СЛУЖБЕНИ ГЛАСНИК БОСНЕ И ХЕРЦЕГОВИНЕ
Издање на српском, босанском и хрватском језику

SLUŽBENI GLASNIK BOSNE I HERCEGOVINE
Izdanje na srpskom, bosanskom i hrvatskom jeziku

Година XXIX
Петак, 28. фебруара 2025. године

Број/Broj
12

Godina XXIX
Petak, 28. februara/veljače 2025. godine

ISSN 1512-7508 - српски језик
ISSN 1512-7486 - босански језик
ISSN 1512-7494 - хрватски језик

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:
   а) правила у вези са заштитом физичких лица у вези с обрадом личних података и правила повезана са слободним кретањем личних података;
   б) 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;
   ц) 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 дијела 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 употријебљени у овом закону имају сљедећа значења:

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

утврдити, 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 потврдном 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) 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) 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 сљедећих 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 над тим интересима претежу интереси или основна права и слободе 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 података 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 посљедице 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. Дио 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 сљедећих 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 слободе 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 идентификовање 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 носилац 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 носилац података поднесе захтјев електронским путем, информације се пружају електронским путем ако је то могуће, осим у случају када носилац 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, обавијести 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 пружио 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 примјењиво;

б) контактне податке службеника за заштиту података, ако је примјењиво;

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 примјењиво.

(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 личном 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 дâ лични податак и које су могуће посљедице 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 дâ информације о начину рада, као и значају и предвиђеним посљедицама 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 примјењиво;
б) контактним подацима службеника за заштиту података, ако је примјењиво;
ц) правном основу за обраду и за сврхе обраде којој су намијењени 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 примјењиво.

(2) Осим информација из става (1) овог члана, контролор података пружа носиоцу података сљедеће информације ако је то неопходно да би се обезбиједила 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 посљедицама 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 посљедицама 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 провјери 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 података или ограничењу обраде)

(1) Контролор података обавјештава све примаоце којима су лични подаци откривени о свакој исправци или брисању личног података 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 података)

(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 података, 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 података 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 података, 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 превладавају 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 података 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 података 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 учинак 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 повреде 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 сљедеће:
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 примијенити узимајући у обзир природу, обим и сврхе обраде или категорије обраде;
г) ризик за права и слободе 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 примијени 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 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 механизама сертификације из члана 44. овог закона може служити као елеменат 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 сврхе обраде, као и ризике различитих нивоа вјероватноће и озбиљности за права и слободе 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 обезбјеђује 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 обезбјеђује 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 елеменат 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 сврхе и начине обраде, сматрају се заједничким контролорима података. Они на транспарентан начин, међусобним споразумом, одређују одговорности сваког од њих с циљем извршавања обавеза из овог закона, посебно у вези са остваривањем права носиоца података и дужностима сваког 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) Именовање 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:

а) 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;

б) обезбјеђује да су се лица овлашћена за обраду личног податка обавезала на поштовање повјерљивости или да их на поштовање повјерљивости обавезује одговарајући закон;

ц) предузима све потребне мјере у складу са чланом 34. овог закона;

д) поштује услове из ст. (2) и (5) овог члана за ангажовање другог обрађивача;

е) 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;

ф) 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;

г) 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;

х) 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;

и) 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 елеменат 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 примјењиво, води евиденцију активности обраде за које је одговоран. Евиденција садржи сљедеће информације:
   а) име и контакт податке контролора података и, ако је примјењиво, 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 примјењиво, 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 примјењиво, 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 примјењиво, 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 примјењиво, 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 примјењиво, 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 повремена 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 подразумијева:
   а) псеудонимизацију и енкрипцију личног податка;
   б) могућност обезбјеђивања трајне повјерљивости, цјеловитости, 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 елеменат за доказивање усклађености са захтјевима из става (1) овог члана.

(4) Контролор података и обрађивач предузимају мјере како би обезбиједили 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 сљедеће:
   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 посљедице повреде личног податка;
   д) опис мјера које је контролор података предузео или чије је предузимање предложио ради рјешавања проблема повреде личног податка, укључујући према потреби и мјере за ублажавање њених могућих штетних посљедица.

(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 посљедице 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 сљедећих услова:
   а) ако је контролор података предузео одговарајуће техничке и организационе заштитне мјере и те мјере су примијењене 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 накнадне 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 учинак 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 намјераваној 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 процјеном 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 умањио 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 одгађања.

(5) Протицање 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 примјењиво, 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 примјењиво;
   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 сљедеће 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 процјеном 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 кодексе 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 дјеце 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 обезбиједили 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 обавеже 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 МЕЂУНАРОДНУ ОРГАНИЗАЦИЈУ

Члан 46.

(Општи принципи преноса)

Сваки пренос личног податка чија је обрада у току или је намијењен даљој обради послије 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 обезбијеђен 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:

а) 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;

б) постојање и ефикасност рада надзорног органа у другој држави или органа који је надлежан за међународну организацију у овој области, с овлашћењем да обезбиједи 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;

ц) 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)

(1) 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 обезбиједио одговарајуће заштитне мјере тих података и ако су носиоцу личних података обезбијеђени остварива права и дјелотворна судска заштита.

(2) Одговарајуће заштитне мјере из става (1) овог члана могу се, без посебног одобрења Агенције, обезбиједити:

а) правно обавезујућим актом сачињеним између јавних органа;

б) обавезујућим пословним правилима у складу са чланом 49. овог закона;

ц) одобреним 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

д) одобреним 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.

