranoj obradi, uključujući profiliranje, i koja je osnov za donošenje odluka koje proizvode pravni učinak u odnosu na fizičko lice ili na sličan način značajno utiču na fizičko lice;
 - obimne obrade posebnih kategorija ličnih podataka iz člana 11. stav (1) ovog zakona ili podataka koji se odnose na krivičnu osuđivanost i krivična djela iz člana 12. ovog zakona ili
 - sistemskog praćenja javno dostupnog područja u velikoj mjeri.
- (4) Agencija utvrđuje i javno objavljuje listu vrsta postupaka obrade na koje se primjenjuje obaveza obavljanja procjene uticaja na zaštitu ličnih podataka, u skladu sa stavom (1) ovog člana.
- (5) Agencija može da utvrdi i javno objavi listu vrsta postupaka obrade za koje nije potrebna procjena uticaja na zaštitu ličnog podatka.
- (6) Procjena uticaja obuhvata najmanje:
- sistemski opis predviđenih obrada i svrha obrade, uključujući, ako je primjenjivo, legitiman interes kontrolora podataka;
 - procjenu nužnosti i proporcionalnosti obrada povezanih s njihovim svrhama;
 - procjenu rizika za prava i slobode nosioca podataka;
 - predviđene mjere za rješavanje rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguranje zaštite ličnih podataka i dokazivanje usklađenosti s ovim zakonom, uzimajući u obzir prava i legitime interese nosioca podataka i drugih uključenih lica.
- (7) Usklađenost kodeksa ponašanja iz člana 42. ovog zakona odobrenih od kontrolora podataka ili obradivača uzima se u obzir prilikom procjene uticaja obrade koje primjenjuju ti kontrolori podataka ili obradivači, posebno u svrhe procjene uticaja na zaštitu ličnih podataka.
- (8) Kontrolor podataka, prema potrebi, od nosioca podataka ili njegovog predstavnika traži mišljenje o namjeravanoj obradi, ne dovodeći u pitanje komercijalne ili javne interese ili sigurnost postupka obrade.
- (9) Ako obrada u skladu s članom 8. stav (1) tač. c) ili e) ovog zakona ima pravni osnov u posebnom zakonu koji se primjenjuje na kontrolora podataka, ako su tim zakonom uređene posebne obrade ili skup predmetnih radnji i ako je procjena uticaja na zaštitu ličnih podataka već provedena kao dio opće procjene uticaja u kontekstu donošenja pravnog osnova, st. (1) do (6) ovog člana se ne primjenjuju, osim ako je posebnim propisom utvrđeno da je potrebno provesti takvu procjenu prije obrade.
- (10) Kontrolor podataka, prema potrebi, preispituje da li je obrada izvršena u skladu s procjenom uticaja na zaštitu ličnih podataka, i to najmanje kada dođe do promjene u nivou rizika koji predstavljaju postupci obrade.

Član 38.

(Prethodno savjetovanje kontrolora podataka s Agencijom)

- (1) Kontrolor obrade savjetuje se s Agencijom prije obrade ako je procjena uticaja na zaštitu ličnih podataka iz člana 37. ovog zakona pokazala da bi obrada podataka

- uzrokovala visok rizik za prava i slobode pojedinaca, u slučaju da kontrolor podataka ne donese mjere za ublažavanje rizika.
- (2) Ako Agencija utvrdi da bi se namjeravanom obradom iz stava (1) ovog člana kršio ovaj zakon, posebno ako kontrolor podataka nije u dovoljnoj mjeri utvrdio ili umanjio rizik za prava i slobode pojedinaca, Agencija u roku od najduže 56 dana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje kontrolora podataka, a prema potrebi i obrađivača, i pritom može koristiti ovlaštenja iz člana 103. ovog zakona.
- (3) Rok iz stava (2) ovog člana, po potrebi, može se produžiti za 42 dana, u zavisnosti od složenosti namjeravane obrade.
- (4) Agencija, u roku od 30 dana od zaprimanja zahtjeva, obavještava kontrolora podataka, a prema potrebi i obrađivača, o produženju roka iz stava (3) ovog člana i o razlozima odgađanja.
- (5) Proticanje rokova iz st. (2) i (3) ovog člana može biti privremeno obustavljeno dok Agencija ne dobije informacije koje je zahtijevala za potrebe savjetovanja.
- (6) Pri savjetovanju kontrolor podataka Agenciji dostavlja:
- a) ako je primjenjivo, odgovarajuće odgovornosti kontrolora podataka, zajedničkih kontrolora podataka i obrađivača koji učestvuju u obradi, posebno u slučaju obrade unutar grupe privrednih subjekata;
 - b) svrhu i sredstva namjeravane obrade;
 - c) zaštitne mjere i druge mjere za zaštitu prava i sloboda nosioca podataka na osnovu ovog zakona;
 - d) kontakt-podatke službenika za zaštitu podataka, ako je primjenjivo;
 - e) procjenu uticaja na zaštitu podataka kako je propisano članom 37. ovog zakona;
 - f) sve druge informacije koje Agencija zatraži.
- (7) O prijedlogu zakona kojim se regulira obrada ličnih podataka, prije njegovog upućivanja u parlamentarnu proceduru, predlaže se može prethodno savjetovati s Agencijom.
- (8) Nezavisno od stava (1) ovog člana, posebnim zakonom može se propisati obaveza kontroloru podataka da se savjetuje s Agencijom i da od nje pribavi prethodno odobrenje u vezi s obradom koju obavlja za izvršenje zadataka u javnom interesu, uključujući i obradu u vezi sa socijalnom i zdravstvenom zaštitom.
- Član 39.
- (Imenovanje službenika za zaštitu ličnih podataka)
- (1) Kontrolor podataka i obrađivač dužni su imenovati službenika za zaštitu ličnih podataka u slučajevima:
- a) ako obradu vrši javni organ, osim sudova koji postupaju u okviru sudske nadležnosti;
 - b) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od postupaka obrade koje zbog svoje prirode, obima i/ili svrhe zahtijevaju redovno i sistemsko praćenje nosioca podataka u velikom broju ili
 - c) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od opsežne obrade posebnih kategorija podataka na osnovu člana 11. ovog zakona i ličnih podataka u vezi s krivičnom osuđivanosti i krivičnim djelima iz člana 12. ovog zakona.
- (2) Grupa privrednih subjekata može imenovati jednog službenika za zaštitu ličnih podataka uz uslov da je službenik za zaštitu ličnih podataka lako dostupan iz svakog sjedišta ili poslovnog nastana.
- (3) Ako je kontrolor podataka ili obrađivač javni organ, za više takvih organa može se imenovati jedan službenik za zaštitu ličnih podataka, uzimajući u obzir njihovu organizacionu strukturu i veličinu.
- (4) U slučajevima koji nisu navedeni u stavu (1) ovog člana, kontrolor podataka ili obrađivač ili udruženje i drugi organ koji predstavlja kategoriju kontrolora podataka ili obrađivača mogu, odnosno u slučajevima kada je to propisano posebnim zakonom moraju imenovati službenika za zaštitu ličnih podataka. Službenik za zaštitu ličnih podataka može obavljati poslove u ime tih udruženja i drugih organa koji predstavljaju kontrolore podataka ili obrađivače.
- (5) Službenik za zaštitu ličnih podataka imenuje se na osnovu njegovih stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksi u oblasti zaštite ličnih podataka i sposobnosti obavljanja zadataka iz člana 41. ovog zakona.
- (6) Službenik za zaštitu ličnih podataka može biti zaposlen kod kontrolora podataka ili obrađivača ili može obavljati poslove na osnovu ugovora o djelu.
- (7) Kontrolor podataka ili obrađivač objavljuje kontakt-podatke službenika za zaštitu ličnih podataka i dostavlja ih Agenciji.
- Član 40.
- (Status službenika za zaštitu ličnih podataka)
- (1) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu ličnih podataka bude na odgovarajući način i blagovremeno uključen u sva pitanja koja se tiču zaštite ličnih podataka.
- (2) Kontrolor podataka i obrađivač podržavaju službenika za zaštitu ličnih podataka u izvršavanju zadataka iz člana 41. ovog zakona, pružajući mu potrebna sredstva za izvršavanje tih zadataka i ostvarivanje pristupa ličnim podacima i postupcima obrade, kao i za održavanje njegovog stručnog znanja.
- (3) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu ličnih podataka ne prima nikakve instrukcije pri obavljanju tih zadataka. Kontrolor podataka ili obrađivač ne može ga razriješiti dužnosti ili kazniti zbog toga što obavlja svoje zadatke. Službenik za zaštitu ličnih podataka odgovara neposredno najvišem nivou rukovodstva kontrolora podataka ili obrađivača.
- (4) Nosilac podataka može se obratiti službeniku za zaštitu ličnih podataka za sva pitanja koja se tiču obrade njegovih ličnih podataka i ostvarivanja njegovih prava iz ovog zakona.
- (5) Službenik za zaštitu ličnih podataka, u vezi s obavljanjem svojih zadataka, dužan je sve podatke do kojih dođe u postupku obrade podataka čuvati kao službenu tajnu u skladu sa zakonom.
- (6) Službenik za zaštitu ličnih podataka može obavljati i druge zadatke i dužnosti. Kontrolor podataka ili obrađivač osigurava da ti zadaci i dužnosti ne dovedu do sukoba interesa.
- Član 41.
- (Zadatak službenika za zaštitu ličnih podataka)
- (1) Službenik za zaštitu ličnih podataka obavlja sljedeće zadatke:
- a) informiranje i savjetovanje kontrolora podataka ili obrađivača i zaposlenih koji obavljaju obradu o njihovim obavezama iz ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka;
 - b) praćenje poštivanja ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka, kao i politika kontrolora podataka ili obrađivača u vezi sa

- zaštitom ličnih podataka, uključujući i podjelu odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji učestvuju u radnjama obrade, kao i s tim povezanim revizijama;
- c) pružanje savjeta, kada je to zatraženo, u vezi s procjenom uticaja na zaštitu ličnih podataka i praćenje njenog izvršavanja u skladu s članom 37. ovog zakona;
- d) saradnja s Agencijom;
- e) djelovanje kao kontakt-tačka za Agenciju o pitanjima koja se tiču obrade, što uključuje i prethodno savjetovanje iz člana 38. ovog zakona, te savjetovanje, po potrebi, o svim drugim pitanjima.
- (2) Službenik za zaštitu ličnih podataka prilikom obavljanja svojih zadataka vodi računa o riziku povezanim s radnom obradom i uzima u obzir prirodu, obim, kontekst i svrhe obrade.

Član 42.

(Kodeks ponašanja)

- (1) Agencija izdaje preporuku za izradu kodeksa ponašanja s ciljem pravilne primjene ovog zakona, uzimajući u obzir specifičnost različitih sektora obrade i posebne potrebe mikro, malih i srednjih privrednih subjekata.
- (2) Udruženje i drugi subjekat koji predstavlja kategorije kontrolora podataka ili obrađivača mogu izraditi kodekse ponašanja, odnosno izmijeniti i proširiti takve kodekse ponašanja, radi preciziranja primjene ovog zakona, koji se odnose na:
- a) pravičnu i transparentnu obradu;
 - b) legitimne interese kontrolora podataka u posebnim kontekstima;
 - c) prikupljanje ličnih podataka;
 - d) pseudonimizaciju ličnih podataka;
 - e) informiranost javnosti i nosioca podataka;
 - f) ostvarivanje prava nosioca podataka;
 - g) informiranost i zaštitu djece i način pribavljanja saglasnosti nosioca roditeljskog prava nad djetetom;
 - h) mjere i postupke iz čl. 26. i 27. ovog zakona kao i mjere za postizanje sigurnosti obrade iz člana 34. ovog zakona;
 - i) izvještavanje Agencije o povredama ličnih podataka i obavještavanje nosioca podataka o takvim povredama;
 - j) prijenos ličnih podataka drugim zemljama ili međunarodnim organizacijama ili
 - k) vansudske postupke i druge postupke za rješavanje sporova između kontrolora podataka i nosioca podataka u vezi s obradom, ne dovodeći u pitanje prava nosioca podataka na osnovu čl. 108. i 110. ovog zakona.
- (3) Kodeks ponašanja iz stava (2) ovog člana obavezno sadrži odredbe koje pravnom licu iz člana 43. stav (1) ovog zakona omogućavaju da provodi obavezno praćenje usklađenosti kontrolora podataka ili obrađivača koji su se obavezali na njegovu primjenu, ne dovodeći u pitanje nadležnosti Agencije.
- (4) Udruženja i subjekat iz stava (2) ovog člana koji namjeravaju izraditi kodeks ponašanja ili izmijeniti i proširiti postojeći kodeks ponašanja, nacrt kodeksa ponašanja, odnosno izmjene ili proširenje kodeksa ponašanja dostavljaju Agenciji.
- (5) Agencija daje mišljenje o tome da li je nacrt kodeksa u skladu s ovim zakonom te odobrava nacrt kodeksa ako ocijeni da osigurava dovoljno adekvatne zaštitne mjere.
- (6) Ako Agencija odobri nacrt kodeksa ponašanja, odnosno izmjene ili dopune kodeksa ponašanja, u skladu sa stavom

- (5) ovog člana, Agencija registrira i objavljuje kodeks ponašanja.
- (7) Kontrolor podataka ili obrađivač, na koje se ovaj zakon ne primjenjuje u skladu s članom 6. ovog zakona, mogu primjenjivati kodeks ponašanja koji je odobren, u skladu sa stavom (5) ovog člana, kako bi osigurali odgovarajuće zaštitne mjere u okviru prijenosa ličnih podataka drugoj državi ili međunarodnoj organizaciji, uz uslove iz člana 48. stav (2) tačke d) ovog zakona.
- (8) Kontrolor podataka ili obrađivač iz stava (7) ovog člana, putem ugovornih ili drugih pravnoobavezujućih instrumenata, preuzima obavezujuće i izvršne obaveze za primjenu zaštitnih mjera, uključujući i mjere u vezi s pravima nosioca podataka.

Član 43.

(Praćenje odobrenog kodeksa ponašanja)

- (1) Pravno lice s odgovarajućim stepenom stručnosti za predmet kodeksa ponašanja može obavljati praćenje usklađenosti s kodeksom ponašanja, ako ga je u tu svrhu akreditirala Agencija.
- (2) Pravno lice iz stava (1) ovog člana može biti akreditirano za praćenje usklađenosti s kodeksom ponašanja ako je:
- a) Agenciji dokazalo svoju nezavisnost i stručnost za predmet kodeksa ponašanja;
 - b) uspostavilo postupke koji mu omogućavaju da ocjenjuje kvalificiranost kontrolora podataka i obrađivača za primjenu kodeksa ponašanja, da prati njihove primjene odredbi kodeksa ponašanja i da periodično preispituje njegovo funkcioniranje;
 - c) uspostavilo postupke i strukture za rješavanje prigovora na kršenja kodeksa ponašanja ili na način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio kodeks ponašanja i učinio te postupke i strukture transparentnim nosiocima podataka i javnosti i
 - d) Agenciji dokazalo da njegovi zadaci i dužnosti ne dovode do sukoba interesa.
- (3) Pravno lice iz stava (1) ovog člana, uz primjenu odgovarajućih zaštitnih mjera, preduzima odgovarajuće radnje u slučajevima kršenja kodeksa ponašanja od kontrolora podataka ili obrađivača, što uključuje suspendiranje ili isključenje iz kodeksa ponašanja.
- (4) Pravno lice iz stava (1) ovog člana dužno je obavijestiti Agenciju o radnjama i razlozima iz stava (3) ovog člana.
- (5) Agencija oduzima akreditaciju pravnom licu koje više ne ispunjava uslove za akreditaciju ili ako pravno lice krši odredbe ovog zakona.
- (6) Ovaj član se ne primjenjuje na obradu ličnih podataka koju obavlja javni organ.

Član 44.

(Certifikacija)

- (1) Agencija preporučuje uspostavljanje postupka certifikacije zaštite ličnih podataka, pečata i oznaka za zaštitu podataka s ciljem dokazivanja poštivanja odredbi ovog zakona, posebno uzimajući u obzir potrebe mikro, malih i srednjih pravnih lica.
- (2) Postupak certifikacije zaštite ličnih podataka, pečata i oznaka može biti uspostavljen i radi dokazivanja postojanja odgovarajućih zaštitnih mjera koje osiguravaju kontrolor podataka i obrađivač na koje se ovaj zakon u skladu s članom 6. ovog zakona ne odnosi, u okviru prijenosa ličnih podataka drugoj državi ili međunarodnoj organizaciji, uz uslove iz člana 48. stav (2) tačka d) ovog zakona.

- (3) Kontrolori podataka ili obrađivači, iz stava (2) ovog člana, putem ugovornih ili drugih pravnoobavezujućih instrumenata prihvataju primjenu odgovarajućih zaštitnih mjera, uključujući i mjere u vezi s nosiocem podataka.
- (4) Certifikacija je dobrovoljna i dostupna putem procesa koji je transparentan.
- (5) Certifikacija, u skladu s ovim članom, ne umanjuje odgovornost kontrolora podataka ili obrađivača za poštivanje ovog zakona i ne dovodi u pitanje nadležnosti Agencije.
- (6) Certifikaciju, u skladu s ovim članom, izdaje certifikacioni organ iz člana 45. ovog zakona na osnovu kriterija koje je odobrila Agencija.
- (7) Kontrolor podataka ili obrađivač, u postupku certifikacije, certifikacionom organu pruža sve informacije i omogućava pristup aktivnostima obrade koje su potrebne za postupak certifikacije.
- (8) Certifikat se kontroloru podataka ili obrađivaču izdaje najduže na tri godine i može se obnoviti uz iste uslove.
- (9) Certifikacioni organ oduzima certifikat kontroloru ili obrađivaču ako više ne ispunjava uslove za izdavanje certifikata.
- (10) Agencija postupak certifikacije zaštite ličnih podataka, pečata i oznake unosi u evidenciju i javno objavljuje.

Član 45.

(Certifikacioni organ)

- (1) Akreditaciju certifikacionog organa, s odgovarajućim stepenom stručnosti iz oblasti zaštite ličnih podataka, radi Agencija.
- (2) Certifikacioni organ obavještava Agenciju o odluci o izdavanju i obnavljanju certifikata kako bi Agencija mogla obavljati ovlaštenja iz člana 103. stav (2) tačka h) ovog zakona.
- (3) Certifikacioni organ može biti akreditiran samo ako:
 - a) Agenciji na zadovoljavajući način dokaže svoju nezavisnost i stručnost u predmetu certifikacije;
 - b) se obaveže da će poštovati kriterije iz člana 44. stav (6) ovog zakona;
 - c) uspostavi postupke za izdavanje, periodično preispitivanje i povlačenje certifikacije, pečata i oznaka za zaštitu podataka;
 - d) uspostavi postupke i strukture za rješavanje prigovora na kršenja certifikacije ili način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio certifikaciju i učini te postupke i strukture transparentnim nosiocima podataka i javnosti;
 - e) Agenciji dokaže da njegovi zadaci i dužnosti ne dovode do sukoba interesa.
- (4) Akreditacija certifikacionog organa provodi se na osnovu kriterija koje je propisala Agencija.
- (5) Akreditacija se izdaje najduže na pet godina i može se obnoviti uz iste uslove ako certifikacioni organ i dalje ispunjava zahtjeve iz ovog člana.
- (6) Ne dovodeći u pitanje DIO ČETVRTI ovog zakona, Agencija povlači akreditaciju certifikacionog organa ako se uslovi iz stava (3) ovog člana ne ispune ili više nisu ispunjeni, ili ako se radnjama koje preduzima certifikacioni organ krši ovaj zakon.
- (7) Certifikacioni organ odgovoran je za pravilnu procjenu koja dovodi do certifikacije ili oduzimanja certifikata, ne dovodeći u pitanje odgovornost kontrolora podataka ili obrađivača za poštivanje ovog zakona.
- (8) Certifikacioni organ u pisanoj formi obavještava Agenciju o razlozima za izdavanje ili oduzimanje certifikata.
- (9) Agencija javno objavljuje kriterije iz člana 44. stav (6) ovog zakona.

POGLAVLJE IV. PRIJENOS LIČNOG PODATKA U DRUGU DRŽAVU ILI MEĐUNARODNU ORGANIZACIJU

Član 46.

(Opći principi prijenosa)

Svaki prijenos ličnog podatka čija je obrada u toku ili je namijenjen daljnjoj obradi poslije njegovog prenošenja u drugu državu ili međunarodnu organizaciju može se obavljati samo ako je takav prijenos u skladu s odredbama ovog zakona, što obuhvata i daljnji prijenos ličnog podatka iz druge države ili međunarodne organizacije u još jednu drugu državu ili međunarodnu organizaciju.

Član 47.

(Prijenos na osnovu adekvatnosti nivoa zaštite ličnog podatka)

- (1) Prijenos ličnog podatka u drugu državu, na dio njene teritorije, ili u jedan ili više sektora u toj državi ili međunarodnu organizaciju može se obavljati ako je utvrđeno da ta druga država, dio njene teritorije, ili jedan ili više sektora u toj državi ili ta međunarodna organizacija osigurava adekvatan nivo zaštite ličnog podatka.
- (2) Smatra se da je adekvatan nivo zaštite iz stava (1) ovog člana osiguran u državi, dijelovima njene teritorije, ili jednom ili više sektora u toj državi ili međunarodnoj organizaciji, za koje je od Evropske unije utvrđeno da osiguravaju adekvatan nivo zaštite ličnog podatka.
- (3) Odluku o adekvatnosti nivoa zaštite ličnog podatka iz stava (1) ovog člana donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stava (3) ovog člana, uzimajući u obzir:
 - a) princip vladavine prava, poštivanje ljudskih prava i osnovnih sloboda, sektorsko zakonodavstvo, uključujući zakonodavstvo o javnoj sigurnosti, odbrani, državnoj sigurnosti, krivičnom pravu i pristupu javnih organa ličnim podacima, kao i primjenu tih propisa, pravila o zaštiti ličnih podataka, pravila struke i mjere osiguranja zaštite ličnih podataka, uključujući pravila o daljnjem prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, koja se primjenjuju u praksi sudova i drugih organa vlasti u drugoj državi ili međunarodnoj organizaciji, kao i djelotvornost ostvarivanja prava nosioca ličnog podatka, a posebno djelotvornost upravnih i sudskih postupaka zaštite prava nosioca ličnog podatka;
 - b) postojanje i efikasnost rada nadzornog organa u drugoj državi ili organa koji je nadležan za međunarodnu organizaciju u ovoj oblasti, s ovlaštenjem da osigura primjenu pravila o zaštiti ličnog podatka i pokrene postupke zaštite ličnog podatka u slučaju njihovog nepoštivanja, pruži pomoć i savjetuje nosioce ličnih podataka u ostvarivanju njihovih prava, kao i da saraduje s nadzornim organima drugih država;
 - c) međunarodne obaveze koje je druga država ili međunarodna organizacija preuzela, ili druge obaveze koje proizlaze iz pravnoobavezujućih međunarodnih ugovora ili drugih pravnih instrumenata, kao i iz članstva u multilateralnim ili regionalnim organizacijama, a posebno u vezi sa zaštitom ličnih podataka.
- (5) Agencija kontinuirano prati stanje u oblasti zaštite ličnih podataka u drugoj državi, dijelu njene teritorije, jednom ili više sektora unutar te države ili međunarodnoj

- organizaciji i o tome po potrebi izvještava Vijeće ministara Bosne i Hercegovine.
- (6) Izvještaj iz stava (5) ovog člana uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija, koje su značajne za preispitivanje postojanja adekvatnog nivoa zaštite ličnog podataka, na osnovu čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stava (3) ovog člana.
- (7) Odluka donesena na osnovu stava (3) ovog člana ne dovodi u pitanje prijenos ličnog podataka u drugu državu, na teritoriju ili u jedan ili više određenih sektora unutar te druge države ili međunarodnu organizaciju u skladu s čl. 48. do 51. ovog zakona.
- (8) Lista država, dio njihovih teritorija, jedan ili više sektora unutar države i međunarodnih organizacija, u vezi s kojim je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju adekvatan nivo zaštite ličnih podataka, objavljuju se u "Službenom glasniku BiH" i na službenoj internetskoj stranici Agencije.

Član 48.

(Prijenos na koji se primjenjuju odgovarajuće zaštitne mjere)

- (1) Kontrolor podataka ili obrađivač može prenijeti lične podatke u drugu državu, na dio njene teritorije, jedan ili više sektora unutar te države ili u međunarodnu organizaciju za koju listom iz člana 47. stav (8) ovog zakona nije utvrđeno postojanje adekvatnog nivoa zaštite ličnih podataka samo ako je kontrolor podataka ili obrađivač osigurao odgovarajuće zaštitne mjere tih podataka i ako su nosiocu ličnih podataka osigurana ostvariva prava i djelotvorna sudska zaštita.
- (2) Odgovarajuće zaštitne mjere iz stava (1) ovog člana mogu se, bez posebnog odobrenja Agencije, osigurati:
- pravnoobavezujućim aktom sačinjenim između javnih organa;
 - obavezujućim poslovnim pravilima u skladu s članom 49. ovog zakona;
 - odobrenim kodeksom ponašanja u skladu s članom 42. ovog zakona s obavezujućim i izvršnim obavezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, između ostalog i u vezi s pravom nosioca podataka ili
 - odobrenim postupkom certifikacije u skladu s članom 44. ovog zakona s obavezujućim i izvršnim obavezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, između ostalog i u vezi s pravima nosioca podataka.
- (3) Odgovarajuće zaštitne mjere iz stava (1) ovog člana mogu se osigurati standardnim ugovornim klauzulama o zaštiti podataka koje donosi Agencija.
- (4) Uz uslov da to odobri Agencija, odgovarajuće zaštitne mjere iz stava (1) ovog člana također mogu biti osigurane posebno:
- ugovorom između kontrolora podataka ili obrađivača i kontrolora podataka, obrađivača ili primaoca ličnih podataka u drugoj državi ili međunarodnoj organizaciji ili
 - odredbama koje se unose u sporazume između javnih organa i koje sadrže provediva i djelotvorna prava nosioca podataka.

Član 49.

(Obavezujuća poslovna pravila)

- (1) Obavezujuća poslovna pravila određuju najmanje:

- strukturu i podatke za kontakt-grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost i svakog od njihovih članova;
- prijenose podataka ili skupove prijenosa, uz navođenje kategorije ličnih podataka, vrste obrade i njene svrhe, kategorije nosilaca podataka i određenja druge države ili država o kojima se radi;
- njihovu pravnoobavezujuću prirodu;
- primjenu principa zaštite podataka, a posebno ograničenja svrhe, smanjenja količine podataka, ograničenja roka čuvanja, kvaliteta podataka, tehničke i integrirane zaštite podataka, pravnog osnova obrade, obrade posebnih kategorija ličnih podataka, mjera za postizanje sigurnosti podataka i uslova u vezi s daljnjim prijenosom organima koji nisu obavezani obavezujućim poslovnim pravilima;
- prava nosilaca podataka u vezi s obradom i načine za ostvarenje tih prava, uključujući i pravo da se na njih ne primjenjuju odluke koje se zasnivaju isključivo na automatskoj obradi, što uključuje i izradu profila u skladu s članom 24. ovog zakona, pravo na prigovor Agenciji i pravo na sudska zaštitu, u skladu s članom 110. ovog zakona, a u odgovarajućim slučajevima i pravo na naknadu štete za kršenje obavezujućih poslovnih pravila;
- da kontrolor podataka ili obrađivač sa sjedištem ili poslovnim nastanom na teritoriji Bosne i Hercegovine prihvata odgovornost za sva kršenja obavezujućih poslovnih pravila od bilo kojeg člana koji nema sjedište ili poslovni nastan u Bosni i Hercegovini ili je kontrolor podataka ili obrađivač na cjelini ili djelimično izuzet od odgovornosti ako dokaže da taj član grupe privrednih subjekata nije odgovoran za događaj koji je uzrokovao štetu;
- na koji način se nosiocima podataka, osim informacija iz čl. 15. i 16. ovog zakona, pružaju informacije o obavezujućim poslovnim pravilima, posebno o odredbama iz tač. d), e) i f) ovog stava;
- zadatke svakog službenika za zaštitu podataka imenovanog u skladu s članom 39. ovog zakona ili bilo kojeg drugog lica ili subjekta odgovornog za praćenje usklađenosti s obavezujućim poslovnim pravilima u grupi privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kao i praćenje osposobljenosti i rješavanje prigovora;
- postupke povodom prigovora;
- mehanizme unutar grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kojima se osigurava provjera poštivanja obavezujućih poslovnih pravila, koji uključuju reviziju zaštite podataka i metode za osiguravanje korektivnih mjera za zaštitu prava nosioca podataka. Rezultate takve provjere potrebno je saopćiti licu ili subjektu iz tačke h) ovog stava i upravljačkom organu grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, a na zahtjev ih je potrebno staviti na raspolaganje Agenciji;
- mehanizme za izvještavanje i vođenje evidencije o promjenama pravila i izvještavanje Agencije o tim promjenama;
- mehanizam saradnje s Agencijom radi osiguravanja usklađenosti svakog člana grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, prije svega tako što se Agenciji stave na raspolaganje rezultati provjera mjera iz tačke j) ovog stava;

- m) mehanizme za izvještavanje Agenciji o bilo kakvim pravnim obavezama koje se odnose na člana grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost i primjenjuju se u drugoj državi, a koje bi mogle značajno negativno uticati na garancije sadržane u obavezujućim poslovnim pravilima;
 - n) odgovarajuće osposobljavanje iz oblasti zaštite ličnih podataka za osoblje koje ima stalan ili redovan pristup ličnim podacima.
- (2) Agencija odobrava obavezujuća poslovna pravila uz uslov da:
- a) su pravnoobavezujuća i da se primjenjuju na svakog zainteresiranog člana određene grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, što uključuje i njihove zaposlene, te da ih oni izvršavaju;
 - b) nosiocima podataka izričito daju provediva prava u vezi s obradom njihovih ličnih podataka;
 - c) ispunjavaju uslove iz stava (1) ovog člana.
- (3) Agencija može odrediti format i postupke razmjene informacija između kontrolora podataka, obrađivača i Agencije za obavezujuća poslovna pravila u smislu ovog člana.

Član 50.

(Prijenos ili otkrivanje podataka koji nisu dopušteni)

Svaka presuda suda, tribunala ili odluka upravnog organa druge države kojom se od kontrolora podataka ili obrađivača zahtijeva prijenos ili otkrivanje ličnih podataka može biti priznata ili izvršena samo ako se zasniva na međunarodnom sporazumu, kao što je sporazum o uzajamnoj pravnoj pomoći, između druge države koja je podnijela zahtjev i Bosne i Hercegovine, ne dovodeći u pitanje druge razloge za prijenos u skladu s ovim poglavljem.

Član 51.

(Odstupanje u posebnim slučajevima)

- (1) Prijenos ili skup prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, ako ne postoji odluka o adekvatnosti, u skladu s članom 47. stav (3) ovog zakona ili odgovarajuće zaštitne mjere u skladu s članom 48. ovog zakona, uključujući i obavezujuća poslovna pravila iz člana 49. ovog zakona, obavlja se samo uz jedan od sljedećih uslova:
- a) nosilac podataka je izričito saglasan s predloženim prijenosom, nakon što je upoznat s mogućim rizicima takvih prijenosa zbog nepostojanja odluke o adekvatnosti i odgovarajućih zaštitnih mjera iz člana 48. ovog zakona;
 - b) prijenos je neophodan za izvršenje ugovora između nosioca podataka i kontrolora podataka ili provođenje predugovornih mjera na zahtjev nosioca podataka;
 - c) prijenos je neophodan radi sklapanja ili izvršenja ugovora sklopljenog u interesu nosioca podataka između kontrolora podataka i drugog fizičkog ili pravnog lica;
 - d) prijenos je neophodan iz važnih razloga javnog interesa;
 - e) prijenos je neophodan za postavljanje, ostvarivanje ili odbranu pravnih zahtjeva;
 - f) prijenos je neophodan za zaštitu ključnih interesa nosioca podataka ili drugih lica ako nosilac podataka fizički ili pravno nije sposoban dati saglasnost;
 - g) prijenos se vrši iz registra, koji prema pravnim propisima u Bosni i Hercegovini služi za pružanje

informacija javnosti i koji je dostupan na uvid javnosti ili bilo kojem licu koje može dokazati postojanje legitimnog interesa, ali samo u mjeri u kojoj su ispunjeni uslovi propisani posebnim zakonom za uvid u tom posebnom slučaju.

- (2) Prijenos ili skup prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, u slučaju kada osnov za prijenos ne mogu biti čl. 47. ili 48. ovog zakona, uključujući i obavezujuća poslovna pravila iz člana 49. ovog zakona, i kada se ne primjenjuje nijedno odstupanje u posebnim slučajevima iz stava (1) ovog člana, može se izvršiti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničen broj nosilaca podataka i ako je neophodan za potrebe važnih, legitimnih interesa kontrolora podataka nad kojima ne prevladavaju interesi ili prava i slobode nosioca podataka, a kontrolor podataka je procijenio sve okolnosti prijenosa podataka i na osnovu te procjene je predvidio odgovarajuće zaštitne mjere u vezi sa zaštitom ličnih podataka. Kontrolor podataka o prijenosu obavještava Agenciju. Uz informacije iz čl. 15. i 16. ovog zakona, kontrolor podataka obavještava nosioca podataka o prijenosu i o važnim legitimnim interesima.
- (3) Prijenos na osnovu stava (1) tačke g) ovog člana ne uključuje lične podatke u cjelini ni cijele kategorije ličnih podataka sadržanih u registru. Kada je registar namijenjen za uvid licima koja imaju legitiman interes, prijenos se obavlja samo ako to zahtijevaju ta lica ili ako su oni primaoci.
- (4) Na aktivnosti koje obavljaju javni organi prilikom izvršavanja svojih javnih ovlaštenja ne primjenjuju se stav (1) tač. a), b) i c) i stav (2) ovog člana.
- (5) Javni interes iz stava (1) tačke d) ovog člana mora biti propisan zakonom koji se primjenjuje na kontrolora podataka.
- (6) Ako nije donesena odluka o adekvatnosti, iz važnih razloga javnog interesa posebnim propisom mogu biti izričito propisana ograničenja prijenosa određenih kategorija ličnih podataka drugoj državi ili međunarodnoj organizaciji.
- (7) Kontrolor podataka ili obrađivač dokumentira procjenu, kao i odgovarajuće zaštitne mjere iz st. (1) i (2) ovog člana, u evidencijama iz člana 32. ovog zakona.

POGLAVLJE V. POSEBNI SLUČAJEVI OBRADE

Član 52.

(Obrada ličnog podatka i sloboda izražavanja i informiranja)

- (1) Obrada ličnih podataka prilikom korištenja prava na slobodu izražavanja i informiranja, što uključuje obradu isključivo u novinarske svrhe, u svrhe akademskog, umjetničkog ili književnog izražavanja, obavlja se u skladu s posebnim propisima.
- (2) Posebnim propisima iz stava (1) ovog člana utvrđuju se izuzeci ili odstupanja od primjene Poglavlja I, Poglavlja II, Poglavlja III, Poglavlja IV, Poglavlja V. ovog dijela i DIJELA ČETVRTOG ovog zakona, ako su takvi izuzeci ili odstupanja potrebni da se uskladi pravo na zaštitu ličnih podataka sa slobodom izražavanja i informiranja.

Član 53.

(Obrada ličnog podatka i javni pristup službenim dokumentima)

- (1) Javni organ i nadležni organ, u skladu sa zakonom koji se primjenjuje na taj organ, mogu u javnom interesu otkriti lične podatke iz službenih dokumenata kojima raspolazu, kako bi se javni pristup službenim dokumentima uskladio s pravom na zaštitu ličnih podataka u skladu s ovim zakonom.

- (2) Ovaj zakona primjenjuje se prilikom primjene propisa o slobodi pristupa informacijama u Bosni i Hercegovini.

Član 54.

(Обрада jedinstvenog matičnog broja fizičkog lica)

- (1) Posebni uslovi za obradu jedinstvenog matičnog broja fizičkog lica ili bilo kojeg drugog identifikatora opće primjene propisuju se posebnim zakonom.
- (2) Jedinstveni matični broj fizičkog lica ili bilo koji drugi identifikator opće primjene iz stava (1) ovog člana obrađuje se samo uz primjenu odgovarajućih zaštitnih mjera u vezi s pravima i slobodama nosioca podataka u skladu s ovim zakonom.

Član 55.

(Обрада ličnih podataka u kontekstu zaposlenja)

- (1) Posebnim zakonom ili kolektivnim ugovorom preciziraju se pravila s ciljem osiguravanja zaštite prava i sloboda u vezi s obradom ličnih podataka u kontekstu zaposlenja, posebno za potrebe zapošljavanja, izvršenja ugovora o radu, uključujući i izvršavanje obaveza propisanih zakonom ili kolektivnim ugovorima, za potrebe upravljanja, planiranja i organizacije rada, jednakosti i različitosti na radnom mjestu, zdravstva i sigurnosti na radu, zaštite imovine poslodavca ili klijenta i za potrebe individualnog ili kolektivnog ostvarivanja i uživanja prava i pogodnosti iz radnog odnosa, kao i za potrebe prestanka radnog odnosa.
- (2) Pravila iz stava (1) ovog člana uključuju prikladne i posebne mjere za zaštitu ljudskog dostojanstva nosioca podataka, njegovih legitimnih interesa i osnovnih prava, posebno u vezi s transparentnošću obrade, prijenosom ličnih podataka unutar grupe privrednih subjekata ili grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kao i sistemom praćenja na radnom mjestu.

Član 56.

(Zaštitne mjere i odstupanja u vezi s obradom ličnog podatka u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe)

- (1) Na obradu ličnih podataka u svrhu arhiviranja u javnom interesu, u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe primjenjuju se odgovarajuće zaštitne mjere u skladu s ovim zakonom u pogledu prava i sloboda nosioca podataka.
- (2) Zaštitnim mjerama iz stava (1) ovog člana osigurava se primjena tehničkih i organizacionih mjera, posebno onih kojima se garantira primjena principa smanjenja opsega podataka, koje mogu uključivati pseudonimizaciju, ako se svrhe mogu ostvariti tako.
- (3) Ako se svrhe iz stava (1) ovog člana mogu postići daljnjom obradom koja ne omogućava ili više ne omogućava identifikaciju nosioca podataka, te svrhe se ostvaruju na taj način.
- (4) Ako se lični podaci obrađuju u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih iz čl. 17, 18, 20. i 23. ovog zakona, uz primjenu uslova i mjera zaštite iz stava (1) ovog člana, ako je vjerovatno da bi ta prava mogla spriječiti ili ozbiljno ugroziti ostvarivanje tih posebnih svrha, pa su takva odstupanja neophodna za njihovo postizanje.
- (5) Ako se lični podaci obrađuju u svrhu arhiviranja u javnom interesu, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih u čl. 17, 18, 20, 21, 22. i 23. ovog zakona, uz primjenu uslova i mjera zaštite iz stava (1) ovog člana, ako je vjerovatno da bi ta prava

mogla spriječiti ili ozbiljno ugroziti ostvarivanje te posebne svrhe, pa su takva odstupanja neophodna za njeno postizanje.

- (6) Ako obrada iz st. (2) i (3) ovog člana istovremeno služi i drugoj svrsi, odstupanja se primjenjuju samo za obradu u svrhe koje su navedene u tim stavovima.

Član 57.

(Videonadzor)

- (1) Praćenje određenog prostora putem videonadzora dopušteno je samo ako je to nužno za zaštitu lica i imovine i ako ne prevladaju interesi nosioca podataka.
- (2) Videonadzorom mogu biti obuhvaćeni samo prostori ili dijelovi prostora čiji je nadzor nužan radi postizanja svrhe iz stava (1) ovog člana.
- (3) Uspostavljanje videonadzora javno dostupnih objekata velikih površina, kao što su sportski objekti, zabavni centri, tržni centri ili parkirališta, ili vozila javnog prijevoza, dopušteno je isključivo s ciljem zaštite života, zdravlja i slobode lica te imovine.
- (4) Kontrolor podataka koji obavlja videonadzor dužan je donijeti odluku koja će sadržavati pravila obrade s ciljem poštivanja prava na zaštitu privatnosti i ličnog života nosioca podataka, ako videonadzor nije propisan zakonom.
- (5) Kontrolor podataka ili obrađivač dužan je na vidnom mjestu istaći oznaku o videonadzoru. Oznaka o videonadzoru sadrži sljedeće informacije: da je prostor pod videonadzorom, podatke o kontroloru podataka, odnosno obrađivaču i kontakt-podatke putem kojih nosilac podataka može ostvariti svoja prava. Oznaka treba biti vidljiva najkasnije prilikom ulaska u vidokrug snimanja.
- (6) Kontrolor podataka ili obrađivač dužan je da, kod sistema videonadzora javno dostupnih objekata iz stava (3) ovog člana, bilježi zapise o upotrebi sistema i da ih čuva najmanje 12 mjeseci. Zapisi omogućavaju da se utvrdi datum i vrijeme te identitet lica koje je izvršilo uvid u sistem videonadzora.
- (7) Za uspostavljanje videonadzora u stambenim, odnosno poslovno-stambenim zgradama potrebna je saglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova. Videonadzorom se može obuhvatiti samo pristup ulasku i izlasku iz stambene zgrade, te zajedničke prostorije u stambenim zgradama.
- (8) Praćenje javnih prostora putem videonadzora u svrhe iz člana 1. stav (1) tačka c) ovog zakona dopušteno je samo ako je to propisano posebnim zakonom.

