



Broj: 05-02-1-685-7/24  
Sarajevo, 17. 12. 2024. godine

ŽURNO!

PARLAMENTARNA SKUPŠTINA BOSNE I HERCEGOVINE  
Zastupnički dom

BOSNA I HERCEGOVINA  
PARLAMENTARNA SKUPŠTINA BOSNE I HERCEGOVINE  
SARAJEVO

Trg BiH 1, 71 000 Sarajevo

PRIMLJENO: 17-12-2024			
Organizaciona jedinica	Klasifikaciona oznaka	Redni broj	Broj priloga
01.02	-62-1-	2548	124

PREDMET: Prijedlog Zakona o zaštiti osobnih podataka Bosne i Hercegovine,  
*dostavlja se*

Poštovani,

na 46. izvandrednoj sjednici Vijeća ministara Bosne i Hercegovine, održanoj 17. 12. 2024. godine, na prijedlog Ministarstva civilnih poslova Bosne i Hercegovine, usvojen je Prijedlog Zakona o zaštiti osobnih podataka Bosne i Hercegovine, uz prijedlog da se isti uputi Parlamentarnoj skupštini Bosne i Hercegovine na razmatranje po skraćenom zakonodavnom postupku.

Vijeće ministara Bosne i Hercegovine je uvažilo navode Ministarstva civilnih poslova Bosne i Hercegovine da se Prijedlog Zakona o zaštiti osobnih podataka Bosne i Hercegovine oznakom „P.Z.E.I“, kako bi isti bio razmatran u skraćenom zakonodavnom postupku, sukladno odredbama članka 134. stavak (1) Poslovnika Zastupničkog doma Parlamentarne skupštine BiH („Službeni glasnik BiH“ broj 79/14, 81/15, 97/15, 78/19, 26/20, 53/22, 59/23, 87/23, 50/24 i 74/24) i članka 125. stavak (1) Poslovnika Doma naroda Parlamentarne skupštine BiH („Službeni glasnik BiH“ broj 58/14, 88/15, 96/15, 53/16, 71/24).

U svezi prednje navedenog, u privitku dostavljamo Zakona o zaštiti osobnih podataka Bosne i Hercegovine, na bosanskom, hrvatskom i srpskom jeziku te latiničnom i ćirilničnom pismu, kao i njegovu elektroničku verziju sa svim privicima.

Istovremeno, dostavljamo Obavijest Vijeća ministara Bosne i Hercegovine broj 05-07-1-2758-40/24 od 17. 12. 2024. godine, obrazloženje Prijedloga zakona, Obrazac broj 1 – prethodna procjena učinaka propisa i Obrazac 2a o fisklanoj procjeni, sukladno Jedinim pravilima za izradu pravnih propisa u institucijama Bosne i Hercegovine, te pribavljena mišljenja nadležnih institucija: Ureda za zakonodvstvo Vijeća ministara Bosne i Hercegovine, Direkcije za europske integracije Vijeća ministara Bosne i Hercegovine sa Izjavom o usklađenosti, Ministarstva pravde Bosne i Hercegovine, Agencije za zaštitu osobnih podataka u Bosni i Hercegovini, Ministarstva financija i trezora Bosne i Hercegovine, Ministarstva za ljudska prava i izbjeglice Bosne i Hercegovine.

S poštovanjem,

Privitak: - kao u tekstu-

Dostavljeno:

- naslovu
- a/a

GENERALNI TAJNIK  
VIJEĆE MINISTARA BiH  
mr. Robert Vidović



Broj: 05-07-1-2758-40/24  
Sarajevo, 17. 12. 2024. godine

**MINISTARSTVO CIVILNIH POSLOVA BOSNE I HERCEGOVINE**

- *n/r tajnika Ministarstva* –

Trg Bosne i Hercegovine 1, 71000 Sarajevo

✓ **GENERALNO TAJNIŠTVO VIJEĆA MINISTARA BOSNE I HERCEGOVINE**

- *n/r generalnog tajnika* –

Trg Bosne i Hercegovine 1, 71000 Sarajevo

**PREDMET:** Obavijest, dostavlja se

Vijeće ministara Bosne i Hercegovine, na 46. izvanrednoj sjednici održanoj 17. 12. 2024. godine, razmotrilo je Nacrt zakona o zaštiti osobnih podataka – NOVI TEKST od 9. 12. 2024.g., te s tim u vezi zaključilo:

- Vijeće ministara Bosne i Hercegovine, rješavajući prethodno pitanje, donijelo je zaključak kojim se Ministarstvo civilnih poslova Bosne i Hercegovine u skladu s člankom 24. stavkom (1) točkom a) Pravila za konzultacije u izradi pravnih propisa („Službeni glasnik BiH“, broj 5/17 i 87/23) oslobađa obveze provedbe konzultacija za Nacrt zakona o zaštiti osobnih podataka – NOVI TEKST od 9. 12. 2024. g.;

- Usvaja se Prijedlog zakona o zaštiti osobnih podataka – NOVI TEKST od 9. 12. 2024. godine uz prihvaćenu korekciju da se članku 8. doda novi stavak (5) koji glasi „5) Javni i nadležni organi entiteta i Brčko Distrikta su dužni, uz poštovanje odredbi ovog zakona, ustupiti osobne podatke iz svojih evidencija ovlaštenom kontroloru podataka, u svrhu prethodnog izjašnjavanja građana koji imaju biračko pravo o pitanjima za koje je posebnim propisima omogućeno to pravo.“

- Zadužuje se Ministarstvo civilnih poslova Bosne i Hercegovine da u suradnji s Uredom za zakonodavstvo Vijeća ministara Bosne i Hercegovine nomotehnički pripremi Prijedlog zakona i putem Generalnog tajništva Vijeća ministara Bosne i Hercegovine dostavi ga Parlamentarnoj skupštini Bosne i Hercegovine, uz prijedlog Ministarstva civilnih poslova Bosne i Hercegovine da se razmatra po skraćenom zakonodavnom postupku u skladu s poslovnim odredbama oba doma Parlamentarne skupštine Bosne i Hercegovine.

S poštovanjem,

**DOSTAVLJENO:**

- naslovu
- u spis broj: 05-02-1-685/24
- a/a





Ministry on Civil Affairs

Broj: 04-07-11-3774-4-EM/23  
Sarajevo, 17. 12. 2024. godine

BOSNA I HERCEGOVINA  
VIJEĆE MINISTARA  
GENERALNO TAJNIŠTVO

17-12-2024  
05 02-1 685-6/

24 ŽURNO!

**PREDMET:** Nacrt zakona o zaštiti osobnih podataka - *dostavlja se*  
**VEZA:** Naš akt broj: : 04-07-11-3774-4-EM/23 od 6.12.2024. godine

Poštovani,

U skladu sa Zaključkom Vijeća ministara sa 46. izvanredne sjednice od 17.12.2024. godine, dostavljamo Nacrt zakona o zaštiti osobnih podataka, korigiran u članku 8. tako što je dodan stavak (5).