(3) Одговарајуће заштитне мјере из става (1) овог члана могу се обезбиједити стандардним уговорним клаузулама о заштити података које доноси Агенција.

(4) Уз услов да то одобри Агенција, одговарајуће заштитне мјере из става (1) овог члана такође могу бити обезбијеђене посебно:

а) уговором између контролора података или обрађивача и контролора података, обрађивача или примаоца личних података у другој држави или међународној организацији, или

б) одредбама које се уносе у споразуме између јавних органа и које садрже остварива и дјелотворна права носиоца података.

Члан 49.

(Обавезујућа пословна правила)

(1) Обавезујућа пословна правила одређују најмање:

а) структуру и податке за контакт групе привредних субјеката који обављају заједничку привредну дјелатност и сваког од њихових чланова;

б) преносе података или скупове преноса, уз навођење категорије личних података, врсте

обраде 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 особље 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 сљедећих 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 дâ 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 слободе носиоца података, а контролор података је проценио 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 цјелини 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 угрозити 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 угрозити 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 нужно 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 сљедеће 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 КОНТРОЛОРА ПОДАТАКА У СВРХУ СПРЕЧАВАЊА, ИСТРАГЕ И ОТКРИВАЊА КРИВИЧНИХ ДЈЕЛА ИЛИ ГОЊЕЊА 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 дуже 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 сљедеће информације:
   а) идентитет и контакт податке надлежног органа;
   б) контакт податке службеника за заштиту личних података, ако је примјењиво;
   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 сљедеће 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 примјењиво;
   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 запримања 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 исправци 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 примијени 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 обезбиједио 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, примијени 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 обезбиједити 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 обезбиједи 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 сљедеће 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 примјењиво;
   ф) категорију преноса личних података у другу државу или међународну организацију, ако је примјењиво;
   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 примјењиво;
   б) категорију обраде која се спроводи за сваког контролора података;
   ц) ако је примјењиво, 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 сљедеће 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 провјере 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 умањио 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 процијенити 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 умањио 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) спријечи неовлашћено читање, умножавање, мијењање или уклањање носача података;
   ц) спријечи неовлашћено уношење личних података те неовлашћено прегледање, мијењање или брисање чуваних личних података;
   д) спријечи 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 унио;
   х) спријечи 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, обавијести 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 обавијести 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 сљедеће 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 предложио 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 сљедећих 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. став (3) овог закона.

Члан 88.

(Именовање 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, нису 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 надлежног органа)

(1) Надлежни орган дужан је да обезбиједи 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 надлежног органа)

Надлежни орган службенику за заштиту личних података повјерава најмање сљедеће 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 процјеном 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 сљедећи услови, и то:

а) пренос је неопходан у сврхе утврђене у члану 1. ставу (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 обезбиједило 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 обезбијеђен 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 проценио 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 примаоцу 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 сљедећи 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 Хереговине.

(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 држављани 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, BCC/VII степен, или високо образовање болоњског 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 разријеши 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.
(Неспојивост 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 додијељених 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 сљедеће 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 дјеци;
   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 механизама 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 сљедећа 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 сљедећа 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 сљедећа 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 примијенио 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 механизама 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 обезбиједи примјену ефикасних механизама за повјерљиво пријављивање случајева повреде овог закона.
(2) Механизми који се примјењују у складу са ставом (1) овог члана морају да обезбиједе 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 провјере 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) Рјешење 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 провјере извршења наложених управних мјера.
(10) Рјешење 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 ријеши 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 претрпјело материјалну или нематеријалну штету због кршења овог закона има право на накнаду за претрпљену 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 цјелокупну 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 претрпјели;

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 претрпјели 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

механизама 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 протека 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 повреде овог закона, осим одговорном и запосленом 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 настан 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 настан 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 расподјелу 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 обраде 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	Предсједавајући
Представничког дома	Дома народа
Парламентарне скупштине	Парламентарне скупштине
БиХ	БиХ
Др **Денис Звиздић**, с. р.	Др **Драган Човић**, с. р.

Na osnovu člana IV. 4. a) Ustava Bosne i Hercegovine, Parlamentarna skupština Bosne i Hercegovine, na 16. hitnoj sjednici Predstavničkog doma, održanoj 23. januara 2025. godine, i na 8. hitnoj sjednici Doma naroda, održanoj 30. januara 2025. godine, usvojila je

ZAKON
O ZAŠTITI LIČNIH PODATAKA

DIO PRVI – OPĆE ODREDBE

Član 1.

(Predmet)

(1) Ovim zakonom propisuju se:
   a) pravila u vezi sa zaštitom fizičkih lica u vezi s obradom ličnih podataka i pravila povezana sa slobodnim kretanjem ličnih podataka;
   b) 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;
   c) 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.

Član 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.

Član 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 na muški i ženski rod.

Član 4.

(Definicije)

Pojedini izrazi upotrijebljeni u ovom zakonu imaju sljedeća značenja:

   a) "lični podatak" je svaki podatak koji se odnosi na fizičko lice čiji je identitet utvrđen ili se može utvrditi;
   b) "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 o lokaciji, mrežni identifikator ili pomoću jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet tog lica;
   c) "obrada" je svaki postupak ili skup postupaka koji se obavlja na ličnim podacima ili na skupovima ličnih