Član 57a.

(Обрада biometrijskih podataka u svrhu sigurne identifikacije)

- (1) Obrada biometrijskih podataka može se provoditi samo ako je propisana zakonom ili ako je nužna za zaštitu lica, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačnu i sigurnu identifikaciju korisnika usluga, uzimajući u obzir da ne prevladavaju interesi nosioca podataka koji su u suprotnosti s obradom biometrijskih podataka iz ovog člana.
- (2) Pravni osnov za obradu biometrijskih podataka nosioca podataka radi sigurne identifikacije korisnika usluga izričita je saglasnost takvog nosioca podataka data u skladu s odredbama ovog zakona.

Član 57b.

(Обрада biometrijskih podataka u službenim prostorijama)

Dopuštena je obrada biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija, ako je propisano zakonom ili ako se takva

obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija, uz uslov da je zaposlenik dao izričitu saglasnost za takvu obradu biometrijskih podataka u skladu s odredbama ovog zakona.

Član 58.

(Postojeća pravila o zaštiti ličnih podataka crkava i vjerskih zajednica)

- (1) Ako crkve i vjerske zajednice primjenjuju sveobuhvatna pravila u vezi s obradom ličnih podataka, ta postojeća pravila mogu se i dalje primjenjivati uz uslov da se usklade s ovim zakonom.
- (2) Crkve i vjerske zajednice koje primjenjuju sveobuhvatna pravila nadzire Agencija, osim ako crkva ili vjerska zajednica ne formira poseban nezavisan nadzorni organ, uz uslov da ispunjava uslove utvrđene u DIJELU ČETVRTOM ovog zakona.

Član 59.

(Obaveza čuvanja profesionalne tajne)

- (1) Posebnim propisom može se utvrditi ograničenje Agencije iz člana 103. stav (1) tač. f) i g) u vezi s kontrolorom podataka ili obrađivačem koji, na osnovu posebnog propisa koji je donio nadležni organ, podliježu obavezama profesionalne tajne i drugim jednakovrijednim obavezama tajnosti, ako je to nužno i razmjerno kako bi se uskladilo pravo na zaštitu ličnih podataka s obavezom tajnosti.
- (2) Poseban propis iz stava (1) ovog člana primjenjuje se samo na lične podatke koje je kontrolor podataka ili obrađivač dobio kao rezultat ili primio tokom aktivnosti koja je obuhvaćena obavezom tajnosti.

DIO TREĆI – OBRADA LIČNOG PODATKA OD NADLEŽNOG ORGANA KAO KONTROLORA PODATAKA U SVRHU SPREČAVANJA, ISTRAGE I OTKRIVANJA KRIVIČNIH DJELA ILI GONJENJA POČINILACA KRIVIČNIH DJELA, IZVRŠAVANJE KRIVIČNIH SANKCIJA, UKLJUČUJUĆI ZAŠTITU OD PRIJETNJI JAVNOG SIGURNOSTI I NJIHOVO SPREČAVANJE

Član 60.

(Principi obrade ličnih podataka od nadležnog organa)

- (1) Principi obrade ličnih podataka od nadležnog organa su:
 - a) zakonitost i pravičnost;
 - b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama;
 - c) smanjenje obima podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u svrhe u koje se obrađuju;
 - d) tačnost – podaci moraju biti tačni i prema potrebi ažurirani, moraju se preduzeti sve razumne mjere kako bi se osiguralo da lični podaci koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljani;
 - e) ograničenje čuvanja – podaci moraju biti čuvani u formi koja omogućava identifikaciju nosioca podataka, i to ne duže nego što je potrebno u svrhe u koje se podaci obrađuju;
 - f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigura odgovarajuća sigurnost ličnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera.
- (2) Obrada koju radi isti ili neki drugi nadležni organ u svrhu iz člana 1. stav (1) tačka c) ovog zakona različitu od one za koju su lični podaci prikupljeni dopuštena je ako je:

- a) nadležni organ ovlašten za obradu takvih ličnih podataka u takvu svrhu u skladu s posebnim propisom ili
- b) obrada neophodna i proporcionalna drugoj zakonitoj svrsi.
- (3) Obrada koju radi isti ili neki drugi nadležni organ može uključivati arhiviranje u javnom interesu, u naučne, statističke ili historijske svrhe, za svrhe iz člana 1. stav (1) tačka c) ovog zakona, uz preduzimanje odgovarajućih zaštitnih mjera u vezi s pravima i slobodama nosioca podataka.
- (4) Nadležni organ odgovoran je za usklađenost sa st. (1), (2) i (3) ovog člana i mora biti u mogućnosti dokazati tu usklađenost.

Član 61.

(Rok za čuvanje i brisanje ličnog podatka)

- (1) Rok za brisanje ličnih podataka ili za periodično preispitivanje potrebe njihovog čuvanja propisuje se posebnim zakonom.
- (2) Nadležni organi dužni su uspostaviti pravila i procedure kojima se osigurava poštivanje roka iz stava (1) ovog člana.

Član 62.

(Razlika između različitih kategorija nosilaca podataka)

Nadležni organ dužan je, prema potrebi i ako je to moguće, napraviti jasnu razliku između ličnih podataka različitih kategorija nosilaca podataka, kao što je:

- a) lice za koje postoji osnov sumnje da je izvršilo ili namjerava izvršiti krivično djelo;
- b) lice osuđeno za krivična djela;
- c) lice koje je žrtva krivičnog djela ili lice u pogledu kojeg postoje određene činjenice koje daju osnov za sumnju da bi to lice moglo biti žrtva krivičnog djela;
- d) lice koje se dovodi u vezu s krivičnim djelom, kao što je lice koje se može pozvati da svjedoči u istragama ili naknadnom krivičnom postupku, lice koje može dati informacije o krivičnim djelima ili lice za kontakt ili saradnici lica iz tač. a) i b) ovog stava.

Član 63.

(Razlika između ličnih podataka i provjera kvaliteta ličnih podataka)

- (1) Nadležni organ dužan je utvrditi mehanizam kojim će se osigurati da se lični podaci zasnovani na činjenicama razlikuju, što je više moguće, od ličnih podataka zasnovanih na ličnim procjenama.
- (2) Nadležni organ dužan je preduzeti sve razumne mjere kako bi osigurao da se lični podaci koji su netačni, nepotpuni ili neažurirani ne prenose niti stavljaju na raspolaganje. Nadležni organ, ako je to moguće, provjerava kvalitet ličnih podataka prije njihovog prenošenja ili stavljanja na raspolaganje. Prilikom svakog prenošenja ličnih podataka, što je više moguće, dostavljaju se neophodne informacije nadležnom organu, koji je podatke dobio, omogućava se ocjena stepena tačnosti, potpunosti i pouzdanosti ličnih podataka, kao i u kojoj su mjeri ažurirani.
- (3) Ako se utvrdi da su preneseni netačni lični podaci ili da su lični podaci preneseni nezakonito, nadležni organ mora bez odgađanja o tome obavijestiti primaoca. U tom slučaju lični podaci moraju se ispraviti ili brisati ili obradu ograničiti u skladu s članom 72. ovog zakona.

Član 64.

(Zakonitost obrade ličnog podatka od nadležnog organa)

- (1) Obrada ličnih podataka koju obavlja nadležni organ zakonita je samo ako je nužna i samo u onoj mjeri u kojoj je nužna za obavljanje poslova nadležnog organa u svrhe iz člana 1. stav (1) tačka c) ovog zakona i ako je propisana posebnim zakonom.
- (2) Posebni zakon iz stava (1) ovog člana propisuje najmanje ciljeve obrade, lične podatke koji se obrađuju i svrhe obrade.

Član 65.

(Posebni uslovi obrade)

- (1) Lični podaci koje nadležni organi prikupljaju za svrhe utvrđene u članu 1. stav (1) tačka c) ovog zakona ne smiju se obrađivati u druge svrhe, osim ako je takva obrada propisana posebnim zakonom i u tom slučaju ne primjenjuju se odredbe ovog dijela zakona.
- (2) Ako je posebnim zakonom nadležnom organu povjereno obavljanje poslova drugačijih od onih koje obavljaju u svrhe iz člana 1. stav (1) tačka c) ovog zakona, u tom slučaju ne primjenjuju se odredbe ovog dijela zakona, između ostalog i za svrhu arhiviranja u javnom interesu, ili u svrhu naučnog ili historijskog istraživanja ili u statističke svrhe.
- (3) Ako su posebnim zakonom, koji se odnosi na nadležni organ koji prenosi podatke, propisani posebni uslovi za obradu, nadležni organ koji prenosi te lične podatke primaocu dužan ga je obavijestiti o tim uslovima i o zahtjevima za njihovo poštivanje.

Član 66.

(Obrada posebnih kategorija ličnih podataka od nadležnog organa)

- (1) Zabranjena je obrada ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije lica ili podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji lica.
- (2) Izuzetno od stava (1) ovog člana, obrada posebnih kategorija ličnih podataka je dopuštena isključivo ako je to nužno, pridržavajući se odgovarajućih zaštitnih mjera u vezi s pravima i slobodama nosioca podataka:
 - a) ako je propisana posebnim zakonom;
 - b) radi zaštite vitalnih interesa nosioca podataka ili drugog pojedinca ili
 - c) ako se takva obrada odnosi na podatke za koje je očit da ih je objavio nosilac podataka.

Član 67.

(Automatizirano pojedinačno donošenje odluke od nadležnog organa)

- (1) Nadležnom organu zabranjeno je donošenje odluke isključivo na osnovu automatizirane obrade, uključujući i izradu profila, koja proizvodi negativne pravne efekte za nosioca podataka ili na njega značajno utiče, osim ako je odobreno posebnim zakonom koji propisuje odgovarajuće zaštitne mjere za prava i slobode nosioca podataka, najmanje prava na učešće fizičkog lica u donošenju odluke.
- (2) Odluka iz stava (1) ovog člana ne smije biti zasnovana na posebnim kategorijama ličnih podataka iz člana 66. ovog zakona, osim ako su uspostavljene odgovarajuće mjere zaštite prava i sloboda i legitimnih interesa nosioca podataka.

- (3) Nadležnom organu zabranjena je izrada profila koji dovodi do diskriminacije lica na osnovu posebnih kategorija ličnih podataka iz člana 66. ovog zakona.

Član 68.

(Obavješćavanje i način ostvarivanja prava nosilaca podataka)

- (1) Nadležni organ dužan je preduzeti sve odgovarajuće mjere kako bi se nosiocu podataka pružile sve informacije iz člana 69. ovog zakona te dala sva obavješćenja u vezi s članom 67, čl. 70. do 74. i članom 87. ovog zakona u vezi s obradom.
- (2) Informacije iz stava (1) ovog člana daju se u sažetoj, razumljivoj i lako dostupnoj formi, uz upotrebu jasnog i jednostavnog jezika.
- (3) Informacije iz stava (1) ovog člana pružaju se nosiocu podataka u formi u kojoj je zahtjev podnesen ili na način koji je istaknut u zahtjevu, u roku od 30 dana od dana njegovog podnošenja.
- (4) Nadležni organ dužan je olakšati ostvarivanje prava nosioca podataka iz člana 67, te čl. 70. do 74. ovog zakona.
- (5) Nadležni organ dužan je nosioca podataka pisanim putem obavijestiti o daljnjim radnjama u vezi s njegovim zahtjevom, bez odgađanja.
- (6) Nadležni organ dužan je, bez naknade, pružiti informacije, odnosno preduzeti mjere, na osnovu člana 69. ovog zakona, te sva obavješćenja pružena ili mjere preduzete na osnovu člana 67, čl. 70. do 74. ovog zakona i člana 87. ovog zakona.
- (7) Ako je zahtjev nosioca podataka očito neosnovan ili pretjeran, posebno zbog njegovog učestalog ponavljanja, nadležni organ može:
 - a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnožavanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili preduzimanja traženih mjera ili
 - b) odbiti postupiti po zahtjevu.
- (8) Teret dokazivanja očite neosnovanosti ili pretjeranosti zahtjeva iz stava (7) ovog člana je na nadležnom organu.
- (9) Ako nadležni organ ima opravdanu sumnju u vezi s identitetom fizičkog lica koje podnosi zahtjev iz čl. 70. ili 72. ovog zakona, nadležni organ može zatražiti dodatne informacije neophodne za potvrđivanje identiteta nosioca podataka.

Član 69.

(Informacije koje se stavljaju na raspolaganje ili ustupaju nosiocu podataka)

- (1) Nadležni organ dužan je nosiocu podataka staviti na raspolaganje kao minimum sljedeće informacije:
 - a) identitet i kontakt-podatke nadležnog organa;
 - b) kontakt-podatke službenika za zaštitu ličnih podataka, ako je primjenjivo;
 - c) svrhu obrade ličnih podataka;
 - d) o pravu na podnošenje prigovora Agenciji i kontakt-podacima Agencije ili tužbe nadležnom sudu;
 - e) o postojanju prava da od nadležnog organa zatraži pristup svojim ličnim podacima, njihovu ispravku ili brisanje, ili ograničenje obrade ličnih podataka.
- (2) Osim informacija iz stava (1) ovog člana, radi ostvarivanja njegovih prava, nadležni organ nosiocu podataka daje sljedeće dodatne informacije:
 - a) pravni osnov obrade ličnih podataka;
 - b) rok u kojem će se lični podaci čuvati ili, ako to nije moguće, o kriterijima korištenim za utvrđivanje tog roka;

- c) o kategorijama primalaca ličnih podataka, uključujući druge države ili međunarodne organizacije, ako je primjenjivo;
- d) prema potrebi i dodatne informacije ako se lični podaci prikupljaju bez znanja nosioca podataka.
- (3) Posebnim zakonom mogu se propisati mjere za odgađanje, ograničenje ili uskraćivanje pružanja informacija iz stava (2) ovog člana nosiocu podataka u onoj mjeri i u onom trajanju u kojem takva mjera predstavlja potrebnu i proporcionalnu mjeru u demokratskom društvu, uz poštivanje osnovnih prava i legitimnih interesa nosioca podataka, s ciljem da se:
- a) spriječi ometanje službenog i zakonom uređenog prikupljanja informacija, istraga ili postupaka;
- b) izbjegne ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca krivičnih djela ili izvršavanja krivičnih sankcija;
- c) zaštiti javna sigurnost;
- d) zaštiti državna sigurnost;
- e) zaštite prava i slobode drugih.
- (4) Posebnim zakonom mogu se propisati kategorije obrade koje mogu u cjelini ili djelimično biti obuhvaćene bilo kojom od tačaka iz stava (3) ovog člana.
- Član 70.
- (Pravo nosioca podataka na pristup ličnom podatku kod nadležnog organa)
- (1) Nadležni organ dužan je, u roku od 30 dana od dana zaprimanja zahtjeva za pristup ličnim podacima, nosiocu podataka izdati potvrdu o tome obrađuje li njegove lične podatke te ako se takvi lični podaci obrađuju, pristup ličnim podacima i informacijama o:
- a) svrsi obrade i pravnom osnovu obrade;
- b) kategoriji ličnih podataka koji se obrađuju;
- c) primaocu ili kategoriji primaoca kojem su lični podaci otkriveni, posebno primaocu u drugoj državi ili međunarodnoj organizaciji;
- d) predviđenom roku u kojem će se lični podaci čuvati, ako je to moguće, ili, ako to nije moguće, kriterijima korištenim za utvrđivanje tog roka;
- e) postojanju prava da od nadležnog organa zatraži ispravku ili brisanje svojih ličnih podataka ili ograničenje obrade ličnih podataka;
- f) pravu na podnošenje prigovora Agenciji i kontakt-podacima Agencije ili tužbe nadležnom sudu;
- g) ličnim podacima koji se obrađuju i o svim dostupnim informacijama o izvoru ličnih podataka.
- (2) Potvrda iz stava (1) ovog člana izdaje se u skladu s odredbama člana 71. ovog zakona.
- Član 71.
- (Ograničenja prava pristupa ličnom podatku)
- (1) Posebnim zakonom koji se odnosi na nadležni organ može se nosiocu podataka u cjelini ili djelimično ograničiti pravo pristupa ličnom podatku u onoj mjeri i u onom trajanju u kojem takvo djelimično ili potpuno ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštivanje osnovnih prava i legitimnih interesa nosioca podataka, kako bi se:
- a) spriječilo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka;
- b) izbjeglo ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca krivičnih djela ili izvršavanja krivičnih sankcija;
- c) zaštitila javna sigurnost;
- d) zaštitila državna sigurnost;
- e) zaštitila prava i slobode drugih.
- (2) Posebnim zakonom mogu se odrediti kategorije obrade koje mogu u cjelini ili djelimično biti obuhvaćene bilo kojom tačkom iz stava (1) ovog člana.
- (3) U slučajevima iz st. (1) i (2) ovog člana, nadležni organ dužan je, bez odgađanja, pisanim putem obavijestiti nosioca podataka o svakom odbijanju ili ograničenju pristupa ličnim podacima te o razlozima odbijanja ili ograničenja, osim ako bi pružanje takvih informacija dovelo u pitanje neku od svrha iz stava (1) ovog člana.
- (4) Nadležni organ dužan je obavijestiti nosioca podataka o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu.
- (5) Nadležni organ dužan je dokumentirati činjenične ili pravne razloge na kojima se zasniva odluka.
- (6) Dokumentacija iz stava (5) ovog člana stavlja se Agenciji na raspolaganje.
- Član 72.
- (Pravo na ispravku ili brisanje ličnog podatka i ograničenje obrade od nadležnog organa)
- (1) Nadležni organ dužan je:
- a) bez nepotrebnog odgađanja, nosiocu podataka omogućiti ispravku netačnih ličnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade podataka, nosilac podataka ima pravo dopuniti nepotpune lične podatke, između ostalog i davanjem dodatne izjave;
- b) nosiocu podataka omogućiti brisanje ličnih podataka, bez nepotrebnog odgađanja, ako se obradom krše odredbe čl. 60, 64. ili 66. ovog zakona, ili ako se lični podaci moraju brisati radi poštivanja pravne obaveze iz posebnog zakona;
- c) ograničiti obradu ako:
- 1) nosilac podataka osporava tačnost ličnih podataka, a njihovu tačnost ili netačnost nije moguće utvrditi ili
 - 2) lični podaci moraju biti sačuvani kao dokaz;
- d) obavijestiti nosioca podataka prije uklanjanja ograničenja obrade ako je obrada ograničena na osnovu tačke c) alineje 1) ovog stava;
- e) pisanim putem obavijestiti nosioca podataka o svakom odbijanju ispravke ili brisanja ličnih podataka ili ograničenja obrade te o razlozima odbijanja. Posebnim zakonom koji se odnosi na nadležni organ može se nosiocu podataka potpuno ili djelimično ograničiti pravo pristupa u onoj mjeri i u onom trajanju u kojem takvo potpuno ili djelimično ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštivanje osnovnih prava i legitimnih interesa nosioca podataka, kako bi se:
- 1) izbjeglo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka,
 - 2) izbjeglo ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca krivičnih djela ili izvršavanja krivičnih sankcija,
 - 3) zaštitila javna sigurnost,
 - 4) zaštitila državna sigurnost i
 - 5) zaštitila prava i slobode drugih;
- f) obavijestiti nosioca podataka o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu;
- g) o ispravci netačnih ličnih podataka obavijestiti nadležni organ od kojeg potiču netačni podaci.
- (2) Nadležni organ dužan je, ako su lični podaci ispravljeni ili brisani, ili je obrada bila ograničena na osnovu stava (1)

тач. а), б) или с) овог члана, обавјестити примаоца, а примаоци су дужни исправити или обрисати личне податке или ограничити обраду личних података у оквиру своје одговорности.

Члан 73.

(Остваривање права носилаца података и провјера Агенције)

- (1) Надлежни орган дужан је обавјестити носиоца података о могућности остваривања права путем приговора Агенцији или тужбе надлежном суду.
- (2) Ако је носилац података незадовољан поступком надлежног органа, може подnijети приговор Агенцији или тужбу надлежном суду, у случајевима из члана 69. став (3), члана 71. став (3) и члана 72. став (1) таčka д) овог закона.
- (3) У случају из става (1) овог члана, Агенција је дужна обавјестити носиоца података о томе да су извршене провјере и надзор као и о праву на правни лијек.

Члан 74.

(Права носилаца података у кривичним истрагама и поступцима)

Носилац података остварује права из чл. 69, 70. и 72. овог закона у складу са законима о кривичним поступцима, ако су лични подаци садржани у судској одлуци или евиденцији или спису предмета обрађени током кривичних истрага и поступака.

Члан 75.

(Обавеза надлежног органа)

- (1) Надлежни орган дужан је да примјени одговарајуће техничке и организационе мјере имајући у виду природу, обим, околности и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободу физичких лица, како би осигурао да се обрада обавља у складу с овим законом и како би то могао доказати. Те мјере се према потреби преиспитују и ажурирају.
- (2) Мјере из става (1) овог члана, ако су пропорционалне у односу на активност обраде, укључују провођење одговарајућих политика заштите података од надлежног органа.

Члан 76.

(Техничка и интегрисана заштита личног податка од надлежног органа)

- (1) Надлежни орган дужан је, узимајући у обзир најновија достигнућа и трошак провођења као и природу, обим, контекст и сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободу лица који произлазе из обраде података, и у вријеме одређивања средстава обраде и у вријеме саме обраде, примјенити одговарајуће техничке и организационе мјере, попут псеудонимизације, за омогућавање djelotворне примјене принципа заштите података, као што су смањење количине података те укључивање заштитних мјера у обраду, како би се испунили захтеви из овог закона и заштитила права носилаца података.
- (2) Мјере из става (1) овог члана односе се на количину прикупљених личних података, обим њихове обраде, рок њиховог чувања и њихову доступност, чиме се осигурава да лични подаци нису аутоматски, без интервенције физичког лица, доступни неограниченом броју лица.

Члан 77.

(Надлежни орган као заједнички контролор података)

- (1) Ако два или више надлежних органа одреде сврхе и начине обраде личних података, сматра се да су заједнички контролори података. Они на транспарентан начин међусобним споразумом одређују одговорности svakoga од њих с циљем извршавања обавеза из овог закона, посебно у вези са остваривањем права носилаца података и

дужностима svakoga од њих у вези с пружањем информација из члана 69. овог закона, осим ако су одговорности надлежних органа утврђене законом који се примјењује на те надлежне органе. Споразумом се одређује контакт-тачка за носиоца података. Законом се може одредити који од заједничких контролора података може djelovati као јединствена контакт-тачка за остваривање права носилаца података.

- (2) Независно од услова споразума из става (1) овог члана, носилац података може остваривати своја права из овог закона у односу са svakим надлежним органом и против svakog од њих.

Члан 78.

(Коришћење услуге обрађивача од надлежног органа)

- (1) Надлежни орган користи услугу само оног обрађивача који може у довољној мјери осигурати провођење одговарајућих техничких и организационих мјера propisanih овим законом.
- (2) Коришћење услуге обрађивача од надлежног органа уређује се уговором или другим правним актом којим се уређују: предмет, техничке и организационе мјере propisane овим законом, трајање обраде, обим, садржај и сврха обраде, врста личних података, категорије носилаца података те обавезе и права надлежног органа, као и да обрађивач:
 - a) djeluje само према упутствима надлежног органа;
 - b) осигурава да су се лица овлашћена за обраду личних података обавезала на поштовање повjerljivosti или да подliježu законским одредбама о повjerljivosti;
 - c) било којим одговарајућим средством помаже надлежном органу осигурати усклађеност с одредбама о правима носилаца података;
 - d) према избору надлежног органа, брише или враћа надлежном органу све личне податке након завршетка пружања услуге обраде података те брише постојеће копије, осим ако према некој законској одредби не постоји обавеза чувања личних података;
 - e) надлежном органу ставља на raspolaganje све информације потребне за придржавање одреdbи овога члана;
 - f) поштује одредбе става (3) овог члана за ангажирање другог обрађивача.
- (3) Обрађивач не може користити услугу другог обрађивача без претходног писаног одобрења надлежног органа.
- (4) По заprimanju одобрења обрађивач је дужан обавјестити надлежни орган о свим planiranim измјенама у вези с коришћењем услуге других обрађивача.
- (5) Надлежни орган може ускратити сагласност обрађивачу за коришћење услуге другог обрађивача.
- (6) Ако обрађивач утврђује сврхе и начине обраде kršeći одредбе овог закона, тај обрађивач сматра се надлежним органом у вези с обрадом која му је повjerена.

Члан 79.

(Обрада под контролом надлежног органа)

Лице које djeluje под контролом надлежног органа или обрађивача, а има приступ личним подацима, не смје обрађивати те податке без налога контролора података, осим када је то propisano посебним законом.

Члан 80.

(Евиденција о обради од надлежног органа)

- (1) Надлежни орган води евиденцију обраде за коју је одговоран. Та евиденција садржи sljedeće информације:
 - a) назив и контакт-податке надлежног органа, заједничког надлежног органа и службеника за заштиту личних података;

- b) svrhu obrade;
 - c) kategoriju primaoca kome su lični podaci otkriveni ili će mu biti otkriveni, uključujući primaoca u drugoj državi ili međunarodnoj organizaciji;
 - d) opis kategorije nosioca podataka i kategorije ličnih podataka;
 - e) upotrebu izrade profila, ako je primjenjivo;
 - f) kategoriju prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, ako je primjenjivo;
 - g) pravni osnov za postupak obrade, uključujući prijenose, kojem su lični podaci namijenjeni;
 - h) predviđene rokove za brisanje različitih kategorija ličnih podataka, ako je moguće;
 - i) opći opis tehničkih i organizaciono-sigurnosnih mjera iz člana 85. stava (1) ovog zakona, ako je moguće.
- (2) Nadležni organ osigurava da svaki obrađivač vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju u ime kontrolora podataka, a koja sadrži:
- a) ime i kontakt-podatke jednog ili više obrađivača i svakog kontrolora podataka u čije ime obrađivač djeluje te službenika za zaštitu podataka, ako je primjenjivo;
 - b) kategoriju obrade koja se provodi za svakog kontrolora podataka;
 - c) ako je primjenjivo, podatke o prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, ako za to postoji izričito uputstvo kontrolora podataka, uključujući identifikaciju te druge države ili međunarodne organizacije;
 - d) ako je moguće, opći opis tehničkih i organizaciono-sigurnosnih mjera iz člana 85. stav (1) ovog zakona.
- (3) Evidencija iz stava (1) ovog člana mora biti u pisanoj formi, što uključuje elektronsku formu.
- (4) Nadležni organ na zahtjev Agencije, prilikom nadzora, stavlja evidenciju na uvid.

Član 81.
(Zapisivanje)

- (1) Nadležni organ dužan je, kod automatiziranog sistema obrade ličnih podataka, uspostaviti pristup sistemu koji automatski bilježi najmanje sljedeće informacije o: prikupljanju, izmjeni, izvršenom uvidu, otkrivanju, uključujući prijenose te kombiniranju i brisanju. Zapisi o izvršenom uvidu i otkrivanju omogućavaju da se utvrde obrazloženje, datum i vrijeme takvih postupaka te, ako je to moguće, identitet lica koje je izvršilo uvid ili otkrilo lične podatke i identitet primaoca takvih ličnih podataka.
- (2) Zapis se upotrebljava samo u svrhe provjere zakonitosti obrade, samopraćenja i osiguranja cjelovitosti i sigurnosti ličnih podataka te za krivične postupke.
- (3) Nadležni organ na zahtjev Agencije, prilikom nadzora, stavlja zapise na uvid.

Član 82.
(Saradnja nadležnog organa i obrađivača s Agencijom)

Nadležni organ i obrađivač dužni su saradivati s Agencijom, na obrazložen i na osnovu zakona opravdan zahtjev, pri izvršavanju njene nadležnosti.

Član 83.
(Procjena uticaja na zaštitu ličnog podatka od nadležnog organa)

- (1) Nadležni organ prije obrade radi procjenu uticaja predviđenih postupaka obrade na zaštitu ličnih podataka ako je vjerovatno da će neka vrsta obrade, posebno primjenom novih tehnologija i uzimajući u obzir prirodu,

obim, kontekst i svrhe te obrade, uzrokovati visoki rizik za prava i slobode lica.

- (2) Procjena iz stava (1) ovog člana mora sadržavati najmanje opći opis predviđenih postupaka obrade, procjenu rizika za prava i slobode nosioca podataka, predviđene mjere za rizike, zaštitne i sigurnosne mjere i mehanizme kako bi se osigurala zaštita ličnih podataka i dokazala uskladenost s ovim zakonom, uzimajući u obzir prava i legitimne interese nosioca podataka i drugih uključenih lica.

Član 84.

(Prethodno savjetovanje nadležnog organa s Agencijom)

- (1) Nadležni organ ili obrađivač dužan je da se savjetuje s Agencijom prije obrade ličnih podataka koji će biti uključeni u novu zbirku ličnih podataka ako:
- a) procjena uticaja na zaštitu podataka, kako je predviđeno članom 83. ovog zakona, upućuje na to da bi obrada mogla uzrokovati visok rizik ako nadležni organ ne preduzme mjere kako bi umanjio rizik ili
 - b) vrsta obrade, posebno ako se upotrebljavaju nove tehnologije, mehanizmi ili postupci, predstavlja visok rizik za prava i slobode nosioca podataka.
- (2) Agencija može utvrditi listu postupaka obrade za koje je potrebno obaviti prethodno savjetovanje u skladu sa stavom (1) ovog člana.
- (3) Nadležni organ dužan je Agenciji dostaviti procjenu uticaja na zaštitu podataka na osnovu člana 83. ovog zakona i na njen zahtjev pružiti sve ostale informacije pomoću kojih će Agencija moći procijeniti uskladenost obrade te posebno rizike za zaštitu ličnih podataka nosioca podataka i povezane zaštitne mjere.
- (4) Agencija će u roku od 42 dana od zaprimanja pisanog zahtjeva iz stava (1) ovog člana pisanim putem dati savjet nadležnom organu te može iskoristiti bilo koje od svojih ovlaštenja, ako smatra da bi se namjeravanom obradom iz stava (1) ovog člana kršile odredbe ovog zakona, posebno ako nadležni organ nije u dovoljnoj mjeri utvrdio ili umanjio rizik.
- (5) Rok iz stava (4) ovog člana može se, prema potrebi, produžiti za 30 dana, uzimajući u obzir složenost namjeravane obrade.
- (6) Agencija u roku od 30 dana od zaprimanja zahtjeva obavještava nadležni organ i, prema potrebi, obrađivača o svakom produženju i razlozima odgađanja.
- (7) O prijedlogu zakona kojim se regulira obrada ličnih podataka, a prije njegovog upućivanja u parlamentarnu proceduru, predlagač se može prethodno savjetovati s Agencijom.

Član 85.

(Sigurnost obrade od nadležnog organa i obrađivača)

- (1) Nadležni organ i obrađivač dužni su, uzimajući u obzir najnovija dostignuća, troškove provođenja, prirodu, obim, kontekst i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica, primijeniti odgovarajuće tehničke i organizacione mjere kako bi se postigao odgovarajući nivo sigurnosti shodno riziku, posebno u vezi s obradom posebnih kategorija ličnih podataka.
- (2) U vezi s automatiziranom obradom, nadležni organ ili obrađivač, nakon procjene rizika, dužan je uspostaviti mjere koje osiguravaju da se:
- a) onemogući neovlaštenim licima pristup opremi koja se koristi za obradu;
 - b) spriječi neovlašteno čitanje, umnožavanje, mijenjanje ili uklanjanje nosača podataka;

- c) spriječiti neovlašteno unošenje ličnih podataka te neovlašteno pregledanje, mijenjanje ili brisanje čuvanih ličnih podataka;
- d) spriječiti korištenje sistema za automatsku obradu od neovlaštenog lica upotrebom opreme za prijenos podataka;
- e) lice koje je ovlašteno za korištenje sistema za automatsku obradu ima pristup samo onim ličnim podacima na koje se odnosi njegovo odobrenje za pristup;
- f) može provjeriti i utvrditi kome su lični podaci preneseni, odnosno bi mogli biti preneseni ili učinjeni dostupnim upotrebom opreme za prijenos podataka;
- g) može naknadno provjeriti, odnosno utvrditi koji su lični podaci uneseni u sistem automatske obrade te ko ih je i kada unio;
- h) spriječiti neovlašteno čitanje, umnožavanje, mijenjanje ili brisanje ličnih podataka tokom prijenosa ličnih podataka ili prijenosa nosača podataka;
- i) omogućiti ponovno uspostavljanje instaliranih sistema u slučaju prekida njihovog rada;
- j) održava ispravnu funkciju sistema, da se pojava grešaka u funkcioniranju sistema prijavi te da čuvani lični podaci ne mogu biti ugroženi zbog nedostataka u funkcioniranju sistema.

Član 86.

(Obavješćavanje Agencije o povredi ličnog podatka od nadležnog organa)

- (1) Nadležni organ dužan je u slučaju povrede ličnih podataka, bez odgađanja, a najkasnije 72 sata nakon saznanja za povredu, obavijestiti Agenciju o povredi ličnih podataka, osim ako povreda ličnih podataka ne ugrožava prava i slobode fizičkog lica.
- (2) Obradivač je dužan u slučaju povrede ličnih podataka, bez odgađanja, obavijestiti nadležni organ, nakon što sazna za povredu ličnih podataka.
- (3) Ako obavješćavanje Agencije iz stava (1) ovog člana nije izvršeno u roku od 72 sata, mora se sačiniti pisano obrazloženje s navođenjem razloga za kašnjenje.
- (4) Obavješćenje iz stava (1) ovog člana sadrži najmanje sljedeće informacije:
 - a) opis povrede ličnih podataka, uključujući, ako je moguće, kategorije i približan broj nosilaca podataka, kao i kategorije i približan broj evidencija ličnih podataka o kojima je riječ;
 - b) ime i prezime i kontakt-podatke službenika za zaštitu podataka ili druge kontakt-tačke od koje se može dobiti još informacija;
 - c) opis vjerovatne posljedice povrede ličnih podataka;
 - d) opis mjera koje je nadležni organ preduzeo ili čije je preduzimanje predložio radi rješavanja problema povrede ličnih podataka, uključujući prema potrebi i mjere za ublažavanje mogućih štetnih posljedica.
- (5) Informacije se mogu dostavljati u dijelovima, bez odgađanja, ako i u mjeri u kojoj nije moguće istovremeno dostaviti sve informacije.
- (6) Nadležni organ dokumentira svaku povredu ličnih podataka iz stava (1) ovog člana, uključujući i činjenice u vezi s povredom ličnih podataka, njene posljedice i mjere preduzete za popravljivanje situacije.
- (7) Dokumentacija iz stava (4) ovog člana mora biti dostupna Agenciji s ciljem provjere primjene ovog člana.
- (8) Nadležni organ osigurava da se, u slučaju povrede ličnih podataka koja uključuje lične podatke koje je prenio

kontrolor podataka druge države ili koji su preneseni njemu, informacije iz stava (4) ovog člana prenose kontroloru podataka te države bez nepotrebnog odgađanja.

Član 87.

(Obavješćavanje nosioca podatka o povredi ličnog podatka)

- (1) Ako je vjerovatno da će povreda ličnih podataka uzrokovati visok rizik za prava i slobode fizičkog lica, nadležni organ, bez odgađanja, obavješćava nosioca podataka o povredi ličnih podataka.
- (2) U obavješćenju iz stava (1) ovog člana se jasnim i jednostavnim jezikom opisuje priroda povrede ličnih podataka te se navode najmanje informacije i mjere iz člana 86. stav (4) tač. b), c) i d) ovog zakona.
- (3) Obavješćavanje nosioca podataka nije obavezno ako je ispunjen jedan od sljedećih uslova:
 - a) ako je nadležni organ preduzeo odgovarajuće tehničke i organizacione mjere zaštite i te mjere su primijenjene na lične podatke u vezi s kojima je došlo do povrede ličnih podataka, a prije svega mjere koje lične podatke čine nerazumljivim licu koje nije ovlašteno pristupiti im, kao što je enkripcija;
 - b) ako je kontrolor podataka preduzeo naknadne mjere kojima se osigurava da više nije vjerovatno da će doći do visokog rizika za prava i slobode nosioca podataka;
 - c) ako bi to zahtijevalo neproporcionalan napor. U tom slučaju se objavljuje javno obavješćenje ili se preduzima slična mjera kojom se nosioci podataka obavješćavaju na jednako djelotvoran način.
- (4) Ako nadležni organ do tog trenutka nije obavijestio nosioca podataka o povredi ličnih podataka, Agencija, nakon razmatranja stepena vjerovatnoće da će povreda ličnih podataka uzrokovati visok rizik, može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uslova iz stava (3) ovog člana.
- (5) Obavješćavanje nosioca podataka može se odgoditi, ograničiti ili uskratiti u skladu sa uslovima i na osnovu razloga iz člana 69. stav (3) ovog zakona.

Član 88.

(Imenovanje službenika za zaštitu ličnih podataka od nadležnog organa)

- (1) Nadležni organ dužan je imenovati službenika za zaštitu ličnih podataka.
- (2) Sudovi i drugi nezavisni pravosudni organi kada postupaju u okviru svoje pravosudne nadležnosti nisu dužni imenovati službenika za zaštitu ličnih podataka.
- (3) Službenik za zaštitu ličnih podataka imenuje se na osnovu njegovih stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksi iz oblasti zaštite ličnih podataka i sposobnosti obavljanja zadataka iz člana 90. ovog zakona.
- (4) Više nadležnih organa može imenovati jednog službenika za zaštitu ličnih podataka, uzimajući u obzir njihovu organizacionu strukturu i veličinu.
- (5) Nadležni organ dužan je objaviti kontakt-podatke službenika za zaštitu ličnih podataka i saopćiti ih Agenciji.

Član 89.

(Radno mjesto službenika za zaštitu ličnih podataka nadležnog organa)

- (1) Nadležni organ dužan je osigurati da službenik za zaštitu ličnih podataka bude na odgovarajući način i blagovremeno uključen u sva pitanja koja se tiču zaštite ličnih podataka.

- (2) Nadležni organ dužan je podržavati službenika za zaštitu ličnih podataka u izvršavanju zadataka pružajući mu potrebna sredstva za izvršavanje tih zadataka i pristup ličnim podacima i postupcima obrade, kao i za održavanje njegovog stručnog znanja.

Član 90.

(Zadaci službenika za zaštitu ličnih podataka nadležnog organa)
Nadležni organ službeniku za zaštitu ličnih podataka povjerava najmanje sljedeće zadatke:

- informiranost i savjetovanje nadležnog organa i zaposlenih koji rade obradu o njihovim obavezama iz ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka;
- praćenje primjene ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka, kao i politika nadležnog organa u vezi sa zaštitom ličnih podataka, uključujući i podjelu odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji učestvuju u radnjama obrade, kao i s tim povezanim revizijama;
- pružanje savjeta, kada je to zahtijevano, u vezi s procjenom uticaja na zaštitu ličnih podataka i praćenje njenog izvršavanja u skladu s članom 83. ovog zakona;
- saradnju s Agencijom;
- djelovanje kao kontakt-tačka za Agenciju o pitanjima koja se tiču obrade, što uključuje i prethodno savjetovanje iz člana 84. ovog zakona te savjetovanje, po potrebi, o svim drugim pitanjima.

Član 91.