S poštovanjem,



**Privitak:**

1. Nacrt zakona o zaštiti osobnih podataka sa obrazloženjem (u tiskanoj i elektroničkoj formi);
2. Mišljenje Ureda za zakonodavstva Vijeća ministara Bosne i Hercegovine broj: 04-02-1-220-5/24 od 13.11.2024.g.
3. Mišljenje Direkcije za europske integracije Bosne i Hercegovine broj: 03/A-07-6-AA-974-27/23 od 1.11.2024.g.;
4. Izjava o usklađenosti;
5. Mišljenje Ministarstva pravde Bosne i Hercegovine broj: 09-02-4-8798/24 od 12.11.2024.g.
6. Mišljenje Agencije za zaštitu osobnih podataka u Bosni i Hercegovini broj: 03-02-1-1061-2/24 od 24.10.2024.g.
7. Mišljenje Ministarstva za ljudska prava i izbjeglice Bosne i Hercegovine broj: 03-02-1-442-2/24 od 23.2.2024. g.
8. Ministarstva financija i trezora Bosne i Hercegovine broj: 05-02-2-1901-6/24 od 05.12.2024. g.
9. Obrazac broj 1.
10. CD .

**Dostavljeno:**

- naslovu;
- a/a.

2775.

Hama

BOSNA I HERCEGOVINA  
Ministarstvo civilnih poslova



БОСНА И ХЕРЦЕГОВИНА  
Министарство цивилних послова

Ministry on Civil Affairs

Broj: 04-07-11-3774-4-EM/23  
Sarajevo, 6. 12. 2024. godine



BOSNA I HERCEGOVINA  
VIJEĆE MINISTARA  
SARAJEVO

BOSNA I HERCEGOVINA  
VIJEĆE MINISTARA  
GENERALNO TAJNIŠTVO

PRIMLJENO: 09-12-2024			
Organizaciona jedinica	Klasifikaciona oznaka	Redni broj	Broj priloga
OS	02-1	685-4/	CD

ŽURNO!

**PREDMET:** Nacrt zakona o zaštiti osobnih podataka – **NOVI TEKST**, *dostavlja se*  
**VEZA:** Naš akt broj: 04-07-11-3774-4-EM/23 od 5.12.2024. godine

Poštovani,

Sukladno članku 30. Poslovnika o radu Vijeća ministara Bosne i Hercegovine („Službeni glasnik BiH“, broj 22/03), ovo ministarstvo dostavilo je aktom, broj i datum iz veze, Nacrt zakona o zaštiti osobnih podataka na razmatranje i usvajanje.

U dostavljenom Nacrtu zakona o zaštiti osobnih podataka izvršili smo korekcije u st. (7), (8), (9) i (11) u članku 113. te u privitku dostavljamo **NOVI TEKST** Nacrta zakona o zaštiti osobnih podataka.

S poštovanjem,



**Privitak:**

1. Nacrt zakona o zaštiti osobnih podataka sa obrazloženjem (u tiskanoj i elektroničkoj formi);
2. Mišljenje Ureda za zakonodavstva Vijeća ministara Bosne i Hercegovine broj: 04-02-1-220-5/24 od 13.11.2024.g.
3. Mišljenje Direkcije za europske integracije Bosne i Hercegovine broj: 03/A-07-6-AA-974-27/23 od 1.11.2024.g.;
4. Izjava o usklađenosti;
5. Mišljenje Ministarstva pravde Bosne i Hercegovine broj: 09-02-4-8798/24 od 12.11.2024.g.
6. Mišljenje Agencije za zaštitu osobnih podataka u Bosni i Hercegovini broj: 03-02-1-1061-2/24 od 24.10.2024.g.
7. Mišljenje Ministarstva financija i trezora Bosne i Hercegovine broj: 05-02-2-1901-6/24 od 5.12.2024.g.
8. Mišljenje Ministarstva za ljudska prava, izbjeglice i raseljena lica Bosne i Hercegovine broj: 03-02-1-442-2/24 od 23.2.2024.g.;
9. Obrazac broj 1;
10. CD.

**Dostavljeno:**

- naslovu;
- a/a.



Ministry on Civil Affairs

Broj: 04-07-11-3774-4-EM/23  
Sarajevo, 5. 12. 2024. godine

BOSNA I HERCEGOVINA  
VIJEĆE MINISTARA  
GENERALNO TAJNIŠTVO

05-12-2024

OS 02-1 685-3/  
124

ŽURNO!

**PREDMET:** Nacrt zakona o zaštiti osobnih podataka - *dostavlja se na razmatranje i usvajanje*

**VEZA:** Naš akt broj: 04-07-11-3774-11-EM/23 od 13.3.2024. godine

Naš akt broj: : 04-07-11-3774-3-EM/23 od 9.7.2024. godine

Poštovani,

Sukladno članku 30. Poslovnika o radu Vijeća ministara Bosne i Hercegovine („Službeni glasnik BiH“, broj 22/03), ovo ministarstvo dostavilo je aktom, broj i datum iz veze, Nacrt zakona o zaštiti osobnih podataka (u daljnjem tekstu: Zakon) na razmatranje i usvajanje.

S obzirom da su, u međuvremenu, obavljene dodatne konzultacije sa Uredom za zakonodavstvo Vijeća ministara Bosne i Hercegovine, Direkcijom za europske integracije Bosne i Hercegovine, Agencijom za zaštitu osobnih podataka u Bosni i Hercegovini i Ministarstvom pravde Bosne i Hercegovine o pojedinim terminima, rokovima i institutima koji su preuzeti iz europskih propisa u tekst Zakona, dostavljamo inovirani tekst Zakona u odnosu na prethodno dostavljeni teksta Zakona.

U nastavku teksta obrazložena su rješenja pojedinih prijedloga.

Prijedlog Direkcije za europske integracije Bosne i Hercegovine u svezi članka 97. stavka (6) Zakona, nije uvažen s obzirom da *UREDBA (EU) 2016/679* precizno ne definira način donošenja pravilnika o unutarnjem ustrojstvu nadzornog tijela. Postupak u kojem ravnatelj Agencije za zaštitu osobnih podataka u Bosni i Hercegovini podnosi pravilnik o unutarnjem ustrojstvu Agencije za zaštitu osobnih podataka u Bosni i Hercegovini Vijeću ministara Bosne i Hercegovine na odobrenje, ne utječe na neovisnost ove agencije.

Primjedbe Ureda za zakonodavstvo Vijeća ministara Bosne i Hercegovine su najvećim dijelom uvažene i uvrštene u tekst Zakona osim primjedbi koje su se odnosile na drugačije definiranje materijalne sadržine pojedinih odredbi Zakona, koje su preuzete iz *UREDBE (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)*, (u daljnjem tekstu: *Uredba*) i *DIREKTIVE (EU) 2016/680 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP*), (u

daljem tekstu: Direktive) jer one nisu mogle biti modificirane zbog toga što je intencija normi u Uredbi i Direktivi nalagala takvo njihovo definiranje.

Slijedeće primjedbe nisu uvažene:

1. Prema dostavljenom mišljenju Ureda za zakonodavstvo Bosne i Hercegovine navedeno je: „uočeno je da se u velikoj mjeri u predmetnom Zakonu koriste neprecizne odrednice“ kao što su: „duži period“, „ključni interesi“, „u najvećoj mogućoj mjeri“, „na odgovarajući način“, „nepotrebno odlaganje“, „najmanje pravo“, „ako je primjenjivo“, „u dovoljnoj mjeri“, „u velikom broju“, „opsežna obrada“, „pretjeran zahtjev“, „ozbiljno ugrožavanje“, „po potrebi“, „povremena obrada“, „u velikom broju“, „odmah“, „periodično preispitivanje“, „lako dostupan“.

Zakon se usklađuje sa Uredbom i Direktivom u kojima se koristi navedena terminologija s ciljem omogućavanja kontrolorima da u svakom pojedinačnom slučaju primjene odgovarajuće mjere s obzirom na predmet reguliranja svake pojedine norme. Zamjenom navedene terminologije drugim izrazima izmijenio bi se karakter norme i njen cilj. U vezi s navedenim napominjemo da se Zakon odnosi na sve kontrolore u javnom i privatnim sektoru. Aktivnosti obrade osobnih podataka kontrolora iz privatnog i javnog sektora se razlikuju, kao i unutar navedenih sektora. Nije isto primijeniti normu od samostalnog poduzetnika i javnog organa. Nadalje, termini kao što su: „u najvećoj mogućoj mjeri“, „ako je primjenjivo“, „po potrebi“ i slično, ukoliko bi se zamijenili preciznim izrazima, norma bi izgubila svoje značenje i dobila imperativni karakter. Na taj način kontrolori i nosioci osobnog podatka (zavisno o kojoj normi se radi) u Bosni i Hercegovini imali bi drugi režim obaveza u postupanju s osobnim podacima i ne bi bili u mogućnosti realizirati konkretnu normu. Dakle, usklađivanje domaćeg zakonodavstva sa europskim zakonodavstvom, što je bio cilj donošenja ovog Zakona, u skladu sa zaključkom Vijeća Ministara Bosne i Hercegovine sa 30. sjednice održane dana 27.11.2023. godine, ne bi bilo postignut ukoliko bi se prihvatila sugestija o preciziranju navedenih termina i čime bi svi akteri u Bosni i Hercegovini dovedeni u nepovoljan položaj u odnosu na europske zemlje.

Ovo ministarstvo je održalo nekoliko radnih sastanaka sa Uredom za zakonodavstvo Vijeća ministara Bosne i Hercegovine, Direkcijom za europske integracije Bosne i Hercegovine, Agencijom za zaštitu osobnih podataka u Bosni i Hercegovini i Ministarstvom pravde Bosne i Hercegovine u cilju usklađivanja terminologije sa domaćim zakonodavstvom nakon čega je ovo Ministarstvo pokušalo uvažiti pojedine primjedbe. Međutim, Direkcija za europske integracije Bosne i Hercegovine je u svom mišljenju prepoznala takve norme kao neusklađene, npr. odredbama članka 7. stavak (2) Uredbe propisano je da je kontrolor podatka odgovoran za usklađenost te „mora biti u mogućnosti dokazati“ postupanje u skladu sa načelima iz stavka (1) istog članka, dok je odredbama članka 7. stavka (2) Zakona propisano da „mora dokazati“. Drugi primjer je odredba članka 6. stavak (1) točka d) Uredbe u kojoj je propisano da je obrada zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedan od taksativno navedenih uvjeta, među kojima je i da je, stoji u navedenoj odredbi: „obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe“. Konzultiranjem i uvidom sadržaja odredbe na još tri službena jezika EU (engleskom, francuskom i talijanskom jeziku) utvrđeno je da to i jeste korištena odrednica, te se sugerira korekcija odredbe članka 8. stavka (1) točka d) koja glasi: „obrada je neophodna radi zaštite ključnih interesa nosioca podataka ili druge fizičke osobe“. Naprijed navedeno obrazloženje odnosi se i na primjedbu da se rokovi propisani u Zakonu, usklađeni sa Uredbom i Direktivom, propišu na drugi način. Nadalje, Zakon o upravnom postupku ostavlja mogućnost da s posebnim zakonom propišu drugačiji rokovi, što je ovim zakonom i propisano kod pojedinih instituta.

Također, Agencija za zaštitu osobnih podataka u Bosni i Hercegovini je u svom mišljenju naglasila da je potrebno slijediti terminologiju koja se koristi u Uredbi i Direktivi kako bi ona mogla slijediti praksu zemalja članica EU koje iste norme primjenjuju šest godina.

2. Primjedba koja se odnosi na upotrebu termina „pritužba“ i njegova zamjena terminom „prigovor“ nije mogla biti prihvaćena jer se radi o dva različita instituta. Pritužba se podnosi Agenciji za zaštitu osobnih podataka kao nezavisnom nadzornom tijelu, a prigovor se podnosi kontroloru. Uredba i Direktiva propisuju dva instituta: „prigovor“ kontroloru i „pritužbu“ Agenciji za zaštitu osobnih podataka, i upravo ovi različiti instituti moraju imati različitu terminologiju.
3. Primjedba Ureda za zakonodavstvo BiH koja se odnosi na preciziranje smjera za VSS u odredbama koje propisuju uvjete za direktora i zamjenika nije mogla biti prihvaćena zbog toga što postojećim uvjetom omogućava širi krug osoba koje se mogu imenovati na tu funkciju.
4. Primjedba Ureda za zakonodavstvo BiH koja se odnosi na uvjete koji propisuju potrebno iskustvo za imenovanje direktora i zamjenika direktora nije mogla biti uvažena jer se zakonom mogu propisati drugačiji uvjeti u odnosu na podzakonski akt.

Bosna i Hercegovina ratificirala je Konvenciju Vijeća Europe za zaštitu osoba s obzirom na automatsku obradu osobnih podataka (ETS br. 108), koja je od ključnog značaja za osiguranje prava na privatnost, a time i zaštitu osobnog podataka svake fizičke osobe, kao i Protokol kojim se mijenja i dopunjuje ETS br. 108 i koja propisuje nova pravila koja korespondiraju sa novim europskim zakonodavstvom u oblasti osobnih podataka.

Potpisivanjem Sporazuma o stabilizaciji i pridruživanju između Europskih zajednica i njihovih država članica i Bosne i Hercegovine preuzeta je obaveza usklađivanja zakonodavstva, koje se odnosi na zaštitu osobnih podataka, s pravom Zajednice (Europska zajednica i Europska zajednica za atomsku energiju) i drugim europskim i međunarodnim zakonodavstvom o privatnosti. Ovim Sporazumom Bosna i Hercegovine se obavezala da će uspostaviti nezavisni nadzorni organ sa dovoljno finansijskih i ljudskih potencijala, s ciljem provođenja nacionalnog zakonodavstva o zaštiti osobnih podataka (Članak 79.)

Vijeće ministara BiH je na 30. sjednici, održanoj 27.11.2023. godine, a nakon upoznavanja sa Informacijom o hitnosti i neophodnosti usklađivanja zakona u Bosni i Hercegovini s europskim standardima o zaštiti osobnih podataka, donijelo Odluku o formiranju interresorne radne grupe za izradu Nacrta zakona za zaštitu osobnih podataka sa zadatkom da pripremi nacrt zakona o zaštiti osobnih podataka kojim će zaštita osobnih podataka u Bosni i Hercegovini biti uređena u skladu sa usvojenim propisima Europske unije.

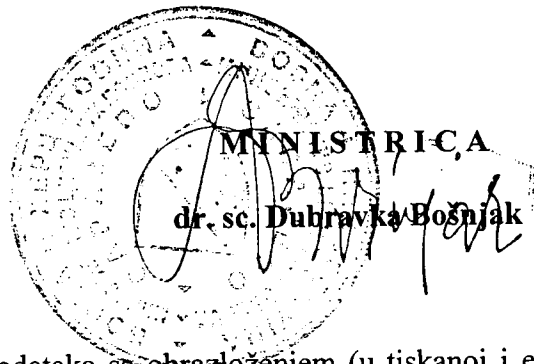
Također, Bosna i Hercegovina je dana 29.10.2024. godine potpisala Sporazum o suradnji sa EUROJUST-om (Agencijom Europske unije za pravosudnu suradnju u kaznenim stvarima), te je u Izvještaju Europske komisije o Bosni i Hercegovini za 2024. godinu, koji je objavljen 30.10.2024. godine, naznačeno da je preduvjet za stupanje na snagu Sporazuma o suradnji sa EUROJUST-om usvajanje novog zakona o zaštiti osobnih podataka.