(Opći principi prijenosa ličnog podatka u drugu državu ili međunarodnu organizaciju od nadležnog organa)

- (1) Nadležni organ dužan je svaki prijenos ličnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u drugu državu ili međunarodnu organizaciju, uključujući daljnji prijenos u još jednu drugu državu ili međunarodnu organizaciju, izvršavati pridržavajući se odredbi ovog dijela zakona, samo ako su ispunjeni sljedeći uslovi, i to:
 - prijenos je neophodan u svrhe utvrđene u članu 1. stav (1) tačka c) ovog zakona;
 - lični podaci prenose se nadležnom organu u drugoj državi ili međunarodnoj organizaciji, koji predstavlja javni organ nadležan za potrebe iz člana 1. stav (1) tačka c) ovog zakona;
 - ako su lični podaci preneseni ili stavljeni na raspolaganje iz druge države, ta je država dala prethodno odobrenje za prijenos u skladu sa svojim pravom;
 - ako je Vijeće ministara Bosne i Hercegovine, na prijedlog Agencije, donijelo odluku o adekvatnosti iz člana 92. stav (3) ovog zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o adekvatnosti iz člana 92. stav (3) ovog zakona, moraju biti osigurane ili postoje odgovarajuće zaštitne mjere iz člana 93. ovog zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o adekvatnosti iz člana 92. stav (3) ovog zakona i nisu osigurane ili ne postoje odgovarajuće zaštitne mjere iz člana 93. ovog zakona, primjenjuju se odstupanja za posebne situacije iz člana 94. ovog zakona;
 - u slučaju daljnjeg prijenosa u još jednu drugu državu ili međunarodnu organizaciju, nadležni organ koji je izvršio prvi prijenos ili drugi nadležni organ u Bosni

i Hercegovini može, nakon što je uzeo u obzir sve relevantne činjenice, uključujući ozbiljnost krivičnog djela, svrhu u koju su lični podaci prvo preneseni i nivo zaštite ličnih podataka u drugoj državi ili međunarodnoj organizaciji, odobriti daljnji prijenos.

- (2) Nadležnom organu dopušten je prijenos, bez prethodnog odobrenja druge države, u skladu sa stavom (1) tačka c) ovog člana, izuzetno, ako je prijenos ličnih podataka potreban za sprečavanje neposredne i ozbiljne prijetnje javnoj sigurnosti Bosne i Hercegovine ili druge države ili bitnim interesima Bosne i Hercegovine, a prethodno odobrenje se ne može blagovremeno dobiti.
- (3) Nadležni organ dužan je obavijestiti organ u drugoj državi, odgovoran za izdavanje prethodnog odobrenja, o slučaju iz stava (2) ovog člana.
- (4) Sve odredbe u vezi s prijenosom ličnih podataka u drugu državu ili međunarodnu organizaciju primjenjuju se kako bi se osiguralo da se ne ugrozi nivo zaštite fizičkih lica koji je zagarantiran ovim dijelom zakona.

Član 92.

(Prijenos od nadležnog organa na osnovu odluke o adekvatnosti)

- (1) Prijenos ličnih podataka u drugu državu ili međunarodnu organizaciju može se vršiti ako Vijeće ministara Bosne i Hercegovine odluči da druga država, teritorija, ili jedan ili više konkretnih sektora unutar te druge države, ili međunarodna organizacija osigurava adekvatan nivo zaštite, i u tom slučaju takav prijenos ne zahtijeva posebno odobrenje.
- (2) Smatra se da je adekvatan nivo zaštite iz stava (1) ovog člana osiguran u državi, dijelovima njene teritorije, ili jednom ili više sektora u toj državi, međunarodnoj organizaciji, za koje je od Evropske unije utvrđeno da osiguravaju adekvatan nivo zaštite ličnih podataka.
- (3) Odluku o adekvatnosti nivoa zaštite ličnih podataka iz stava (1) ovog člana donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stava (3) ovog člana uzimajući u obzir:
 - vladavinu prava, poštovanje ljudskih prava i osnovnih sloboda, relevantno opće i sektorsko zakonodavstvo, što uključuje zakonodavstvo o javnoj sigurnosti, odbrani, državnoj sigurnosti, krivično pravo i pristup javnih organa ličnim podacima, kao i primjenu tog zakonodavstva, pravila o zaštiti ličnih podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos ličnih podataka u još jednu drugu državu ili međunarodnu organizaciju, koja se poštuju u toj drugoj državi ili međunarodnoj organizaciji, sudsku praksu, kao i postojanje djelatovnih i provedivih prava nosilaca podataka i efikasnu upravnu i sudsku zaštitu nosilaca podataka;
 - postojanje i efikasno funkcioniranje jednog ili više nezavisnih nadzornih organa u drugoj državi ili organa kojem podliježe međunarodna organizacija, odgovornih za osiguravanje i provođenje pravila o zaštiti podataka, što uključuje adekvatna izvršna ovlaštenja za pružanje pomoći nosiocima podataka u ostvarivanju njihovih prava, kao i za saradnju s Agencijom;
 - međunarodne obaveze koje je druga država ili međunarodna organizacija preuzela ili druge obaveze koje proizlaze iz pravnoobavezujućih konvencija ili instrumenata, kao i iz njenog učešća u

- multilateralnim ili regionalnim organizacijama, posebno u vezi sa zaštitom ličnih podataka.
- (5) Agencija kontinuirano prati stanje u oblasti zaštite ličnih podataka u drugoj državi, dijelu njene teritorije, jednom ili više sektora unutar te države ili međunarodnoj organizaciji i o tome po potrebi izvještava Vijeće ministara Bosne i Hercegovine.
 - (6) Izvještaj iz stava (5) ovog člana uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija, koje su značajne za preispitivanje postojanja adekvatnog nivoa zaštite ličnih podataka, na osnovu čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stava (3) ovog člana.
 - (7) Odluka donesena na osnovu stava (3) ovog člana ne dovodi u pitanje prijenos ličnih podataka u drugu državu, na teritoriji ili u jedan ili više određenih sektora unutar te druge države ili međunarodnu organizaciju, u skladu s čl. 93. i 94. ovog zakona.
 - (8) Lista država, dijela njihovih teritorija, jedan ili više sektora unutar tih država i međunarodnih organizacija, u vezi s kojim je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju adekvatan nivo zaštite ličnih podataka objavljuje se u "Službenom glasniku BiH" i na službenoj internetskoj stranici Agencije.

Član 93.

(Prijenos od nadležnog organa na koji se primjenjuju odgovarajuće zaštitne mjere)

- (1) Nadležni organ može izvršiti prijenos ličnih podataka u drugu državu ili međunarodnu organizaciju, ako nije donesena odluka na osnovu člana 92. stav (3) ovog zakona, uz sljedeće uslove:
 - a) ako su odgovarajuće zaštitne mjere u vezi sa zaštitom ličnih podataka predviđene u pravnoobavezujućem instrumentu ili
 - b) ako je nadležni organ procijenio sve okolnosti u vezi s prijenosom ličnih podataka i zaključio da postoje odgovarajuće zaštitne mjere u vezi sa zaštitom ličnih podataka.
- (2) Nadležni organ dužan je obavijestiti Agenciju o kategorijama prijenosa u skladu sa stavom (1) tačka b) ovog člana.
- (3) Kada se prijenos ličnih podataka zasniva na stavu (1) tačka b) ovog člana, nadležni organ dužan je takav prijenos dokumentirati, a dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom organu koji je dobio podatke, obrazloženje prijenosa i koji su lični podaci preneseni.

Član 94.

(Odstupanje u posebnim slučajevima prijenosa ličnog podatka od nadležnog organa)

- (1) Ako ne postoji odluka o adekvatnosti iz člana 92. stav (3) ovog zakona ili odgovarajuće zaštitne mjere iz člana 93. ovog zakona, prijenos ili skup prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju vrši se samo ako je prijenos neophodan i ako ispunjava jedan od sljedećih uslova:
 - a) kako bi se zaštitili ključni interesi nosioca podataka ili drugog lica;
 - b) kako bi se zaštitili legitimni interesi nosioca podataka, ako je to predviđeno posebnim zakonom;
 - c) kako bi se spriječila neposredna i ozbiljna prijetnja javnoj sigurnosti na teritoriji Bosne i Hercegovine ili druge države;

- d) u pojedinačnim slučajevima u svrhe navedene u članu 1. stavu (1) tački c) ovog zakona ili
- e) u pojedinačnom slučaju radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva u vezi sa svrhama navedenim u članu 1. stavu (1) tački c) ovog zakona.
- (2) Lični podaci ne smiju se prenositi ako nadležni organ koji obavlja prijenos utvrdi da osnovna prava i slobode odnosno nosioca podataka imaju prednost pred javnim interesom u vezi s prijenosom iz stava (1) tač. d) i e) ovog člana.
- (3) Ako se prijenos obavlja na osnovu stava (1) ovog člana, nadležni organ dužan je takav prijenos dokumentirati i dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom organu koji je dobio podatke, obrazloženje prijenosa i koji su lični podaci preneseni.

Član 95.

(Prijenos ličnog podatka primaocu sa sjedištem ili poslovnim nastanom u drugoj državi)

- (1) Nadležni organ može, u skladu s posebnim zakonom, odstupajući od člana 91. stav (1) tačka b) ovog zakona i ne dovodeći u pitanje nijedan međunarodni sporazum iz stava (2) ovog člana, u pojedinačnim i posebnim slučajevima, prenijeti lične podatke direktno primaocima sa sjedištem ili poslovnim nastanom u drugoj državi samo ako se pridržavaju odredbi ovog dijela zakona i ako su ispunjeni sljedeći uslovi:
 - a) ako je prijenos isključivo neophodan za obavljanje zadatka nadležnog organa koji obavlja prijenos kako je predviđeno posebnim zakonom u svrhe navedene u članu 1. stav (1) tačka c) ovog zakona;
 - b) ako nadležni organ koji obavlja prijenos utvrdi da osnovna prava i slobode dotičnog nosioca podataka nemaju prednost nad javnim interesom koji iziskuje prijenos u predmetnom slučaju;
 - c) ako nadležni organ koji obavlja prijenos smatra da je prijenos organu nadležnom za postupanje u svrhu iz člana 1. stav (1) tačka c) ovog zakona u drugu državu nedjelotvoran ili neprimjeren, posebno zato što se prijenos ne može pravovremeno ostvariti;
 - d) ako je organ koji je u drugoj državi nadležan za postupanje u svrhu iz člana 1. stav (1) tačka c) ovog zakona obaviješten bez odgađanja, osim ako je to nedjelotvorno ili neprimjereno;
 - e) ako nadležni organ koji obavlja prijenos obavijesti primaoca o određenoj svrsi ili svrhama u koje taj primalac isključivo može obrađivati lične podatke, samo ako je takva obrada neophodna.
- (2) Međunarodni sporazum iz stava (1) ovog člana je svaki bilateralni ili multilateralni međunarodni sporazum na snazi između Bosne i Hercegovine i druge države u oblasti pravosudne saradnje u krivičnim stvarima i policijske saradnje.
- (3) Nadležni organ koji obavlja prijenos dužan je obavijestiti Agenciju o prijenosima u skladu s ovim članom.
- (4) Nadležni organ koji obavlja prijenos ličnih podataka na osnovu stava (1) ovog člana dužan je takav prijenos dokumentirati.

DIO ČETVRTI – AGENCIJA ZA ZAŠTITU LIČNIH PODATAKA U BOSNI I HERCEGOVINI

Član 96.

(Agencija)

- (1) Agencija je nezavisan nadzorni organ za praćenje primjene ovog zakona, s ciljem zaštite osnovnih prava i

sloboda fizičkih lica u vezi s obradom ličnih podataka u Bosni i Hercegovini.

- (2) Sjedište Agencije je u Sarajevu.
- (3) Na sva pitanja organizacije i upravljanja te druga pitanja značajna za funkcioniranje Agencije primjenjuju se propisi kojima se regulira organizacija rada organa uprave, osim ako nije drugačije propisano ovim zakonom.

Član 97.

(Nezavisnost Agencije)

- (1) Agencija djeluje potpuno nezavisno pri obavljanju svojih nadležnosti u skladu s ovim zakonom.
- (2) Direktor, zamjenik direktora i zaposleni u Agenciji, pri obavljanju svojih dužnosti i ovlaštenja u skladu s ovim zakonom, ne smiju biti izloženi neposrednom ili posrednom vanjskom uticaju i ne smiju ni od koga tražiti ili primati instrukcije.
- (3) Direktor, zamjenik direktora i zaposleni u Agenciji moraju se sudržavati od svih radnji koje nisu u skladu s njihovim dužnostima i tokom svog mandata i zaposlenja ne smiju se baviti nespojivom djelatnošću, bez obzira na to da li je ona plaćena ili ne.
- (4) Agencija mora imati ljudske, tehničke i finansijske resurse, prostorije i infrastrukturu potrebne za efikasno obavljanje svojih nadležnosti, uključujući i ovlaštenja koja se odnose na međunarodnu uzajamnu pomoć i saradnju.
- (5) Zaposleni u Agenciji su državni službenici i zaposlenici i na njih se primjenjuju Zakon o državnoj službi u institucijama Bosne i Hercegovine i Zakon o radu u institucijama Bosne i Hercegovine.
- (6) Pravilnik o unutrašnjoj organizaciji Agencije, na prijedlog direktora Agencije, odobrava Parlamentarna skupština Bosne i Hercegovine.
- (7) Agencija, u skladu s odredbama Zakona o finansiranju institucija Bosne i Hercegovine, priprema nacrt godišnjeg budžeta i dostavlja ga parlamentarnoj komisiji na odobravanje. Agencija, nakon dobivanja odobrenja parlamentarne komisije, u skladu s rokovima propisanim odredbama Zakona o finansiranju institucija Bosne i Hercegovine, dostavlja Ministarstvu finansija i trezora Bosne i Hercegovine nacrt budžeta radi uvrštavanja u budžet institucija Bosne i Hercegovine i međunarodnih obaveza Bosne i Hercegovine. Ministarstvo finansija i trezora Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine i Predsjedništvo Bosne i Hercegovine mogu dati mišljenje o nacrtu budžeta Agencije, bez mogućnosti izmjene nacrta budžeta koji je prethodno odobrila parlamentarna komisija.
- (8) Agencija podliježe finansijskoj kontroli u skladu s propisima o finansijskoj kontroli.

Član 98.

(Rukovođenje Agencijom)

- (1) Agencijom rukovodi direktor.
- (2) Direktor ima jednog zamjenika.
- (3) Zamjenik direktora zamjenjuje direktora u obavljanju poslova, ako direktor nije u mogućnosti obavljati poslove u skladu sa svojim ovlaštenjima i obavezama.
- (4) Direktor je odgovoran za zakonit rad Agencije.

Član 99.

(Uslovi za imenovanje, privremena suspenzija i razrješenje direktora i zamjenika direktora)

- (1) Direktora i zamjenika direktora imenuje Parlamentarna skupština Bosne i Hercegovine (u daljnjem tekstu: Parlamentarna skupština) na osnovu javnog konkursa.
- (2) Direktor i zamjenik direktora imenuju se na period od šest godina uz mogućnost još jednog ponovnog imenovanja.

- (3) Uslovi za imenovanje direktora i zamjenika direktora su:

- a) da je stariji od 18 godina;
- b) da je državljanin Bosne i Hercegovine (svi državljani Federacije BiH, Republike Srpske i Brčko Distrikta BiH su državljani Bosne i Hercegovine);
- c) da nije osuđivan i da se protiv njega ne vodi krivični postupak;
- d) da nije obuhvaćen odredbom člana IX.1. Ustava Bosne i Hercegovine;
- e) da je zdravstveno sposoban;
- f) da ima završen fakultet društvenog smjera, VSS/VII stepen ili visoko obrazovanje bolonjskog sistema studiranja s najmanje 240 ECTS bodova;
- g) da ima najmanje 10 godina radnog iskustva u struci, od čega najmanje pet godina radnog iskustva na poslovima rukovođenja;
- h) da ima stručna znanja i iskustva iz oblasti zaštite ličnih podataka;
- i) da nije član političke stranke;
- (4) Parlamentarna skupština može privremeno suspendirati direktora i zamjenika direktora ako se otkrije teška povreda službene dužnosti. Privremena suspenzija traje dok se teška povreda službene dužnosti ne utvrdi konačnom odlukom.
- (5) Parlamentarna skupština može razriješiti direktora i zamjenika direktora prije isteka mandata:
 - a) na njegov zahtjev;
 - b) ako se utvrdi teška povreda službene dužnosti;
 - c) kada navrš 65 godina života i najmanje 20 godina staža osiguranja ili 40 godina staža osiguranja, nezavisno od godina života;
 - d) ako više ne ispunjava uslove potrebne za imenovanje.

Član 100.

(Nespojivost funkcije i obaveza čuvanja profesionalne tajne)

- (1) Direktor i zamjeniku direktora kao i zaposlenima u Agenciji zabranjeni su djelovanje, poslovanje i pogodnosti koje nisu u skladu s principom nezavisnosti i nepristranosti, za vrijeme trajanja mandata, odnosno radnog odnosa i jednu godinu nakon njegovog prestanka.
- (2) Direktor, zamjenik direktora i zaposleni u Agenciji, za vrijeme trajanja mandata, odnosno radnog odnosa, i nakon prestanka mandata, odnosno radnog odnosa, dužni su čuvati profesionalnu tajnu koja se odnosi na sve povjerljive informacije koje saznaju prilikom obavljanja svojih dužnosti ili ovlaštenja, u skladu s propisima u Bosni i Hercegovini. Tokom trajanja njihovog mandata, dužnost čuvanja profesionalne tajne posebno se odnosi na prijave fizičkih lica o kršenjima ovog zakona.

Član 101.

(Nadležnosti Agencije)

- (1) Agencija je nadležna za:
 - a) obavljanje zadataka i ovlaštenja dodijeljenih ovim zakonom;
 - b) nadzor postupaka obrade ličnih podataka koje obavljaju kontrolori podataka i obrađivači.
- (2) Agencija nije nadležna za nadzor postupaka obrade ličnih podataka koje obavljaju sudovi kada obavljaju sudsku funkciju.

Član 102.

(Zadaci Agencije)

- (1) Agencija obavlja sljedeće zadatke:
 - a) prati i primjenjuje ovaj zakon;
 - b) promovira javnu svijest o rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom ličnih

- podataka te njihovo razumijevanje, a posebnu pažnju posvećuje aktivnostima koje su izričito namijenjene djeci;
- c) savjetuje, u skladu s ovim zakonom, javne organe i druge institucije i organe o zakonodavnim i upravnim mjerama u vezi sa zaštitom prava i sloboda fizičkih lica u vezi s obradom;
- d) podiže svijest kontrolora podataka i obrađivača o njihovim obavezama iz ovog zakona;
- e) na zahtjev svakog nosioca podataka pruža informacije u vezi sa ostvarivanjem njegovih prava iz ovog zakona;
- f) razmatra prigovor nosioca podataka ili organa, organizacije ili udruženja u skladu s članom 111. ovog zakona i u roku od 90 dana donosi rješenje po prigovoru, o čemu obavještava podnosioca prigovora;
- g) provodi provjere u vezi s primjenom ovog zakona, između ostalog i na osnovu informacija primljenih od javnih organa;
- h) prati bitna kretanja, u mjeri u kojoj utiču na zaštitu ličnih podataka, a posebno razvoj informacionih i komunikacionih tehnologija i komercijalnih praksi;
- i) donosi standardne ugovorne klauzule iz člana 30. stav (8) i člana 48. stav (3) ovog zakona;
- j) utvrđuje i vodi spisak obrada u vezi s obavezom obavljanja procjene uticaja na zaštitu podataka u skladu s članom 37. stav (4) ovog zakona;
- k) daje savjete o postupku obrade ličnih podataka iz člana 38. stav (2) ovog zakona i člana 84. stav (4) ovog zakona;
- l) podstiče izradu kodeksa ponašanja i daje mišljenje i odobrava takve kodekse ponašanja koji pružaju dovoljne zaštitne mjere u skladu s članom 42. stav (5) ovog zakona;
- m) podstiče uspostavljanje mehanizama certifikacije zaštite podataka, kao i pečata i oznaka za zaštitu podataka u skladu s članom 44. stav (1) ovog zakona i odobrava kriterije certifikacije u skladu s članom 44. stav (6) ovog zakona;
- n) u određenim slučajevima periodično preispituje izdate certifikate u skladu s članom 44. st. (8) i (9) ovog zakona;
- o) sačinjava i objavljuje kriterije za akreditaciju organa za praćenje kodeksa ponašanja u skladu s članom 43. ovog zakona i akreditaciju certifikacionog organa u skladu s članom 45. ovog zakona;
- p) akreditira organe za praćenje kodeksa ponašanja u skladu s članom 43. ovog zakona te akreditira certifikacioni organ u skladu s članom 45. ovog zakona;
- r) odobrava odgovarajuće zaštitne mjere iz člana 48. stav (4) ovog zakona;
- s) odobrava obavezujuća poslovna pravila u skladu s članom 49. ovog zakona;
- t) vodi internu evidenciju o kršenjima ovog zakona i mjerama koje su preduzete u skladu s članom 103. stav (2) ovog zakona;
- u) daje mišljenje na prijedlog zakona institucijama na nivou Bosne i Hercegovine, koji se odnosi na obradu ličnih podataka;
- v) izvršava sve ostale zadatke u vezi sa zaštitom ličnih podataka.
- (2) Agencija propisuje izgled i sadržaj obrasca za podnošenje prigovora.
- (3) Agencija obavlja zadatke besplatno za nosioce podataka i, ako je to primjenjivo, i za službenike za zaštitu ličnih podataka.
- (4) Agencija obavlja zadatke besplatno za nosioce podataka i za službenike za zaštitu ličnih podataka iz DIJELA TREĆEG ovog zakona.
- (5) Ako su zahtjevi nosilaca podataka očito neosnovani ili pretjerani, posebno zbog učestalog ponavljanja, Agencija može da naplati naknadu stvarnih administrativnih troškova ili da odbije da postupi po zahtjevu, pri čemu Agencija snosi teret dokazivanja očite neosnovanosti ili pretjeranosti zahtjeva.
- (6) Agencija naplaćuje naknadu za izdavanje akreditacije certifikacionom organu.
- (7) Agencija naplaćuje naknadu za davanje mišljenja i drugih usluga, poslovnim subjektima u svrhu obavljanja njihove redovne djelatnosti.
- (8) Kriterije za određivanje visine naknade iz st. (5), (6) i (7) ovog člana utvrđuje Agencija uz prethodnu saglasnost Vijeća ministara Bosne i Hercegovine i oni se objavljuju u "Službenom glasniku BiH".
- (9) Naknada se uplaćuje na Jedinствени račun trezora institucija Bosne i Hercegovine.
- Član 103.
(Ovlaštenja Agencije)
- (1) Agencija ima sljedeća ovlaštenja:
- a) preispituje certifikate izdate u skladu s članom 44. st. (8) i (9) ovog zakona;
- b) provodi inspeksijske nadzore;
- c) obavlja reviziju zaštite podataka;
- d) nalaže kontroloru podataka i obrađivaču, a prema potrebi i predstavniku kontrolora podataka ili obrađivača, dostavljanje svih informacija potrebnih za obavljanje njenih zadataka;
- e) obavještava kontrolora podataka ili obrađivača o navodnom kršenju ovog zakona;
- f) ostvaruje pristup svim ličnim podacima i svim informacijama u posjedu kontrolora podataka i obrađivača, koji su potrebni za obavljanje njenih zadataka;
- g) ostvaruje pristup svim prostorijama kontrolora podataka i obrađivača, u kojima se obavlja obrada ličnih podataka, uključujući svu opremu i sredstva za obradu podataka.
- (2) Agencija ima sljedeća korektivna ovlaštenja:
- a) izriče upozorenja kontroloru podataka ili obrađivaču da bi namjeravane obrade mogle lako predstavljati kršenje ovog zakona;
- b) izriče opomenu kontroloru podataka ili obrađivaču ako se obradom krši ovaj zakon;
- c) nalaže kontroloru podataka ili obrađivaču da postupi po zahtjevu nosioca podataka za ostvarivanje njegovih prava u skladu s ovim zakonom;
- d) nalaže kontroloru podataka ili obrađivaču da obrade, ako je potrebno, uskladi s odredbama ovog zakona na tačno određen način i u tačno zadatom roku;
- e) nalaže kontroloru podataka da nosioca podataka obavijesti o povredi ličnih podataka;
- f) privremeno ili trajno ograničava ili zabranjuje obradu;
- g) nalaže ispravljanje ili brisanje ličnih podataka ili ograničenje obrade i obavještavanje o takvim radnjama primalaca kojima su lični podaci otkriveni;
- h) oduzima certifikat izdat u skladu s čl. 44. i 45. ovog zakona ili nalaže certifikacionom organu da ne izda certifikat ako zahtjevi za certifikaciju nisu ispunjeni

- ili da povuče certifikat ako zahtjevi više nisu ispunjeni;
- i) izdaje prekršajni nalog u okviru prekršajnog postupka ili podnosi zahtjev za pokretanje prekršajnog postupka u skladu s ovim zakonom;
 - j) nalaže privremeno obustavljanje prijenosa podataka primaocu u drugoj državi ili međunarodnoj organizaciji.
- (3) Agencija ima sljedeća ovlaštenja u vezi s odobravanjem i savjetovanjem:
- a) savjetuje kontrolora podataka u skladu s postupkom prethodnog savjetovanja iz čl. 38. i 84. ovog zakona;
 - b) daje mišljenja o svim pitanjima koja se tiču zaštite ličnih podataka, na vlastitu inicijativu ili na zahtjev zakonodavnih organa, vlada ili, u slučajevima kada je to posebnim zakonom propisano, drugim institucijama i organima, kao i javnosti;
 - c) odobrava obradu iz člana 38. stav (8) ovog zakona ako je posebnim zakonom propisano takvo prethodno odobrenje;
 - d) daje mišljenja i odobrava nacрте kodeksa ponašanja u skladu s članom 42. stav (5) ovog zakona;
 - e) akreditira certifikacione organe u skladu s članom 45. ovog zakona;
 - f) odobrava kriterije certifikacije u skladu s članom 44. stav (6) ovog zakona;
 - g) usvaja standardne klauzule o zaštiti podataka iz člana 30. stav (8) i člana 48. stav (3) ovog zakona;
 - h) odobrava odgovarajuće zaštitne mjere iz člana 48. stav (4) tačka a) ovog zakona;
 - i) odobrava odgovarajuće zaštitne mjere iz člana 48. stav (4) tačka b) ovog zakona;
 - j) odobrava obavezujuća poslovna pravila u skladu s članom 49. ovog zakona.
- (4) Odluka Agencije je konačna u upravnom postupku i protiv nje nije dopuštena žalba, ali se može pokrenuti upravni spor pred Sudom Bosne i Hercegovine.
- (5) Agencija u postupku odlučivanja primjenjuje pravila upravnog postupka, osim ako ovim zakonom nije drugačije propisano.
- (6) Agencija je ovlaštena da po potrebi obavijesti nadležne istražne organe o povredama ovog zakona ili pokrene pravne postupke, ili u tim postupcima na drugi način učestvuje kako bi se proveo ovaj zakon.
- (7) Svaka obrada ličnih podataka koji imaju određen stepen tajnosti na osnovu posebnog zakona provodi se u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.
- (8) Obradu ličnih podataka iz stava (7) ovog člana provode službenici Agencije koji imaju dozvolu za pristup tajnim podacima, u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.
- Član 104.
- (Međunarodna saradnja radi zaštite ličnih podataka)
- Agencija preduzima odgovarajuće mjere u vezi s drugim državama i međunarodnim organizacijama radi:
- a) razvoja mehanizama međunarodne saradnje za olakšavanje efikasne primjene zakonodavstva o zaštiti ličnih podataka;
 - b) osiguravanja uzajamne međunarodne pomoći u primjeni zakonodavstva o zaštiti ličnih podataka, što podrazumijeva obavještanje, upućivanje prigovora, pružanje pomoći u istragama i razmjenu informacija, u skladu s odgovarajućim mjerama za zaštitu ličnih podataka i drugim osnovnim pravima i slobodama;
 - c) uključivanja relevantnih interesnih grupa u raspravu i aktivnosti čiji je cilj unapređenje međunarodne saradnje na provođenju zakonodavstva o zaštiti ličnih podataka;
 - d) promoviranje razmjene i dokumentiranja zakonodavstva i prakse u vezi sa zaštitom ličnih podataka, uključujući i sporove u vezi s nadležnošću s drugim državama.
- Član 105.
- (Povjerljivo prijavljivanje povreda zakona)
- (1) Nadležni organ koji obrađuje lične podatke u svrhe iz člana 1. stav (1) tačka c) ovog zakona dužan je osigurati primjenu efikasnih mehanizama za povjerljivo prijavljivanje slučajeva povrede ovog zakona.
 - (2) Mehanizmi koji se primjenjuju u skladu sa stavom (1) ovog člana moraju osigurati da se povreda može prijaviti nadležnom organu ili Agenciji.
 - (3) Ovi mehanizmi uključuju podizanje svijesti o zaštiti ličnih podataka i mjere o zaštiti lica koja prijavljuju povrede.
- Član 106.
- (Izvjestaji Agencije)
- (1) Agencija podnosi Parlamentarnoj skupštini godišnji izvještaj o zaštiti ličnih podataka za proteklu godinu najkasnije do kraja juna tekuće godine i čini ga dostupnim javnosti.
 - (2) Godišnji izvještaj o zaštiti ličnih podataka iz stava (1) ovog člana sadrži podatke o:
 - a) svim aktivnostima Agencije a posebno o vrstama povreda ličnih podataka i mjerama koje su preduzete;
 - b) stanju zaštite ličnih podataka u Bosni i Hercegovini;
 - c) ključnim pitanjima iz oblasti zaštite ličnih podataka;
 - d) kapacitetima Agencije.
- Član 107.
- (Inspeksijski nadzor)
- (1) Inspeksijski nadzor nad provođenjem ovog zakona obavlja inspektor Agencije.
 - (2) Inspektor svoj identitet, svojstvo i ovlaštenje dokazuje legitimacijom inspektora.
 - (3) Inspeksijskim nadzorom ostvaruje se neposredan uvid u zakonitost rada i postupanje kontrolora podataka i obrađivača s ciljem provjere usklađenosti njegovog rada s ovim zakonom i drugim propisima koji se odnose na zaštitu ličnih podataka.
 - (4) Inspeksijski nadzor može biti redovni, vanredni i revizijski.
 - (5) Redovni inspeksijski nadzor provodi se na osnovu godišnjeg i mjesečnog plana inspeksijskog nadzora, koji se donosi na nivou Agencije.
 - (6) Rješenje iz redovnog inspeksijskog nadzora donosi inspektor, protiv kojeg je dozvoljena žalba direktoru Agencije u roku od 15 dana od dana prijema rješenja.
 - (7) Vanredni inspeksijski nadzor provodi se na osnovu prigovora ili postupanja po službenoj dužnosti kada je, u odnosu na konkretni slučaj, potrebno izvršiti inspeksijski nadzor.
 - (8) Zapisnik iz vanrednog inspeksijskog nadzora je dokazno sredstvo u postupku po prigovoru ili po službenoj dužnosti, koji provodi i rješava Agencija.
 - (9) Revizijski inspeksijski nadzor provodi se nakon redovnog ili vanrednog inspeksijskog nadzora s ciljem provjere izvršenja naloženih upravnih mjera.
 - (10) Rješenje u postupku nakon izvršenog vanrednog i revizijskog inspeksijskog nadzora donosi direktor Agencije i ono je konačno u upravnom postupku.

- (11) Nakon provedenog inspeksijskog nadzora, inspektor sastavlja zapisnik o utvrđenom činjeničnom stanju, koji potpisuju inspektor i ovlašteno lice kontrolora podataka ili obrađivača.
- (12) Inspektor ima pravo pregledati sve poslovne prostorije i objekte u kojima se obrađuju lični podaci, proces rada, uređaje, isprave i dokumentaciju, kao i obavljati druge radnje u vezi sa svrhom inspeksijskog nadzora, u skladu s članom 103. stav (1) tač. f) i g) i članom 103. st. (7) i (8) ovog zakona.
- (13) Kontrolor podataka i obrađivač dužni su inspektoru omogućiti nesmetano provođenje inspeksijskog nadzora.
- (14) Ako se inspektoru u toku inspeksijskog nadzora onemogućava provođenje nadzora ili pruži fizički otpor, ili ako se taj otpor osnovano očekuje, inspektor može zatražiti pomoć policije.
- (15) O izvršenom inspeksijskom nadzoru inspektor vodi evidenciju.

DIO PETI – PRAVNA SREDSTVA, ODGOVORNOST I KAZNE

Član 108.

(Pravo na prigovor Agenciji)

- (1) Nosilac podataka ima pravo podnijeti prigovor Agenciji ako smatra da se obradom ličnih podataka u vezi s njim krši ovaj zakon, ne dovodeći u pitanje druga upravna ili sudska pravna sredstva.
- (2) Agencija obavještava podnosioca prigovora o napretku i ishodu postupka, uključujući i mogućnost primjene pravnog sredstva na osnovu člana 109. ovog zakona i pruža dodatnu pomoć na zahtjev podnosioca prigovora.

Član 109.

- (Pravo na djelotvorno pravno sredstvo protiv odluke Agencije)
- (1) Fizičko lice, kontrolor podataka ili obrađivač ima pravo pokrenuti upravni spor protiv odluke Agencije pred Sudom Bosne i Hercegovine u roku od 60 dana od dana prijema odluke, ne dovodeći u pitanje druga upravna ili vanskudska pravna sredstva.
 - (2) Nosilac podataka ima pravo pokrenuti upravni spor pred Sudom Bosne i Hercegovine ako Agencija, u roku od 90 dana, ne riješi prigovor ili ne obavijesti nosioca podataka o napretku ili ishodu postupka po prigovoru, ne dovodeći u pitanje druga upravna ili vanskudska pravna sredstva.

Član 110.

(Pravo na djelotvorno pravno sredstvo protiv kontrolora podataka ili obrađivača)

- (1) Nosilac podataka ima pravo na sudsku zaštitu protiv kontrolora podataka ili obrađivača ako smatra da su zbog obrade ličnih podataka prekršena njegova prava iz ovog zakona, ne dovodeći u pitanje druga upravna ili vanskudska pravna sredstva, uključujući pravo na podnošenje prigovora Agenciji iz člana 108. stav (1) ovog zakona.
- (2) Postupak sudske zaštite iz stava (1) ovog člana vodi se u skladu sa zakonima kojima se uređuje parnični postupak.

Član 111.

(Zastupanje nosilaca podataka)

Nosilac podataka ima pravo dati ovlaštenje neprofitnom organu, organizaciji ili udruženju osnovanom u skladu sa zakonom, čija je svrha osnivanja ostvarivanje ciljeva od javnog interesa i koje je aktivno u oblasti zaštite prava i sloboda nosioca podataka u vezi sa zaštitom ličnih podataka, da u njegovo ime ostvaruju prava iz čl. 108, 109. i 110. ovog zakona, kao i da u njegovo ime i za njegov račun ostvaruju pravo na naknadu štete.

Član 112.

(Pravo na naknadu štete i odgovornost)

- (1) Svako lice koje je pretrpjelo materijalnu ili nematerijalnu štetu zbog kršenja ovog zakona ima pravo na naknadu za pretrpljenu štetu od kontrolora podataka ili obrađivača.
- (2) Svaki kontrolor podataka odgovoran je za štetu uzrokovanu obradom kojom se krši ovaj zakon. Obradivač je odgovoran za štetu uzrokovanu obradom samo ako nije poštovao obaveze iz ovog zakona koje su posebno propisane za obrađivače ili ako je prekršio zakonite instrukcije kontrolora podataka ili je postupio protivno njima.
- (3) Kontrolor podataka ili obrađivač izuzet je od odgovornosti ako dokaže da nije ni na koji način odgovoran za događaj koji je uzrokovao štetu.
- (4) Ako je u istu obradu uključeno više od jednog kontrolora podataka ili obrađivača ili su u istu obradu uključeni i kontrolor podataka i obrađivač i ako su odgovorni za štetu uzrokovanu obradom, svaki kontrolor podataka ili obrađivač odgovoran je za cjelokupnu štetu.
- (5) Ako je kontrolor podataka ili obrađivač platio punu odštetu u skladu sa stavom (4) ovog člana, taj kontrolor podataka ili obrađivač ima pravo od drugih kontrolora podataka ili obrađivača, koji su uključeni u istu obradu, zahtijevati povrat dijela odštete koji odgovara njihovom udjelu u odgovornosti za štetu.
- (6) Pravo na naknadu štete ostvaruje se u sudskom postupku, a mjesna nadležnost utvrđuje se u skladu s članom 110. stav (2) ovog zakona.

Član 113.

(Opći uslovi za izricanje novčane kazne)

- (1) Agencija osigurava da je izricanje novčane kazne, u skladu s ovim članom i u vezi s povredama ovog zakona, u svakom pojedinačnom slučaju djelotvorno, razmjerno i odvraćajuće.
- (2) Agencija izdaje prekršajni nalog ili podnosi zahtjev za pokretanje prekršajnog postupka nadležnom sudu, pored mjera iz člana 103. stav (2) tač. a) do h) i tačke j) ovog zakona, u zavisnosti od okolnosti svakog pojedinačnog slučaja. Prilikom odlučivanja o novčanoj kazni i iznosu kazne u svakom pojedinačnom slučaju u obzir se uzima posebno:
 - a) priroda, težina i trajanje povrede, imajući u vidu prirodu, obim i svrhu predmetne obrade, kao i broj nosilaca podataka i stepen štete koju su pretrpjeli;
 - b) da li povreda ima obilježje namjere ili nepažnje;
 - c) svaka radnja koju je kontrolor podataka ili obrađivač preduzeo kako bi ublažio štetu koju su pretrpjeli nosioci podataka;
 - d) stepen odgovornosti kontrolora podataka ili obrađivača, pri čemu se uzimaju u obzir tehničke i organizacione mjere koje su primijenili, u skladu s čl. 27. i 34. ovog zakona;
 - e) sve utvrđene prethodne povrede od kontrolora podataka ili obrađivača;
 - f) stepen saradnje s Agencijom na otklanjanju povrede i ublažavanju mogućih štetnih posljedica povrede;
 - g) kategorija ličnih podataka na koje povreda utiče;
 - h) način na koji je Agencija saznala za povredu, a posebno da li je u kojem opsegu kontrolor podataka ili obrađivač obavijestio o povredi;
 - i) ako su protiv kontrolora podataka ili obrađivača u vezi sa istim predmetom prethodno izrečene mjere iz člana 103. stav (2) ovog zakona, i poštivanje tih mjera;

- j) poštivanje odobrenih kodeksa ponašanja, u skladu s članom 42. ovog zakona ili odobrenih mehanizama certifikacije, u skladu s članom 44. ovog zakona;
- k) sve ostale otežavajuće ili olakšavajuće okolnosti, kao što su finansijska dobit ostvarena kršenjem ili gubici izbjegnuti, direktno ili indirektno, tim kršenjem.
- (3) Ako kontrolor podataka ili obrađivač za istu ili povezane obrade namjerno ili iz nepažnje prekrši više odredbi ovog zakona, ukupan iznos novčane kazne ne smije biti veći od iznosa utvrđenog za najtežu povredu.
- (4) Novčanom kaznom u iznosu od 10.000 KM do 20.000.000 KM, ili u slučaju preduzetnika do 2% ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, zavisno od toga koji je iznos viši kažnjava se:
- kontrolor podataka i obrađivač za obradu ličnih podataka izvršenu suprotno čl. 10. i 13, čl. 27. do 41, te čl. 44. i 45. ovog zakona;
 - certifikacioni organ koji postupi suprotno čl. 44. i 45. ovog zakona;
 - organ za praćenje odobrenih kodeksa ponašanja ako postupi suprotno članu 43. stav (3) ovog zakona.
- (5) Novčanom kaznom u iznosu od 20.000 KM do 40.000.000 KM, ili u slučaju preduzetnika do 4% ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, zavisno od toga koji je iznos viši kaznit će se:
- ko obavlja obradu ličnih podataka suprotno čl. 7, 8, 9. i 11. ovog zakona;
 - ko krši prava nosilaca podataka iz čl. 14. do 24. ovog zakona;
 - ko prenese lične podatke primaocu u drugu državu ili međunarodnu organizaciju suprotno čl. 46. do 51. ovog zakona;
 - ko postupi suprotno obavezama iz posebnih zakona donesenih na osnovu DIJELA DRUGOG Poglavlja V. ovog zakona.
 - ko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenom obustavljanju prijenosa podataka u skladu s članom 103. stav (2) ovog zakona ili uskrati pristup suprotno članu 103. stav (1) ovog zakona.
- (6) Za nepostupanje po nalogu Agencije iz člana 103. stav (2) ovog zakona u skladu sa stavom (2) ovog člana izriče se novčana kazna u iznosu od 20.000 KM do 40.000.000 KM, ili u slučaju preduzetnika do 4% ukupnog godišnjeg prometa na svjetskom nivou za prethodnu finansijsku godinu, zavisno od toga koji je iznos viši.
- (7) Za povredu iz st. (4), (5) i (6) ovog člana novčanom kaznom u iznosu od 5.000 KM do 70.000 KM kaznit će se odgovorno lice, a novčanom kaznom od 500 KM do 5.000 KM kaznit će se zaposleno lice kod kontrolora podataka ili obrađivača.
- (8) Novčanom kaznom u iznosu od 5.000 KM do 70.000 KM kaznit će se odgovorno lice, a novčanom kaznom u iznosu od 500 KM do 5.000 KM kaznit će se zaposleno lice u javnom i nadležnom organu za prekršaj:
- iz čl. 7. do 11, člana 13, čl. 14. do 24, čl. 27. do 41, čl. 44. i 45, čl. 52. do 59, člana 60, člana 64, člana 66, čl. 67. do 73, čl. 76. i 77. i čl. 79. do 90. ovog zakona;
 - ko prenese lične podatke primaocu u drugu državu ili međunarodnu organizaciju suprotno čl. 46. do 51, te čl. 91. do 95. ovog zakona;
- ko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenom obustavljanju prijenosa podataka u skladu s članom 103. stav (2) ovog zakona ili uskrati pristup suprotno članu 103. stav (1) ovog zakona;
- (9) Zastarijevanje izricanja novčane kazne nastupa nakon proteka perioda od pet godina od dana kada je povreda izvršena.
- (10) Ne dovodeći u pitanje nadležnosti i ovlaštenja Agencije, novčane kazne ne mogu se izreći javnom i nadležnom organu za povredu ovog zakona, osim odgovornom i zaposlenom licu iz stava (8) ovog člana.
- (11) Na postupak izricanja novčane kazne iz ovog člana primjenjuju se odredbe Zakona o prekršajima Bosne i Hercegovine, a iznosi novčanih kazni propisani su ovim zakonom.
- (12) Izuzetno od odredbe stava (11) ovog člana, prihod ostvaren na osnovu naplate novčanih kazni dijeli se na način propisan članom 114. ovog zakona.