Budući da je razlog za donošenje ovog zakona usuglašavanje sa pravnom stečevinom Europske unije i priznatim međunarodnim standardima u području zaštite osobnih podataka, predmetni zakon nosi oznaku „EI“.

Posebno naglašavamo da je Bosna i Hercegovina, nakon što je dobila preporuku Europske komisije za kandidatski status, obvezna ispuniti postavljene zahtjeve, među kojima je i usvajanje Zakona o zaštiti osobnih podataka. Predložena rješenja u Nacrtu zakona o zaštiti osobnih podataka predstavljaju pomak u odnosu na dosadašnji zakon u pogledu ostvarivanja prava fizičkih osoba - vlasnika osobnih podataka, izvršavanje obveza i odgovornosti kontrolora i obrađivača, zaštita osobnih podataka od strane nadležnih tijela u svrhe sprječavanja, istrage, otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela, izvršenja kaznenih sankcija uključujući i zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje, pravila za prijenos osobnih podataka u druge zemlje ili međunarodne organizacije, pravila za uspostavljanje neovisnog nadzornog tijela, pravila za provođenje pravnih sredstava, utvrđivanje odgovornosti i izricanje sankcija.

Slijedom navedenog, predlažemo da Vijeće ministara Bosne i Hercegovine usvoji Prijedlog zakona o zaštiti osobnih podataka i isti označi oznakom „P.Z.E.I.“, kako bio isti bio **razmatran u skraćenom zakonodavnom postupku**, sukladno odredbama članka 134. stavak (1) Poslovnika Zastupničkog doma Parlamentarne skupštine Bosne i Hercegovine („Službeni glasnik BiH“, br. 79/14, 81/15, 97/15, 78/19, 26/20, 53/22, 59/23, 87/23, 50/24 i 73/24) i članka 125. stavak (1) Poslovnika Doma naroda Parlamentarne skupštine Bosne i Hercegovine („Službeni glasnik BiH“, br. 58/14, 88/15, 96/15, 53/16 i 71/24).

S poštovanjem,



**Privitak:**

1. Nacrt zakona o zaštiti osobnih podataka sa obrazloženjem (u tiskanoj i elektroničkoj formi);
2. Mišljenje Ureda za zakonodavstva Vijeća ministara Bosne i Hercegovine broj: 04-02-1-220-5/24 od 13.11.2024.g.
3. Mišljenje Direkcije za europske integracije Bosne i Hercegovine broj: 03/A-07-6-AA-974-27/23 od 1.11.2024.g.;
4. Izjava o usklađenosti;
5. Mišljenje Ministarstva pravde Bosne i Hercegovine broj: 09-02-4-8798/24 od 12.11.2024.g.
6. Mišljenje Agencije za zaštitu osobnih podataka u Bosni i Hercegovini broj: 03-02-1-1061-2/24 od 24.10.2024.g.
7. CD .

**Dostavljeno:**

- naslovu;
- a/a.

## NACRT

„EI“

Na osnovu člana IV. 4. a) Ustava Bosne i Hercegovine, Parlamentarna skupština Bosne i Hercegovine, na \_\_. sjednici Predstavničkog doma, održanoj \_\_\_\_\_. godine, i na \_\_. sjednici Doma naroda, održanoj \_\_\_\_\_. 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 funkcionisanje;
- c) zaštita fizičkih lica u vezi s obradom ličnih podataka od strane nadležnih organa u svrhe sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinitelaca 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. godine 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 počinitelaca 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 informisanja o preuzimanju pravne stečevine 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 u samo 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 podataka, automatiziranim ili neautomatiziranim sredstvima, kao što su prikupljanje, evidentiranje, organizacija, strukturiranje, čuvanje, prilagođavanje ili izmjena, pronalaženje, obavljanje uvida, upotreba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombinovanje, ograničenje, brisanje ili uništavanje;
- d) „ograničenje obrade“ je obilježavanje čuvanog ličnog podatka s ciljem ograničenja njegove obrade u budućnosti;
- e) „izrada profila“ je svaki oblik automatske obrade ličnog podatka koji se sastoji od korištenja ličnog podatka za procjenu određenih ličnih aspekata u vezi s fizičkim licem, posebno za analizu ili predviđanje aspekata u vezi s radnim rezultatom, ekonomskim stanjem, zdravljem, ličnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog fizičkog lica;
- f) „pseudonimizacija“ je obrada ličnog podatka tako da se lični podatak više ne može pripisati određenom nosiocu podataka bez korištenja dodatnih informacija, uz uvjet da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacionim mjerama kako bi se osiguralo da se lični podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi;

- g) „zbirka ličnih podataka“ je svaki strukturirani skup ličnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to jesu li centralizovani, decentralizovani ili rasprostranjeni na funkcionalnoj ili geografskoj osnovi;
- h) „kontrolor podataka“ je fizičko ili pravno lice, javni organ ili nadležni organ koji samostalno ili s drugim određuje svrhe i sredstva obrade ličnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriteriji za njegovo imenovanje propisuju se zakonom;
- i) „javni organ“ je svaki zakonodavni, izvršni i sudski organ na svim nivoima vlasti u Bosni i Hercegovini.
- j) „nadležni organ“ je organ koji je nadležan za sprečavanje, istragu i otkrivanje krivičnih djela, gonjenje učinilaca krivičnih djela ili izvršenje krivičnih sankcija, uključujući i zaštitu i sprečavanje prijetnji javnoj sigurnosti, kao i pravna lica ako su zakonom ovlaštena za obavljanje tih poslova, kao posebna kategorija kontrolora podataka;
- k) „obrađivač“ je fizičko ili pravno lice, javni organ koji obrađuje lične podatke u ime kontrolora podataka;
- l) „primalac“ je fizičko ili pravno lice, javni organ kome se otkrivaju lični podaci, nezavisno od toga da li je u pitanju treća strana. Javni organi koji mogu primiti lične podatke u okviru određene istrage u skladu sa zakonom ne smatraju se primaocima, ali obrada tih podataka mora biti u skladu s važećim pravilima o zaštiti podataka prema svrhama obrade;
- m) „treća strana“ znači fizičko ili pravno lice, javni organ, Agencija ili drugo tijelo koji nije nosilac podataka, kontrolor podataka, obrađivač ni lica koja su ovlaštena za obradu ličnih podataka pod neposrednom nadležnošću kontrolora podataka ili obrađivača;
- n) „saglasnost“ nosioca podataka je svako dobrovoljno, posebno, informisano i nedvosmisleno izražavanje volje nosioca podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu ličnih podataka koji se na njega odnose;
- o) „povreda ličnog podatka“ je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa ličnim podacima koji su preneseni, čuvani ili na drugi način obrađivani;
- p) „genetski podatak“ je lični podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičkog lica koja daju jedinstvene informacije o fiziologiji ili zdravlju tog fizičkog lica i koji su dobijeni posebnom analizom biološkog uzorka tog fizičkog lica;
- r) „biometrijski podatak“ je lični podatak dobijen posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičkog lica koja omogućavaju ili potvrđuju jedinstvenu identifikaciju tog fizičkog lica, kao što su fotografije lica ili daktiloskopski podaci;
- s) „podatak koji se odnosi na zdravlje“ je lični podatak u vezi s fizičkim ili mentalnim zdravljem fizičkog lica, uključujući pružanje zdravstvenih usluga, koji daje informacije o njegovom zdravstvenom stanju;
- t) „predstavnik“ je fizičko ili pravno lice s prebivalištem ili boravištem, odnosno sjedištem ili poslovnim nastanom u Bosni i Hercegovini koje je kontrolor podataka ili obrađivač pisanim putem imenovao u skladu s članom 29. ovog zakona;
- u) „privredni subjekat“ je fizičko ili pravno lice koje obavlja privrednu djelatnost, bez obzira na pravni oblik te djelatnosti;

- v) „grupa privrednih subjekata“ je privredni subjekt koji ostvaruje kontrolu i privredni subjekti koji su pod njegovom kontrolom;
- z) „obavezujuće poslovno pravilo“ su politike zaštite ličnih podataka kojih se kontrolor podataka i obrađivač sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini pridržava prilikom prijenosa ili skupova prijenosa ličnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih država u okviru grupe privrednih subjekata ili grupe privrednih subjekata koji se bave zajedničkom privrednom djelatnošću;
- aa) „usluga informacionog društva“ jeste svaka usluga koja se obično pruža uz naknadu, na daljinu, elektronskim sredstvima te na lični zahtjev primaoca usluga, gdje:
  - 1) „na daljinu” znači da se usluga pruža a da pri tome strane nisu istovremeno prisutne;
  - 2) „elektronskim sredstvima” znači da se usluga na početku šalje i prima na određitu pomoću elektronske opreme za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radiovezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima;
  - 3) „na lični zahtjev primaoca usluga” znači da se usluga pruža prijenosom podataka na lični zahtjev“;
- bb) „međunarodna organizacija“ je organizacija sa svojim organima uređena međunarodnim javnim pravom ili bilo koji drugi organ koji su sporazumom ili na osnovu sporazuma osnovale dvije zemlje ili više zemalja;
- cc) „poslovni nastan“ je djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana;
- dd) „videonadzor“ je informacijsko-komunikacijski sistem koji ima mogućnost prikupljanja i daljnje obrade ličnih podataka, koji obuhvata stvaranje snimka koji čini ili je namijenjen da čini dio sistema skadištenja.

## **Član 5.**

### **(Glavna oblast primjene)**

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

## **Član 6.**

### **(Teritorijalno područje primjene)**

- (1) Ovaj zakon primjenjuje se na obradu ličnog podatka koju obavlja kontrolor podataka ili obrađivač koji ima sjedište ili poslovni nastan, prebivalište ili boravište u Bosni i Hercegovini, nezavisno od toga obavlja li se obrada u Bosni i Hercegovini ili ne.

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

## **DIO DRUGI – OBRADA LIČNOG PODATKA OD STRANE FIZIČKOG LICA, PRAVNOG LICA ILI JAVNOG ORGANA KAO KONTROLORA PODATAKA**

### **POGLAVLJE I. NAČELA OBRADJE LIČNOG PODATKA**

#### **Član 7.**

##### **(Načela obrade ličnog podatka)**

(1) Načela obrade ličnog podatka su:

- a) zakonitost, pravičnost i transparentnost u odnosu na nosioca podataka;
- b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu s članom 56. stavom (1) ovog zakona ne smatra se neusklađenom s prvobitnim svrhama;
- c) smanjenje opsega podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhe za koje se obrađuju;
- d) tačnost – podaci moraju biti tačni i prema potrebi ažurirani. Moraju se preduzeti sve razumne mjere kako bi se osiguralo da lični podaci, koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni;
- e) ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nosioca podataka i to ne duže nego što je potrebno u svrhe u koje se lični podaci obrađuju.

Lični podaci se mogu čuvati na duži period ako će se lični podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu s članom 56. stavom (1) ovog zakona, što podliježe provođenju primjerenih tehničkih i organizacionih mjera propisanih ovim zakonom radi zaštite prava i sloboda nosioca podataka;

- f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigurava odgovarajuća sigurnost ličnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera.
- (2) Načelo pouzdanosti – kontrolor podataka odgovoran je za usklađenost obrade ličnog podatka sa stavom (1) ovog člana i mora biti u mogućnosti dokazati tu usklađenost.

## **Član 8.**

### **(Zakornost obrade ličnog podatka)**

- (1) Obrada ličnog podatka je zakonita samo ako je ispunjen najmanje jedan od sljedećih uvjeta:
- a) ako je nosilac podataka dao saglasnost za obradu svojih ličnih podataka u jednu ili više posebnih svrha;
  - b) ako je obrada neophodna radi izvršenja ugovora u kojem je nosilac podataka ugovorna strana ili radi preduzimanja radnji na zahtjev nosioca podataka prije zaključenja ugovora;
  - c) ako je obrada neophodna radi poštovanja pravnih obaveza kontrolora podataka;
  - d) obrada je neophodna radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica;
  - e) ako je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka;
  - f) ako je obrada neophodna zbog legitimnih interesa kontrolora podataka ili treće strane, osim kada nad tim interesima pretežu interesi ili osnovna prava i slobode nosioca podataka, a koji zahtijevaju zaštitu ličnih podataka, posebno ako je nosilac podataka dijete. Ova tačka se ne primjenjuje na obradu koju vrše javni organi pri obavljanju svojih poslova.
- (2) Pravni osnov za obradu ličnog podatka iz stava (1) tač. c) i e) ovog člana utvrđuje se posebnim zakonom, tako da se preciznije propišu posebni uvjeti za obradu te druge mjere za osiguranje zakonite i pravične obrade, između ostalog i za druge posebne obrade kako je to predviđeno u poglavlju V ovog zakona.
- (3) Posebnim zakonom, za obradu podatka iz stava (1) tač. c) i e) ovog člana, propisuje se svrha obrade, koja u vezi s obradom iz stava (1) tačke e) ovog člana mora biti neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja kontrolora podataka. Tim zakonom propisuju se: opći uvjeti kojima se uređuje zakonitost obrade koju obavlja kontrolor podataka, vrste podataka koji se obrađuju, kategorije nosilaca podataka, subjekti kojima se lični podaci mogu otkriti i svrhe u koje se podaci mogu otkriti, ograničenje svrhe, rokovi čuvanja te radnje obrade i postupci obrade, uključujući i mjere za osiguranje zakonite i pravične obrade, kao i za druge posebne obrade kako je navedeno u poglavlju V ovog zakona. Tim zakonom mora se ostvariti cilj od javnog interesa i obrada mora biti proporcionalna zakonitom cilju kojem se teži.
- (4) Ako se obrada vrši u svrhu koja je različita od svrhe u koju su lični podaci prikupljeni i ne zasniva se na saglasnosti nosilaca podataka ili posebnom zakonu koji predstavlja neophodnu i proporcionalnu mjeru u demokratskom društvu za zaštitu ciljeva iz člana 25. stava (1) ovog zakona, kontrolor podataka, s ciljem utvrđivanja da li je obrada u drugu

svrhu u skladu sa svrhom u koju su lični podaci prvobitno prikupljeni, uzima u obzir, između ostalog:

- a) svaku vezu između svrha u koje su lični podaci prikupljeni i svrha namjeravane daljnje obrade;
  - b) kontekst u kojem su lični podaci prikupljeni, posebno u vezi s odnosom između nosioca podataka i kontrolora podataka;
  - c) prirodu ličnih podataka, posebno činjenicu da li se obrađuju posebne kategorije ličnih podataka u skladu s članom 11. ovog zakona ili lični podaci koji se odnose na krivičnu osuđivanost i krivična djela u skladu s članom 12. ovog zakona;
  - d) moguće posljedice namjeravane daljnje obrade za nosioce podataka;
  - e) postojanje odgovarajućih mjera zaštite, koje mogu uključivati enkripciju ili pseudonimizaciju.
- (5) Javni i nadležni organi entiteta i Brčko Distrikta su dužni, uz poštovanje odredbi ovog zakona, ustupiti lične podatke iz svojih evidencija ovlaštenom kontroloru podataka, u svrhu prethodnog izjašnjavanja građana koji imaju biračko pravo o pitanjima za koje je posebnim propisima omogućeno to pravo.