Član 114.

(Izvršenje i naplata novčane kazne)

Novčana kazna uplaćuje se na Jedinstveni račun trezora institucija Bosne i Hercegovine i dijeli se kako slijedi:

Član 115.

(Kazne)

Krivičnim zakonima propisuju se kazne za krivično djelo protuzakonite obrade ličnih podataka, u slučaju grubog kršenja odredbi ovog zakona.

DIO ŠESTI – PRIJELAZNE I ZAVRŠNE ODREDBE

Član 116.

(Mjere u prijelaznom periodu)

Član 117.
(Podzakonski akti)

Svi podzakonski akti propisani ovim zakonom bit će doneseni u roku od 210 dana od dana stupanja na snagu ovog zakona.

Član 118.
(Odnos s prethodno sklopljenim sporazumima)

Međunarodni sporazumi koji uključuju prijenos ličnih podataka drugim državama ili međunarodnim organizacijama koje je Bosna i Hercegovina sklopila prije donošenja ovog zakona, a koji su u skladu sa Zakonom o zaštiti ličnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11), ostaju na snazi dok se ne izmijene, zamijene ili stave van snage.

Član 119.
(Prestanak važenja)

- (1) Početkom primjene ovog zakona prestaje važiti Zakon o zaštiti ličnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11).
- (2) Početkom primjene ovog zakona prestaju važiti podzakonski akti doneseni na osnovu zakona iz stava (1) ovog člana: Pravilnik o postupku po prigovoru nosioca ličnih podataka u Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini ("Službeni glasnik BiH", broj 51/09), Pravilnik o inspekcijском nadzoru u oblasti zaštite ličnih podataka ("Službeni glasnik BiH", broj 51/09), Instrukcija o načinu provjere obrade ličnih podataka prije uspostavljanja zbirke ličnih podataka ("Službeni glasnik BiH", broj 51/09), Pravilnik o načinu vođenja i obrascu evidencije o zbirkama ličnih podataka ("Službeni glasnik BiH", broj 52/09) i Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite ličnih podataka ("Službeni glasnik BiH", broj 67/09).

Član 120.
(Stupanje na snagu)

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku BiH", a primjenjuje se nakon isteka 210 dana od dana stupanja na snagu.

Broj 01,02-02-1-2548/24
30. januara 2025. godine
Sarajevo

Predsjedavajući Predstavničkog doma Parlamentarne skupštine BiH Dr. Denis Zvizdić, s. r.	Predsjedavajući Doma naroda Parlamentarne skupštine BiH Dr. Dragan Čović, s. r.
---	--

Na temelju članka IV.4.a) Ustava Bosne i Hercegovine, Parlamentarna skupština Bosne i Hercegovine, na 16. hitnoj sjednici Zastupničkog doma, održanoj 23. siječnja 2025. godine, i na 8. hitnoj sjednici Doma naroda, održanoj 30. siječnja 2025. godine, usvojila je

**ZAKON
O ZAŠTITI OSOBNIH PODATAKA**

DIO PRVI – OPĆE ODREDBE

Članak 1.
(Predmet)

- (1) Ovim Zakonom propisuju se:
 - a) pravila u vezi sa zaštitom fizičkih osoba u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka;
 - b) nadležnosti Agencije za zaštitu osobnih podataka u Bosni i Hercegovini (u daljnjem tekstu: Agencija),

organizacija i upravljanje, kao i druga pitanja značajna za njezin rad i zakonito funkcioniranje;

- c) zaštita fizičkih osoba u vezi s obradom osobnih podataka od nadležnih tijela u svrhe sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela, izvršenje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje.
- (2) Ovim Zakonom obavlja se usklađivanje s odredbama Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i odredbama Direktive (EU) 2016/680 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka od nadležnih tijela s ciljem sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela ili izvršenja kaznenih sankcija i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.
- (3) Navođenje odredaba Uredbe i Direktive iz stavka (2) ovog članka obavlja se isključivo s ciljem praćenja i informiranja o preuzimanju pravne stečevine Europske unije u zakonodavstvo Bosne i Hercegovine.

Članak 2.
(Cilj Zakona)

Ovim Zakonom štite se temeljna prava i slobode fizičkih osoba u Bosni i Hercegovini bez obzira na njihovo državljanstvo i prebivalište, a posebice njihovo pravo na zaštitu osobnih podataka.

Članak 3.

(Uporaba muškog ili ženskog roda)

Izrazi koji su radi preglednosti dani u samo jednom gramatičkom rodu u ovom Zakonu se bez diskriminacije odnose i na muški i ženski rod.

Članak 4.
(Definicije)

Pojedini izrazi upotrijebljeni u ovom Zakonu imaju sljedeća značenja:

- a) "osobni podatak" je svaki podatak koji se odnosi na fizičku osobu čiji je identitet utvrđen ili se može utvrditi;
- b) "nositelj podataka" je fizička osoba čiji je identitet utvrđen ili čiji se identitet može utvrditi, neizravno ili izravno, posebno s pomoću identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili s pomoću jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet te osobe;
- c) "obrada" je svaki postupak ili skup postupaka koji se provodi na osobnim podacima ili na skupovima osobnih podataka, automatiziranim ili neautomatiziranim sredstvima, kao što su prikupljanje, evidentiranje, organiziranje, strukturiranje, čuvanje, prilagodavanje ili izmjena, pronalaženje, ostvarivanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničenje, brisanje ili uništavanje;
- d) "ograničenje obrade" je obilježavanje čuvanog osobnog podatka s ciljem ograničenja njegove obrade u budućnosti;

- e) "izrada profila" je svaki oblik automatske obrade osobnog podatka koji se sastoji od korištenja osobnog podatka za procjenu određenih osobnih aspekata u vezi s fizičkom osobom, posebno za analizu ili predviđanje aspekata u vezi s radnim rezultatom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem te fizičke osobe;
- f) "pseudonimizacija" je obrada osobnog podatka tako da se osobni podatak više ne može pripisati određenom nositelju podataka bez korištenja dodatnih informacija, uz uvjet da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;
- g) "zbirka osobnih podataka" je svaki strukturirani skup osobnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to jesu li centralizirani, decentralizirani ili rasprostranjeni na funkcionalnoj ili zemljopisnoj osnovi;
- h) "kontrolor podataka" je fizička ili pravna osoba, javno tijelo ili nadležno tijelo koje samostalno ili s drugim određuje svrhe i sredstva obrade osobnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriteriji za njegovo imenovanje propisuju se zakonom;
- i) "javno tijelo" je svako zakonodavno, izvršno i sudbeno tijelo na svim razinama vlasti u Bosni i Hercegovini;
- j) "nadležno tijelo" je tijelo koje je nadležno za sprječavanje, istragu i otkrivanje kaznenih djela, progon počinitelja kaznenih djela ili izvršenje kaznenih sankcija, uključujući i zaštitu i sprječavanje prijetnji javnoj sigurnosti, kao i pravne osobe ako su zakonom ovlaštene za obavljanje tih poslova kao posebna kategorija kontrolora podataka;
- k) "obrađivač" je fizička ili pravna osoba, javno tijelo koje obrađuje osobne podatke u ime kontrolora podataka;
- l) "primatelj" je fizička ili pravna osoba, javno tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li u pitanju treća strana. Javna tijela koja mogu primiti osobne podatke unutar određene istrage u skladu sa zakonom ne smatraju se primateljima, ali obrada tih podataka mora biti sukladna s važećim pravilima o zaštiti podataka prema svrhama obrade;
- m) "treća strana" označuje fizičku ili pravnu osobu, javno tijelo, Agenciju ili drugo tijelo koje nije nositelj podataka, kontrolora podataka, obrađivača i osobe ovlaštene za obradu osobnih podataka pod izravnom nadležnošću kontrolora podataka ili obrađivača;
- n) "suglasnost" nositelja podataka je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje nositelja podataka kada on izjavom ili jasnom potvrdom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose;
- o) "povreda osobnog podatka" je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, čuvani ili na drugi način obrađivani;
- p) "genetski podatak" je osobni podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičke osobe koja daju jedinstvene informacije o fiziologiji ili zdravlju te fizičke osobe i koji su dobiveni posebnom analizom biološkog uzorka te fizičke osobe;
- r) "biometrijski podatak" je osobni podatak dobiven posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičke osobe koja omogućavaju ili potvrđuju jedinstvenu identifikaciju te fizičke osobe, kao što su fotografije osoba ili daktiloskopski podaci;
- s) "podatak koji se odnosi na zdravlje" je osobni podatak u vezi s fizičkim ili mentalnim zdravljem fizičke osobe, uključujući pružanje zdravstvenih usluga, koji daje informacije o njegovom zdravstvenom stanju;
- t) "predstavnik" je fizička ili pravna osoba s prebivalištem ili boravištem, odnosno sjedištem ili poslovnim nastanom u Bosni i Hercegovini, koju je kontrolor podataka ili obrađivač pisanim putem imenovao u skladu s člankom 29. ovog Zakona;
- u) "gospodarski subjekt" je fizička ili pravna osoba koja obavlja gospodarsku djelatnost, bez obzira na pravni oblik te djelatnosti;
- v) "skupina gospodarskih subjekata" je gospodarski subjekt koji ostvaruje nadzor i gospodarski subjekti koji su pod njegovim nadzorom;
- z) "obvezujuće poslovno pravilo" su politike zaštite osobnih podataka kojih se kontrolor podataka i obrađivač sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini pridržava prilikom prijenosa ili skupova prijenosa osobnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih zemalja unutar skupine gospodarskih subjekata ili skupine gospodarskih subjekata koji se bave zajedničkom gospodarskom djelatnošću;
- aa) "usluga informacijskog društva" je svaka usluga koja se obično pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga, gdje:
 - 1) "na daljinu" znači da se usluga pruža, a pritom stranke nisu istodobno prisutne,
 - 2) "elektroničkim sredstvima" znači da se usluga na početku šalje i prima na određitu s pomoću elektroničke opreme za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radiovezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima,
 - 3) "na osobni zahtjev primatelja usluga" znači da se usluga pruža prijenosom podataka na osobni zahtjev;
- bb) "međunarodna organizacija" je organizacija sa svojim tijelima uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na temelju sporazuma osnovale dvije ili više zemalja;
- cc) "poslovni nastan" je djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana;
- dd) "videonadzor" je informacijsko-komunikacijski sustav koji ima mogućnost prikupljanja i daljnje obrade osobnih podataka, koji obuhvaća stvaranje snimke koja čini ili je namijenjena da čini dio sustava skladištenja.

Članak 5.

(Glavno područje primjene)

- (1) Ovaj se Zakon primjenjuje na obradu osobnog podatka koja se u potpunosti obavlja automatizirano te na neautomatiziranu obradu osobnog podatka koji čini dio zbirke osobnih podataka ili je namijenjen da bude dio zbirke osobnih podataka.
- (2) Ovaj se Zakon ne primjenjuje na obradu osobnog podatka koju obavlja fizička osoba isključivo u svrhu osobnih aktivnosti ili aktivnosti kućanstva.
- (3) Na obradu osobnog podatka od nadležnog tijela u svrhu zaštite fizičkih osoba u vezi s obradom osobnih podataka u svrhu sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela, izvršenja kaznenih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje, ne primjenjuje se Dio drugi ovog Zakona.

Članak 6.

(Teritorijalno područje primjene)

- (1) Ovaj Zakon primjenjuje se na obradu osobnog podatka koju obavlja kontrolor podataka ili obrađivač koji ima sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, neovisno o tome obavlja li se obrada u Bosni i Hercegovini ili ne.
- (2) Ovaj Zakon primjenjuje se na obradu osobnog podatka nositelja podataka u Bosni i Hercegovini koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, ako je aktivnost obrade povezana s:
 - a) nudjenjem roba ili usluga tim nositeljima podataka u Bosni i Hercegovini, neovisno o tome treba li nositelj podataka izvršiti plaćanje ili
 - b) praćenjem ponašanja nositelja podataka, uz uvjet da se njihovo ponašanje očituje unutar Bosne i Hercegovine.
- (3) Ovaj Zakon primjenjuje se na obradu osobnog podatka koju obavlja kontrolor podataka ili obrađivač koji nema sjedište ili poslovni nastan u Bosni i Hercegovini nego u mjestu na kojem se pravo Bosne i Hercegovine primjenjuje na temelju međunarodnog prava.
- (4) Na obradu osobnog podatka od nadležnog tijela u svrhu zaštite fizičke osobe u vezi s obradom osobnog podatka u svrhu sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela, izvršenja kaznenih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje, ne primjenjuje se ovaj članak.

**DIO DRUGI – OBRADA OSOBNOG PODATKA OD STRANE FIZIČKE OSOBE, PRAVNE OSOBE ILI JAVNOG TIJELA KAO KONTROLORA PODATAKA
POGLAVLJE I. NAČELA OBRADE OSOBNOG PODATKA**

Članak 7.

(Načela obrade osobnog podatka)

- (1) Načela obrade osobnog podatka su:
 - a) zakonitost, pravednost i transparentnost u odnosu na nositelja podataka;
 - b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije sukladan s tim svrhama. Daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 56. stavkom (1) ovog Zakona ne smatra se neusklađenom s prvobitnim svrhama;

- c) smanjenje opsega podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju;
 - d) točnost – podaci moraju biti točni i po potrebi ažurirani. Moraju se poduzeti sve razumne mjere kako bi se osiguralo da osobni podaci koji nisu točni, imajući u vidu svrhe u koje se obrađuju, budu bez odgode izbrisani ili ispravljeni;
 - e) ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nositelja podataka, i to ne duže nego što je potrebno u svrhe u koje se osobni podaci obrađuju. Osobni podaci mogu se čuvati na duže razdoblje ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 56. stavkom (1) ovog Zakona, što podliježe provođenju primjerenih tehničkih i organizacijskih mjera propisanih ovim Zakonom radi zaštite prava i sloboda nositelja podataka;
 - f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigurava odgovarajuća sigurnost osobnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.
- (2) Načelo pouzdanosti – kontrolor podataka odgovoran je za usklađenost obrade osobnog podatka sa stavkom (1) ovog članka i mora biti u mogućnosti dokazati tu usklađenost.

Članak 8.

(Zakonitost obrade osobnog podatka)

- (1) Obrada osobnog podatka zakonita je samo ako je ispunjen najmanje jedan od sljedećih uvjeta:
 - a) ako je nositelj podataka dao suglasnost za obradu svojih osobnih podataka za jednu ili više posebnih svrha;
 - b) ako je obrada potrebna radi izvršenja ugovora u kojem je nositelj podataka ugovorna stranka ili radi poduzimanja radnji na zahtjev nositelja podataka prije sklapanja ugovora;
 - c) ako je obrada potrebna radi poštivanja pravnih obveza kontrolora podataka;
 - d) ako je obrada potrebna radi zaštite ključnih interesa nositelja podataka ili druge fizičke osobe;
 - e) ako je obrada potrebna za izvršenje zadatka koji se obavlja u javnom interesu ili u sklopu izvršenja službenih ovlasti kontrolora podataka;
 - f) ako je obrada potrebna zbog legitimnih interesa kontrolora podataka ili treće strane, osim kada nad tim interesima pretežu interesi ili temeljna prava i slobode nositelja podataka, a koji zahtijevaju zaštitu osobnih podataka, posebno ako je nositelj podataka dijete. Ova se točka ne primjenjuje na obradu koju obavljaju javna tijela pri izvršenju svojih poslova.
- (2) Pravni temelj za obradu osobnog podatka iz stavka (1) toč. c) i e) ovog članka utvrđuje se zakonima institucija BiH, entiteta i kantona u skladu s nadležnostima, tako da se preciznije propišu posebni uvjeti za obradu te druge mjere za osiguranje zakonite i pravedne obrade, među ostalim i za druge posebne obrade, kako je to propisano u Poglavlju V. ovog Zakona.
- (3) Posebnim zakonom o obradi podatka iz stavka (1) toč. c) i e) ovog članka institucija BiH, entiteta i kantona, u skladu s nadležnostima, propisuje se svrha obrade, koja u pogledu obrade iz stavka (1) točke e) ovog članka mora biti potrebna za izvršenje zadatka koji se obavlja u javnom

interesu ili u sklopu izvršenja službenih ovlasti kontrolora podataka. Tim zakonom propisuju se: opći uvjeti kojima se uređuje zakonitost obrade koju obavlja kontrolor podataka, vrste podataka koji se obrađuju, kategorije nositelja podataka, subjekti kojima se osobni podaci mogu otkriti i svrhe u koje se podaci mogu otkriti, ograničenje svrhe, rokovi čuvanja te radnje obrade i postupci obrade, uključujući i mjere za osiguranje zakonite i pravedne obrade, kao i za druge posebne obrade, kako je to navedeno u Poglavlju V. ovog Zakona. Tim zakonom mora se ostvariti cilj od javnog interesa i obrada mora biti razmjerna zakonitom cilju kojem se teži.

- (4) Ako se obrada obavlja u svrhu koja se razlikuje od svrhe za koju su osobni podaci prikupljeni i ne temelji se na suglasnosti nositelja podataka ili posebnom zakonu koji predstavlja potrebnu i razmjernu mjeru u demokratskom društvu za zaštitu ciljeva iz članka 25. stavka (1) ovog Zakona, kontrolor podataka, s ciljem utvrđivanja je li obrada u drugu svrhu sukladna sa svrhom za koju su osobni podaci prvotno prikupljeni, uzima u obzir, među ostalim:
- svaku vezu između svrha za koje su osobni podaci prikupljeni i svrha namjeravane daljnje obrade;
 - kontekst u kojem su osobni podaci prikupljeni, posebno u pogledu odnosa između nositelja podataka i kontrolora podataka;
 - prirodu osobnih podataka, posebno činjenicu obrađuju li se posebne kategorije osobnih podataka u skladu s člankom 11. ovog Zakona ili osobni podaci koji se odnose na kaznenu osuđivanost i kaznena djela u skladu s člankom 12. ovog Zakona;
 - moгуће posljedice namjeravane daljnje obrade za nositelje podataka;
 - postojanje odgovarajućih mjera zaštite, koje mogu uključivati enkripciju ili pseudonimizaciju.
- (5) Javna i nadležna tijela entiteta i Brčko distrikta BiH dužna su, uz poštivanje odredaba ovog Zakona, ustupiti osobne podatke iz svojih evidencija ovlaštenom kontroloru podataka, u svrhu prethodnog izjašnjavanja građana koji imaju biračko pravo o pitanjima za koje je posebnim propisima omogućeno to pravo.

Članak 9. (Suglasnost)

- Kada je obrada utemeljena na suglasnosti, kontrolor podataka mora dokazati da je nositelj podataka dao suglasnost za obradu svojih osobnih podataka.
- Ako nositelj podataka daje suglasnost u pisanoj izjavi koja se odnosi i na druga pitanja, zahtjev za suglasnost mora biti predočen tako da se jasno razlikuje od drugih pitanja, u razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika. Dio suglasnosti koji predstavlja kršenje ovog Zakona se ne primjenjuje.
- Nositelj podataka ima pravo u bilo kojem trenutku povući svoju suglasnost. Povlačenje suglasnosti ne utječe na zakonitost obrade podataka na temelju suglasnosti prije njezinog povlačenja. Prije davanja suglasnosti o tome se obavještava nositelj podataka. Povlačenje suglasnosti mora biti jednako jednostavno kao i njezino davanje.
- Kada se procjenjuje je li suglasnost dana dobrovoljno, u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, provedba ugovora, uključujući i obavljanje usluge, uvjetovana suglasnošću za obradu osobnih podataka koja nije nužna za provedbu tog ugovora.

Članak 10.

(Uvjeti koji se primjenjuju na suglasnost djeteta u vezi s uslugom informacijskog društva)

- Kada se primjenjuje članak 8. stavak (1) točka a) ovog Zakona u pogledu izravnog nudića usluge informacijskog društva djetetu, obrada osobnog podatka djeteta zakonita je ako dijete ima najmanje 16 godina. Ako je dijete mlađe od 16 godina, takva obrada je zakonita samo ako i u mjeri u kojoj je suglasnost dao ili odobrio roditelj, posvojitelj, skrbnik djeteta ili drugi zastupnik djeteta.
- Kontrolor podataka mora uložiti razumne napore prilikom provjere je li suglasnost u tim slučajevima dao ili odobrio roditelj, posvojitelj odnosno skrbnik djeteta, uzimajući u obzir dostupnu tehnologiju.
- Stavak (1) ovog članka ne utječe na opća pravila obveznog prava koja se tiču važenja, sklapanja ili učinka ugovora u vezi s djetetom.

Članak 11.

(Obrada posebnih kategorija osobnih podataka)

- Obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije osobe, podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji osobe je zabranjena.
- Iznimno od odredbe stavka (1) ovog članka, obrada posebne kategorije osobnih podataka dopuštena je ako je ispunjen jedan od sljedećih uvjeta:
 - ako je nositelj podataka dao izričitu suglasnost za obradu tih osobnih podataka za jednu ili više konkretnih svrha, osim kada je posebnim zakonom propisano da se obrada tih podataka ne može obavljati na temelju suglasnosti;
 - ako je obrada potrebna radi ispunjavanja obveza i ostvarivanja posebnih prava kontrolora podataka ili nositelja podataka iz područja radnog prava i prava socijalnog osiguranja i socijalne skrbi, u mjeri u kojoj je to propisano zakonom ili kolektivnim ugovorom, u skladu s posebnim zakonom kojim se propisuju odgovarajuće mjere zaštite temeljnih prava i interesa nositelja podataka;
 - ako je obrada potrebna radi zaštite ključnih interesa nositelja podataka ili druge fizičke osobe, ukoliko nositelj podataka fizički ili pravno ne može dati suglasnost;
 - ako se obrada obavlja u sklopu legitimnih aktivnosti, uz odgovarajuće zaštitne mjere, zaklade, udruge ili bilo koje druge neprofitne organizacije s političkim, filozofskim, vjerskim ili sindikalnim ciljem, i to uz uvjet da se obrada odnosi isključivo na članove ili bivše članove te organizacije ili na fizičke osobe koje imaju redovit kontakt s njom, a u vezi s njezinim svrhama, te da se osobni podaci ne otkrivaju izvan te organizacije bez suglasnosti nositelja podataka;
 - ako se obrada odnosi na osobne podatke za koje je očito da ih je objavio nositelj podataka;
 - ako je obrada potrebna za uspostavljanje, ostvarivanje ili obranu pravnih zahtjeva ili kad sudovi postupaju u sudskom svojstvu;
 - ako je obrada potrebna za potrebe bitnog javnog interesa, na temelju zakona koji je razmjernan legitimnom cilju i kojim se poštuje bit prava na zaštitu osobnih podataka i osiguravaju primjerene i

- posebne mjere za zaštitu temeljnih prava i interesa nositelja podataka;
- h) ako je obrada potrebna za potrebe preventivne medicine ili medicine rada zbog procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja sustavima i uslugama zdravstvene ili socijalne skrbi na temelju posebnog zakona ili u skladu s ugovorom sa zdravstvenim radnikom i uz uvjete i mjere zaštite iz stavka (3) ovog članka;
- i) ako je obrada potrebna iz razloga javnog interesa u području javnog zdravlja, poput zaštite od ozbiljnih prekograničnih prijetnji po zdravlje ili osiguranja visokih standarda kvalitete i sigurnosti zdravstvene zaštite i lijekova i medicinskih sredstava, na temelju posebnog zakona kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda nositelja podataka, a posebno čuvanje profesionalne tajne;
- j) ako je obrada potrebna za potrebe arhiviranja u javnom interesu, potrebe znanstvenog ili povijesnog istraživanja ili statističke potrebe u skladu s člankom 56. stavak (1) ovog Zakona, a na temelju posebnog zakona, koji je razmjern legitiman cilju i kojim se poštuje bit prava na zaštitu podataka i osiguravaju primjerene i posebne mjere za zaštitu temeljnih prava i interesa nositelja podataka.
- (3) Osobni podaci iz stavka (1) ovog članka mogu se obrađivati u svrhe navedene u stavku (2) točki h) ovog članka kada te podatke obrađuje stručna osoba ili se podaci obrađuju pod odgovornošću stručne osobe na koju se primjenjuje obveza čuvanja profesionalne tajne u skladu s posebnim zakonom ili pravilima koja su utvrdila nadležna javna tijela ili druge osobe na koju se primjenjuje obveza čuvanja tajne u skladu s posebnim zakonom ili pravilima koja su utvrdila nadležna javna tijela.
- (4) Posebnim zakonima mogu se zadržati ili uvesti dodatni uvjeti, uključujući i ograničenja u odnosu na obradu genetskih podataka, biometrijskih podataka ili podataka o zdravlju.

Članak 12.

(Obrada osobnih podataka koji se odnose na kaznenu osuđivanost i kaznena djela)

Obrada osobnih podataka koji se odnose na kaznenu osuđivanost i kaznena djela ili povezane mjere sigurnosti na temelju članka 8. stavka (1) ovog Zakona može se obavljati samo pod nadzorom javnog tijela ili kada je obrada propisana posebnim zakonom kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode nositelja podataka. Registar kaznenih presuda vodi se isključivo pod nadzorom javnog tijela.

Članak 13.

(Obrada za koju nije potrebna identifikacija)

- (1) Ako kontrolor podataka obrađuje osobne podatke za čiju se svrhu obrade ne zahtijeva ili više ne zahtijeva identifikiranje nositelja podataka, kontrolor podataka nije dužan čuvati, pribavljati ili obrađivati dodatne informacije radi identifikacije nositelja podataka samo zbog poštivanja ovog Zakona.
- (2) Ako u slučajevima iz stavka (1) ovog članka kontrolor podataka može dokazati da ne može identificirati nositelja podataka, kontrolor podataka o tome na odgovarajući način obavještava nositelja podataka, ako je moguće. U tim slučajevima se ne primjenjuju čl. 17. – 22. ovog Zakona, osim u slučaju kada nositelj podataka, u svrhu

ostvarivanja svojih prava iz tih članaka, pruži dodatne informacije koje omogućavaju njegovu identifikaciju.

POGLAVLJE II. PRAVA NOSITELJA PODATAKA

Članak 14.

(Transparentna informacija, komunikacija i način ostvarivanja prava nositelja podataka)

- (1) Kontrolor podataka poduzima odgovarajuće mjere kako bi se nositelju podataka pružile sve informacije iz čl. 15. i 16. ovog Zakona i svi oblici komunikacije za ostvarivanje prava iz čl. 17. – 24. ovog Zakona i članka 36. ovog Zakona u vezi s obradom podataka, i to u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, što se posebno odnosi na sve informacije koje su izričito namijenjene djetetu. Informacije se pružaju u pisanom obliku ili na druge načine, uključujući i elektronički oblik kada je to primjereno. Ako nositelj podataka zahtijeva, informacije se mogu pružiti usmeno, uz uvjet da je identitet nositelja podataka utvrđen drugim sredstvima.
- (2) Kontrolor podataka olakšava ostvarivanje prava nositelja podataka iz čl. 17. – 24. ovog Zakona. U slučajevima iz članka 13. stavka (1) ovog Zakona, kontrolor podataka ne smije odbiti postupiti po zahtjevu nositelja podataka za ostvarivanje njegovih prava iz čl. 17. – 24. ovog Zakona, osim ako kontrolor podataka dokaže da ne može utvrditi identitet nositelja podataka.
- (3) Kontrolor podataka nositelju podataka, na njegov zahtjev, pruža informacije o poduzetim radnjama iz čl. 17. – 24. ovog Zakona bez nepotrebne odgode i u svakom slučaju u roku od 30 dana od dana zaprimanja zahtjeva. Taj rok se može, po potrebi, produžiti za 60 dana, uzimajući u obzir složenost i broj zaprimljenih zahtjeva. Kontrolor podataka obavještava nositelja podataka o svakom takvom produženju u roku od 30 dana od dana zaprimanja zahtjeva, pri čemu navodi razloge za odgodu. Ako nositelj podataka podnese zahtjev elektroničkim putem, informacije se pružaju elektroničkim putem ako je to moguće, osim u slučaju kada nositelj podataka zahtijeva drukčije.
- (4) Ako kontrolor podataka ne postupi po zahtjevu nositelja podataka, dužan je bez odgode, a najkasnije 30 dana od dana zaprimanja zahtjeva, obavijestiti nositelja podataka o razlozima zbog kojih nije postupio po zahtjevu i o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu i drugim pravnim sredstvima.
- (5) Informacije pružene u skladu s čl. 15. i 16. ovog Zakona i sva komunikacija i djelovanja iz čl. 17. – 24. ovog Zakona i članka 36. ovog Zakona pružaju se bez naknade. Ako su zahtjevi nositelja podataka očito neutemeljeni ili pretjerani, posebice zbog učestalog ponavljanja, kontrolor podataka može:
- a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnožanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili postupanja po zahtjevu, ili
- b) odbiti postupiti po zahtjevu.
- (6) Teret dokazivanja očite neutemeljenosti ili pretjeranosti zahtjeva je na kontroloru podataka.
- (7) Ako kontrolor podataka ima opravdane sumnje u pogledu identiteta fizičke osobe koja podnosi zahtjev iz čl. 17. – 23. ovog Zakona, on može, ne dovodeći u pitanje članak 13. ovog Zakona, zatražiti dodatne informacije potrebne za potvrdu identiteta nositelja podataka.
- (8) Informacije koje moraju biti pružene nositeljima podataka, u skladu s čl. 15. i 16. ovog Zakona, mogu se

pružiti u kombinaciji sa standardiziranim simbolima, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio logičan pregled namjeravane obrade. Ako su simboli prikazani elektronički, moraju biti strojno čitljivi.

- (9) Agencija je ovlaštena donijeti propise u svrhu određivanja informacija koje se prikazuju simbolima i postupke za utvrđivanje standardiziranih simbola.

Članak 15.

(Informacije koje treba dostaviti ako se osobni podatak prikuplja od nositelja podataka)

- (1) Ako se osobni podatak prikuplja od nositelja podataka, kontrolor podataka u trenutku prikupljanja osobnog podatka nositelju podataka pruža sljedeće informacije:
- identitet i kontaktne podatke kontrolora podataka i kontaktne podatke predstavnika kontrolora podataka, ako je primjenjivo;
 - kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
 - pravni temelj za obradu te svrhu obrade osobnog podatka;
 - legitimni interes kontrolora podataka ili treće osobe, ako je obrada utemeljena na članku 8. stavku (1) točki f) ovog Zakona;
 - o primatelju ili kategoriji primatelja osobnih podataka, ako ih ima;
 - činjenicu da kontrolor podataka namjerava prenijeti osobne podatke u drugu zemlju ili međunarodnu organizaciju i o postojanju ili nepostojanju odluke Vijeća ministara Bosne i Hercegovine o primjerenosti, odnosno u slučaju prijenosa iz čl. 48. ili 49. ovog Zakona ili članka 51. stavka (2) ovog Zakona upućivanja na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove preslike ili mjesto na kojem su stavljene na raspolaganje, ako je to primjenjivo.
- (2) Osim informacija iz stavka (1) ovog članka, kontrolor podataka u trenutku prikupljanja osobnog podatka pruža nositelju podataka sljedeće dodatne informacije, ako je to potrebno da bi se osigurala pravedna i transparentna obrada:
- o roku u kojem će se osobni podatak čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog roka;
 - o pravu na traženje od kontrolora podataka pristupa osobnom podatku, ispravak ili brisanje osobnog podatka ili ograničenje obrade u vezi s nositeljem podataka ili pravu na ulaganje prigovora na obradu takvog podatka te pravu na prenosivost podatka;
 - o pravu na povlačenje suglasnosti u bilo kojem trenutku, bez utjecaja na zakonitost obrade koja se temeljila na suglasnosti prije njezinog povlačenja, ako je obrada utemeljena na članku 8. stavku (1) točki a) ovog Zakona ili članku 11. stavku (2) točki a) ovog Zakona;
 - o pravu na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;
 - informacije o tome je li davanje osobnog podatka zakonska ili ugovorna obveza ili potreban uvjet za sklapanje ugovora, kao i ima li nositelj podataka obvezu dati osobni podatak i koje su moguće posljedice ako se takav podatak ne pruži;
 - o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz članka 24. st. (1) i (4) ovog Zakona, pri čemu je najmanje dužan dati informacije o načinu rada, kao i značaju i

predviđenim posljedicama takve obrade za nositelja podataka.

- (3) Ako kontrolor podataka namjerava dodatno obrađivati osobne podatke u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade pruža nositelju podataka informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stavka (2) ovog članka.
- (4) Kontrolor podataka nije dužan pružiti informacije nositelju podataka iz st. (1), (2) i (3) ovog članka u onoj mjeri u kojoj nositelj podataka već raspolaže tim informacijama.

Članak 16.

(Informacije koje se pružaju ako osobni podatak nije dobiven od nositelja podataka)

- (1) Ako osobni podatak nije dobiven od nositelja podataka, kontrolor podataka pruža nositelju podataka sljedeće informacije:
- o identitetu i kontaktnim podacima kontrolora podataka i predstavnika kontrolora podataka, ako je primjenjivo;
 - o kontaktnim podacima službenika za zaštitu podataka, ako je primjenjivo;
 - o pravnom temelju za obradu i svrsi obrade kojoj su namijenjeni osobni podaci;
 - o kategorijama osobnih podataka koji se obrađuju;
 - o primatelju ili kategorijama primatelja osobnih podataka, po potrebi;
 - o činjenicama da kontrolor podataka namjerava prenijeti osobne podatke primatelju u drugoj zemlji ili međunarodnoj organizaciji i o postojanju ili nepostojanju odluke Vijeća ministara Bosne i Hercegovine o primjerenosti iz članka 47. stavka (3) ovog Zakona ili u slučaju prijenosa osobnih podataka iz čl. 48. ili 49. ovog Zakona ili članka 51. stavka (2) ovog Zakona uz upućivanje na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove preslike ili mjesta na kojem su stavljene na raspolaganje, ako je primjenjivo.
- (2) Osim informacija iz stavka (1) ovog članka, kontrolor podataka pruža nositelju podataka sljedeće informacije ako je to potrebno da bi se osigurala pravedna i transparentna obrada u odnosu na nositelja podataka:
- o roku u kojem će se osobni podatak čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog roka;
 - o legitimnim interesima kontrolora podataka ili treće osobe ako je obrada utemeljena na članku 8. stavku (1) točki f) ovog Zakona;
 - o pravu na traženje od kontrolora podataka pristupa osobnim podacima, ispravak ili brisanje osobnih podataka ili ograničenja obrade u vezi s nositeljem podataka i pravu na prigovor na obradu, kao i pravu na prenosivost podataka;
 - o pravu na povlačenje suglasnosti u bilo kojem trenutku, bez utjecaja na zakonitost obrade utemeljene na suglasnosti prije povlačenja, ako je obrada utemeljena na članku 8. stavku (1) točki a) ovog Zakona ili članku 11. stavku (2) točki a) ovog Zakona;
 - o pravu na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;
 - o izvoru osobnih podataka i, po potrebi, dolaze li iz javno dostupnih izvora;
 - o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz članka 24. st. (1) i (4) ovog Zakona te, najmanje u tim slučajevima,

- razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nositelja podataka.
- (3) Kontrolor podataka pruža informacije iz st. (1) i (2) ovog članka:
- u razumnom roku nakon dobivanja osobnih podataka, a najkasnije u roku od 30 dana, uzimajući u obzir posebne okolnosti obrade osobnog podatka;
 - ako se osobni podatak koristi za komunikaciju s nositeljem podataka, najkasnije prilikom prve komunikacije ili
 - ako je predviđeno otkrivanje podataka drugom primatelju, najkasnije u trenutku kada je osobni podatak prvi put otkriven.
- (4) Ako kontrolor podataka namjerava dodatno obrađivati osobni podatak u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade pruža nositelju podataka informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stavka (2) ovog članka.
- (5) Stavci (1) - (4) ovog članka ne primjenjuju se ako i u mjeri u kojoj:
- nositelj podataka već posjeduje informacije;
 - je pružanje takvih informacija nemoguće ili bi zahtijevalo nesrazmjerne napore, posebno za obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s uvjetima i mjerama zaštite iz članka 56. stavka (1) ovog Zakona ili u mjeri u kojoj je vjerojatno da se obvezom iz stavka (1) ovog članka može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade. U takvim slučajevima, kontrolor podataka poduzima odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nositelja podataka, među ostalim i stavljanjem informacija na raspolaganje javnosti;
 - je dobivanje ili otkrivanje podataka izričito propisano posebnim zakonom koji se primjenjuje na nositelja podataka, a kojim su predviđene odgovarajuće mjere za zaštitu legitimnih interesa nositelja podataka ili
 - osobni podatak mora ostati povjerljiv u skladu s obvezom čuvanja profesionalne tajne koja je propisana posebnim zakonom, uključujući i druge zakonske obveze čuvanja tajne.
- Članak 17.
(Pravo nositelja podataka na pristup osobnom podatku)
- (1) Nositelj podataka ima pravo dobiti potvrdu od kontrolora podataka o tome obrađuju li se njegovi osobni podaci i ako se obrađuju, pristup osobnim podacima i sljedećim informacijama o:
- svrsi obrade;
 - kategoriji osobnog podatka koji se obrađuje;
 - primatelju ili kategorijama primatelja kojima je osobni podatak otkriven ili će im biti otkriven, a posebno primatelju u drugoj zemlji ili međunarodnoj organizaciji;
 - predviđenom roku u kojem se osobni podaci čuvaju, ako je to moguće ili ako to nije moguće, kriterijima korištenim za određivanje tog roka;
 - pravu na traženje od kontrolora podataka ispravka ili brisanja osobnog podatka ili ograničenja obrade osobnog podatka koji se odnosi na nositelja podataka ili pravo na prigovor na takvu obradu;
 - pravu na podnošenje prigovora Agenciji ili tužbe nadležnom sudu;
- ako se osobni podatak ne prikuplja od nositelja podataka, svakoj dostupnoj informaciji o njegovom izvoru;
 - postojanju automatiziranog donošenja odluka, uključujući i profiliranje iz članka 24. st. (1) i (4) ovog Zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nositelja podataka.
- (2) Ako se osobni podatak prenosi u drugu zemlju ili međunarodnu organizaciju, nositelj podataka ima pravo biti obaviješten o odgovarajućim mjerama zaštite u skladu s člankom 48. ovog Zakona koje se odnose na prijenos podataka.
- (3) Kontrolor podataka osigurava presliku osobnog podatka koji se obrađuje. Za sve dodatne preslike koje zatraži nositelj podataka, kontrolor podataka može naplatiti opravdanu naknadu na temelju administrativnih troškova. Ako nositelj podataka podnese zahtjev elektroničkim putem, osim ako nositelj podataka ne zahtijeva drukčije, informacije se pružaju u uobičajenom elektroničkom obliku.
- (4) Pravo na dobivanje preslike iz stavka (3) ovog članka ne smije negativno utjecati na prava i slobode drugih.
- Članak 18.
(Pravo na ispravak)
- (1) Nositelj podataka ima pravo da mu kontrolor podataka omogući ispravak netočnog osobnog podatka, bez nepotrebne odgode.
- (2) Uzimajući u obzir svrhu obrade, nositelj podataka ima pravo dopuniti nepotpun osobni podatak, među ostalim i davanjem dodatne izjave.
- Članak 19.
(Pravo na brisanje)
- (1) Nositelj podataka ima pravo da mu kontrolor podataka omogući brisanje osobnog podatka koji se na njega odnosi, a kontrolor podataka ima obvezu obrisati osobni podatak, bez nepotrebne odgode, ako je ispunjen jedan od sljedećih uvjeta:
- osobni podatak više nije potreban za svrhe za koje je prikupljen ili na drugi način obrađen;
 - nositelj podataka povukao je suglasnost na kojoj je obrada utemeljena u skladu s člankom 8. stavkom (1) točkom a) ovog Zakona ili člankom 11. stavkom (2) točkom a) ovog Zakona i ako ne postoji drugi pravni temelj za obradu;
 - nositelj podataka uložio je prigovor na obradu u skladu s člankom 23. stavkom (1) ovog Zakona i ne postoje zakonski razlozi za obradu ili je nositelj podataka uložio prigovor na obradu u skladu s člankom 23. stavkom (2) ovog Zakona;
 - osobni podatak je nezakonito obrađen;
 - osobni podatak mora biti obrisani radi postupanja sukladno sa zakonskom obvezom kojoj podliježe kontrolor podataka;
 - osobni podatak je prikupljen u vezi s ponudom usluga informacijskog društva iz članka 10. stavka (1) ovog Zakona.
- (2) Ako je kontrolor podataka javno objavio osobni podatak, a dužan je u skladu sa stavkom (1) ovog članka taj osobni podatak brisati, uzimajući u obzir dostupnu tehnologiju i troškove provođenja, kontrolor podataka poduzima razumne mjere, uključujući i tehničke mjere, da bi obavijestio kontrolore podataka koji obrađuju osobni podatak da je nositelj podataka zatražio od tih kontrolora

- podataka da brišu sve poveznice do njega ili presliku ili rekonstrukciju tog osobnog podatka.
- (3) Stavci (1) i (2) ovog članka ne primjenjuju se u mjeri u kojoj je obrada potrebna:
- radi ostvarivanja prava na slobodu izražavanja i informiranja;
 - radi poštivanja zakonske obveze kojom se zahtijeva obrada propisana posebnim zakonom, a koja se primjenjuje na kontrolora podataka ili radi izvršenja zadatka koji se obavlja u javnom interesu ili u izvršenju službenih ovlasti dodijeljenih kontroloru podataka;
 - radi javnog interesa u području javnog zdravlja u skladu s člankom 11. stavkom (2) toč. h) i i) ovog članka, kao i člankom 11. stavkom (3) ovog Zakona;
 - u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 56. stavkom (1) ovog Zakona u mjeri u kojoj je vjerojatno da se pravom iz stavka (1) ovog članka može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade ili
 - radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Članak 20.