#### **Član 9.**

##### **(Saglasnost)**

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

#### **Član 10.**

##### **(Uvjeti koji se primjenjuju na saglasnost djeteta u vezi s uslugom informacionog društva)**

- (1) Kada se primjenjuje član 8. stav (1) tačka a) ovog zakona u vezi s neposrednim nudenjem usluge informacionog društva djetetu, obrada ličnog podatka djeteta zakonita je ako dijete

ima najmanje 16 godina. Ako je dijete mlađe od 16 godina, takva obrada je zakonita samo ako i u mjeri u kojoj je saglasnost dao ili odobrio roditelj, usvojlac, staratelj djeteta ili drugi zastupnik djeteta.

- (2) Kontrolor podataka mora da uloži razumne napore prilikom provjere da li je saglasnost u tim slučajevima dao ili odobrio roditelj, usvojlac, odnosno staratelj djeteta, uzimajući u obzir dostupnu tehnologiju.
- (3) Stav (1) ovog člana ne utiče na opća pravila obligacionog prava koja se tiču važenja, zaključenja ili učinka ugovora u vezi s djetetom.

## **Član 11.**

### **(Obrada posebnih kategorija ličnih podataka)**

- (1) Obrada ličnih podataka koji otkrivaju rasno ili etničko porijeklo, politička mišljenja, vjerska ili filozofska uvjerenja ili pripadnost sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije lica, podataka o zdravlju ili podataka o spolnom životu ili seksualnoj orijentaciji lica je zabranjena.
- (2) Izuzetno od odredbe stava (1) ovog člana, obrada posebne kategorije ličnih podataka dopuštena je ako je ispunjen jedan od sljedećih uvjeta:
  - a) ako je nosilac podataka dao izričitu saglasnost za obradu tih ličnih podataka za jednu ili više konkretnih svrha, osim kada je posebnim zakonom propisano da se obrada tih podataka ne može obavljati na osnovu saglasnosti;
  - b) ako je obrada neophodna radi izvršavanja obaveza i ostvarivanja posebnih prava kontrolora podataka ili nosioca podataka u oblasti radnog prava i prava socijalnog osiguranja i socijalne zaštite, u mjeri u kojoj je to propisano zakonom ili kolektivnim ugovorom u skladu s posebnim zakonom koji propisuje odgovarajuće mjere zaštite osnovnih prava i interesa nosioca podataka;
  - c) ako je obrada neophodna radi zaštite ključnih interesa nosioca podataka ili drugog fizičkog lica ako nosilac podataka fizički ili pravno ne može dati saglasnost;
  - d) ako se obrada obavlja u okviru legitimnih aktivnosti, uz odgovarajuće zaštitne mjere, fondacije, udruženja ili bilo koje druge neprofitne organizacije s političkim, filozofskim, vjerskim ili sindikalnim ciljem i to uz uvjet da se obrada odnosi isključivo na članove ili bivše članove te organizacije ili na fizička lica koja imaju redovan kontakt s njom, a u vezi s njenim svrhama i da se lični podaci ne otkrivaju van te organizacije bez saglasnosti nosioca podataka;
  - e) ako se obrada odnosi na lične podatke za koje je očito da ih je objavio nosilac podataka;
  - f) ako je obrada neophodna za uspostavljanje, ostvarivanje ili odbranu pravnih zahtjeva ili kad sudovi postupaju u sudskom svojstvu;
  - g) ako je obrada neophodna za potrebe značajnog javnog interesa, na osnovu zakona koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu ličnih podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka;
  - h) ako je obrada neophodna za potrebe preventivne medicine ili medicine rada zbog procjene radne sposobnosti zaposlenih, medicinske dijagnoze, pružanja zdravstvene ili

socijalne zaštite ili tretmana ili upravljanja sistemima i uslugama zdravstvene ili socijalne zaštite na osnovu posebnog zakona ili u skladu s ugovorom sa zdravstvenim radnikom i uz uvjete i mjere zaštite iz stava (3) ovog člana;

- i) ako je obrada neophodna iz razloga javnog interesa u oblasti javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih prijetnji za zdravlje ili osiguranje visokih standarda kvaliteta i sigurnosti zdravstvene zaštite i lijekova i medicinskih sredstava, na osnovu posebnog zakona kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda nosioca podataka, a posebno čuvanje profesionalne tajne;
  - j) ako je obrada neophodna za potrebe arhiviranja u javnom interesu, potrebe naučnog ili historijskog istraživanja ili statističke potrebe u skladu s članom 56. stavom (1) ovog zakona, a na osnovu posebnog zakona, koji je proporcionalan legitimnom cilju i kojim se poštuje suština prava na zaštitu podataka i osiguravaju primjerene i posebne mjere za zaštitu osnovnih prava i interesa nosioca podataka.
- (3) Lični podaci iz stava (1) ovog člana mogu se obrađivati u svrhe navedene u stavu (2) tački h) ovog člana kada te podatke obrađuje stručno lice ili se podaci obrađuju pod odgovornošću stručnog lica na koje se primjenjuje obaveza čuvanja profesionalne tajne u skladu s posebnim zakonom ili pravilima koja su utvrdili nadležni javni organi ili druga lica na koje se primjenjuje obaveza čuvanja tajne u skladu s posebnim zakonom ili pravilima koja su utvrdili nadležni javni organi.
- (4) Posebnim zakonima mogu se zadržati ili uvesti dodatni uvjeti, uključujući i ograničenja u odnosu na obradu genetskih podataka, biometrijskih podataka ili podataka o zdravlju.

## **Član 12.**

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

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

## **Član 13.**

### **(Obrada za koju nije potrebna identifikacija)**

- (1) Ako kontrolor podataka obrađuje lične podatke za čiju svrhu obrade ne zahtijeva ili više ne zahtijeva identificiranje nosioca podataka, kontrolor podataka nije dužan čuvati, pribavljati ili obrađivati dodatne informacije radi identifikacije nosioca podataka samo za potrebe poštovanja ovog zakona.
- (2) Ako u slučajevima iz stava (1) ovog člana kontrolor podataka može dokazati da ne može identificirati nosioca podataka, kontrolor podataka o tome, na odgovarajući način, obavještava nosioca podataka, ako je moguće. U tim slučajevima se ne primjenjuju čl. 17. do 22. ovog zakona, osim u slučaju da nosilac podataka u svrhu ostvarivanja svojih prava iz tih članova pruži dodatne informacije koje omogućavaju njegovu identifikaciju.