(Pravo na ograničenje obrade)

- (1) Nositelj podataka ima pravo na ograničenje obrade podatka ako je ispunjen jedan od sljedećih uvjeta:
- nositelj podataka osporava točnost osobnog podatka u roku u kojem se kontroloru podataka omogućava da provjeri točnost osobnog podatka;
 - obrada je nezakonita, a nositelj podataka se protivi brisanju osobnog podatka i umjesto toga traži ograničenje njegove obrade;
 - kontroloru podataka više nije potreban osobni podatak za potrebe obrade, ali ga nositelj podataka zahtijeva radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
 - nositelj podataka uložio je prigovor na obradu u skladu s člankom 23. stavkom (1) ovog Zakona i očekuje potvrdu prevladavaju li njegovi razlozi nad legitimnim razlozima kontrolora podataka.
- (2) Ako je obrada ograničena u skladu sa stavkom (1) ovog članka, taj osobni podatak smije se obrađivati samo uz suglasnost nositelja podataka, izuzev čuvanja, ili za postavljanje, ostvarivanje ili obranu pravnih zahtjeva ili zaštitu prava druge fizičke ili pravne osobe ili zbog bitnog javnog interesa.
- (3) Nositelja podataka koji je ostvario pravo na ograničenje obrade u skladu sa stavkom (1) ovog članka kontrolor podataka obavještava prije ukidanja ograničenja obrade.

Članak 21.

(Obveza obavještanja o ispravku ili brisanju osobnog podatka ili ograničenju obrade)

- (1) Kontrolor podataka obavještava sve primatelje kojima su osobni podaci otkriveni o svakom ispravku ili brisanju osobnog podatka ili ograničenju obrade izvršenom u skladu s člankom 18., člankom 19. stavkom (1) i člankom 20. ovog Zakona, osim u slučaju kada je to nemoguće ili ako to zahtijeva nesrazmjeran napor.
- (2) Kontrolor podataka obavještava nositelja podataka o tim primateljima ako nositelj podataka to zahtijeva.

Članak 22.

(Pravo na prenosivost osobnog podatka)

- (1) Nositelj podataka ima pravo preuzeti osobni podatak koji se odnosi na njega, a koji je dao kontroloru podataka u

strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, te ima pravo prenositi taj podatak drugom kontroloru podataka, bez ometanja od kontrolora podataka kojem je osobni podatak dan, ako:

- se obrada obavlja u skladu s člankom 8. stavkom (1) točkom a) ovog Zakona ili člankom 11. stavkom (2) točkom a) ovog Zakona ili na temelju ugovora u skladu s člankom 8. stavkom (1) točkom b) ovog Zakona,
 - se obrada obavlja automatski.
- (2) Prilikom ostvarivanja svojeg prava na prenosivost podatka u skladu sa stavkom (1) ovog članka, nositelj podatka ima pravo na neposredni prijenos od jednog kontrolora podataka drugom kontroloru podataka, ako je to tehnički izvedivo.
- (3) Ostvarivanjem prava na prenosivost podataka iz stavka (1) ovog članka ne dovodi se u pitanje članak 19. ovog Zakona. To se pravo ne primjenjuje na obradu potrebnu za izvršenje zadatka koji se obavlja u javnom interesu ili u sklopu službenih ovlasti dodijeljenih kontroloru podataka.
- (4) Pravo na prenosivost podatka iz stavka (1) ovog članka ne smije negativno utjecati na prava i slobode drugih.

Članak 23.

(Pravo na prigovor)

- (1) Nositelj podataka ima pravo na temelju svoje posebne situacije u svakom trenutku kontroloru podataka podnijeti prigovor na obradu njegovog osobnog podatka u skladu s člankom 8. stavkom (1) toč. e) ili f) ovog Zakona, uključujući profiliranje utemeljeno na tim odredbama. Kontrolor podataka ne smije daljnje obrađivati osobni podatak, osim u slučaju kada dokaže da postoje uvjerljivi legitimni razlozi za obradu koji prevladavaju nad interesima, pravima i slobodama nositelja podataka ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.
- (2) Ako se osobni podatak obrađuje za potrebe izravnog marketinga, nositelj podataka ima pravo u bilo kojem trenutku uložiti prigovor na obradu osobnog podatka koji se odnosi na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri u kojoj je povezano s takvim izravnim marketingom.
- (3) Ako se nositelj podataka protivi obradi za potrebe izravnog marketinga, osobni podatak više se ne smije obrađivati u te svrhe.
- (4) Najkasnije u trenutku prve komunikacije s nositeljem podataka, nositelj podataka izričito se mora uputiti na prava iz st. (1) i (2) ovog članka te se to mora učiniti na jasan način i odvojeno od bilo koje druge informacije.
- (5) U kontekstu korištenja usluga informacijskog društva i ne uzimajući u obzir propise iz područja elektroničkih komunikacija, nositelj podataka može ostvariti svoje pravo na prigovor automatiziranim putem s pomoću tehničkih specifikacija.
- (6) Ako se osobni podatak obrađuje u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe na temelju članka 56. stavka (1) ovog Zakona, nositelj podataka na temelju svoje posebne situacije ima pravo uložiti prigovor na obradu osobnog podatka koji se na njega odnosi, osim ako je obrada potrebna za izvršenje zadatka koji se obavlja u javnom interesu.

Članak 24.

(Automatizirano pojedinačno donošenje odluke, uključujući i profiliranje)

- (1) Nositelj podataka ima pravo da se na njega ne primjenjuje odluka utemeljena isključivo na automatiziranoj obradi, uključujući i profiliranje, koja proizvodi pravni učinak

- koji se na njega odnosi ili na sličan način značajno na njega utječe.
- (2) Stavak (1) ovog članka ne primjenjuje se ako je odluka:
- potrebna za sklapanje ili provedbu ugovora između nositelja podataka i kontrolora podataka;
 - dopuštena zakonom koji se primjenjuje na kontrolora podataka i kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode te legitimne interese nositelja podataka ili
 - utemeljena na izričitoj suglasnosti nositelja podataka.
- (3) U slučajevima iz stavka (2) toč. a) i c) ovog članka, kontrolor podataka poduzima odgovarajuće mjere za zaštitu prava i sloboda te legitimnih interesa nositelja podataka, najmanje prava na sudjelovanje fizičke osobe u donošenju odluke, prava na izražavanje vlastitog stajališta i prava na osporavanje odluke.
- (4) Odluka iz stavka (2) ovog članka ne smije biti utemeljena na posebnim kategorijama osobnih podataka iz članka 11. stavka (1) ovog Zakona, osim ako se primjenjuje članak 11. stavak (2) toč. a) ili g) ovog Zakona te ako su uspostavljene odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nositelja podataka.

Članak 25. (Ograničenja)

- (1) Na temelju posebnog zakona koji se primjenjuje na kontrolora podataka i obrađivača, može se ograničiti opseg prava i obveza iz članka 7., čl. 14. – 24. ovog Zakona i članka 36. ovog Zakona ako odredbe tog zakona odgovaraju pravima i obvezama propisanim u čl. 14. – 24. ovog Zakona, ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda i ako ono predstavlja potrebnu i razmjernu mjeru u demokratskom društvu za zaštitu:
- državne sigurnosti;
 - obrane;
 - javne sigurnosti;
 - sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje;
 - drugih bitnih ciljeva od općeg javnog interesa u Bosni i Hercegovini, a posebice bitnog gospodarskog ili financijskog interesa, što uključuje monetarna, proračunska i porezna pitanja, javno zdravstvo i socijalnu skrb;
 - neovisnosti pravosuđa i sudskih postupaka;
 - sprječavanja, istrage, otkrivanja i progona povrede etike u zakonski reguliranim profesijama;
 - nadzorne, inspeksijske ili regulatorne funkcije koja je, najmanje povremeno, povezana s izvršenjem službenih ovlasti u slučajevima iz toč. a) – e) i točke g) ovog stavka;
 - nositelja podataka ili prava i sloboda drugih;
 - ostvarivanja potraživanja u građanskim sporovima.
- (2) Posebni zakon iz stavka (1) ovog članka sadrži, po potrebi, posebne odredbe koje sadrže najmanje sljedeće:
- svrhu obrade ili kategoriju obrade;
 - kategoriju osobnog podatka;
 - opseg uvedenih ograničenja;
 - mjere zaštite za sprječavanje zlorabe ili nezakonitog pristupa ili prijenosa;
 - određivanje kontrolora podataka ili kategoriju kontrolora podataka;
 - rok čuvanja i mjere zaštite koje se mogu primijeniti uzimajući u obzir prirodu, opseg i svrhe obrade ili kategorije obrade;

- rizik za prava i slobode nositelja podataka;
- pravo nositelja podataka da bude obaviješten o ograničenju, osim ako to može biti štetno za svrhu tog ograničenja.

POGLAVLJE III. KONTROLOR PODATAKA I OBRADIVAČ

Članak 26.

(Obveza kontrolora podataka)

- (1) Kontrolor podataka dužan je primijeniti odgovarajuće tehničke i organizacijske mjere imajući u vidu prirodu, opseg, okolnosti i svrhe obrade, kao i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode fizičkih osoba, kako bi osigurao obavljanje obrade u skladu s ovim Zakonom i kako bi to mogao dokazati. Te mjere se po potrebi preispituju i ažuriraju.
- (2) Ako su mjere iz stavka (1) ovog članka razmjerne u odnosu na aktivnosti obrade, uključuju provedbu odgovarajućih politika zaštite podataka od kontrolora podataka.
- (3) Poštivanje odobrenih kodeksa ponašanja iz članka 42. ovog Zakona ili odobrenih mehanizama certifikacije iz članka 44. ovog Zakona može služiti kao element za dokazivanje usklađenosti s obvezama kontrolora podataka.

Članak 27.

(Tehnička i integrirana zaštita podataka)

- (1) Uzimajući u obzir najnovija postignuća, troškove provođenja i prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode fizičkih osoba koje proizlaze iz obrade podataka, kontrolor podataka, prilikom određivanja sredstava obrade i pri samoj obradi, primjenjuje odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje djelotvorne primjene načela zaštite podataka, kao što je smanjenje količine podataka te uključivanje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz ovog Zakona i zaštitila prava nositelja podataka.
- (2) Kontrolor podataka primjenjuje odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su potrebni za svaku posebnu svrhu obrade. Ta se obveza primjenjuje na sve prikupljene osobne podatke, opseg njihove obrade, rok njihovog čuvanja i njihovu dostupnost. Tim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije fizičke osobe, dostupni neograničenom broju drugih fizičkih osoba.
- (3) Odobreni mehanizam certifikacije iz članka 44. ovog Zakona može služiti kao element za dokazivanje usklađenosti sa zahtjevima iz st. (1) i (2) ovog članka.

Članak 28.

(Zajednički kontrolori podataka)

- (1) Ako dva ili više kontrolora podataka zajednički odrede svrhe i načine obrade, smatraju se zajedničkim kontrolorima podataka. Oni na transparentan način, međusobnim sporazumom, određuju odgovornosti svakoga od njih s ciljem ispunjavanja obveza iz ovog Zakona, posebno u vezi s ostvarivanjem prava nositelja podataka i dužnostima svakoga od njih u pogledu pružanja informacija iz čl. 15. i 16. ovog Zakona, osim u slučaju kada su odgovornosti svakog od kontrolora podataka utvrđene zakonom koji se primjenjuje na kontrolore podataka. Sporazumom se može odrediti kontaktna točka za nositelje podataka.

- (2) Sporazum iz stavka (1) ovog članka mora na odgovarajući način odražavati pojedinačne uloge i odnose zajedničkih kontrolora podataka u odnosu na nositelje podataka. Bit sporazuma mora biti dostupna nositelju podataka.
- (3) Neovisno o uvjetima sporazuma iz stavka (1) ovog članka, nositelj podataka može ostvarivati svoja prava iz ovog Zakona u odnosu sa svakim kontrolorom podataka i protiv svakog od njih.

Članak 29.

- (Predstavnik kontrolora podataka ili obrađivača koji nema sjedište ili poslovni nastan u Bosni i Hercegovini)
- (1) Ako se primjenjuje članak 6. stavak (2) ovog Zakona, kontrolor podataka ili obrađivač obavezan je pisanim putem imenovati svojeg predstavnika u Bosni i Hercegovini.
- (2) Obveza iz stavka (1) ovog članka ne primjenjuje se na:
- obrađu koja je povremena, ne podrazumijeva u većoj mjeri obradu posebnih kategorija podataka iz članka 11. stavka (1) ovog Zakona ili obradu osobnih podataka koji se odnose na kaznenu osuđivanost i kaznena djela iz članka 12. ovog Zakona i za koju nije vjerovatno da će prouzročiti rizik za prava i slobode fizičkih osoba, uzimajući u obzir prirodu, okolnosti, opseg i svrhe obrade ili
 - javna tijela.
- (3) Kontrolor podataka ili obrađivač ovlašćuje predstavnika kako bi se, uz obraćanje kontroloru podataka ili obrađivaču ili umjesto obraćanja njima, njemu obraćali posebno Agencija i nositelj podataka u vezi sa svim pitanjima koja se odnose na obradu osobnog podatka radi osiguranja usklađenosti obrade osobnog podatka s ovim Zakonom.
- (4) Imenovanje predstavnika kontrolora podataka ili obrađivača ne utječe na pravne zahtjeve koji mogu biti postavljeni protiv samog kontrolora podataka ili obrađivača.

Članak 30.

(Обрађивач)

- (1) Ako se obrada osobnog podatka obavlja u ime kontrolora podataka, kontrolor podataka koristi isključivo obrađivača koji u dovoljnoj mjeri jamči primjenu odgovarajućih tehničkih i organizacijskih mjera tako da obrada bude sukladna sa zahtjevima iz ovog Zakona i da se obradom osigurava zaštita prava nositelja podataka.
- (2) Обрађивач не смеје ангажирати другог обрађивача без претходног посебног или опћег писаног одобрења контролора података. У случају опћег писаног одобрења, обрађивач обавјештава контролора података о свим планираним измјенама у вези с додавањем или замијеном других обрађивача како би тиме контролору података омогућио да уложи приговор на те измјене.
- (3) Обрада коју обавља обрађивач уређује се уговором или другим правним актом у складу са законом којим је обавезан обрађивач према контролору података, у којем се наводе предмет и трајање обраде, природа и сврха обраде, врста особних података и категорија носитеља података, као и обавезе и права контролора података.
- (4) Уговором или другим правним актом из ставка (3) ovog članka propisuje se da je obrađivač dužan:
- obrađivati osobni podatak samo prema dokumentiranim uputama kontrolora podataka, među ostalim i u pogledu prijenosa osobnog podatka u drugu zemlju ili međunarodnu organizaciju, osim ako je to propisano posebnim zakonom koji se primjenjuje na obrađivača, a u tom slučaju obrađivač

- obavještava kontrolora podataka o tom pravnom zahtjevu prije obrade, osim ako se tim zakonom zabranjuje takvo obavještanje zbog bitnih razloga od javnog interesa;
- osiguravati da su se osobe ovlaštene za obradu osobnog podatka obvezale na poštivanje povjerljivosti ili da ih na poštivanje povjerljivosti obavezuje odgovarajući zakon;
 - poduzimati sve potrebne mjere u skladu s člankom 34. ovog Zakona;
 - poštivati uvjete iz st. (2) i (5) ovog članka za angažiranje drugog obrađivača;
 - uzimajući u obzir prirodu obrade, pomagati kontroloru podataka putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu kontrolora podataka da odgovori na zahtjeve za ostvarivanje prava nositelja podataka iz Poglavlja II. ovog Zakona;
 - pomagati kontroloru podataka u osiguravanju usklađenosti s obavezama iz čl. 34. – 38. ovog Zakona, uzimajući u obzir prirodu obrade i informacije koje su dostupne obrađivaču;
 - po izboru kontrolora podataka, brisati ili vraćati kontroloru podataka sve osobne podatke nakon završetka pružanja usluga vezanih uz obradu i brisati postojeće preslike, osim u slučaju kada je posebnim zakonom propisana obveza čuvanja osobnih podataka;
 - kontroloru podataka stavljati na raspolaganje sve informacije koje su potrebne za dokazivanje poštivanja obaveza iz ovog članka i kontroloru podataka ili drugom revizoru kojeg ovlasti kontrolor podataka omogućavati provođenje revizije, uključujući i inspekcije, i pomagati u njihovom provođenju;
 - u slučaju iz točke h) ovog stavka, obrađivač odmah obavještava kontrolora podataka ako, po njegovom mišljenju, određena uputa krši ovaj Zakon ili druga pravila o zaštiti podataka.
- (5) Ako obrađivač angažira drugog obrađivača za provođenje posebnih aktivnosti obrade u ime kontrolora podataka, iste obaveze za zaštitu podataka kao one koje su navedene u ugovoru ili drugom pravnom aktu između kontrolora podataka i obrađivača iz stavka (4) ovog članka nameću se tom drugom obrađivaču ugovorom ili drugim pravnim aktom u skladu s posebnim zakonom, a posebno obveza davanja dovoljno jamstava za primjenu odgovarajućih tehničkih i organizacijskih mjera na način kojim se osigurava da obrada udovoljava zahtjevima iz ovog Zakona. Ako taj drugi obrađivač ne ispunjava obaveze zaštite podataka, prvi obrađivač ostaje u potpunosti odgovoran kontroloru podataka za ispunjavanje obaveza tog drugog obrađivača.
- (6) Poštivanje odobrenih kodeksa ponašanja od obrađivača iz članka 42. ovog Zakona ili odobrenog mehanizma certifikacije iz članka 44. ovog Zakona može služiti kao element za dokazivanje pružanja dovoljno jamstava iz st. (1) i (5) ovog članka.
- (7) Ne dovodeći u pitanje pojedinačni ugovor između kontrolora podataka i obrađivača, ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog članka može se u cjelini ili djelomično temeljiti na standardnim ugovornim klauzulama iz st. (8) i (9) ovog članka, uključujući, među ostalima, i klauzule koje su dio certifikata dodijeljenog kontroloru podataka ili obrađivaču u skladu s čl. 44. i 45. ovog Zakona.

- (8) Agencija može donijeti standardne ugovorne klauzule za pitanja iz st. (3), (4) i (5) ovog članka s ciljem dosljedne primjene ovog Zakona.
- (9) Ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog članka mora biti u pisanom obliku, što uključuje i elektronički oblik.
- (10) Ne dovodeći u pitanje čl. 112., 113., 114. i 115. ovog Zakona, ako obrađivač krši ovaj Zakon time što određuje svrhu i načine obrade podataka, obrađivač se smatra kontrolorom podataka u vezi s tom obradom.

Članak 31.

(Obrada osobnog podatka pod nadzorom kontrolora podataka ili obrađivača)

Obrađivač i osoba koja radi pod nadzorom kontrolora podataka ili obrađivača, a ima pristup osobnom podatku, ne smije obrađivati taj podatak bez naloga kontrolora podataka, osim kada je to posebnim zakonom propisano.

Članak 32.

(Evidencija o obradi osobnog podatka)

- (1) Svaki kontrolor podataka i predstavnik kontrolora podataka, ako je primjenjivo, vodi evidenciju o aktivnostima obrade za koje je odgovoran. Evidencija sadrži sljedeće informacije:
 - a) ime i kontaktne podatke kontrolora podataka i, ako je primjenjivo, zajedničkog kontrolora podataka, predstavnika kontrolora podataka i službenika za zaštitu podataka;
 - b) svrhe obrade;
 - c) opis kategorija nositelja podataka i kategorija osobnih podataka;
 - d) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući i primatelje u drugim zemljama ili međunarodnim organizacijama;
 - e) ako je primjenjivo, o prijenosu osobnih podataka u drugu zemlju ili međunarodnu organizaciju, uključujući identifikaciju druge zemlje ili međunarodne organizacije i, u slučaju prijenosa iz članka 51. stavka (2) ovog Zakona, dokumentaciju o odgovarajućim zaštitnim mjerama;
 - f) ako je moguće, predviđene rokove za brisanje različitih kategorija podataka;
 - g) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 34. stavka (1) ovog Zakona.
- (2) Svaki obrađivač i predstavnik obrađivača, ako je primjenjivo, vodi evidenciju o svim aktivnostima obrade koje se provode u ime kontrolora podataka, koja sadrži:
 - a) ime i kontaktne podatke jednog ili više obrađivača i svakog kontrolora podataka u čije ime obrađivač djeluje te, ako je primjenjivo, predstavnika kontrolora podataka ili obrađivača kao i službenika za zaštitu podataka;
 - b) vrste obrade koje se obavljaju u ime svakog kontrolora podataka;
 - c) ako je primjenjivo, informacije o prijenosu osobnih podataka u drugu zemlju ili međunarodnu organizaciju, s identifikacijom te druge zemlje ili međunarodne organizacije i u slučaju prijenosa iz članka 51. stavka (2) ovog Zakona, dokumentaciju o odgovarajućim zaštitnim mjerama;
 - d) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 34. stavka (1) ovog Zakona.

- (3) Evidencija iz st. (1) i (2) ovog članka mora biti u pisanom obliku, što uključuje i elektronički oblik.
- (4) Kontrolor podataka ili obrađivač te predstavnik kontrolora podataka ili obrađivača, ako je primjenjivo, na zahtjev Agencije omogućavaju uvid u evidenciju.
- (5) Obveze iz st. (1) i (2) ovog članka ne primjenjuju se na gospodarski subjekt ili organizaciju u kojoj je zaposleno manje od 250 osoba, osim kada je vjerojatno da će obrada koju obavlja predstavljati visok rizik za prava i slobode nositelja podataka ako obrada nije povremena ili ako obrada obuhvaća posebne kategorije podataka iz članka 11. stavka (1) ovog Zakona ili su u pitanju osobni podaci koji se odnose na kaznenu osuđivanost i kaznena djela.

Članak 33.

(Suradnja s Agencijom)

Kontrolor podataka i obrađivač te ako su određeni njihovi predstavnici dužni su, na obrazložen i na temelju zakona opravdan zahtjev, surađivati s Agencijom u obavljanju njezinih zadataka.

Članak 34.

(Sigurnost obrade osobnog podatka)

- (1) Uzimajući u obzir najnovija postignuća, troškove provođenja i prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode fizičkih osoba, provodeći postupak iz članka 37. ovog Zakona kontrolor podataka i obrađivač primjenjuju odgovarajuće tehničke i organizacijske mjere kako bi postigli odgovarajuću razinu sigurnosti s obzirom na rizik, što po potrebi podrazumijeva:
 - a) pseudonimizaciju i enkripciju osobnog podatka;
 - b) mogućnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
 - c) sposobnost pravodobne ponovne uspostave dostupnosti osobnog podatka i pristupa njemu u slučaju fizičkog ili tehničkog incidenta;
 - d) postupak redovitog testiranja, ocjenjivanja i procjene djelotvornosti tehničkih i organizacijskih mjera za postizanje sigurnosti obrade.
- (2) Pri procjeni odgovarajuće razine sigurnosti u obzir se uzimaju, prije svega, rizici koje predstavlja obrada, a posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnog podatka ili neovlaštenog pristupa osobnom podatku koji je prenesen, čuvan ili na drugi način obrađivan.
- (3) Primjena odobrenog kodeksa ponašanja iz članka 42. ovog Zakona ili odobrenog mehanizma certifikacije iz članka 44. ovog Zakona može se koristiti kao element za dokazivanje usklađenosti sa zahtjevima iz stavka (1) ovog članka.
- (4) Kontrolor podataka i obrađivač poduzimaju mjere kako bi osigurali da svaka fizička osoba koja djeluje pod nadležnošću kontrolora podataka ili obrađivača, a koja ima pristup osobnom podatku, ne obrađuje taj podatak ako to nije po uputama kontrolora podataka, osim u slučajevima kada je to propisano posebnim zakonom.

Članak 35.

(Izvjешćivanje Agencije o povredi osobnog podatka)

- (1) Kontrolor podataka dužan je o povredi osobnog podatka, bez nepotrebne odgode i ako je moguće, najkasnije u roku od 72 sata nakon saznanja za tu povredu izvijestiti Agenciju o povredi osobnog podatka, osim u slučaju ako je vjerojatno da ta povreda neće ugroziti prava i slobode fizičke osobe. Ako izvjешćivanje nije učinjeno u roku od

72 sata, kontrolor podataka dužan je Agenciji navesti razloge za kašnjenje.

- (2) Obradivač je dužan, nakon saznanja za povredu osobnog podataka, bez nepotrebne odgode o tome izvijestiti kontrolora podataka.
- (3) Izvješće iz stavka (1) ovog članka sadrži najmanje sljedeće:
 - a) opis prirode povrede osobnih podataka, i ako je moguće, s navedenim kategorijama i približnim brojem nositelja podataka, kao i kategorijama i približnim brojem evidencija osobnih podataka;
 - b) ime i prezime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
 - c) opis vjerojatne posljedice povrede osobnog podataka;
 - d) opis mjera koje je kontrolor podataka poduzeo ili čije je poduzimanje predložio radi rješavanja problema povrede osobnog podataka, uključujući, po potrebi, i mjere za ublažavanje njezinih mogućih štetnih posljedica.
- (4) Ako i u mjeri u kojoj nije moguće istodobno dostaviti informacije, informacije se mogu dostavljati u dijelovima, bez nepotrebne daljnje odgode.
- (5) Kontrolor podataka dokumentira svaku povredu osobnog podataka, uključujući i činjenice u vezi s povredom osobnog podataka, njezine posljedice i mjere poduzete za otklanjanje štete. Dokumentacija iz ovog stavka omogućava Agenciji postupanje po ovom članku.

Članak 36.

- (Obavješćavanje nositelja podataka o povredi osobnog podataka)
- (1) Kontrolor podataka dužan je, bez odgode, pisanim putem obavijestiti nositelja podataka o povredi osobnog podataka ako je vjerojatno da će povreda osobnog podataka prouzročiti visok rizik za prava i slobode fizičke osobe.
 - (2) Kontrolor podataka u obavijesti iz stavka (1) ovog članka jasnim i jednostavnim jezikom opisuje prirodu povrede osobnog podataka te se najmanje navode informacije i mjere iz članka 35. stavka (3) toč. b), c) i d) ovog Zakona.
 - (3) Obavješćavanje nositelja podataka iz stavka (1) ovog članka nije obvezno ako je ispunjen jedan od sljedećih uvjeta:
 - a) ako je kontrolor podataka poduzeo odgovarajuće tehničke i organizacijske zaštitne mjere i te mjere su primijenjene na osobni podatak u vezi s kojim je došlo do povrede osobnog podataka, a prije svega mjere koje osobni podatak čine nerazumljivim osobi koja nije ovlaštena pristupiti mu, kao što je enkripcija;
 - b) ako je kontrolor podataka poduzeo naknadne mjere kojima se osigurava da više nije moguće da će doći do visokog rizika za prava i slobode nositelja podataka iz stavka (1) ovog članka;
 - c) ako bi to zahtijevalo nerazmjeran napor, mora se objaviti javna obavijest ili se poduzima slična mjera kojom se nositelji podataka obavješćavaju na jednako djelotvoran način.
 - (4) Ako kontrolor podataka nije obavijestio nositelja podataka o povredi osobnog podataka, Agencija, nakon razmatranja stupnja vjerojatnoće da će povreda osobnog podataka prouzročiti visok rizik za prava i slobode fizičkih osoba, može zahtijevati od kontrolora podataka da to učini ako nije ispunjen neki od uvjeta iz stavka (3) ovog članka.

Članak 37.

(Procjena utjecaja obrade na zaštitu osobnog podataka)

- (1) Ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode fizičkih osoba, kontrolor podataka prije obrade obavlja procjenu utjecaja predviđenih obrada na zaštitu osobnog podataka.
- (2) Prilikom obavljanja procjene utjecaja obrade na zaštitu osobnog podataka, kontrolor podataka traži savjet službenika za zaštitu osobnog podataka, ako je imenovan.
- (3) Procjena utjecaja obrade na zaštitu osobnog podataka iz stavka (1) ovog članka obvezna je posebno u slučaju:
 - a) sustavne i opsežne procjene osobnih aspekata u vezi s fizičkim osobama koja se temelji na automatiziranoj obradi, uključujući i profiliranje, a koja je temelj za donošenje odluka koje proizvode pravni učinak u odnosu na fizičku osobu ili na sličan način bitno utječu na fizičku osobu;
 - b) opsežne obrade posebnih kategorija osobnog podataka iz članka 11. stavka (1) ovog Zakona ili podataka koji se odnose na kaznenu osuđivanost i kaznena djela iz članka 12. ovog Zakona ili
 - c) sustavnog praćenja javno dostupnog područja u velikoj mjeri.
- (4) Agencija utvrđuje i javno objavljuje popis vrsta postupaka obrade na koje se primjenjuje obveza obavljanja procjene utjecaja na zaštitu osobnog podataka, u skladu sa stavkom (1) ovog članka.
- (5) Agencija može utvrditi i javno objaviti popis vrsta postupaka obrade za koje nije potrebna procjena utjecaja na zaštitu osobnog podataka.
- (6) Procjena utjecaja obuhvaća najmanje:
 - a) sustavni opis predviđenih obrada i svrha obrade, uključujući, ako je primjenjivo, legitiman interes kontrolora podataka;
 - b) procjenu nužnosti i proporcionalnosti obrada povezanih s njihovim svrhama;
 - c) procjenu rizika za prava i slobode nositelja podataka;
 - d) predviđene mjere za rješavanje rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje usklađenosti s ovim Zakonom, uzimajući u obzir prava i legitimne interese nositelja podataka i drugih uključenih osoba.
- (7) Usklađenost kodeksa ponašanja iz članka 42. ovog Zakona odobrenih od kontrolora podataka ili obradivača uzima se u obzir prilikom procjene utjecaja obrade koje primjenjuju ti kontrolori podataka ili obradivači, posebno u svrhe procjene utjecaja na zaštitu osobnih podataka.
- (8) Kontrolor podataka, po potrebi, od nositelja podataka ili njegovog predstavnika traži mišljenje o namjeravanoj obradi, ne dovodeći u pitanje komercijalne ili javne interese ili sigurnost postupka obrade.
- (9) Ako obrada u skladu s člankom 8. stavkom (1) toč. c) ili e) ovog Zakona ima pravni temelj u posebnom zakonu koji se primjenjuje na kontrolora podataka, ukoliko su tim zakonom uređene posebne obrade ili skup predmetnih radnji i ukoliko je procjena utjecaja na zaštitu osobnih podataka već provedena kao dio opće procjene utjecaja u kontekstu donošenja pravnog temelja, st. (1) do (6) ovog članka se ne primjenjuju, osim ako je posebnim propisom utvrđeno da je potrebno provesti takvu procjenu prije obrade.

- (10) Kontrolor podataka, po potrebi, preispituje je li obrada obavljena u skladu s procjenom utjecaja na zaštitu osobnih podataka, i to najmanje kada dođe do promjene u razini rizika koji predstavljaju postupci obrade.

Članak 38.

(Prethodno savjetovanje kontrolora podataka s Agencijom)

- (1) Kontrolor obrade savjetuje se s Agencijom prije obrade ako je procjena utjecaja na zaštitu osobnih podataka iz članka 37. ovog Zakona pokazala da bi obrada podataka prouzročila visok rizik za prava i slobode pojedinaca u slučaju da kontrolor podataka ne donese mjere za ublažavanje rizika.
- (2) Ako Agencija ustvrdi da bi se namjeravanom obradom iz stavka (1) ovog članka kršio ovaj Zakon, posebice ako kontrolor podataka nije u dovoljnoj mjeri utvrdio ili umanjio rizik za prava i slobode pojedinaca, Agencija u roku od najviše 56 dana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje kontrolora podataka, a po potrebi i obrađivača, i pritom može primijeniti ovlasti iz članka 103. ovog Zakona.
- (3) Rok iz stavka (2) ovog članka, po potrebi, može se produžiti za 42 dana, ovisno o složenosti namjeravane obrade.
- (4) Agencija, u roku od 30 dana od zaprimanja zahtjeva, obavještava kontrolora podataka, a po potrebi i obrađivača, o produženju roka iz stavka (3) ovog članka i razlozima odgode.
- (5) Protjecanje rokova iz st. (2) i (3) ovog članka može biti privremeno obustavljeno dok Agencija ne dobije informacije koje je zahtijevala za potrebe savjetovanja.
- (6) Pri savjetovanju kontrolor podataka Agenciji dostavlja:
 - a) ako je primjenjivo, odgovarajuće odgovornosti kontrolora podataka, zajedničkih kontrolora podataka i obrađivača koji sudjeluju u obradi, posebno u slučaju obrade unutar skupine gospodarskih subjekata;
 - b) svrhu i sredstva namjeravane obrade;
 - c) zaštitne mjere i druge mjere za zaštitu prava i sloboda nositelja podataka na temelju ovog Zakona;
 - d) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
 - e) procjenu utjecaja na zaštitu podataka kako je to propisano člankom 37. ovog Zakona;
 - f) sve druge informacije koje Agencija traži.
- (7) O prijedlogu zakona kojim se uređuje obrada osobnih podataka, prije njegovog upućivanja u parlamentarnu proceduru, predlagatelj se može prethodno savjetovati s Agencijom.
- (8) Neovisno o stavku (1) ovog članka, posebnim zakonom može se propisati obveza kontroloru podataka da se savjetuje s Agencijom i da od nje pribavi prethodno odobrenje u vezi s obradom koju obavlja za izvršenje zadataka u javnom interesu, uključujući i obradu u vezi sa socijalnom i zdravstvenom zaštitom.

Članak 39.

(Imenovanje službenika za zaštitu osobnih podataka)

- (1) Kontrolor podataka i obrađivač dužni su imenovati službenika za zaštitu osobnih podataka u slučajevima:
 - a) ako obradu obavlja javno tijelo, osim sudova koji postupaju u granicama sudske nadležnosti;
 - b) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od postupaka obrade koje zbog svoje prirode, opsega i/ili svrhe zahtijevaju redovito i sustavno praćenje nositelja podataka u velikom broju ili

- c) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od opsežne obrade posebnih kategorija podataka na temelju članka 11. ovog Zakona i osobnih podataka u vezi s kaznenom osuđivanosti i kaznenim djelima iz članka 12. ovog Zakona.
- (2) Skupina gospodarskih subjekata može imenovati jednog službenika za zaštitu osobnih podataka, uz uvjet da je službenik za zaštitu osobnih podataka lako dostupan iz svakog sjedišta ili poslovnog nastana.
- (3) Ako je kontrolor podataka ili obrađivač javno tijelo, za više takvih tijela može se imenovati jedan službenik za zaštitu osobnih podataka uzimajući u obzir njihovu organizacijsku strukturu i veličinu.
- (4) U slučajevima koji nisu navedeni u stavku (1) ovog članka, kontrolor podataka ili obrađivač ili udruga i drugo tijelo koje predstavlja kategoriju kontrolora podataka ili obrađivača mogu, odnosno moraju u slučajevima kada je to propisano posebnim zakonom, imenovati službenika za zaštitu osobnih podataka. Službenik za zaštitu osobnih podataka može obavljati poslove u ime tih udruga i drugih tijela koja predstavljaju kontrolore podataka ili obrađivače.
- (5) Službenik za zaštitu osobnih podataka imenuje se na temelju njegovih stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksi u području zaštite osobnih podataka i sposobnosti obavljanja zadataka iz članka 41. ovog Zakona.
- (6) Službenik za zaštitu osobnih podataka može biti zaposlen kod kontrolora podataka ili obrađivača ili može obavljati poslove na temelju ugovora o djelu.
- (7) Kontrolor podataka ili obrađivač objavljuje kontaktne podatke službenika za zaštitu osobnih podataka i dostavlja ih Agenciji.

Članak 40.

(Status službenika za zaštitu osobnih podataka)

- (1) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu osobnih podataka bude na odgovarajući način i pravodobno uključen u sva pitanja koja se tiču zaštite osobnih podataka.
- (2) Kontrolor podataka i obrađivač podržavaju službenika za zaštitu osobnih podataka u obavljanju zadataka iz članka 41. ovog Zakona, pružajući mu potrebna sredstva za obavljanje tih zadataka i ostvarivanje pristupa osobnim podacima i postupcima obrade, kao i za održavanje njegovog stručnog znanja.
- (3) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu osobnih podataka ne prima nikakve instrukcije pri obavljanju tih zadataka. Kontrolor podataka ili obrađivač ne može ga razriješiti dužnosti ili kazniti zbog toga što vrši svoje zadatke. Službenik za zaštitu osobnih podataka odgovara izravno najvišoj razini rukovodstva kontrolora podataka ili obrađivača.
- (4) Nositelj podataka može se obratiti službeniku za zaštitu osobnih podataka za sva pitanja koja se tiču obrade njegovih osobnih podataka i ostvarivanja njegovih prava iz ovog Zakona.
- (5) Službenik za zaštitu osobnih podataka, u vezi s obavljanjem svojih zadataka, dužan je sve podatke do kojih dođe u postupku obrade podataka čuvati kao službenu tajnu u skladu sa zakonom.
- (6) Službenik za zaštitu osobnih podataka može izvršavati i druge zadatke i dužnosti. Kontrolor podataka ili obrađivač osigurava da ti zadaci i dužnosti ne dovedu do sukoba interesa.

Članak 41.

(Zadatak službenika za zaštitu osobnih podataka)

- (1) Službenik za zaštitu osobnih podataka obavlja sljedeće zadatke:
 - a) informiranje i savjetovanje kontrolora podataka ili obrađivača i zaposlenih koji obavljaju obradu podataka njihovih obveza iz ovog Zakona i drugih zakona kojima se propisuje zaštita osobnih podataka;
 - b) praćenje poštivanja ovog Zakona i drugih zakona kojima se propisuje zaštita osobnih podataka, kao i politika kontrolora podataka ili obrađivača u vezi sa zaštitom osobnih podataka, uključujući i podjelu odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji sudjeluju u radnjama obrade, kao i s tim povezanim revizijama;
 - c) pružanje savjeta, kada je to zatraženo, u pogledu procjene utjecaja na zaštitu osobnih podataka i praćenje njezinog izvršenja u skladu s člankom 37. ovog Zakona;
 - d) suradnja s Agencijom;
 - e) djelovanje kao kontaktna točka za Agenciju o pitanjima koja se tiču obrade, što uključuje i prethodno savjetovanje iz članka 38. ovog Zakona, te savjetovanje, po potrebi, o svim drugim pitanjima.
- (2) Službenik za zaštitu osobnih podataka pri obavljanju svojih zadataka vodi računa o riziku povezanim s radnjom obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade.

Članak 42.

(Kodeks ponašanja)

- (1) Agencija izdaje preporuku za izradu kodeksa ponašanja s ciljem pravilne primjene ovog Zakona, uzimajući u obzir specifičnost različitih sektora obrade i posebne potrebe mikro, malih i srednjih gospodarskih subjekata.
- (2) Udruga i drugi subjekt koji predstavlja kategorije kontrolora podataka ili obrađivača mogu izraditi kodekse ponašanja, radi preciziranja primjene ovog Zakona, a koji se odnose na:
 - a) pravednu i transparentnu obradu;
 - b) legitimne interese kontrolora podataka u posebnim kontekstima;
 - c) prikupljanje osobnih podataka;
 - d) pseudonimizaciju osobnih podataka;
 - e) informiranje javnosti i nositelja podataka;
 - f) ostvarivanje prava nositelja podataka;
 - g) informiranje i zaštitu djece i način pribavljanja suglasnosti nositelja roditeljskog prava nad djetetom;
 - h) mjere i postupke iz čl. 26. i 27. ovog Zakona, kao i mjere za postizanje sigurnosti obrade iz članka 34. ovog Zakona;
 - i) izvješćivanje Agencije o povredama osobnih podataka i obavješćavanje nositelja podataka o takvim povredama;
 - j) prijenos osobnih podataka drugim zemljama ili međunarodnim organizacijama ili
 - k) izvansudske postupke i druge postupke za rješavanje sporova između kontrolora podataka i nositelja podataka u vezi s obradom, ne dovodeći u pitanje prava nositelja podataka na temelju čl. 108. i 110. ovog Zakona.
- (3) Kodeks ponašanja iz stavka (2) ovog članka obvezno sadrži odredbe koje pravnoj osobi iz članka 43. stavka (1) ovog Zakona omogućavaju da provodi obvezno praćenje

usklađenosti kontrolora podataka ili obrađivača koji su se obvezali na njegovu primjenu, ne dovodeći u pitanje nadležnosti Agencije.

- (4) Udruga i subjekt iz stavka (2) ovog članka koji namjeravaju izraditi kodeks ponašanja ili izmijeniti i proširiti postojeći kodeks ponašanja dostavljaju Agenciji nacrt kodeksa ponašanja, odnosno izmjene ili proširenje kodeksa ponašanja.
- (5) Agencija daje mišljenje o tome je li nacrt kodeksa sukladan s ovim Zakonom te odobrava nacrt kodeksa ako ocijeni da osigurava dovoljno odgovarajuće zaštitne mjere.
- (6) Ako Agencija odobri nacrt kodeksa ponašanja, odnosno izmjene ili dopune kodeksa ponašanja, u skladu sa stavkom (5) ovog članka, Agencija registrira i objavljuje kodeks ponašanja.
- (7) Kontrolor podataka ili obrađivač na koje se ovaj Zakon ne primjenjuje, u skladu s člankom 6. ovog Zakona, mogu primjenjivati kodeks ponašanja koji je odobren u skladu sa stavkom (5) ovog članka, kako bi osigurali odgovarajuće zaštitne mjere u sklopu prijenosa osobnih podataka drugoj zemlji ili međunarodnoj organizaciji, uz uvjete iz članka 48. stavka (2) točke d) ovog Zakona.
- (8) Kontrolor podataka ili obrađivač iz stavka (7) ovog članka, putem ugovornih ili drugih pravno obvezujućih instrumenata, preuzima obvezujuće i provedive obveze za primjenu zaštitnih mjera, uključujući i mjere vezane za prava nositelja podataka.

Članak 43.

(Praćenje odobrenog kodeksa ponašanja)

- (1) Pravna osoba s odgovarajućim stupnjem stručnosti za predmet kodeksa ponašanja može pratiti usklađenost s kodeksom ponašanja, ako ju je u tu svrhu akreditirala agencija.
- (2) Pravna osoba iz stavka (1) ovog članka može biti akreditirana za praćenje usklađenosti s kodeksom ponašanja ako je:
 - a) Agenciji dokazala svoju neovisnost i stručnost za predmet kodeksa ponašanja;
 - b) uspostavila postupke koji joj omogućavaju da ocjenjuje kvalificiranost kontrolora podataka i obrađivača za primjenu kodeksa ponašanja, da prati njihovu primjenu odredaba kodeksa ponašanja te da periodično preispituje njezino funkcioniranje;
 - c) uspostavila postupke i strukture za rješavanje prigovora na kršenja kodeksa ponašanja ili na način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio kodeks ponašanja i učinio te postupke i strukture transparentnim nositeljima podataka i javnosti i
 - d) Agenciji dokazala da njezini zadaci i dužnosti ne dovode do sukoba interesa.
- (3) Pravna osoba iz stavka (1) ovog članka, uz primjenu odgovarajućih zaštitnih mjera, poduzima odgovarajuće radnje u slučajevima kršenja kodeksa ponašanja od kontrolora podataka ili obrađivača, što uključuje suspendiranje ili isključenje iz kodeksa ponašanja.
- (4) Pravna osoba iz stavka (1) ovog članka dužna je obavijestiti Agenciju o radnjama i razlozima iz stavka (3) ovog članka.
- (5) Agencija oduzima akreditaciju pravnoj osobi koja više ne ispunjava uvjete za akreditaciju ili ako pravna osoba krši odredbe ovog Zakona.
- (6) Ovaj se članak ne primjenjuje na obradu osobnih podataka koju obavlja javno tijelo.

Članak 44.
(Certifikacija)

- (1) Agencija preporučuje uspostavu postupka certifikacije zaštite osobnih podataka, pečata i oznaka za zaštitu podataka s ciljem dokazivanja poštivanja odredaba ovog Zakona, posebno uzimajući u obzir potrebe mikro, malih i srednjih pravnih osoba.
- (2) Postupak certifikacije zaštite osobnih podataka, pečata i oznaka može biti uspostavljen i radi dokazivanja postojanja odgovarajućih zaštitnih mjera koje osiguravaju kontrolor podataka i obrađivač na koje se ovaj Zakon, u skladu s člankom 6. ovog Zakona, ne odnosi u sklopu prijenosa osobnih podataka drugoj zemlji ili međunarodnoj organizaciji, uz uvjete iz članka 48. stavka (2) točke d) ovog Zakona.
- (3) Kontrolori podataka ili obrađivači iz stavka (2) ovog članka, putem ugovornih ili drugih pravno obvezujućih instrumenata, prihvaćaju primjenu odgovarajućih zaštitnih mjera, uključujući i mjere u vezi s nositeljem podataka.
- (4) Certifikacija je dobrovoljna i dostupna putem postupka koji je transparentan.
- (5) Certifikacija, u skladu s ovim člankom, ne umanjuje odgovornost kontrolora podataka ili obrađivača za poštivanje ovog Zakona i ne dovodi u pitanje nadležnosti Agencije.
- (6) Certifikaciju, u skladu s ovim člankom, izdaje certifikacijsko tijelo iz članka 45. ovog Zakona na temelju kriterija koje je odobrila Agencija.
- (7) Kontrolor podataka ili obrađivač, u postupku certifikacije, certifikacijskom tijelu pruža sve informacije i omogućava pristup aktivnostima obrade koje su potrebne za postupak certifikacije.
- (8) Certifikat se izdaje kontroloru podataka ili obrađivaču najduže na tri godine i može se obnoviti pod istim uvjetima.
- (9) Certifikacijsko tijelo oduzima certifikat kontroloru ili obrađivaču ako više ne ispunjava uvjete za izdavanje certifikata.
- (10) Agencija postupak certifikacije zaštite osobnih podataka, pečata i oznake unosi u evidenciju i javno objavljuje.

Članak 45.
(Certifikacijsko tijelo)

- (1) Agencija provodi akreditiranje certifikacijskog tijela, s odgovarajućim stupnjem stručnosti iz područja zaštite osobnih podataka.
- (2) Certifikacijsko tijelo obavještava Agenciju o odluci o izdavanju i obnavljanju certifikata kako bi Agencija mogla primijeniti ovlasti iz članka 103. stavka (2) točke h) ovog Zakona.
- (3) Certifikacijsko tijelo može biti akreditirano samo ako:
 - a) Agenciji na zadovoljavajući način dokaže svoju neovisnost i stručnost u predmetu certifikacije;
 - b) se obveže da će poštivati kriterije iz članka 44. stavka (6) ovog Zakona;
 - c) uspostavi postupke za izdavanje, periodično preispitivanje i povlačenje certifikacije, pečata i oznaka za zaštitu podataka;
 - d) uspostavi postupke i strukture za rješavanje prigovora na kršenja certifikacije ili način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio certifikaciju i učini te postupke i strukture transparentnim nositeljima podataka i javnosti;
 - e) Agenciji dokaže da njegovi zadaci i dužnosti ne dovode do sukoba interesa.
- (4) Akreditiranje certifikacijskog tijela provodi se na temelju kriterija koje je propisala Agencija.

- (5) Akreditiranje se izdaje na najviše pet godina i može se obnoviti pod istim uvjetima ako certifikacijsko tijelo i dalje ispunjava zahtjeve iz ovog članka.
- (6) Ne dovodeći u pitanje Dio četvrti ovog Zakona, Agencija povlači akreditaciju certifikacijskog tijela ako se uvjeti iz stavka (3) ovog članka ne ispune ili više nisu ispunjeni, ili ako se radnjama koje poduzima certifikacijsko tijelo krši ovaj Zakon.
- (7) Certifikacijsko tijelo odgovorno je za pravilnu procjenu koja dovodi do certifikacije ili oduzimanja certifikata, ne dovodeći u pitanje odgovornost kontrolora podataka ili obrađivača za poštivanje ovog Zakona.
- (8) Certifikacijsko tijelo u pisanom obliku obavještava Agenciju o razlozima za izdavanje ili oduzimanje certifikata.
- (9) Agencija javno objavljuje kriterije iz članka 44. stavka (6) ovog Zakona.

POGLAVLJE IV. PRIENOS OSOBNOG PODATKA U DRUGU ZEMLJU ILI MEĐUNARODNU ORGANIZACIJU

Članak 46.

(Opća načela prijenosa)

Svaki prijenos osobnog podatka čija je obrada u tijeku ili je namijenjen daljnjoj obradi nakon njegovog prenošenja u drugu zemlju ili međunarodnu organizaciju može se izvršiti samo ako je takav prijenos sukladan s odredbama ovog Zakona, što obuhvaća i daljnji prijenos osobnog podatka iz druge zemlje ili međunarodne organizacije u još jednu drugu zemlju ili međunarodnu organizaciju.

Članak 47.

(Prijenos na temelju prikladnosti razine zaštite osobnog podatka)

- (1) Prijenos osobnog podatka u drugu zemlju, na dio njezina teritorija ili u jedan ili više sektora u toj zemlji ili međunarodnu organizaciju može se obaviti ako je utvrđeno da ta druga zemlja, dio njezina teritorija ili jedan ili više sektora u toj zemlji ili ta međunarodna organizacija osiguravaju prikladnu razinu zaštite osobnog podatka.
- (2) Smatra se da je prikladna razina zaštite iz stavka (1) ovog članka osigurana u zemlji, dijelovima njezina teritorija ili jednom ili više sektora u toj zemlji ili međunarodnoj organizaciji za koju je Europska unija utvrdila da osigurava prikladnu razinu zaštite osobnog podatka.
- (3) Odluku o prikladnosti razine zaštite osobnog podatka iz stavka (1) ovog članka donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stavka (3) ovog članka uzimajući u obzir:
 - a) načelo vladavine prava, poštivanje ljudskih prava i temeljnih sloboda, sektorsko zakonodavstvo, uključujući zakonodavstvo o javnoj sigurnosti, obrani, državnoj sigurnosti, kaznenom pravu i pristupu javnih tijela osobnim podacima, kao i primjenu tih propisa, pravila o zaštiti osobnih podataka, pravila struke i mjere osiguranja zaštite osobnog podatka, uključujući pravila o daljnjem prijenosu osobnog podatka u drugu zemlju ili međunarodnu organizaciju koja se primjenjuju u praksi sudova i drugih tijela vlasti u drugoj zemlji ili međunarodnoj organizaciji, kao i djelotvornost ostvarivanja prava nositelja osobnih podataka, a posebno djelotvornost upravnih i sudskih postupaka zaštite prava nositelja osobnih podataka;

- b) postojanje i učinkovitost rada nadzornog tijela u drugoj zemlji ili tijela koje je nadležno za međunarodnu organizaciju u ovom području, s ovlašću da osigura primjenu pravila o zaštiti osobnih podataka i pokrene postupke zaštite osobnih podataka u slučaju njihovog nepoštivanja, pruži pomoć i savjetuje nositelje osobnih podataka u ostvarivanju njihovih prava, kao i da surađuje s nadzornim tijelima drugih zemalja;
- c) međunarodne obveze koje je druga zemlja ili međunarodna organizacija preuzela ili druge obveze koje proizlaze iz pravno obvezujućih međunarodnih ugovora ili drugih pravnih instrumenata, kao i iz članstva u multilateralnim ili regionalnim organizacijama, a posebno u vezi sa zaštitom osobnih podataka.
- (5) Agencija kontinuirano prati stanje u području zaštite osobnog podatka u drugoj zemlji, dijelu njezina teritorija, jednom ili više sektora unutar te zemlje ili međunarodnoj organizaciji i o tome po potrebi izvještuje Vijeće ministara Bosne i Hercegovine.
- (6) Izvješće iz stavka (5) ovog članka uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija koje su od značaja za preispitivanje postojanja prikladne razine zaštite osobnih podataka, na temelju čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stavka (3) ovog članka.
- (7) Odluka donesena na temelju stavka (3) ovog članka ne dovodi u pitanje prijenos osobnih podataka u drugu zemlju, na teritorij ili u jedan ili više određenih sektora unutar te druge zemlje ili međunarodnu organizaciju u skladu s čl. 48. – 51. ovog Zakona.
- (8) Popis zemalja, dio njihovih teritorija, jedan ili više sektora unutar zemlje i međunarodnih organizacija, za koje je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju prikladnu razinu zaštite osobnih podataka, objavljuje se u "Službenom glasniku BiH" i na službenoj internetskoj stranici Agencije.
- Članak 48.
- (Prijenos na koji se primjenjuju odgovarajuće zaštitne mjere)
- (1) Kontrolor podataka ili obrađivač može prenijeti osobne podatke u drugu zemlju, na dio njezina teritorija, u jedan ili više sektora unutar te zemlje ili u međunarodnu organizaciju za koju popisom iz članka 47. stavka (8) ovog Zakona nije utvrđeno postojanje prikladne razine zaštite osobnih podataka samo ako je kontrolor podataka ili obrađivač osigurao odgovarajuće zaštitne mjere tih podataka i ako su nositelji osobnih podataka osigurana provediva prava i djelotvorna sudska zaštita.
- (2) Odgovarajuće zaštitne mjere iz stavka (1) ovog članka mogu se, bez posebnog odobrenja Agencije, osigurati:
- pravno obvezujućim aktom sačinjenim između javnih tijela;
 - obvezujućim poslovnim pravilima u skladu s člankom 49. ovog Zakona;
 - odobrenim kodeksom ponašanja u skladu s člankom 42. ovog Zakona s obvezujućim i izvršnim obvezama kontrolora podataka ili obrađivača u drugoj zemlji za primjenu odgovarajućih zaštitnih mjera, među ostalim i u pogledu prava nositelja podataka ili
 - odobrenim postupkom certifikacije u skladu s člankom 44. ovog Zakona s obvezujućim i izvršnim obvezama kontrolora podataka ili obrađivača u drugoj zemlji za primjenu odgovarajućih zaštitnih
- mjera, među ostalim i u pogledu prava nositelja podataka.
- (3) Odgovarajuće zaštitne mjere iz stavka (1) ovog članka mogu se osigurati standardnim ugovornim klauzulama o zaštiti podataka koje donosi Agencija.
- (4) Uz uvjet da to odobri Agencija, odgovarajuće zaštitne mjere iz stavka (1) ovog članka također mogu biti posebno osigurane:
- ugovorom između kontrolora podataka ili obrađivača i kontrolora podataka, obrađivača ili primatelja osobnih podataka u drugoj zemlji ili međunarodnoj organizaciji ili
 - odredbama koje se unose u sporazume između javnih tijela i koji sadrže provediva i djelotvorna prava nositelja podataka.
- Članak 49.
- (Obvezujuća poslovna pravila)
- (1) Obvezujuća poslovna pravila određuju najmanje:
- strukturu i podatke za kontakt skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost i svakog od njihovih članova;
 - prijenose podataka ili skupove prijenosa, uz navođenje kategorije osobnih podataka, vrste obrade i njezine svrhe, kategorije nositelja podataka i određenja druge zemlje ili zemalja o kojima se radi;
 - njihovu pravno obvezujuću prirodu;
 - primjenu načela zaštite podataka, a posebice ograničenja svrhe, smanjenja količine podataka, ograničenja roka čuvanja, kvalitete podataka, tehničke i integrirane zaštite podataka, pravnog temelja obrade, obrade posebnih kategorija osobnih podataka, mjera za postizanje sigurnosti podataka i uvjeta u vezi s daljnjim prijenosom tijelima koja nisu obvezana obvezujućim poslovnim pravilima;
 - prava nositelja podataka u vezi s obradom i načine ostvarivanja tih prava, uključujući i pravo da se na njih ne primjenjuju odluke koje se temelje isključivo na automatskoj obradi, što uključuje i izradu profila u skladu s člankom 24. ovog Zakona, pravo na prigovor Agenciji i pravo na sudska zaštitu, u skladu s člankom 110. ovog Zakona, a u odgovarajućim slučajevima i pravo na naknadu štete za kršenje obvezujućih poslovnih pravila;
 - da kontrolor podataka ili obrađivač sa sjedištem ili poslovnim nastanom na teritoriju Bosne i Hercegovine prihvaća odgovornost za sva kršenja obvezujućih poslovnih pravila od bilo kojeg člana koji nema sjedište ili poslovni nastan u Bosni i Hercegovini ili je kontrolor podataka ili obrađivač u cjelini ili djelomično izuzet od odgovornosti ako dokaže da taj član skupine gospodarskih subjekata nije odgovoran za događaj koji je prouzročio štetu;
 - na koji način se nositeljima podataka, osim informacija iz čl. 15. i 16. ovog Zakona, pružaju informacije o obvezujućim poslovnim pravilima, posebice o odredbama iz toč. d), e) i f) ovog stavka;
 - zadatke svakog službenika za zaštitu podataka imenovanog u skladu s člankom 39. ovog Zakona ili bilo koje druge osobe ili subjekta odgovornog za praćenje usklađenosti s obvezujućim poslovnim pravilima u skupini gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, kao i praćenje osposobljenosti i rješavanje prigovora;
 - postupke povodom prigovora;
 - mehanizme unutar skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost

- kojima se osigurava provjera poštivanja obvezujućih poslovnih pravila, što uključuje reviziju zaštite podataka i metode za osiguravanje korektivnih mjera za zaštitu prava nositelja podataka. Rezultate takve provjere potrebno je priopćiti osobi ili subjektu iz točke h) ovog stavka i upravljačkom tijelu skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, a na zahtjev ih je potrebno staviti na raspolaganje Agenciji;
- k) mehanizme za izvješćivanje i vođenje evidencije o promjenama pravila i izvješćivanje Agencije o tim promjenama;
- l) mehanizam suradnje s Agencijom radi osiguravanja usklađenosti svakog člana skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, prije svega tako što se Agenciji stave na raspolaganje rezultati provjera mjera iz točke j) ovog stavka;
- m) mehanizme za izvješćivanje Agencije o bilo kakvim pravnim obvezama koje se odnose na člana skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost i primjenjuju se u drugoj zemlji, a koji bi mogli imati značajan negativan utjecaj na jamstva sadržana u obvezujućim poslovnim pravilima;
- n) odgovarajuće osposobljavanje iz područja zaštite osobnih podataka za osoblje koje ima stalan ili redovit pristup osobnim podacima.
- (2) Agencija odobrava obvezujuća poslovna pravila uz uvjet da:
- a) su pravno obvezujuća i da se primjenjuju na svakog zainteresiranog člana određene skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, što uključuje i njihove zaposlenike, te da ih oni primjenjuju;
- b) nositeljima podataka izričito daju provediva prava u vezi s obradom njihovih osobnih podataka;
- c) ispunjavaju uvjete iz stavka (1) ovog članka.
- (3) Agencija može odrediti format i postupke razmjene informacija između kontrolora podataka, obrađivača i Agencije za obvezujuća poslovna pravila u smislu ovog članka.
- Članak 50.
- (Prijenos ili otkrivanje podataka koji nisu dopušteni)
- Svaka presuda suda, tribunala ili odluka upravnog tijela druge zemlje kojom se od kontrolora podataka ili obrađivača zahtijeva prijenos ili otkrivanje osobnih podataka može biti priznata ili provedena samo ako se temelji na međunarodnom sporazumu, poput sporazuma o uzajamnoj pravnoj pomoći, između druge zemlje koja je podnijela zahtjev i Bosne i Hercegovine, ne dovodeći u pitanje druge razloge za prijenos u skladu s ovim poglavljem.
- Članak 51.
- (Odstupanje u posebnim slučajevima)
- (1) Prijenos ili skup prijenosa osobnih podataka u drugu zemlju ili međunarodnu organizaciju, ako ne postoji odluka o prikladnosti u skladu s člankom 47. stavkom (3) ovog Zakona ili odgovarajuće zaštitne mjere u skladu s člankom 48. ovog Zakona, uključujući i obvezujuća poslovna pravila iz članka 49. ovog Zakona, obavlja se samo uz jedan od sljedećih uvjeta:
- a) nositelj podataka je izričito suglasan s predloženim prijenosom, nakon što je upoznat s mogućim rizicima takvih prijenosa zbog nepostojanja odluke o prikladnosti i odgovarajućih zaštitnih mjera iz članka 48. ovog Zakona;
- b) prijenos je potreban za provedbu ugovora između nositelja podataka i kontrolora podataka ili provođenje predugovornih mjera na zahtjev nositelja podataka;
- c) prijenos je potreban radi sklapanja ili provedbe ugovora sklopljenog u interesu nositelja podataka između kontrolora podataka i druge fizičke ili pravne osobe;
- d) prijenos je potreban iz bitnih razloga javnog interesa;
- e) prijenos je potreban za postavljanje, ostvarivanje ili obranu pravnih zahtjeva;
- f) prijenos je potreban za zaštitu ključnih interesa nositelja podataka ili drugih osoba ako nositelj podataka fizički ili pravno nije sposoban dati suglasnost;
- g) prijenos se obavlja iz registra koji, prema pravnim propisima u Bosni i Hercegovini, služi za pružanje informacija javnosti i koji je dostupan na uvid javnosti ili bilo kojoj osobi koja može dokazati postojanje legitimnog interesa, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani posebnim zakonom za uvid u tom posebnom slučaju.
- (2) Prijenos ili skup prijenosa osobnih podataka u drugu zemlju ili međunarodnu organizaciju u slučaju kada temelj za prijenos ne može biti čl. 47. ili 48. ovog Zakona, uključujući i obvezujuća poslovna pravila iz članka 49. ovog Zakona, i kada se ne primjenjuje nijedno odstupanje u posebnim slučajevima iz stavka (1) ovog članka, može se obaviti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničeni broj nositelja podataka i ako je potreban za potrebe bitnih, legitimnih interesa kontrolora podataka nad kojima ne prevladavaju interesi ili prava i slobode nositelja podataka, a kontrolor podataka je procijenio sve okolnosti prijenosa podataka i na temelju te procjene predvidio je odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka. Kontrolor podataka o prijenosu obavještava Agenciju. Uz informacije iz čl. 15. i 16. ovog Zakona, kontrolor podataka obavještava nositelja podataka o prijenosu i o važnim legitimnim interesima.
- (3) Prijenos na temelju stavka (1) točke g) ovog članka ne uključuje osobne podatke u cjelini ni cijele kategorije osobnih podataka sadržanih u registru. Kada je registar namijenjen za uvid osobama koje imaju legitiman interes, prijenos se obavlja samo ako to zahtijevaju te osobe ili ako su one primatelji.
- (4) Na aktivnosti koje obavljaju javna tijela prilikom izvršenja svojih javnih ovlasti ne primjenjuju se stavak (1) toč. a), b) i c) i stavak (2) ovog članka.
- (5) Javni interes iz stavka (1) točke d) ovog članka mora biti propisan zakonom koji se primjenjuje na kontrolora podataka.
- (6) Ako nije donesena odluka o prikladnosti, iz bitnih razloga javnog interesa posebnim propisom mogu biti izričito propisana ograničenja prijenosa određenih kategorija osobnih podataka drugoj zemlji ili međunarodnoj organizaciji.
- (7) Kontrolor podataka ili obrađivač dokumentira procjenu, kao i odgovarajuće zaštitne mjere iz st. (1) i (2) ovog članka, u evidencije iz članka 32. ovog Zakona.

POGLAVLJE V. POSEBNI SLUČAJEVI OBRADE**Članak 52.**

- (Obrada osobnog podatka i sloboda izražavanja i informiranja)
- (1) Obrada osobnih podataka prilikom korištenja prava na slobodu izražavanja i informiranja, što uključuje obradu isključivo u novinarske svrhe, u svrhe akademskog, umjetničkog ili književnog izričaja, obavlja se u skladu s posebnim propisima.
 - (2) Posebnim propisima iz stavka (1) ovog članka utvrđuju se iznimke ili odstupanja od primjene Poglavlja I., Poglavlja II., Poglavlja III., Poglavlja IV., Poglavlja V. ovog dijela i Dijela četvrtog ovog Zakona, ako su takve iznimke ili odstupanja potrebni za usklađivanje prava na zaštitu osobnih podataka sa slobodom izražavanja i informiranja.

Članak 53.

(Obrada osobnog podatka i javni pristup službenim dokumentima)

- (1) Javno tijelo i nadležno tijelo, u skladu sa zakonom koji se primjenjuje na to tijelo, mogu u javnom interesu otkriti osobne podatke iz službenih dokumenata kojima raspolažu kako bi se javni pristup službenim dokumentima uskladio s pravom na zaštitu osobnih podataka u skladu s ovim Zakonom.
- (2) Ovaj Zakon primjenjuje se prilikom primjene propisa o slobodi pristupa informacijama u Bosni i Hercegovini.

Članak 54.

(Obrada jedinstvenog matičnog broja fizičke osobe)

- (1) Posebni uvjeti za obradu jedinstvenog matičnog broja fizičke osobe ili bilo kojeg drugog identifikatora opće primjene propisuju se posebnim zakonom.
- (2) Jedinstveni matični broj fizičke osobe ili bilo koji drugi identifikator opće primjene iz stavka (1) ovog članka obrađuje se samo uz primjenu odgovarajućih zaštitnih mjera u pogledu prava i sloboda nositelja podataka u skladu s ovim Zakonom.

Članak 55.

(Obrada osobnih podataka u kontekstu zaposlenja)

- (1) Posebnim zakonom ili kolektivnim ugovorom preciziraju se pravila s ciljem osiguravanja zaštite prava i sloboda u vezi s obradom osobnih podataka u kontekstu zaposlenja, posebice za potrebe zapošljavanja, provedbe ugovora o radu, uključujući i ispunjavanje obveza propisanih zakonom ili kolektivnim ugovorima, za potrebe upravljanja, planiranja i organiziranja rada, jednakosti i različitosti na radnom mjestu, zdravlja i sigurnosti na radu, zaštite imovine poslodavca ili klijenta i za potrebe individualnog ili kolektivnog ostvarivanja i uživanja prava i pogodnosti iz radnog odnosa, kao i za potrebe prestanka radnog odnosa.
- (2) Pravila iz stavka (1) ovog članka uključuju prikladne i posebne mjere za zaštitu ljudskog dostojanstva nositelja podataka, njegovih legitimnih interesa i temeljnih prava, posebice u vezi s transparentnošću obrade, prijenosom osobnih podataka unutar skupine gospodarskih subjekata ili skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, kao i sustavima praćenja na radnom mjestu.

Članak 56.

(Zaštitne mjere i odstupanja u vezi s obradom osobnog podatka u svrhu arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe)

- (1) Na obradu osobnih podataka u svrhu arhiviranja u javnom interesu, u svrhu znanstvenog ili povijesnog istraživanja ili u statističke svrhe primjenjuju se odgovarajuće zaštitne

mjere u skladu s ovim Zakonom glede prava i sloboda nositelja podataka.

- (2) Zaštitnim mjerama iz stavka (1) ovog članka osigurava se primjena tehničkih i organizacijskih mjera, posebice onih kojima se jamči primjena načela smanjenja opsega podataka, koje mogu uključivati pseudonimizaciju, ako se svrhe mogu ostvariti tako.
- (3) Ako se svrhe iz stavka (1) ovog članka mogu postići daljnjom obradom koja ne omogućava ili više ne omogućava identifikaciju nositelja podataka, te svrhe se ostvaruju na taj način.
- (4) Ako se osobni podaci obrađuju u svrhu znanstvenog ili povijesnog istraživanja ili u statističku svrhu, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih u čl. 17., 18., 20. i 23. ovog Zakona, uz primjenu uvjeta i mjera zaštite iz stavka (1) ovog članka, ako je vjerojatno da bi ta prava mogla spriječiti ili ozbiljno ugroziti ostvarivanje tih posebnih svrha pa su takva odstupanja nužna za postizanje tih svrha.
- (5) Ako se osobni podaci obrađuju u svrhu arhiviranja u javnom interesu, samo se posebnim zakonom mogu predvidjeti odstupanja od prava navedenih u čl. 17., 18., 20., 21., 22. i 23. ovog Zakona, uz primjenu uvjeta i mjera zaštite iz stavka (1) ovog članka, ako je vjerojatno da bi ta prava mogla spriječiti ili ozbiljno ugroziti ostvarivanje te posebne svrhe pa su takva odstupanja nužna za postizanje te svrhe.
- (6) Ako obrada iz st. (2) i (3) ovog članka istodobno služi i drugoj svrsi, odstupanja se primjenjuju samo za obradu u svrhe koje su navedene u tim stavcima.

Članak 57.

(Videonadzor)

- (1) Praćenje određenog prostora putem videonadzora dopušteno je samo ako je to nužno za zaštitu osoba i imovine i ako ne prevladaju interesi nositelja podataka.
- (2) Videonadzorom mogu biti obuhvaćeni samo prostori ili dijelovi prostora čiji je nadzor nužan radi postizanja svrhe iz stavka (1) ovog članka.
- (3) Uspostavljanje videonadzora nad javno dostupnim objektima velikih površina, kao što su sportski objekti, zabavni centri, trgovački centri ili parkirališta ili vozila javnog prijevoza, dopušteno je isključivo u cilju zaštite života, zdravlja i slobode osobe te imovine.
- (4) Kontrolor podataka koji se služi videonadzorom dužan je donijeti odluku koja će sadržavati pravila obrade s ciljem poštivanja prava na zaštitu privatnosti i osobnog života nositelja podataka, ako videonadzor nije propisan zakonom.
- (5) Kontrolor podataka ili obrađivač dužan je na vidnom mjestu istaknuti oznaku o videonadzoru. Oznaka o videonadzoru sadrži sljedeće informacije: da je prostor pod videonadzorom, podatke o kontroloru podataka odnosno obrađivaču i kontaktne podatke putem kojih nositelj podataka može ostvariti svoja prava. Oznaka treba biti vidljiva najkasnije prilikom ulaska u vidokrug snimanja.
- (6) Kontrolor podataka ili obrađivač dužan je, u sustavu videonadzora javno dostupnih objekata iz stavka (3) ovog članka, bilježiti zapise o uporabi sustava i čuvati ih najmanje 12 mjeseci. Zapisi omogućavaju utvrđivanje datuma i vremena te identiteta osobe koja je ostvarila uvid u sustav videonadzora.
- (7) Za uspostavu videonadzora u stambenim odnosno poslovno-stambenim zgradama potrebna je suglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova. Videonadzorom se može obuhvatiti samo pristup ulasku i

- izlasku iz stambene zgrade te zajedničke prostorije u stambenim zgradama.
- (8) Praćenje javnih prostora putem videonadzora u svrhe iz članka 1. stavka (1) točke c) ovog Zakona dopušteno je samo ako je to propisano posebnim zakonom.

Članak 57a.

- (Obrada biometrijskih podataka u svrhu sigurne identifikacije)
- (1) Obrada biometrijskih podataka može se provesti samo ako je propisana zakonom ili ako je nužna za zaštitu osobe, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačnu i sigurnu identifikaciju korisnika usluga, uzimajući u obzir da ne prevladavaju interesi nositelja podataka koji su u suprotnosti s obradom biometrijskih podataka iz ovog članka.
- (2) Pravni temelj za obradu biometrijskih podataka nositelja podataka, radi sigurne identifikacije korisnika usluga, izričita je suglasnost takvog nositelja podataka dana u skladu s odredbama ovog Zakona.

Članak 57b.

(Obrada biometrijskih podataka u službenim prostorijama)

Dopuštena je obrada biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija, ako je to propisano zakonom ili ako se takva obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija, uz uvjet da je zaposlenik dao izričitu suglasnost za takvu obradu biometrijskih podataka u skladu s odredbama ovog Zakona.

Članak 58.

- (Postojeća pravila o zaštiti osobnih podataka crkava i vjerskih zajednica)
- (1) Ako crkve i vjerske zajednice primjenjuju sveobuhvatna pravila u pogledu obrade osobnih podataka, ta postojeća pravila mogu se i dalje primjenjivati uz uvjet da se usklade s ovim Zakonom.
- (2) Crkve i vjerske zajednice koje primjenjuju sveobuhvatna pravila nadzire Agencija, osim ako crkva ili vjerska zajednica ne osnuje posebno neovisno nadzorno tijelo, pod uvjetom da ispunjava uvjete utvrđene u Dijelu četvrtom ovog Zakona.

Članak 59.

- (Obveza čuvanja profesionalne tajne)
- (1) Posebnim propisom može se utvrditi ograničenje Agencije iz članka 103. stavka (1) toč. f) i g) u pogledu kontrolora podataka ili obrađivača koji, na temelju posebnog propisa koji je donijelo nadležno tijelo, podliježu obvezi profesionalne tajne i drugim jednakovrijednim obvezama tajnosti, ako je to nužno i razmjerno kako bi se uskladilo pravo na zaštitu osobnih podataka s obvezom tajnosti.
- (2) Poseban propis iz stavka (1) ovog članka primjenjuje se samo na osobne podatke koje je kontrolor podataka ili obrađivač dobio kao rezultat ili primio tijekom aktivnosti koja je obuhvaćena obvezom tajnosti.

DIO TREĆI – OBRADA OSOBNOG PODATKA OD NADLEŽNOG TIJELA KAO KONTROLORA PODATAKA U SVRHU SPRJEČAVANJA, ISTRAGE I OTKRIVANJA KAZNENIH DJELA ILI PROGONA POČINITELJA KAZNENIH DJELA, IZVRŠENJE KAZNENIH SANKCIJA, UKLJUČUJUĆI ZAŠTITU OD PRIJETNJI JAVNOJ SIGURNOSTI I NJIHOVO SPRJEČAVANJE

Članak 60.

- (Načela obrade osobnih podataka od nadležnog tijela)
- (1) Načela obrade osobnih podataka od nadležnog tijela su:

- zakonitost i pravednost;
 - ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se daljnje ne smiju obrađivati na način koji nije sukladan s tim svrhama;
 - smnjenje opsega podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je potrebno za svrhe za koje se obrađuju;
 - točnost – podaci moraju biti točni i po potrebi ažurirani, moraju se poduzeti sve razumne mjere kako bi se osiguralo da osobni podaci koji nisu točni, imajući u vidu svrhe za koje se obrađuju, budu bez odgode izbrisani ili ispravljeni;
 - ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nositelja podataka, i to ne duže no što je potrebno za svrhe za koje se podaci obrađuju;
 - cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigura odgovarajuća sigurnost osobnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.
- (2) Obrada koju obavlja isto ili neko drugo nadležno tijelo u svrhu iz članka 1. stavka (1) točke c) ovog Zakona različitu od one za koju su osobni podaci prikupljeni dopuštena je:
- ako je nadležno tijelo ovlašteno za obradu takvih osobnih podataka u takvu svrhu u skladu s posebnim propisom ili
 - ako je obrada potrebna i srazmjerna drugoj zakonitoj svrsi.
- (3) Obrada koju obavlja isto ili neko drugo nadležno tijelo može uključivati arhiviranje u javnom interesu, u znanstvene, statističke ili povijesne svrhe, za svrhe iz članka 1. stavka (1) točke c) ovog Zakona, uz poduzimanje odgovarajućih zaštitnih mjera u pogledu prava i sloboda nositelja podataka.
- (4) Nadležno tijelo odgovorno je za usklađenost sa st. (1), (2) i (3) ovog članka i mora biti u mogućnosti dokazati tu usklađenost.

Članak 61.

- (Rok za čuvanje i brisanje osobnog podatka)
- (1) Rok za brisanje osobnih podataka ili za periodično preispitivanje potrebe njihovog čuvanja propisuje se posebnim zakonom.
- (2) Nadležna tijela dužna su uspostaviti pravila i procedure kojima se osigurava poštivanje roka iz stavka (1) ovog članka.

Članak 62.

- (Razlika između različitih kategorija nositelja podataka)
- Nadležno tijelo dužno je, po potrebi i ako je to moguće, napraviti jasnu razliku između osobnih podataka različitih kategorija nositelja podataka, kao što je:
- osoba za koju postoji osnova sumnje da je počinila ili namjerava počiniti kazneno djelo;
 - osoba osuđena za kaznena djela;
 - osoba koja je žrtva kaznenog djela ili osoba glede koje postoje određene činjenice koje daju osnovu za sumnju da bi ta osoba mogla biti žrtva kaznenog djela;
 - osoba koja se dovodi u vezu s kaznenim djelom, kao što je osoba koju se može pozvati da svjedoči u istragama ili naknadnom kaznenom postupku, osoba koja može dati informacije o kaznenim djelima ili

osoba za kontaktiranje ili suradnici osoba iz toč. a) i b) ovog stavka.

Članak 63.

(Razlika između osobnih podataka i provjera kvalitete osobnih podataka)

- (1) Nadležno tijelo dužno je utvrditi mehanizam kojim će se osigurati razlikovanje osobnih podataka temeljenih na činjenicama, što je više moguće, od osobnih podataka temeljenih na osobnim procjenama.
- (2) Nadležno tijelo dužno je poduzeti sve razumne mjere kako bi osiguralo da se osobni podaci koji su netočni, nepotpuni ili neažurirani ne prenose niti stavljaju na raspolaganje. Nadležno tijelo, ako je to moguće, provjerava kvalitetu osobnih podataka prije njihova prenošenja ili stavljanja na raspolaganje. Prilikom svakog prenošenja osobnih podataka, što je više moguće, dostavljaju se potrebne informacije nadležnom tijelu koje je podatke dobilo, omogućava se ocjena stupnja točnosti, potpunosti i pouzdanosti osobnih podataka, kao i u kojoj su mjeri ažurirani.
- (3) Ako se utvrdi da su preneseni netočni osobni podaci ili da su osobni podaci preneseni nezakonito, nadležno tijelo mora bez odgode o tome obavijestiti primatelja. U tom slučaju osobni podaci moraju se ispraviti ili brisati ili obradu ograničiti u skladu s člankom 72. ovog Zakona.

Članak 64.

(Zakonitost obrade osobnog podatka od nadležnog tijela)

- (1) Obrada osobnih podataka koju obavlja nadležno tijelo zakonita je samo ako je nužna i samo u onoj mjeri u kojoj je nužna za obavljanje poslova nadležnog tijela u svrhe iz članka 1. stavka (1) točke c) ovog Zakona i ako je propisana posebnim zakonom.
- (2) Posebnim zakonom iz stavka (1) ovog članka propisuju se najmanje ciljevi obrade, osobni podaci koji se obrađuju i svrhe obrade.

Članak 65.