## POGLAVLJE II. PRAVA NOSIOCA PODATAKA

### Član 14.

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

- (1) Kontrolor podataka preuzima odgovarajuće mjere kako bi se nosiocu podataka pružile sve informacije iz čl. 15. i 16. ovog zakona i svi vidovi komunikacije za ostvarivanje prava iz čl. 17. do 24. ovog zakona i člana 36. ovog zakona u vezi s obradom podataka, i to u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika, što se posebno odnosi na sve informacije koje su izričito namijenjene djetetu. Informacije se pružaju u pisanom obliku ili na druge načine, uključujući i elektronski oblik kada je primjereno. Ako nosilac podataka zahtijeva, informacije se mogu pružiti usmeno, uz uvjet da je identitet nosioca podataka utvrđen drugim sredstvima.
- (2) Kontrolor podataka olakšava ostvarivanje prava nosioca podataka iz čl. 17. do 24. ovog zakona. U slučajevima iz člana 13. stava (1) ovog zakona kontrolor podataka ne smije odbiti da postupi po zahtjevu nosioca podataka za ostvarivanje njegovih prava iz čl. 17. do 24. ovog zakona, osim ako kontrolor podataka dokaže da ne može utvrditi identitet nosioca podataka.
- (3) Kontrolor podataka nosiocu podataka na njegov zahtjev pruža informacije o preduzetim radnjama iz čl. 17. do 24. ovog zakona bez nepotrebnog odgađanja i u svakom slučaju u roku od 30 dana od dana zaprimanja zahtjeva. Taj se rok može, prema potrebi, produžiti za 60 dana, uzimajući u obzir složenost i broj zaprimljenih zahtjeva. Kontrolor podataka obavještava nosioca podataka o svakom takvom produženju u roku od 30 dana od dana zaprimanja zahtjeva, pri čemu navodi razloge za odgađanje. Ako nosilac podataka podnese zahtjev elektronskim putem, informacije se pružaju elektronskim putem ako je to moguće, osim u slučaju kada nosilac podataka zahtijeva drugačije.
- (4) Ako kontrolor podataka ne postupi po zahtjevu nosioca podataka, dužan je bez odgađanja, a najkasnije 30 dana od dana zaprimanja zahtjeva, obavijestiti nosioca podataka o razlozima zbog kojih nije postupio po zahtjevu i o mogućnosti podnošenja pritužbe Agenciji ili tužbe nadležnom sudu i drugim pravnim sredstvima.
- (5) Informacije pružene u skladu s čl. 15. i 16. ovog zakona i sva komunikacija i djelovanja iz čl. 17. do 24. ovog zakona i člana 36. ovog zakona pružaju se bez naknade. Ako su zahtjevi nosioca podataka očito neosnovani ili pretjerani, posebno zbog učestalog ponavljanja, kontrolor podataka može:
  - a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnožavanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili postupanja po zahtjevu, ili
  - b) odbiti postupiti po zahtjevu.
- (6) Teret dokazivanja očite neosnovanosti ili pretjeranosti zahtjeva je na kontroloru podataka.
- (7) Ako kontrolor podataka ima opravdane sumnje u vezi s identitetom fizičkog lica koje podnosi zahtjev iz čl. 17. do 23. ovog zakona, on može, ne dovodeći u pitanje član 13. ovog

zakona, zatražiti dodatne informacije neophodne za potvrđivanje identiteta nosioca podataka.

- (8) Informacije koje moraju biti pružene nosiocima podataka, u skladu s čl. 15. i 16. ovog zakona, mogu se pružiti u kombinaciji sa standardiziranim simbolima, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio logičan pregled namjeravane obrade. Ako su simboli prikazani elektronski, moraju biti mašinski čitljivi.
- (9) Agencija je ovlaštena da donese propise u svrhu određivanja informacija koje se prikazuju simbolima i postupke za utvrđivanje standardiziranih simbola.

## **Član 15.**

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

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

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

## **Član 16.**

### **(Informacije koje se pružaju ako lični podatak nije dobijen od nosioca podataka)**

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

- g) o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz člana 24. st. (1) i (4) ovog zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nosioca podataka.
- (3) Kontrolor podataka pruža informacije iz st. (1) i (2) ovog člana:
- a) u razumnom roku nakon dobijanja ličnih podataka, a najkasnije u roku od 30 dana i uzimajući u obzir posebne okolnosti obrade ličnog podatka;
  - b) ako se lični podatak koristi za komunikaciju s nosiocem podataka, najkasnije prilikom prve komunikacije ili
  - c) ako je predviđeno otkrivanje podataka drugom primaocu, najkasnije u trenutku kada je lični podatak prvi put otkriven.
- (4) Ako kontrolor podataka namjerava dodatno obrađivati lični podatak u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade pruža nosiocu podataka informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stava (2) ovog člana.
- (5) St. (1) do (4) ovog člana ne primjenjuju se ako i u mjeri u kojoj:
- a) nosilac podataka već posjeduje informacije;
  - b) pružanje takvih informacija je nemoguće ili bi zahtijevalo neproporcionalne napore, posebno za obrade u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe, u skladu s uvjetima i mjerama zaštite iz člana 56. stava (1) ovog zakona ili u mjeri u kojoj je vjerovatno da se obavezom iz stava (1) ovog člana može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade. U takvim slučajevima, kontrolor podataka preduzima odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nosioca podataka, između ostalog i stavljanjem informacija na raspolaganje javnosti;
  - c) dobijanje ili otkrivanje podataka je izričito propisano posebnim zakonom koji se primjenjuje na nosioca podataka, a koji predviđa odgovarajuće mjere za zaštitu legitimnih interesa nosioca podataka ili
  - d) lični podatak mora ostati povjerljiv u skladu s obavezom čuvanja profesionalne tajne koju propisuje posebni zakon, uključujući i druge zakonske obaveze čuvanja tajne.

## **Član 17.**

### **(Pravo nosioca podataka na pristup ličnom podatku)**

- (1) Nosilac podataka ima pravo da dobije potvrdu od kontrolora podataka o tome obrađuju li se njegovi lični podaci i, ako se obrađuju, pristup ličnim podacima i sljedećim informacijama:
- a) svrsi obrade;
  - b) kategoriji ličnog podatka koji se obrađuje;
  - c) primaocu ili kategorijama primalaca kojima je lični podatak otkriven ili će im biti otkriven, a posebno primaocu u drugoj državi ili međunarodnoj organizaciji;

- d) predviđenom roku u kojem se lični podaci čuvaju, ili ako to nije moguće, kriterijima korištenim za određivanje tog roka;
  - e) pravo da se od kontrolora podataka zatraži ispravka ili brisanje ličnog podatka ili ograničavanje obrade ličnog podatka koji se odnosi na nosioca podataka ili pravo na prigovor na takvu obradu;
  - f) pravo na podnošenje pritužbe Agenciji ili tužbe nadležnom sudu;
  - g) ako se lični podatak ne prikuplja od nosioca podataka, svakoj dostupnoj informaciji o njegovom izvoru;
  - h) postojanju automatiziranog donošenja odluka, uključujući i profiliranje iz člana 24. st. (1) i (4) ovog zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nosioca podataka.
- (2) Ako se lični podatak prenosi u drugu državu ili međunarodnu organizaciju, nosilac podataka ima pravo da bude informisan o odgovarajućim mjerama zaštite u skladu s članom 48. ovog zakona koje se odnose na prijenos podataka.
- (3) Kontrolor podataka osigurava kopiju ličnog podatka koji se obrađuje. Za sve dodatne kopije koje zatraži nosilac podataka, kontrolor podataka može naplatiti opravdanu naknadu na osnovu administrativnih troškova. Ako nosilac podataka podnese zahtjev elektronskim putem, osim ako nosilac podataka ne zahtijeva drugačije, informacije se pružaju u uobičajenom elektronskom obliku.
- (4) Pravo na dobijanje kopije iz stava (3) ovog člana ne smije negativno uticati na prava i slobode drugih.