(Posebni uvjeti obrade)

- (1) Osobni podaci koje nadležno tijelo prikuplja za svrhe utvrđene u članku 1. stavku (1) točki c) ovog Zakona ne smiju se obrađivati u druge svrhe, osim ako je takva obrada propisana posebnim zakonom i u tom slučaju ne primjenjuju se odredbe ovog dijela Zakona.
- (2) Ako je posebnim zakonom nadležnom tijelu povjereno obavljanje poslova drukčijih od onih koje obavljaju u svrhe iz članka 1. stavka (1) točke c) ovog Zakona, u tom slučaju ne primjenjuju se odredbe ovog dijela Zakona, među ostalim i za svrhu arhiviranja u javnom interesu ili u svrhu znanstvenog ili povijesnog istraživanja ili u statističke svrhe.
- (3) Ako su posebnim zakonom koji se odnosi na nadležno tijelo koje prenosi podatke propisani posebni uvjeti za obradu, nadležno tijelo koje prenosi te osobne podatke primatelju dužno ga je obavijestiti o tim uvjetima i o zahtjevima za poštivanje tih uvjeta.

Članak 66.

(Obrada posebnih kategorija osobnih podataka od nadležnog tijela)

- (1) Zabranjena je obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije osobe ili podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji osobe.

- (2) Iznimno od stavka (1) ovog članka, obrada posebnih kategorija osobnih podataka dopuštena je isključivo ako je to nužno, pridržavajući se odgovarajućih zaštitnih mjera u pogledu prava i sloboda nositelja podataka:
 - a) ako je propisana posebnim zakonom;
 - b) radi zaštite vitalnih interesa nositelja podataka ili drugog pojedinca ili
 - c) ako se takva obrada odnosi na podatke za koje je očito da ih je objavio nositelj podataka.

Članak 67.

(Automatizirano pojedinačno donošenje odluke od nadležnog tijela)

- (1) Nadležnom tijelu zabranjeno je donositi odluke isključivo na temelju automatizirane obrade, uključujući i izradu profila, koja proizvodi negativne pravne učinke za nositelja podataka ili na njega bitno utječe, osim ako je odobreno posebnim zakonom kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode nositelja podataka, najmanje prava na sudjelovanje fizičke osobe u donošenju odluke.
- (2) Odluka iz stavka (1) ovog članka ne smije biti utemeljena na posebnim kategorijama osobnih podataka iz članka 66. ovog Zakona, osim ako su uspostavljene odgovarajuće mjere zaštite prava i sloboda i legitimnih interesa nositelja podataka.
- (3) Nadležnom tijelu zabranjena je izrada profila koji dovodi do diskriminacije osoba na temelju posebnih kategorija osobnih podataka iz članka 66. ovog Zakona.

Članak 68.

(Obavješćavanje i način ostvarivanja prava nositelja podataka)

- (1) Nadležno tijelo dužno je poduzeti sve odgovarajuće mjere kako bi se nositelju podataka pružile sve informacije iz članka 69. ovog Zakona te dale sve obavijesti u pogledu članka 67., čl. 70. – 74. i članka 87. ovog Zakona u vezi s obradom.
- (2) Informacije iz stavka (1) ovog članka daju se u sažetom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika.
- (3) Informacije iz stavka (1) ovog članka pružaju se nositelju podataka u obliku u kojem je zahtjev podnesen ili na način koji je istaknut u zahtjevu, u roku od 30 dana od dana podnošenja zahtjeva.
- (4) Nadležno tijelo dužno je olakšati ostvarivanje prava nositelja podataka iz članka 67. i čl. 70. – 74. ovog Zakona.
- (5) Nadležno tijelo dužno je nositelja podataka pisanim putem obavijestiti o daljnjim radnjama u vezi s njegovim zahtjevom, bez odgode.
- (6) Nadležno tijelo dužno je, bez naknade, pružiti informacije, odnosno poduzeti mjere na temelju članka 69. ovog Zakona, te sve pružene obavijesti ili poduzete mjere na temelju članka 67., čl. 70. – 74. ovog Zakona i članka 87. ovog Zakona.
- (7) Ako je zahtjev nositelja podataka očito neutemeljen ili pretjeran, posebice zbog njegovog učestalog ponavljanja, nadležno tijelo može:
 - a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnažanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili poduzimanja traženih mjera ili
 - b) odbiti postupiti po zahtjevu.
- (8) Teret dokazivanja očite neutemeljenosti ili pretjeranosti zahtjeva iz stavka (7) ovog članka je na nadležnom tijelu.
- (9) Ako nadležno tijelo ima opravdanu sumnju u pogledu identiteta fizičke osobe koja podnosi zahtjev iz čl. 70.

ili 72. ovog Zakona, nadležno tijelo može zatražiti dodatne informacije potrebne za potvrdu identiteta nositelja podataka.

Članak 69.

(Informacije koje se stavljaju na raspolaganje ili ustupaju nositelju podataka)

- (1) Nadležno tijelo dužno je nositelju podataka staviti na raspolaganje kao minimum sljedeće informacije:
 - a) identitet i kontaktne podatke nadležnog tijela;
 - b) kontaktne podatke službenika za zaštitu osobnih podataka, ako je primjenjivo;
 - c) svrhu obrade osobnih podataka;
 - d) o pravu na podnošenje prigovora Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu;
 - e) o postojanju prava da se od nadležnog tijela zatraži pristup svojim osobnim podacima, njihov ispravak ili brisanje ili ograničenje obrade osobnih podataka.
- (2) Osim informacija iz stavka (1) ovog članka, radi ostvarivanja njegovih prava, nadležno tijelo daje nositelju podataka sljedeće dodatne informacije:
 - a) pravni temelj obrade osobnih podataka;
 - b) rok u kojem će se osobni podaci čuvati ili ako to nije moguće, o kriterijima korištenim za utvrđivanje tog roka;
 - c) o kategorijama primatelja osobnih podataka, uključujući druge zemlje ili međunarodne organizacije, ako je primjenjivo;
 - d) po potrebi i dodatne informacije ako se osobni podaci prikupljaju bez znanja nositelja podataka.
- (3) Posebnim zakonom mogu se propisati mjere za odgodu, ograničenje ili uskraćivanje pružanja informacija iz stavka (2) ovog članka nositelju podataka u onoj mjeri i onom trajanju u kojem takva mjera predstavlja potrebnu i proporcionalnu mjeru u demokratskom društvu, uz poštivanje temeljnih prava i legitimnih interesa nositelja podataka, s ciljem:
 - a) sprječavanja ometanja službenog i zakonom uređenog prikupljanja informacija, istraga ili postupaka;
 - b) izbjegavanja ometanja sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela ili izvršenja kaznenih sankcija;
 - c) zaštite javne sigurnosti;
 - d) zaštite državne sigurnosti;
 - e) zaštite prava i slobode drugih.
- (4) Posebnim zakonom mogu se propisati kategorije obrade koje mogu, u cjelini ili djelomično, biti obuhvaćene bilo kojom od točaka iz stavka (3) ovog članka.

Članak 70.

(Pravo nositelja podataka na pristup osobnom podatku kod nadležnog tijela)

- (1) Nadležno tijelo dužno je, u roku od 30 dana od dana zaprimanja zahtjeva za pristup osobnim podacima, nositelju podataka izdati potvrdu o tome obrađuje li njegove osobne podatke te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacijama o:
 - a) svrsi obrade i pravnom temelju obrade;
 - b) kategoriji osobnih podataka koji se obrađuju;
 - c) primatelju ili kategoriji primatelja kojemu su osobni podaci otkriveni, posebno primatelju u drugoj zemlji ili međunarodnoj organizaciji;
 - d) predviđenom roku u kojem će se osobni podaci čuvati ako je to moguće ili ako to nije moguće, kriterijima korištenim za utvrđivanje tog roka;

- e) postojanju prava da se od nadležnog tijela zatraži ispravak ili brisanje svojih osobnih podataka ili ograničenje obrade osobnih podataka;
 - f) pravu na podnošenje prigovora Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu;
 - g) osobnim podacima koji se obrađuju i o svim dostupnim informacijama o izvoru osobnih podataka.
- (2) Potvrda iz stavka (1) ovog članka izdaje se u skladu s odredbama članka 71. ovog Zakona.

Članak 71.

(Ograničenje prava pristupa osobnom podatku)

- (1) Posebnim zakonom koji se odnosi na nadležno tijelo može se nositelju podataka u cjelini ili djelomično ograničiti pravo pristupa osobnom podatku u onoj mjeri i onom trajanju u kojem takvo djelomično ili potpuno ograničenje čini potrebnu i razmjernu mjeru u demokratskom društvu, uz poštivanje temeljnih prava i legitimnih interesa nositelja podataka, kako bi se:
 - a) spriječilo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka;
 - b) izbjeglo ometanje sprječavanja istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela ili izvršenja kaznenih sankcija;
 - c) zaštitila javna sigurnost;
 - d) zaštitila državna sigurnost;
 - e) zaštitila prava i slobode drugih.
- (2) Posebnim zakonom mogu se odrediti kategorije obrade koje mogu u cjelini ili djelomično biti obuhvaćene bilo kojom točkom iz stavka (1) ovog članka.
- (3) U slučajevima iz st. (1) i (2) ovog članka, nadležno tijelo dužno je, bez odgode, pisanim putem obavijestiti nositelja podataka o svakom odbijanju ili ograničenju pristupa osobnim podacima te o razlozima odbijanja ili ograničenja, osim ako bi pružanje takvih informacija dovelo u pitanje neku od svrha iz stavka (1) ovog članka.
- (4) Nadležno tijelo dužno je obavijestiti nositelja podataka o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu.
- (5) Nadležno tijelo dužno je dokumentirati činjenične ili pravne razloge na kojima se temelji odluka.
- (6) Dokumentacija iz stavka (5) ovog članka stavlja se Agenciji na raspolaganje.

Članak 72.

(Pravo na ispravak ili brisanje osobnog podatka i ograničenje obrade od nadležnog tijela)

- (1) Nadležno tijelo dužno je:
 - a) bez nepotrebne odgode, nositelju podataka omogućiti ispravak netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade podataka, nositelj podataka ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;
 - b) nositelju podataka omogućiti brisanje osobnih podataka, bez nepotrebe odgode, ako se obradom krše odredbe čl. 60., 64. ili 66. ovog Zakona ili ako se osobni podaci moraju brisati radi poštivanja pravne obveze iz posebnog zakona;
 - c) ograničiti obradu ako:
 - 1) nositelj podataka osporava točnost osobnih podataka, a njihovu točnost ili netočnost nije moguće utvrditi ili
 - 2) osobni podaci moraju biti sačuvani kao dokaz;

- d) obavijestiti nositelja podataka prije uklanjanja ograničenja obrade ako je obrada ograničena na temelju točke c) alineje 1) ovog stavka;
 - e) pisanim putem obavijestiti nositelja podataka o svakom odbijanju ispravka ili brisanja osobnih podataka ili ograničenja obrade te o razlozima odbijanja. Posebnim zakonom koji se odnosi na nadležno tijelo može se nositelju podataka potpuno ili djelomično ograničiti pravo pristupa u onoj mjeri i u onom trajanju u kojem takvo potpuno ili djelomično ograničenje čini potrebnu i srazmjernu mjeru u demokratskom društvu, uz poštivanje temeljnih prava i legitimnih interesa nositelja podataka, kako bi se:
 - 1) izbjeglo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka,
 - 2) izbjeglo ometanje sprječavanja, istrage i otkrivanja kaznenih djela ili progona počinitelja kaznenih djela ili izvršenje kaznenih sankcija,
 - 3) zaštitila javna sigurnost,
 - 4) zaštitila državna sigurnost,
 - 5) zaštitila prava i slobode drugih;
 - f) obavijestiti nositelja podataka o mogućnosti podnošenja prigovora Agenciji ili tužbe nadležnom sudu;
 - g) obavijestiti nadležno tijelo od kojeg potječu netočni podaci o ispravku netočnih osobnih podataka.
- (2) Nadležno tijelo dužno je, ako su osobni podaci ispravljani ili brisani ili je obrada bila ograničena na temelju stavka (1) toč. a), b) ili c) ovog članka, obavijestiti primatelje, a primatelji su dužni ispraviti ili obrisati osobne podatke ili ograničiti obradu osobnih podataka u granicama svoje odgovornosti.

Članak 73.

(Ostvarivanje prava nositelja podataka i provjera Agencije)

- (1) Nadležno tijelo dužno je obavijestiti nositelja podataka o mogućnosti ostvarivanja prava putem prigovora Agenciji ili tužbe nadležnom sudu.
- (2) Ako je nositelj podataka nezadovoljan postupkom nadležnog tijela, može podnijeti prigovor Agenciji ili tužbu nadležnom sudu u slučajevima iz članka 69. stavka (3), članka 71. stavka (3) i članka 72. stavak (1) točke d) ovog Zakona.
- (3) U slučaju iz stavka (1) ovog članka, Agencija je dužna obavijestiti nositelja podataka o tome da su obavljene provjere i nadzor te o pravu na pravni lijek.

Članak 74.

(Prava nositelja podataka u kaznenim istragama i postupcima)
Nositelj podataka ostvaruje prava iz čl. 69., 70. i 72. ovog Zakona u skladu sa zakonima o kaznenim postupcima ako su osobni podaci, sadržani u sudskoj odluci ili evidenciji ili spisu predmeta, obrađeni tijekom kaznenih istraga i postupaka.

Članak 75.

(Obveza nadležnog tijela)

- (1) Nadležno tijelo dužno je primijeniti odgovarajuće tehničke i organizacijske mjere imajući u vidu prirodu, opseg, okolnosti i svrhe obrade, kao i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode fizičkih osoba, kako bi osiguralo obavljanje obrade u skladu s ovim Zakonom i kako bi to moglo dokazati. Te mjere se po potrebi preispituju i ažuriraju.
- (2) Ako su mjere iz stavka (1) ovog članka razmjerne u odnosu na aktivnosti obrade, uključuju provedbu

odgovarajućih politika zaštite podataka od nadležnog tijela.

Članak 76.

(Tehnička i integrirana zaštita osobnog podatka od nadležnog tijela)

- (1) Nadležno tijelo dužno je, uzimajući u obzir najnovija postignuća i trošak provođenja te prirodu, opseg, kontekst i svrhe obrade, te i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode osobe koji proizlaze iz obrade podataka, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, primijeniti odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje djelotvorne primjene načela zaštite podataka, kao što je smanjenje količine podataka te uključivanje zaštitnih mjera u obradu, kako bi se ispunili zahtjevi iz ovog Zakona i zaštitila prava nositelja podataka.
- (2) Mjere iz stavka (1) ovog članka odnose se na količinu prikupljenih osobnih podataka, opseg njihove obrade, rok njihovog čuvanja i njihovu dostupnost, čime se osigurava da osobni podaci nisu automatski, bez intervencije fizičke osobe, dostupni neograničenom broju osoba.

Članak 77.

(Nadležno tijelo kao zajednički kontrolor podataka)

- (1) Ako dva ili više nadležnih tijela odrede svrhe i načine obrade osobnih podataka, smatra se da su zajednički kontrolori podataka. Oni na transparentan način međusobnim sporazumom određuju odgovornosti svakoga od njih u cilju ispunjenja obveza iz ovog Zakona, posebice u vezi s ostvarivanjem prava nositelja podataka i dužnostima svakoga od njih u pogledu pružanja informacija iz članka 69. ovog Zakona, osim ako su odgovornosti nadležnih tijela utvrđene zakonom koji se primjenjuje na ta nadležna tijela. Sporazumom se određuje kontaktna točka za nositelje podataka. Zakonom se može odrediti koji od zajedničkih kontrolora podataka može djelovati kao jedinstvena kontaktna točka za ostvarivanje prava nositelja podataka.
- (2) Neovisno o uvjetima sporazuma iz stavka (1) ovog članka, nositelj podataka može ostvarivati svoja prava iz ovog Zakona u odnosu sa svakim nadležnim tijelom i protiv svakog od njih.

Članak 78.

(Korištenje usluge obrađivača od nadležnog tijela)

- (1) Nadležno tijelo koristi uslugu samo onog obrađivača koji može u dovoljnoj mjeri osigurati provođenje odgovarajućih tehničkih i organizacijskih mjera propisanih ovim Zakonom.
- (2) Korištenje usluge obrađivača od nadležnog tijela uređuje se ugovorom ili drugim pravnim aktom kojim se uređuju predmet, tehničke i organizacijske mjere propisane ovim Zakonom, trajanje obrade, opseg, sadržaj i svrha obrade, vrsta osobnih podataka, kategorije nositelja podataka te obveze i prava nadležnog tijela, kao i da obrađivač:
 - a) djeluje samo prema uputama nadležnog tijela;
 - b) osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštivanje povjerljivosti ili da podliježu zakonskim odredbama o povjerljivosti;
 - c) bilo kojim odgovarajućim sredstvom pomaže nadležnom tijelu osigurati usklađenost s odredbama o pravima nositelja podataka;
 - d) prema izboru nadležnog tijela, briše ili vraća nadležnom tijelu sve osobne podatke nakon završetka pružanja usluge obrade podataka te briše

- postojeće preslike, osim ako prema nekoj zakonskoj odredbi ne postoji obveza čuvanja osobnih podataka;
- e) nadležnom tijelu stavlja na raspolaganje sve informacije potrebne za pridržavanje odredaba ovog članka;
- f) poštuje odredbe stavka (3) ovog članka za angažiranje drugog obrađivača.
- (3) Обрађивач не може користити услугу другог обрађивача без претходног писаног одобрења надлежног тијела.
- (4) По заprimанју одобрења обрађивач је дужан обавијестити надлежно тијело о свим планираним измјенама у вези с коришћењем услуге других обрађивача.
- (5) Надлежно тијело може ускратити обрађивачу suglasnost за коришћење услуге другог обрађивача.
- (6) Ако обрађивач утврђује сврхе и начине обраде кршећи одредбе овог Закона, тај се обрађивач сматра надлежним тијелом гледе обраде која му је повјерена.

Чланак 79.

(Обрада под надзором надлежног тијела)

Особа која djeluje под надзором надлежног тијела или обрађивача, а има приступ особним подацима, не смеје обрађивати те податке без налога контролора података, осим када је то propisano посебним законом.

Чланак 80.

(Евиденција о обради од надлежног тијела)

- (1) Надлежно тијело води евиденцију о обради за коју је одговорно. Та евиденција садржи sljedeće информације:
- назив и контактне податке надлежног тијела, заједничког надлежног тијела и службеника за заштиту особних података;
 - сврху обраде;
 - категорију примателја којем су особни подаци откривени или ће му бити откривени, укључујући примателја у другој земљи или међународној организацији;
 - опис категорије носитеља података и категорије особних података;
 - упорabu израде профила, ако је примјенљиво;
 - категорију пријеноса особних података у другу земљу или међународну организацију, ако је примјенљиво;
 - правни темељ за поступак обраде, укључујући пријеносе, за који су особни подаци намјенjeni;
 - предвиђене рокове за брисање различитих категорија особних података, ако је могуће;
 - опћи опис техничких и организацијско-сигурносних мјера из чланка 85. ставка (1) овог Закона, ако је могуће.
- (2) Надлежно тијело осигурава да сваки обрађивач води евиденцију о свим категоријама активности обраде које се обављају uиme контролора података, а која садржи:
- име и контактне податке једног или више обрађивача и сваког контролора података у чије име обрађивач djeluje те службеника за заштиту података, ако је примјенљиво;
 - категорију обраде која се проводи за сваког контролора података;
 - ако је примјенљиво, податке о пријеносу особних података у другу земљу или међународну организацију, ако за то постоји изричита упута контролора података, укључујући идентификацију те друге земље или међународне организације;
 - ако је могуће, опћи опис техничких и организацијских сигурносних мјера из чланка 85. ставка (1) овог Закона.

- (3) Евиденција из ставка (1) овог чланка мора бити у писаном облику, што укључује електронички облик.

- (4) Надлежно тијело на захтев Агенције, приликом надзора, ставља евиденцију на увид.

Чланак 81.

(Зачис)

- (1) Надлежно тијело дужно је, у случају аутоматизираног система обраде особних података, успоставити приступ систему који аутоматски билежи најмање sljedeće информације о: прикупљању, измјени, оствареном увиду, откривању, укључујући пријеносе, те комбинарању и брисању. Зачиси о оствареном увиду и откривању омогућавају да се утврде образложење, датум и вријеме таквих поступака те, ако је то могуће, идентитет особе која је остварила увид или открила особне податке и идентитет примателја таквих особних података.
- (2) Зачис се користи само у сврхе провере законитости обраде, самопраћења и осигурања cjелovitosti и сигурности особних података те за казнене поступке.
- (3) Надлежно тијело на захтев Агенције, приликом надзора, ставља записе на увид.

Чланак 82.

(Сарадња надлежног тијела и обрађивача с Агенцијом)

- Надлежно тијело и обрађивач дужни су сарађивати с Агенцијом, на образложено и на темељу закона оправдан захтев, при извршењу њезине надлежности.

Чланак 83.

(Процена утјецая на заштиту особног податка од надлежног тијела)

- (1) Надлежно тијело прије обраде проценjuje утјечaj предвиђених поступака обраде на заштиту особних података ако је вјероватно да ће нека врста обраде, посебно примјеном нових технологија и узимајући у обзир природу, опсег, контекст и сврхе те обраде, проузрочити високи ризик за права и слободe особа.
- (2) Процена из ставка (1) овог чланка мора садржавати најмање опћи опис предвиђених поступака обраде, процену ризика за права и слободe носитеља података, предвиђене мјере за ризике, заштите и сигурносне мјере и механизме како би се осигурала заштита особних података и доказала усклађеност с овим Законом, узимајући у обзир права и легитимне интересе носитеља података и других укључених особа.

Чланак 84.

(Претходно саветовање надлежног тијела с Агенцијом)

- (1) Надлежно тијело или обрађивач дужно је саветовати се с Агенцијом прије обраде особних података који ће бити укључени у нову збирку особних података ако:
- процена утјецая на заштиту података, како је propisano чланком 83. овог Закона, упућује на то да би обрада могла проузрочити висок ризик уколико надлежно тијело не подuzме мјере како би уманјило ризик или
 - врста обраде, посебice ако се примјенjuју нове технологије, механизми или поступци, представља висок ризик за права и слободe носитеља података.
- (2) Агенција може утврдити попис поступака обраде за које је потребно обавити претходно саветовање у складу са ставком (1) овог чланка.
- (3) Надлежно тијело дужно је Агенцији доставити процену утјецая на заштиту података на темељу чланка 83. овог Закона и на њен захтев пружити све остале информације с помоћу којих ће Агенција моћи проценити усклађеност обраде, а посебice ризике за заштиту особних података носитеља података и повезане заштитне мјере.

- (4) Agencija će, u roku od 42 dana od zaprimanja pisanog zahtjeva iz stavka (1) ovog članka, pisanim putem dati savjet nadležnom tijelu te može iskoristiti bilo koju od svojih ovlasti ako smatra da bi se namjeravanom obradom iz stavka (1) ovog članka kršile odredbe ovog Zakona, posebice ako nadležno tijelo nije u dovoljnoj mjeri utvrdilo ili umanjilo rizik.
- (5) Rok iz stavka (4) ovog članka može se po potrebi produžiti za 30 dana, uzimajući u obzir složenost namjeravane obrade.
- (6) Agencija u roku od 30 dana od zaprimanja zahtjeva obavještava nadležno tijelo i, po potrebi, obrađivača o svakom produženju i razlozima odgode.
- (7) O prijedlogu zakona kojim se uređuje obrada osobnih podataka, a prije njegovog upućivanja u parlamentarnu proceduru, predlagatelj se može prethodno savjetovati s Agencijom.

Članak 85.

(Sigurnost obrade od nadležnog tijela i obrađivača)

- (1) Nadležno tijelo i obrađivač dužni su, uzimajući u obzir najnovija postignuća, troškove provođenja, prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerovatnoće i ozbiljnosti za prava i slobode fizičkih osoba, primijeniti odgovarajuće tehničke i organizacijske mjere kako bi se postigla odgovarajuća razina sigurnosti shodno riziku, posebno glede obrade posebnih kategorija osobnih podataka.
- (2) Glede automatizirane obrade, nadležno tijelo ili obrađivač, nakon procjene rizika, dužno je uspostaviti mjere kojima se osigurava da se:
 - a) onemogućiti neovlaštenim osobama pristup opremi koja se koristi za obradu;
 - b) spriječiti neovlašteno čitanje, umnažanje, mijenjanje ili uklanjanje nosača podataka;
 - c) spriječiti neovlašteni unos osobnih podataka te neovlašteno pregledanje, mijenjanje ili brisanje čuvanih osobnih podataka;
 - d) spriječiti korištenje sustava za automatsku obradu od neovlaštene osobe korištenjem opreme za prijenos podataka;
 - e) osoba koja je ovlaštena za korištenje sustava za automatsku obradu ima pristup samo onim osobnim podacima na koje se odnosi njezino odobrenje za pristup;
 - f) može provjeriti i utvrditi kome su osobni podaci preneseni, odnosno kome bi mogli biti preneseni ili učinjeni dostupnim korištenjem opreme za prijenos podataka;
 - g) može naknadno provjeriti, odnosno utvrditi, koji su osobni podaci uneseni u sustav automatske obrade te tko ih je i kada unio;
 - h) spriječiti neovlašteno čitanje, umnažanje, mijenjanje ili brisanje osobnih podataka tijekom prijenosa osobnih podataka ili prijenosa nosača podataka;
 - i) omogućiti ponovno uspostavljanje instaliranih sustava u slučaju prekida njihovog rada;
 - j) održava ispravna funkcija sustava, da se pojava grešaka u funkcioniranju sustava prijavi i da čuvani osobni podaci ne mogu ugroziti zbog nedostataka u funkcioniranju sustava.

Članak 86.

(Obavješćavanje Agencije o povredi osobnog podatka od nadležnog tijela)

- (1) Nadležno tijelo dužno je u slučaju povrede osobnih podataka, bez odgode, a najkasnije 72 sata nakon saznanja

za povredu, obavijestiti Agenciju o povredi osobnih podataka, osim ako povreda osobnih podataka ne ugrožava prava i slobode fizičke osobe.

- (2) Obrađivač je dužan u slučaju povrede osobnih podataka, bez odgode, obavijestiti nadležno tijelo, nakon što dozna za povredu osobnih podataka.
- (3) Ako obavješćavanje Agencije iz stavka (1) ovog članka nije učinjeno u roku od 72 sata, mora se sastaviti pisano obrazloženje s navođenjem razloga za kašnjenje.
- (4) Obavijest iz stavka (1) ovog članka sadrži najmanje sljedeće informacije:
 - a) opis povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj nositelja podataka, kao i kategorije i približan broj evidencija osobnih podataka o kojima je riječ;
 - b) ime i prezime te kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;
 - c) opis vjerovatne posljedice povrede osobnih podataka;
 - d) opis mjera koje je nadležno tijelo poduzelo ili čije je poduzimanje predložilo radi rješavanja problema povrede osobnih podataka, uključujući, po potrebi, i mjere za ublažavanje mogućih štetnih posljedica.
- (5) Informacije se mogu dostavljati u dijelovima, bez odgode, ako i u mjeri u kojoj nije moguće istovremeno dostaviti sve informacije.
- (6) Nadležno tijelo dokumentira svaku povredu osobnih podataka iz stavka (1) ovog članka, uključujući i činjenice u vezi s povredom osobnih podataka, njezine posljedice i mjere poduzete za popravljivanje situacije.
- (7) Dokumentacija iz stavka (4) ovog članka mora biti dostupna Agenciji s ciljem provjere primjene ovog članka.
- (8) U slučaju povrede osobnih podataka koja uključuje osobne podatke koje je prenio kontrolor podataka druge zemlje ili koji su preneseni njemu, nadležno tijelo osigurava prijenos informacija iz stavka (4) ovog članka kontroloru podataka te zemlje bez nepotrebne odgode.

Članak 87.

(Obavješćavanje nositelja podatka o povredi osobnog podatka)

- (1) Ako je vjerovatno da će povreda osobnih podataka prouzročiti visok rizik za prava i slobode fizičke osobe, nadležno tijelo bez odgode obavještava nositelja podataka o povredi osobnih podataka.
- (2) U obavijesti iz stavka (1) ovog članka jasnim i jednostavnim jezikom opisuje se priroda povrede osobnih podataka te se navode najmanje informacije i mjere iz članka 86. stavka (4) toč. b), c) i d) ovog Zakona.
- (3) Obavješćavanje nositelja podataka nije obvezno ako je ispunjen jedan od sljedećih uvjeta:
 - a) ako je nadležno tijelo poduzelo odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke u vezi s kojima je došlo do povrede osobnih podataka, a prije svega mjere koje osobne podatke čine nerazumljivim osobi koja nije ovlaštena pristupiti im, kao što je enkripcija;
 - b) ako je kontrolor podataka poduzeo naknadne mjere kojima se osigurava da više nije vjerovatno da će doći do visokog rizika za prava i slobode nositelja podataka;
 - c) ako bi to zahtijevalo nesrazmjeran napor. U tom slučaju objavljuje se javna obavijest ili se poduzima slična mjera kojom se nositelji podataka obavještavaju na jednako djelotvoran način.
- (4) Ako nadležno tijelo do tog trenutka nije obavijestilo nositelja podataka o povredi osobnih podataka, Agencija,

nakon razmatranja stupnja vjerojatnoće da će povreda osobnih podataka prouzročiti visok rizik, može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uvjeta iz stavka (3) ovog članka.

- (5) Obavješćavanje nositelja podataka može se odgoditi, ograničiti ili uskratiti u skladu s uvjetima i na temelju razloga iz članka 69. stavka (3) ovog Zakona.

Članak 88.

(Imenovanje službenika za zaštitu osobnih podataka od nadležnog tijela)

- (1) Nadležno tijelo dužno je imenovati službenika za zaštitu osobnih podataka.
- (2) Kada sudovi i druga neovisna pravosudna tijela postupaju u granicama svoje pravosudne nadležnosti, nisu dužni imenovati službenika za zaštitu osobnih podataka.
- (3) Službenik za zaštitu osobnih podataka imenuje se na temelju njegovih stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksi iz područja zaštite osobnih podataka te sposobnosti izvršenja zadataka iz članka 90. ovog Zakona.
- (4) Više nadležnih tijela može imenovati jednog službenika za zaštitu osobnih podataka, uzimajući u obzir njihovu organizacijsku strukturu i veličinu.
- (5) Nadležno tijelo dužno je objaviti kontaktne podatke službenika za zaštitu osobnih podataka i priopćiti ih Agenciji.

Članak 89.

(Radno mjesto službenika za zaštitu osobnih podataka nadležnog tijela)

- (1) Nadležno tijelo dužno je osigurati da službenik za zaštitu osobnih podataka bude na odgovarajući način i pravodobno uključen u sva pitanja koja se tiču zaštite osobnih podataka.
- (2) Nadležno tijelo dužno je podržavati službenika za zaštitu osobnih podataka u izvršavanju zadataka pružajući mu potrebna sredstva za izvršenje tih zadataka i pristup osobnim podacima te postupcima obrade, kao i za održavanje njegova stručnog znanja.

Članak 90.

(Zadaci službenika za zaštitu osobnih podataka nadležnog tijela)

Nadležno tijelo povjerava službeniku za zaštitu osobnih podataka najmanje sljedeće zadatke:

- a) informiranje i savjetovanje nadležnog tijela i zaposlenih koji obavljaju obradu o njihovim obvezama iz ovog Zakona i drugih zakona kojima se propisuje zaštita osobnih podataka;
- b) praćenje primjene ovog Zakona i drugih zakona kojima se propisuje zaštita osobnih podataka, kao i politika nadležnog tijela u vezi sa zaštitom osobnih podataka, uključujući i podjelu odgovornosti, podizanje svijesti i osposobljavanje zaposlenih koji sudjeluju u radnjama obrade, kao i s tim povezanim revizijama;
- c) pružanje savjeta, kada je to zahtijevano, glede procjene utjecaja na zaštitu osobnih podataka i praćenje njezinog izvršavanja u skladu s člankom 83. ovog Zakona;
- d) suradnju s Agencijom;
- e) djelovanje kao kontaktna točka za Agenciju o pitanjima koja se tiču obrade, što uključuje i prethodno savjetovanje iz članka 84. ovog Zakona te savjetovanje, po potrebi, o svim drugim pitanjima.

Članak 91.

(Opća načela prijenosa osobnog podatka u drugu zemlju ili međunarodnu organizaciju od nadležnog tijela)

- (1) Nadležno tijelo dužno je svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u drugu zemlju ili međunarodnu organizaciju, uključujući daljnji prijenos u još jednu drugu zemlju ili međunarodnu organizaciju, obavljati pridržavajući se odredaba ovog dijela Zakona samo ako su ispunjeni sljedeći uvjeti, i to:
 - a) prijenos je potreban za svrhe utvrđene u članku 1. stavku (1) točki c) ovog Zakona;
 - b) osobni podaci prenose se nadležnom tijelu u drugoj zemlji ili međunarodnoj organizaciji koji je javno tijelo nadležno za potrebe iz članka 1. stavka (1) točka c) ovog Zakona;
 - c) ako su osobni podaci preneseni ili stavljeni na raspolaganje iz druge zemlje, ta je zemlja dala prethodno odobrenje za prijenos u skladu sa svojim pravom;
 - d) ako je Vijeće ministara Bosne i Hercegovine, na prijedlog Agencije, donijelo odluku o prikladnosti iz članka 92. stavka (3) ovog Zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o prikladnosti iz članka 92. stavka (3) ovog Zakona, moraju biti osigurane ili postoje odgovarajuće zaštitne mjere iz članka 93. ovog Zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o prikladnosti iz članka 92. stavka (3) ovog Zakona i nisu osigurane ili ne postoje odgovarajuće zaštitne mjere iz članka 93. ovog Zakona, primjenjuju se odstupanja za posebne situacije iz članka 94. ovog Zakona;
 - e) u slučaju daljnjeg prijenosa u još jednu drugu zemlju ili međunarodnu organizaciju, nadležno tijelo koje je izvršilo prvi prijenos ili drugo nadležno tijelo u Bosni i Hercegovini može, nakon što je uzelo u obzir sve relevantne činjenice, uključujući ozbiljnost kaznenog djela, svrhu u koju su osobni podaci prvo preneseni i razinu zaštite osobnih podataka u drugoj državi ili međunarodnoj organizaciji, odobriti daljnji prijenos.
- (2) Nadležnom tijelu dopušten je prijenos, bez prethodnog odobrenja druge zemlje, u skladu sa stavkom (1) točkom c) ovog članka, iznimno ako je prijenos osobnih podataka potreban za sprječavanje neposredne i ozbiljne prijetnje javnoj sigurnosti Bosne i Hercegovine ili druge zemlje ili bitnim interesima Bosne i Hercegovine, a prethodno odobrenje se ne može pravodobno dobiti.
- (3) Nadležno tijelo dužno je obavijestiti tijelo u drugoj zemlji odgovorno za izdavanje prethodnog odobrenja o slučaju iz stavka (2) ovog članka.
- (4) Sve odredbe u vezi s prijenosom osobnih podataka u drugu zemlju ili međunarodnu organizaciju primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite fizičkih osoba koja je zajamčena ovim dijelom Zakona.

Članak 92.

(Prijenos od nadležnog tijela na temelju odluke o prikladnosti)

- (1) Prijenos osobnih podataka u drugu zemlju ili međunarodnu organizaciju može se obaviti ako Vijeće ministara Bosne i Hercegovine odluči da druga zemlja, teritorij ili jedan ili više konkretnih sektora unutar te druge zemlje ili međunarodna organizacija osigurava prikladnu razinu zaštite, a u tom slučaju takav prijenos ne zahtijeva posebno odobrenje.

- (2) Smatra se da je prikladna razina zaštite iz stavka (1) ovog članka osigurana u zemlji, dijelovima njezina teritorija ili jednom ili više sektora u toj zemlji ili u međunarodnoj organizaciji za koje je Europska unija utvrdila da osiguravaju prikladnu razinu zaštite osobnih podataka.
- (3) Odluku o prikladnosti razine zaštite osobnih podataka iz stavka (1) ovog članka donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stavka (3) ovog članka uzimajući u obzir:
- vladavinu prava, poštivanje ljudskih prava i temeljnih sloboda, relevantno opće i sektorsko zakonodavstvo, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, državnoj sigurnosti, kazneno pravo i pristup javnih tijela osobnim podacima, kao i primjenu tog zakonodavstva, pravila o zaštiti osobnih podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos osobnih podataka u još jednu drugu zemlju ili međunarodnu organizaciju, koja se poštuju u toj drugoj zemlji ili međunarodnoj organizaciji, sudsku praksu, kao i postojanje djelotvornih i provedivih prava nositelja podataka i učinkovitu upravnu i sudsku zaštitu nositelja podataka;
 - postojanje i učinkovito funkcioniranje jednog ili više neovisnih nadzornih tijela u drugoj zemlji ili tijela kojemu podliježe međunarodna organizacija, odgovornih za osiguravanje i provođenje pravila o zaštiti podataka, što uključuje odgovarajuće izvršne ovlasti za pružanje pomoći nositeljima podataka u ostvarivanju njihovih prava, kao i za suradnju s Agencijom;
 - međunarodne obveze koje je preuzela druga zemlja ili međunarodna organizacija ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezinog sudjelovanja u multilateralnim ili regionalnim organizacijama, posebice u vezi sa zaštitom osobnih podataka.
- (5) Agencija kontinuirano prati stanje u području zaštite osobnih podataka u drugoj zemlji, dijelu njezinog teritorija, jednom ili više sektora unutar te zemlje ili u međunarodnoj organizaciji i o tome po potrebi izvješćuje Vijeće ministara Bosne i Hercegovine.
- (6) Izvješće iz stavka (5) ovog članka uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija koje su od značaja za preispitivanje postojanja prikladne razine zaštite osobnih podataka, na temelju čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stavka (3) ovog članka.
- (7) Odluka donesena na temelju stavka (3) ovog članka ne dovodi u pitanje prijenos osobnih podataka u drugu zemlju, na teritorij ili u jedan ili više određenih sektora unutar te druge zemlje ili u međunarodnu organizaciju, u skladu s čl. 93. i 94. ovog Zakona.
- (8) Popis zemalja, dijela njihovih teritorija, jedan ili više sektora unutar tih zemalja i međunarodnih organizacija glede kojih je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju prikladnu razinu zaštite osobnih podataka objavljuje se u "Službenom glasniku BiH" i na službenoj internetskoj stranici Agencije.

Članak 93.

(Prijenos od nadležnog tijela na koje se primjenjuju odgovarajuće zaštitne mjere)

- (1) Nadležno tijelo može izvršiti prijenos osobnih podataka u drugu zemlju ili međunarodnu organizaciju ako nije

donesena odluka na temelju članka 92. stavka (3) ovog Zakona pod sljedećima uvjetima:

- ako su odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka predviđene u pravno obvezujućem instrumentu ili
 - ako je nadležno tijelo procijenilo sve okolnosti u vezi s prijenosom osobnih podataka i zaključilo da postoje odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.
- (2) Nadležno tijelo dužno je obavijestiti Agenciju o kategorijama prijenosa u skladu sa stavkom (1) točkom b) ovog članka.
- (3) Kada se prijenos osobnih podataka temelji na stavku (1) točki b) ovog članka, nadležno tijelo dužno je takav prijenos dokumentirati, a dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje je dobilo podatke, obrazloženje prijenosa i koji su osobni podaci preneseni.

Članak 94.

(Odstupanje u posebnim slučajevima prijenosa osobnog podatka od nadležnog tijela)

- (1) Ako ne postoji odluka o prikladnosti iz članka 92. stavka (3) ovog Zakona ili odgovarajuće zaštitne mjere iz članka 93. ovog Zakona, prijenos ili skup prijenosa osobnih podataka u drugu zemlju ili međunarodnu organizaciju obavlja se samo ako je prijenos nužan i ako ispunjava jedan od sljedećih uvjeta:
- kako bi se zaštitili ključni interesi nositelja podataka ili druge osobe;
 - kako bi se zaštitili legitimni interesi nositelja podataka, ako je to propisano posebnim zakonom;
 - kako bi se spriječila neposredna i ozbiljna prijetnja javnoj sigurnosti na teritoriju Bosne i Hercegovine ili druge zemlje;
 - u pojedinačnim slučajevima za svrhe navedene u članku 1. stavku (1) točki c) ovog Zakona ili
 - u pojedinačnom slučaju radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva u vezi sa svrhama navedenim u članku 1. stavku (1) točki c) ovog Zakona.
- (2) Osobni podaci ne smiju se prenositi ako nadležno tijelo koje obalja prijenos utvrdi da temeljna prava i slobode dotičnog nositelja podataka imaju prednost pred javnim interesom glede prijenosa iz stavka (1) toč. d) i e) ovog članka.
- (3) Ako se prijenos obavlja na temelju stavka (1) ovog članka, nadležno tijelo dužno je takav prijenos dokumentirati i dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje je dobilo podatke, obrazloženje prijenosa i koji su osobni podaci preneseni.

Članak 95.

(Prijenos osobnog podatka primatelju sa sjedištem ili poslovnim nastanom u drugoj zemlji)

- (1) Nadležno tijelo može, u skladu s posebnim zakonom, odstupajući od članka 91. stavka (1) točke b) ovog Zakona i ne dovodeći u pitanje nijedan međunarodni sporazum iz stavka (2) ovog članka, u pojedinačnim i posebnim slučajevima prenijeti osobne podatke izravno primateljima sa sjedištem ili poslovnim nastanom u drugoj zemlji samo ako se pridržavaju odredaba ovog dijela Zakona i ako su ispunjeni sljedeći uvjeti:

- a) ako je prijenos isključivo potreban za obavljanje zadatka nadležnog tijela koje obavlja prijenos kako je to propisano posebnim zakonom za svrhe navedene u članku 1. stavku (1) točki c) ovog Zakona;
 - b) ako nadležno tijelo koje obavlja prijenos utvrdi da temeljna prava i slobode dotičnog nositelja podataka nemaju prednost nad javnim interesom koji iziskuje prijenos u predmetnom slučaju;
 - c) ako nadležno tijelo koje obavlja prijenos smatra da je prijenos tijelu nadležnom za postupanje u svrhu iz članka 1. stavka (1) točke c) ovog Zakona u drugu zemlju nedjelotvoran ili neprimjeren, posebno zato što se prijenos ne može pravodobno ostvariti;
 - d) ako tijelo koje je u drugoj zemlji nadležno za postupanje u svrhu iz članka 1. stavka (1) točke c) ovog Zakona obaviješteno je bez odgode, osim ako je to nedjelotvorno ili neprimjereno;
 - e) ako nadležno tijelo koje obavlja prijenos obavijesti primatelja o određenoj svrsi ili svrhama u koje taj primatelj isključivo može obrađivati osobne podatke, samo ako je takva obrada nužna.
- (2) Međunarodni sporazum iz stavka (1) ovog članka je svaki bilateralni ili multilateralni međunarodni sporazum na snazi između Bosne i Hercegovine i druge zemlje u području pravosudne suradnje u kaznenim stvarima i policijske suradnje.
- (3) Nadležno tijelo koje obavlja prijenos dužno je obavijestiti Agenciju o prijenosima u skladu s ovim člankom.
- (4) Nadležno tijelo koje obavlja prijenos osobnih podataka na temelju stavka (1) ovog članka dužno je dokumentirati takav prijenos.

DIO ČETVRTI – AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA U BOSNI I HERCEGOVINI

Članak 96.

(Agencija)

- (1) Agencija je neovisno nadzorno tijelo za praćenje primjene ovog Zakona, s ciljem zaštite temeljnih prava i sloboda fizičkih osoba u vezi s obradom osobnih podataka u Bosni i Hercegovini.
- (2) Sjedište Agencije je u Sarajevu.
- (3) Na sva pitanja organizacije i upravljanja te druga pitanja značajna za funkcioniranje Agencije primjenjuju se propisi kojima se uređuje organizacija rada tijela uprave, osim ako nije drukčije propisano ovim Zakonom.

Članak 97.

(Neovisnost Agencije)

- (1) Agencija djeluje potpuno neovisno u obavljanju svojih nadležnosti u skladu s ovim Zakonom.
- (2) Ravnatelj, zamjenik ravnatelja i zaposleni u Agenciji pri obavljanju svojih dužnosti i ovlasti u skladu s ovim Zakonom ne smiju biti izloženi izravnom ili neizravnom vanjskom utjecaju i ne smiju ni od koga tražiti ili primiti instrukcije.
- (3) Ravnatelj, zamjenik ravnatelja i zaposleni u Agenciji moraju se suzdržavati od svih radnji koje nisu u skladu s njihovim dužnostima i tijekom svog mandata i zaposlenja ne smiju se baviti nespojivom djelatnošću, bez obzira na to je li ona plaćena ili ne.
- (4) Agencija mora imati ljudske, tehničke i financijske resurse, prostorije i infrastrukturu potrebne za učinkovito izvršenje svojih nadležnosti, uključujući i ovlasti koje se odnose na međunarodnu uzajamnu pomoć i suradnju.
- (5) Zaposleni u Agenciji su državni službenici i zaposlenici i na njih se primjenjuju Zakon o državnoj službi u

- institucijama Bosne i Hercegovine i Zakon o radu u institucijama Bosne i Hercegovine.
- (6) Pravilnik o unutarnjem ustrojstvu Agencije, na prijedlog ravnatelja Agencije, odobrava Parlamentarna skupština Bosne i Hercegovine.
- (7) Agencija, u skladu s odredbama Zakona o financiranju institucija Bosne i Hercegovine, priprema nacrt godišnjeg proračuna i dostavlja ga parlamentarnom povjerenstvu na odobravanje. Agencija, nakon dobivanja odobrenja parlamentarnog povjerenstva, u skladu s rokovima propisanim odredbama Zakona o financiranju institucija Bosne i Hercegovine, dostavlja Ministarstvu financija i trezora Bosne i Hercegovine nacrt proračuna radi uvrštavanja u proračun institucija Bosne i Hercegovine i međunarodnih obveza Bosne i Hercegovine. Ministarstvo financija i trezora Bosne i Hercegovine, Vijeće ministara Bosne i Hercegovine i Predsjedništvo Bosne i Hercegovine mogu dati mišljenje o nacrtu proračuna Agencije, bez mogućnosti izmjene nacrta proračuna koji je prethodno odobrilo parlamentarno povjerenstvo.
- (8) Agencija podliježe financijskoj kontroli u skladu s propisima o financijskoj kontroli.

Članak 98.

(Rukovođenje Agencijom)

- (1) Agencijom rukovodi ravnatelj.
- (2) Ravnatelj ima jednog zamjenika.
- (3) Zamjenik ravnatelja zamjenjuje ravnatelja u obavljanju poslova, ako ravnatelj nije u mogućnosti obavljati poslove u skladu sa svojim ovlastima i obvezama.
- (4) Ravnatelj je odgovoran za zakonit rad Agencije.

Članak 99.

(Uvjeti za imenovanje, privremena suspenzija i razrješenje ravnatelja i zamjenika ravnatelja)

- (1) Ravnatelja i zamjenika ravnatelja imenuje Parlamentarna skupština Bosne i Hercegovine (u daljnjem tekstu: Parlamentarna skupština) na temelju javnog natječaja.
- (2) Ravnatelj i zamjenik ravnatelja imenuju se na razdoblje od šest godina uz mogućnost još jednog ponovnog imenovanja.
- (3) Uvjeti za imenovanje ravnatelja i zamjenika ravnatelja su:
 - a) da je stariji od 18 godina;
 - b) da je državljanin Bosne i Hercegovine (svi državljani Federacije BiH, Republike Srpske i Brčko distrikta BiH su državljani BiH);
 - c) da nije osuđivan i da se protiv njega ne vodi kazneni postupak;
 - d) da nije obuhvaćen odredbom članka IX.1. Ustava Bosne i Hercegovine;
 - e) da je zdravstveno sposoban;
 - f) da ima završen fakultet društvenog smjera, VSS/VII stupanj ili visoko obrazovanje bolonjskog sustava studiranja s najmanje 240 ECTS bodova;
 - g) da ima najmanje deset godina radnog iskustva u struci, od čega najmanje pet godina radnog iskustva na poslovima rukovođenja;
 - h) da ima stručna znanja i iskustva iz područja zaštite osobnih podataka;
 - i) da nije član političke stranke.
- (4) Parlamentarna skupština može privremeno suspendirati ravnatelja i zamjenika ravnatelja ako se otkrije teška povreda službene dužnosti. Privremena suspenzija traje dok se konačnom odlukom ne utvrdi teška povreda službene dužnosti.
- (5) Parlamentarna skupština može razriješiti ravnatelja i zamjenika ravnatelja prije isteka mandata:

- a) na njegov zahtjev,
- b) ako se utvrdi teška povreda službene dužnosti;
- c) kada navrši 65 godina života i najmanje 20 godina staža osiguranja ili 40 godina staža osiguranja, neovisno o godinama života;
- d) ako više ne ispunjava uvjete potrebne za imenovanje.

Članak 100.

(Nespojivost funkcije i obveza čuvanja profesionalne tajne)

- (1) Ravnatelj i zamjeniku ravnatelja te zaposlenima u Agenciji zabranjeni su djelovanje, poslovanje i pogodnosti koji nisu sukladni s načelom neovisnosti i nepristranosti, za vrijeme trajanja mandata odnosno radnog odnosa i jednu godinu nakon njegovog prestanka.
- (2) Ravnatelj, zamjenik ravnatelja i zaposleni u Agenciji za vrijeme trajanja mandata odnosno radnog odnosa i nakon prestanka mandata odnosno radnog odnosa dužni su čuvati profesionalnu tajnu koja se odnosi na sve povjerljive informacije koje doznaju prilikom obavljanja svojih dužnosti ili ovlasti, u skladu s propisima u Bosni i Hercegovini. Tijekom trajanja njihova mandata, dužnost čuvanja profesionalne tajne posebno se odnosi na prijave fizičkih osoba o kršenjima ovog Zakona.

Članak 101.

(Nadležnosti Agencije)

- (1) Agencija je nadležna za:
 - a) obavljanje zadataka i ovlasti dodijeljenih ovim Zakonom,
 - b) nadzor postupaka obrade osobnih podataka koje obavljaju kontrolori podataka i obrađivači.
- (2) Agencija nije nadležna za nadzor postupaka obrade osobnih podataka koje provode sudovi kada obavljaju sudsku funkciju.

Članak 102.

(Zadaci Agencije)

- (1) Agencija obavlja sljedeće zadatke:
 - a) prati i primjenjuje ovaj Zakon;
 - b) promiče javnu svijest o rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom osobnih podataka te njihovo razumijevanje, a posebnu pozornost posvećuje aktivnostima koje su izričito namijenjene djeci;
 - c) savjetuje, u skladu s ovim Zakonom, javna tijela i druge institucije i tijela o zakonodavnim i upravnim mjerama u vezi sa zaštitom prava i sloboda fizičkih osoba u vezi s obradom;
 - d) podiže svijest kontrolora podataka i obrađivača o njihovim obvezama iz ovog Zakona;
 - e) na zahtjev svakog nositelja podataka, pruža informacije u vezi s ostvarivanjem njegovih prava iz ovog Zakona;
 - f) razmatra prigovor nositelja podataka ili tijela, organizacije ili udruge u skladu s člankom 111. ovog Zakona i u roku od 90 dana donosi rješenje po prigovoru, o čemu obavještava podnositelja prigovora;
 - g) provodi provjere u vezi s primjenom ovog Zakona, među ostalim i na temelju informacija primljenih od javnih tijela;
 - h) prati bitna kretanja, u mjeri u kojoj utječu na zaštitu osobnih podataka, a posebno razvoj informacijskih i komunikacijskih tehnologija i komercijalnih praksi;
 - i) donosi standardne ugovorne klauzule iz članka 30. stavka (8) i članka 48. stavka (3) ovog Zakona;

- j) utvrđuje i vodi popis obrada u vezi s obvezom obavljanja procjene utjecaja na zaštitu podataka u skladu s člankom 37. stavkom (4) ovog Zakona;
- k) daje savjete o postupku obrade osobnih podataka iz članka 38. stavka (2) ovog Zakona i članka 84. stavka (4) ovog Zakona;
- l) potiče izradu kodeksa ponašanja i daje mišljenje i odobrava takve kodekse ponašanja koji pružaju dovoljne zaštitne mjere u skladu s člankom 42. stavkom (5) ovog Zakona;
- m) potiče uspostavu mehanizama certifikacije zaštite podataka, kao i pečata i oznaka za zaštitu podataka u skladu s člankom 44. stavkom (1) ovog Zakona, i odobrava kriterije za certifikaciju u skladu s člankom 44. stavkom (6) ovog Zakona;
- n) u određenim slučajevima periodično preispituje izdane certifikate u skladu s člankom 44. st. (8) i (9) ovog Zakona;
- o) sastavlja i objavljuje kriterije za akreditiranje tijela za praćenje kodeksa ponašanja u skladu s člankom 43. ovog Zakona i akreditiranje certifikacijskog tijela u skladu s člankom 45. ovog Zakona;
- p) akreditira tijela za praćenje kodeksa ponašanja u skladu s člankom 43. ovog Zakona i akreditira certifikacijsko tijelo u skladu s člankom 45. ovog Zakona;
- r) odobrava odgovarajuće zaštitne mjere iz članka 48. stavka (4) ovog Zakona;
- s) odobrava obvezujuća poslovna pravila u skladu s člankom 49. ovog Zakona;
- t) vodi internu evidenciju o kršenjima ovog Zakona i mjerama koje su poduzete u skladu s člankom 103. stavkom (2) ovog Zakona;
- u) daje mišljenje o prijedlogu zakona institucijama na razini Bosne i Hercegovine koji se odnosi na obradu osobnih podataka;
- v) obavlja sve ostale zadatke u vezi sa zaštitom osobnih podataka.

- (2) Agencija propisuje izgled i sadržaj obrasca za podnošenje prigovora.
- (3) Agencija obavlja zadatke besplatno za nositelje podataka i ako je to primjenjivo, i za službenike za zaštitu osobnih podataka.
- (4) Agencija obavlja zadatke besplatno za nositelje podataka i za službenike za zaštitu osobnih podataka iz Dijela trećeg ovog Zakona.
- (5) Ako su zahtjevi nositelja podataka očito neutemeljeni ili pretjerani, posebice zbog učestalog ponavljanja, Agencija može naplatiti naknadu stvarnih administrativnih troškova ili odbiti postupiti po zahtjevu, pri čemu Agencija snosi teret dokazivanja očite neutemeljenosti ili pretjeranosti zahtjeva.
- (6) Agencija naplaćuje naknadu za izdavanje akreditacije certifikacijskom tijelu.
- (7) Agencija naplaćuje naknadu za davanje mišljenja i drugih usluga poslovnim subjektima u svrhu obavljanja njihove redovite djelatnosti.
- (8) Kriterije za određivanje visine naknade iz st. (5), (6) i (7) ovog članka utvrđuje Agencija uz prethodnu suglasnost Vijeća ministara Bosne i Hercegovine i oni se objavljuju u "Službenom glasniku BiH".
- (9) Naknada se uplaćuje na Jedinствени račun trezora institucija Bosne i Hercegovine.

Članak 103.

(Ovlasti Agencije)

- (1) Agencija ima sljedeće ovlasti:

- a) preispitivati certifikate izdane u skladu s člankom 44. st. (8) i (9) ovog Zakona;
 - b) provoditi inspeksijske nadzore;
 - c) provoditi reviziju zaštite podataka;
 - d) naložiti kontroloru podataka i obrađivaču, a po potrebi i predstavniku kontrolora podataka ili obrađivača, dostavu svih informacija potrebnih za obavljanje njezinih zadataka;
 - e) obavijestiti kontrolora podataka ili obrađivača o navodnom kršenju ovog Zakona;
 - f) ostvariti pristup svim osobnim podacima i svim informacijama u posjedu kontrolora podataka i obrađivača koje su potrebne za obavljanje njezinih zadataka;
 - g) ostvariti pristup svim prostorijama kontrolora podataka i obrađivača u kojima se obavlja obrada osobnih podataka, uključujući svu opremu i sredstva za obradu podataka.
- (2) Agencija ima sljedeće korektivne ovlasti:
- a) izreći upozorenje kontroloru podataka ili obrađivaču da bi namjeravane obrade mogle lako predstavljati kršenje ovog Zakona;
 - b) izreći opomenu kontroloru podataka ili obrađivaču ako se obradom krši ovaj Zakon;
 - c) naložiti kontroloru podataka ili obrađivaču da postupi po zahtjevu nositelja podataka za ostvarivanje njegovih prava u skladu s ovim Zakonom;
 - d) naložiti kontroloru podataka ili obrađivaču da uskladi obradu, ako je potrebno, s odredbama ovog Zakona na točno određen način i u točno zadanom roku;
 - e) naložiti kontroloru podataka da nositelja podataka obavijesti o povredi osobnih podataka;
 - f) privremeno ili trajno ograničiti ili zabraniti obradu;
 - g) naložiti ispravak ili brisanje osobnih podataka ili ograničenje obrade i obavješćavanje o takvim radnjama primatelja kojima su osobni podaci otkriveni;
 - h) oduzeti certifikat izdan u skladu s čl. 44. i 45. ovog Zakona ili certifikacijskom tijelu naložiti da ne izda certifikat ako zahtjevi za certifikaciju nisu ispunjeni ili da povuče certifikat ako zahtjevi više nisu ispunjeni;
 - i) izdati prekršajni nalog u prekršajnom postupku ili podnijeti zahtjev za pokretanje prekršajnog postupka u skladu sa ovim Zakonom;
 - j) naložiti privremenu obustavu prijenosa podataka primatelju u drugoj zemlji ili međunarodnoj organizaciji.
- (3) Agencija ima sljedeće ovlasti u vezi s odobravanjem i savjetovanjem:
- a) savjetovati kontrolora podataka u skladu s postupkom prethodnog savjetovanja iz čl. 38. i 84. ovog Zakona;
 - b) davati mišljenja o svim pitanjima koja se tiču zaštite osobnih podataka, na vlastitu inicijativu ili na zahtjev zakonodavnih tijela, vlada ili, u slučajevima kada je to posebnim zakonom propisano, drugim institucijama i tijelima, kao i javnosti;
 - c) odobriti obradu iz članka 38. stavka (8) ovog Zakona ako je posebnim zakonom propisano takvo prethodno odobrenje;
 - d) davati mišljenja i odobravati nacрте kodeksa ponašanja u skladu s člankom 42. stavkom (5) ovog Zakona;
 - e) akreditirati certifikacijska tijela u skladu s člankom 45. ovog Zakona;
 - f) odobravati kriterije certifikacije u skladu s člankom 44. stavkom (6) ovog Zakona;
 - g) usvajati standardne klauzule o zaštiti podataka iz članka 30. stavka (8) i članka 48. stavka (3) ovog Zakona;
 - h) odobriti odgovarajuće zaštitne mjere iz članka 48. stavka (4) točke a) ovog Zakona;
 - i) odobriti odgovarajuće zaštitne mjere iz članka 48. stavka (4) točke b) ovog Zakona;
 - j) odobriti obvezujuća poslovna pravila u skladu s člankom 49. ovog Zakona.
- (4) Odluka Agencije je konačna u upravnom postupku i protiv nje nije dopuštena žalba, ali se može pokrenuti upravni spor pred Sudom Bosne i Hercegovine.
- (5) Agencija u postupku odlučivanja primjenjuje pravila upravnog postupka, osim ako ovim Zakonom nije drukčije propisano.
- (6) Agencija je ovlaštena po potrebi obavijestiti nadležna istražna tijela o povredama ovog Zakona ili pokrenuti pravne postupke ili na drugi način sudjelovati u tim postupcima radi provedbe ovog Zakona.
- (7) Svaka obrada osobnih podataka koji imaju određen stupanj tajnosti na temelju posebnog zakona provodi se u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.
- (8) Obradu osobnih podataka iz stavka (7) ovog članka provode službenici Agencije koji imaju dozvolu za pristup tajnim podacima, u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.
- Članak 104.
- (Međunarodna suradnja radi zaštite osobnih podataka)
- Agencija poduzima odgovarajuće mjere u vezi s drugim zemljama i međunarodnim organizacijama radi:
- a) razvoja mehanizama međunarodne suradnje za olakšavanje učinkovite primjene zakonodavstva o zaštiti osobnih podataka;
 - b) osiguravanja uzajamne međunarodne pomoći u primjeni zakonodavstva o zaštiti osobnih podataka, što podrazumijeva obavješćavanje, upućivanje prigovora, pružanje pomoći u istragama i razmjenu informacija, u skladu s odgovarajućim mjerama za zaštitu osobnih podataka i drugim temeljnim pravima i slobodama;
 - c) uključivanja relevantnih interesnih skupina u raspravu i aktivnosti čiji je cilj unaprijediti međunarodnu suradnju u primjeni zakonodavstva o zaštiti osobnih podataka;
 - d) promicanja razmjene i dokumentiranja zakonodavstva i prakse u vezi sa zaštitom osobnih podataka, uključujući i sporove oko nadležnosti s drugim zemljama.
- Članak 105.
- (Povjerljiva prijava povreda Zakona)
- (1) Nadležno tijelo koje obrađuje osobne podatke u svrhe iz članka 1. stavka (1) točke c) ovog Zakona dužno je osigurati primjenu učinkovitih mehanizama za povjerljivu prijavu slučajeva povrede ovog Zakona.
- (2) Mehanizmi koji se primjenjuju u skladu sa stavkom (1) ovog članka moraju osigurati da se povreda može prijaviti nadležnom tijelu ili Agenciji.
- (3) Ti mehanizmi uključuju podizanje svijesti o zaštiti osobnih podataka i mjere o zaštiti osoba koje prijavljuju povrede.

Članak 106.

(Izvješća Agencije)

- (1) Agencija podnosi Parlamentarnoj skupštini godišnje izvješće o zaštiti osobnih podataka za proteklu godinu najkasnije do kraja lipnja tekuće godine i čini ga dostupnim javnosti.
- (2) Godišnje izvješće o zaštiti osobnih podataka iz stavka (1) ovog članka sadrži podatke o:
 - a) svim aktivnostima Agencije, a posebno o vrstama povreda osobnih podataka i poduzetim mjerama;
 - b) stanju zaštite osobnih podataka u Bosni i Hercegovini;
 - c) ključnim pitanjima iz područja zaštite osobnih podataka;
 - d) kapacitetima Agencije.

Članak 107.

(Inspeksijski nadzor)

- (1) Inspeksijski nadzor nad provedbom ovog Zakona obavlja inspektor Agencije.
- (2) Inspektor svoj identitet, svojstvo i ovlasti dokazuje iskaznicom inspektora.
- (3) Inspeksijskim nadzorom ostvaruje se neposredan uvid u zakonitost rada i postupanje kontrolora podataka i obrađivača s ciljem provjere usklađenosti njegova rada s ovim Zakonom i drugim propisima koji se odnose na zaštitu osobnih podataka.
- (4) Inspeksijski nadzor može biti redovit, izvanredan i revizijski.
- (5) Redoviti inspeksijski nadzor provodi se na temelju godišnjeg i mjesečnog plana inspeksijskog nadzora, koji se donosi na razini Agencije.
- (6) Rješenje iz redovitog inspeksijskog nadzora donosi inspektor, a protiv rješenja je dozvoljena žalba ravnatelju Agencije u roku od 15 dana od dana njegovog primitka.
- (7) Izvanredni inspeksijski nadzor provodi se na temelju prigovora ili postupanja po službenoj dužnosti kada je, u odnosu na konkretni slučaj, potrebno obaviti inspeksijski nadzor.
- (8) Zapisnik iz izvanrednog inspeksijskog nadzora je dokazno sredstvo u postupku po prigovoru ili po službenoj dužnosti, koji provodi i rješava Agencija.
- (9) Revizijski inspeksijski nadzor provodi se nakon redovitog ili izvanrednog inspeksijskog nadzora s ciljem provjere izvršenja naloženih upravnih mjera.
- (10) Rješenje u postupku nakon provođenja izvanrednog i revizijskog inspeksijskog nadzora donosi ravnatelj Agencije i ono je konačno u upravnom postupku.
- (11) Nakon provođenja inspeksijskog nadzora inspektor sastavlja zapisnik o utvrđenom činjeničnom stanju, koji potpisuju inspektor i ovlaštena osoba kontrolora podataka ili obrađivača.
- (12) Inspektor ima pravo pregledati sve poslovne prostorije i objekte u kojima se obrađuju osobni podaci, proces rada, uređaje, isprave i dokumentaciju, kao i obavljati druge radnje u vezi sa svrhom inspeksijskog nadzora, u skladu s člankom 103. stavkom (1) toč. f) i g) i člankom 103. st. (7) i (8) ovog Zakona.
- (13) Kontrolor podataka i obrađivač dužni su omogućiti inspektoru nesmetano obavljanje inspeksijskog nadzora.
- (14) Ako se inspektoru tijekom inspeksijskog nadzora onemogućava obavljanje nadzora ili pruži fizički otpor ili ako se taj otpor osnovano očekuje, inspektor može zatražiti pomoć policije.
- (15) O obavljenom inspeksijskom nadzoru inspektor vodi evidenciju.

DIO PETI – PRAVNA SREDSTVA, ODGOVORNOST I KAZNE

Članak 108.

(Pravo na prigovor Agenciji)

- (1) Nositelj podataka ima pravo podnijeti prigovor Agenciji ako smatra da se obradom osobnih podataka u vezi s njim krši ovaj Zakon, ne dovodeći u pitanje druga upravna ili sudska pravna sredstva.
- (2) Agencija obavještava podnositelja prigovora o napretku i ishodu postupka, uključujući i mogućnost primjene pravnog sredstva na temelju članka 109. ovog Zakona, i pruža dodatnu pomoć na zahtjev podnositelja prigovora.

Članak 109.

(Pravo na djelotvorno pravno sredstvo protiv odluka Agencije)

- (1) Fizička osoba, kontrolor podataka ili obrađivač ima pravo pokrenuti upravni spor protiv odluke Agencije pred Sudom Bosne i Hercegovine u roku od 60 dana od dana primitka odluke, ne dovodeći u pitanje druga upravna ili izvansudska pravna sredstva.
- (2) Nositelj podataka ima pravo pokrenuti upravni spor pred Sudom Bosne i Hercegovine ako Agencija u roku od 90 dana ne riješi prigovor ili ne obavijesti nositelja podataka o napretku ili ishodu postupka povodom prigovora, ne dovodeći u pitanje druga upravna ili izvansudska pravna sredstva.

Članak 110.

(Pravo na djelotvorno pravno sredstvo protiv kontrolora podataka ili obrađivača)

- (1) Nositelj podataka ima pravo na sudska zaštitu protiv kontrolora podataka ili obrađivača ako smatra da su zbog obrade osobnih podataka prekršena njegova prava iz ovog Zakona, ne dovodeći u pitanje druga upravna ili izvansudska pravna sredstva, uključujući i pravo na podnošenje prigovora Agenciji iz članka 108. stavka (1) ovog Zakona.
- (2) Postupak sudske zaštite iz stavka (1) ovog članka vodi se u skladu sa zakonima kojima se uređuje parnični postupak.

Članak 111.

(Zastupanje nositelja podataka)

Nositelj podataka ima pravo dati ovlast neprofitnom tijelu, organizaciji ili udruzi osnovanoj u skladu sa zakonom, čija je svrha osnivanja ostvarivanje ciljeva od javnog interesa i koja je aktivna u području zaštite prava i sloboda nositelja podataka u vezi sa zaštitom osobnih podataka, da u njegovo ime ostvaruju prava iz čl. 108., 109. i 110. ovog Zakona, kao i da u njegovo ime i za njegov račun ostvaruju pravo na naknadu štete.

Članak 112.

(Pravo na naknadu štete i odgovornost)

- (1) Svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja ovog Zakona ima pravo na naknadu za pretrpljenu štetu od kontrolora podataka ili obrađivača.
- (2) Svaki kontrolor podataka odgovoran je za štetu prouzročenu obradom kojom se krši ovaj Zakon. Obradivač je odgovoran za štetu prouzročenu obradom samo ako nije poštivao obveze iz ovog Zakona koje su posebno propisane za obrađivače ili ako je prekoracio zakonite instrukcije kontrolora podataka ili je postupio protivno njima.
- (3) Kontrolor podataka ili obrađivač izuzet je od odgovornosti ako dokaže da ni na koji način nije odgovoran za događaj koji je prouzročio štetu.

- (4) Ako je u istu obradu uključeno više od jednog kontrolora podataka ili obrađivača ili su u istu obradu uključeni i kontrolor podataka i obrađivač i ako su odgovori za štetu prouzročenu obradom, svaki kontrolor podataka ili obrađivač odgovoran je za cjelokupnu štetu.
- (5) Ako je kontrolor podataka ili obrađivač platio punu odštetu u skladu sa stavkom (4) ovog članka, taj kontrolor podataka ili obrađivač ima pravo od drugih kontrolora podataka ili obrađivača uključenih u istu obradu zahtijevati povrat dijela odštete koji odgovara njihovom udjelu u odgovornosti za štetu.
- (6) Pravo na naknadu štete ostvaruje se u sudskom postupku, a mjesna nadležnost utvrđuje se u skladu s člankom 110. stavkom (2) ovog Zakona.
- Članak 113.
(Opći uvjeti za izricanje novčane kazne)
- (1) Agencija osigurava da je izricanje novčane kazne, u skladu s ovim člankom i u vezi s povredama ovog Zakona, u svakom pojedinačnom slučaju djelotvorno, razmjerno i odvratajuće.
- (2) Agencija izdaje prekršajni nalog ili podnosi zahtjev za pokretanje prekršajnog postupka nadležnom sudu, pored mjera iz članka 103. stavka (2) toč. a) do h) i točke j) ovog Zakona, ovisno o okolnostima svakog pojedinačnog slučaja. Prilikom odlučivanja o novčanoj kazni i iznosu kazne u svakom pojedinačnom slučaju u obzir se uzima posebno:
- priroda, težina i trajanje povrede, imajući u vidu prirodu, opseg i svrhu predmetne obrade, kao i broj nositelja podataka i stupanj štete koju su pretrpjeli;
 - ima li povreda obilježje namjere ili nepažnje;
 - svaka radnja koju je kontrolor podataka ili obrađivač poduzeo kako bi ublažio štetu koju su pretrpjeli nositelji podataka;
 - stupanj odgovornosti kontrolora podataka ili obrađivača, pri čemu se uzimaju u obzir tehničke i organizacijske mjere koje su primijenili, u skladu s čl. 27. i 34. ovog Zakona;
 - sve utvrđene prethodne povrede kontrolora podataka ili obrađivača;
 - stupanj suradnje s Agencijom na otklanjanju povrede i ublažavanju mogućih štetnih posljedica povrede;
 - kategorija osobnih podataka na koje povreda utječe;
 - način na koji je Agencija doznala za povredu, a posebno je li i u kojem opsegu kontrolor podataka ili obrađivač izvijestio o povredi;
 - ako su protiv kontrolora podataka ili obrađivača u vezi s istim predmetom prethodno izrečene mjere iz članka 103. stavka (2) ovog Zakona, i poštivanje tih mjera;
 - poštivanje odobrenih kodeksa ponašanja u skladu sa člankom 42. ovog Zakona ili odobrenih mehanizama certifikacije u skladu sa člankom 44. ovog Zakona;
 - sve ostale otegotne ili olakotne okolnosti, kao što su financijska dobit ostvarena kršenjem ili izbjegnuti gubici, izravno ili neizravno, tim kršenjem.
- (3) Ako kontrolor podataka ili obrađivač za istu ili povezane obrade namjerno ili iz nepažnje prekrši više odredaba ovog Zakona, ukupan iznos novčane kazne ne smije biti viši od iznosa utvrđenog za najtežu povredu.
- (4) Novčanom kaznom u iznosu od 10.000 KM do 20.000.000 KM ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos viši, kažnjava se:
- kontrolor podataka i obrađivač za obradu osobnih podataka obavljenju suprotno čl. 10. i 13., čl. 27. – 41., te čl. 44. i 45. ovog Zakona;
 - certifikacijsko tijelo koje postupi suprotno čl. 44. i 45. ovog Zakona;
 - tijelo za praćenje odobrenih kodeksa ponašanja ako postupi suprotno članku 43. stavku (3) ovog Zakona.
- (5) Novčanom kaznom u iznosu od 20.000 KM do 40.000.000 KM ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos viši, kaznit će se:
- tko obrađuje osobne podatke suprotno čl. 7., 8., 9. i 11. ovog Zakona;
 - tko krši prava nositelja podataka iz čl. 14. do 24. ovog Zakona;
 - tko prenese osobne podatke primatelju u drugu zemlju ili međunarodnu organizaciju suprotno čl. 46. – 51. ovog Zakona;
 - tko postupi suprotno obvezama iz posebnih zakona donesenih na temelju Dijela drugog Poglavlja V. ovog Zakona;
 - tko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenoj obustavi prijenosa podataka u skladu s člankom 103. stavkom (2) ovog Zakona ili uskrati pristup suprotno članku 103. stavku (1) ovog Zakona.
- (6) Za nepostupanje po nalogu Agencije iz članka 103. stavka (2) ovog Zakona u skladu sa stavkom (2) ovog članka izriče se novčana kazna u iznosu od 20.000 KM do 40.000.000 KM ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos viši.
- (7) Za povredu iz st. (4), (5) i (6) ovog članka novčanom kaznom u iznosu od 5.000 KM do 70.000 KM kaznit će se odgovorna osoba, a novčanom kaznom u iznosu od 500 KM do 5.000 KM kaznit će se zaposlena osoba kod kontrolora podataka ili obrađivača.
- (8) Novčanom kaznom u iznosu od 5.000 KM do 70.000 KM kaznit će se odgovorna osoba, a novčanom kaznom u iznosu od 500 KM do 5.000 KM kaznit će se zaposlena osoba u javnom i nadležnom tijelu za prekršaj:
- iz čl. 7. – 11., članka 13., čl. 14. – 24., čl. 27. – 41., čl. 44. i 45., čl. 52. – 59., članka 60., članka 64., članka 66., čl. 67. – 73., čl. 76. i 77. i čl. 79. – 90. ovog Zakona;
 - tko prenese osobne podatke primatelju u drugu zemlju ili međunarodnu organizaciju suprotno čl. 46. – 51. te čl. 91. – 95. ovog Zakona;
 - tko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenoj obustavi prijenosa podataka u skladu s člankom 103. stavkom (2) ovog Zakona ili uskrati pristup suprotno članku 103. stavku (1) ovog Zakona.
- (9) Zastara izricanja novčane kazne nastupa nakon proteka razdoblja od pet godina od dana kada je povreda učinjena.
- (10) Ne dovodeći u pitanje nadležnosti i ovlasti Agencije, novčane kazne ne mogu se izreći javnom tijelu i nadležnom tijelu za povrede ovog Zakona, osim odgovornoj i zaposlenoj osobi iz stavka (8) ovog članka.
- (11) Na postupak izricanja novčane kazne iz ovog članka primjenjuju se odredbe Zakona o prekršajima Bosne i Hercegovine, a iznosi novčanih kazni propisani su ovim Zakonom.

- (12) Iznimno od odredbe stavka (11) ovog članka, prihod ostvaren na temelju naplate novčanih kazni dijeli se na način propisan člankom 114. ovog Zakona.

Članak 114.

(Izvršenje i naplata novčane kazne)

Novčana kazna uplaćuje se na Jedinствени račun trezora institucija Bosne i Hercegovine i dijeli se kako slijedi:

- a) ako je sjedište ili poslovni nastan pravne osobe ili prebivalište fizičke osobe u Bosni i Hercegovini, sredstva s Jedinственог računa trezora institucija Bosne i Hercegovine uplaćuju se na račun entiteta ili Brčko distrikta BiH, ovisno o sjedištu ili poslovnom nastanu pravne osobe ili prebivalištu fizičke osobe;
- b) ako je sjedište ili poslovni nastan pravne osobe ili prebivalište fizičke osobe izvan Bosne i Hercegovine, sredstva s Jedinственог računa trezora institucija Bosne i Hercegovine raspoređuju se prema Odluci o utvrđivanju privremenih koeficijenata za raspodjelu sredstava s Jedinственог računa. U Federaciji Bosne i Hercegovine sredstva se raspoređuju između kantona i općina u skladu sa Zakonom o pripadnosti javnih prihoda u Federaciji Bosne i Hercegovine.

Članak 115.

(Kazne)

Kaznenim zakonima propisuju se kazne za kazneno djelo protuzakonite obrade osobnih podataka, u slučaju grubog kršenja odredaba ovog Zakona.

DIO ŠESTI – PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 116.

(Mjere u prijelaznom razdoblju)

- (1) Odredbe drugih zakona koje se odnose na obradu osobnih podataka uskladić će se s ovim Zakonom u roku od dvije godine od njegovog stupanja na snagu.
- (2) Kontrolori podataka i obrađivači koji su započeli obradu osobnih podataka dužni su te obrade uskladić s ovim Zakonom u roku od dvije godine od njegovog stupanja na snagu.
- (3) Odluke donesene na temelju članka 18. stavka (4) Zakona o zaštiti osobnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11) ostaju na snazi dok se ne izmijene, zamijene ili stave izvan snage odlukom Agencije.
- (4) Ravnatelj i zamjenik ravnatelja Agencije koji su imenovani u skladu sa Zakonom o zaštiti osobnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11) nastavljaju obavljati dužnost do isteka mandata na koji su imenovani.
- (5) Agencija nastavlja svoj rad u prijelaznom razdoblju.

Članak 117.

(Podzakonski akti)

Svi podzakonski akti propisani ovim Zakonom bit će doneseni u roku od 210 dana od dana stupanja na snagu ovog Zakona.

Članak 118.

(Odnos s prethodno sklopljenim sporazumima)

Međunarodni sporazumi koji uključuju prijenos osobnih podataka drugim zemljama ili međunarodnim organizacijama koje je Bosna i Hercegovina sklopila prije donošenja ovog Zakona, a koji su sukladni sa Zakonom o zaštiti osobnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11), ostaju na snazi dok ih se ne izmijeni, zamijeni ili stavi izvan snage.

Članak 119.

(Prestanak važenja)

- (1) Početkom primjene ovog Zakona prestaje važiti Zakon o zaštiti osobnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11).
- (2) Početkom primjene ovog Zakona prestaju važiti podzakonski akti doneseni na temelju Zakona iz stavka (1) ovog članka: Pravilnik o postupku po prigovoru nositelja osobnih podataka u Agenciji za zaštitu osobnih podataka u Bosni i Hercegovini ("Službeni glasnik BiH", broj 51/09), Pravilnik o inspekcijskom nadzoru u području zaštite osobnih podataka ("Službeni glasnik BiH", broj 51/09), Instrukcija o načinu provjere obrade osobnih podataka prije uspostave zbirke osobnih podataka ("Službeni glasnik BiH", broj 51/09), Pravilnik o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka ("Službeni glasnik BiH", broj 52/09) i Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite osobnih podataka ("Službeni glasnik BiH", broj 67/09).

Članak 120.

(Stupanje na snagu)

Ovaj Zakon stupa na snagu osmoga dana od dana objave u "Službenom glasniku BiH", a primjenjuje se nakon isteka 210 dana od dana stupanja na snagu.

Broj 01.02-02-1-2548/24

30. siječnja 2025. godine

Sarajevo

Predsjedatelj

Zastupničkog doma

Parlamentarne skupštine BiH

Dr. Denis Zvizdić, v. r.

Predsjedatelj

Doma naroda

Parlamentarne skupštine BiH

Dr. Dragan Čović, v. r.

171

Na osnovu člana 28. stav (2) Zakona o državnoj službi u institucijama Bosne i Hercegovine ("Službeni glasnik BiH", br. 19/02, 35/03, 4/04, 17/04, 26/04, 37/04, 48/05, 2/06, 32/07, 43/09, 8/10, 40/12, 93/17 i 18/24), člana 20. tачка x) Poslovnika Predstavničkog doma Parlamentarne skupštine Bosne i Hercegovine ("Službeni glasnik BiH", br. 79/14, 81/15, 97/15, 78/19, 26/20 53/22, 59/23, 87/23, 50/24 i 73/24), člana 18. tачка x) Poslovnika Doma naroda Parlamentarne skupštine Bosne i Hercegovine ("Službeni glasnik BiH", br. 58/14, 88/15, 96/15, 53/16 i 71/24), Mišljenja Agencije za državnu službu Bosne i Hercegovine, broj 03-34-2-837-7/24 od 24. 01. 2025. godine, člana 9. Zakona o platama i naknadama u institucijama Bosne i Hercegovine ("Službeni glasnik BiH", br. 50/08, 35/09, 75/09, 32/12, 42/12, 50/12, 32/13, 87/13, 75/15, 88/15, 16/16, 94/16, 72/17, 25/18, 32/20, 65/20 i 59/22) i Glave III tачка 10. Odluke o organizaciji Sekretarijata Parlamentarne skupštine Bosne i Hercegovine ("Službeni glasnik BiH", br. 92/05 i 63/08), Kolegijum Predstavničkog doma Parlamentarne skupštine Bosne i Hercegovine na 56. sjednici, održanoj 24.02.2025. godine, i Kolegijum Doma naroda Parlamentarne skupštine Bosne i Hercegovine na 30. sjednici, održanoj 20.02.2025. godine, donijeli su

РЈЕШЕЊЕ О ИМЕНОВАЊУ

1. Аида Османовић именује се на радно мјесто руководиоца Истраживачког сектора у Заједничкој служби Секретаријата Парламентарне skupштине Bosne i Hercegovine.