### **Član 18.**

#### **(Pravo na ispravku)**

- (1) Nosilac podataka ima pravo da mu kontrolor podataka omogući ispravku netačnog ličnog podatka, bez nepotrebnog odlaganja.
- (2) Uzimajući u obzir svrhu obrade, nosilac podataka ima pravo dopuniti nepotpun lični podatak, između ostalog i davanjem dodatne izjave.

### **Član 19.**

#### **(Pravo na brisanje)**

- (1) Nosilac podataka ima pravo da mu kontrolor podataka omogući brisanje ličnog podatka koji se na njega odnosi, a kontrolor podataka ima obavezu obrisati lični podatak, bez nepotrebnog odlaganja, ako je ispunjen jedan od sljedećih uvjeta:
- a) lični podatak više nije neophodan za svrhe u koje je prikupljen ili na drugi način obrađen;
  - b) nosilac podataka povukao je saglasnost na kojoj je obrada zasnovana u skladu s članom 8. stavom (1) tačkom a) ovog zakona ili članom 11. stavom (2) tačkom a) ovog zakona i ako ne postoji drugi pravni osnov za obradu;

- c) nosilac podataka uložio je prigovor na obradu u skladu s članom 23. stavom (1) ovog zakona i ne postoje zakonski razlozi za obradu ili je nosilac podataka uložio prigovor na obradu u skladu s članom 23. stavom (2) ovog zakona;
  - d) lični podatak je nezakonito obrađen;
  - e) lični podatak mora biti obrisani radi postupanja u skladu sa zakonskom obavezom kojoj podliježe kontrolor podataka;
  - f) lični podatak je prikupljen u vezi s ponudom usluga informacionog društva iz člana 10. stav (1) ovog zakona.
- (2) Ako je kontrolor podataka javno objavio lični podatak, a dužan je u skladu sa stavom (1) ovog člana taj lični podatak brisati, uzimajući u obzir dostupnu tehnologiju i troškove provođenja, kontrolor podataka preduzima razumne mjere, uključujući i tehničke mjere, da bi obavijestio kontrolore podataka koji obrađuju lični podatak da je nosilac podataka zatražio od tih kontrolora podataka da brišu sve poveznice do njega ili kopiju ili rekonstrukciju tog ličnog podatka.
- (3) St. (1) i (2) ovog člana ne primjenjuju se u mjeri u kojoj je obrada neophodna:
- a) radi ostvarivanja prava na slobodu izražavanja i informisanja;
  - b) radi poštovanja zakonske obaveze kojom se zahtijeva obrada propisana posebnim zakonom, a koja se primjenjuje na kontrolora podataka ili radi izvršenja zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlaštenja dodijeljenih kontroloru podataka;
  - c) radi javnog interesa u oblasti javnog zdravlja u skladu s članom 11. stavom (2) tač. h) i i) ovog člana, kao i članom 11. stavom (3) ovog zakona;
  - d) u svrhe arhiviranja u javnom interesu, u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe u skladu s članom 56. stavom (1) ovog zakona u mjeri u kojoj je vjerovatno da se pravom iz stava (1) ovog člana može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade ili
  - e) radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

## **Član 20.**

### **(Pravo na ograničenje obrade)**

- (1) Nosilac podataka ima pravo na ograničenje obrade podataka ako je ispunjen jedan od sljedećih uvjeta:
- a) nosilac podataka osporava tačnost ličnog podatka, u roku u kojem se kontroloru podataka omogućava da provjeri tačnost ličnog podatka;
  - b) obrada je nezakonita, a nosilac podataka se protivi brisanju ličnog podatka i umjesto toga traži ograničenje njegove obrade;
  - c) kontroloru podataka više nije potreban lični podatak za potrebe obrade, ali ga nosilac podataka zahtijeva radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva;
  - d) nosilac podataka uložio je prigovor na obradu u skladu s članom 23. stavom (1) ovog zakona i očekuje potvrdu prevladavaju li njegovi razlozi nad legitimnim razlozima kontrolora podataka.

- (2) Ako je obrada ograničena u skladu sa stavom (1) ovog člana, taj lični podatak smije se obrađivati samo uz saglasnost nosioca podataka, izuzev čuvanja, ili za postavljanje, ostvarivanje ili odbranu pravnih zahtjeva ili zaštitu prava drugog fizičkog ili pravnog lica ili zbog važnog javnog interesa.
- (3) Nosioca podataka koji je ostvario pravo na ograničenje obrade, u skladu sa stavom (1) ovog člana, kontrolor podataka obavještava prije ukidanja ograničenja obrade.

#### **Član 21.**

##### **(Obaveza obavještavanja o ispravci ili brisanju ličnog podatka ili ograničenju obrade)**

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

#### **Član 22.**

##### **(Pravo na prenosivost ličnog podatka)**

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

#### **Član 23.**

##### **(Pravo na prigovor)**

- (1) Nosilac podataka ima pravo na osnovu svoje posebne situacije u svakom trenutku kontroloru podataka podnijeti prigovor na obradu njegovog ličnog podatka, u skladu s

članom 8. stavom (1) tač. e) ili f) ovog zakona, uključujući profiliranje zasnovano na tim odredbama. Kontrolor podataka ne smije dalje obrađivati lični podatak, osim u slučaju da dokaže da postoje uvjerljivi legitimni razlozi za obradu koji prevladavaju nad interesima, pravima i slobodama nosioca podataka ili radi postavljanja, ostvarivanja ili odbrane pravnih zahtjeva.

- (2) Ako se lični podatak obrađuje za potrebe direktnog marketinga, nosilac podataka ima pravo u bilo kojem trenutku uložiti prigovor na obradu ličnog podatka koji se odnosi na njega, za potrebe takvog marketinga, što uključuje izradu profila u mjeri u kojoj je povezano s takvim direktnim marketingom.
- (3) Ako se nosilac podataka protivi obradi za potrebe direktnog marketinga, lični podatak više se ne smije obrađivati u te svrhe.
- (4) Najkasnije u trenutku prve komunikacije s nosiocem podataka, nosilac podataka se izričito mora uputiti na prava iz st. (1) i (2) ovog člana te se to mora učiniti na jasan način i odvojeno od bilo koje druge informacije.
- (5) U kontekstu korištenja usluga informacionog društva i ne uzimajući u obzir propise iz oblasti elektronskih komunikacija, nosilac podataka može ostvariti svoje pravo na prigovor automatiziranim putem pomoću tehničkih specifikacija.
- (6) Ako se lični podatak obrađuje u svrhe naučnog ili historijskog istraživanja ili u statističke svrhe na osnovu člana 56. stava (1) ovog zakona, nosilac podataka na osnovu svoje posebne situacije ima pravo uložiti prigovor na obradu ličnog podatka koji se na njega odnosi, osim ako je obrada neophodna za izvršenje zadatka koji se obavlja u javnom interesu.

#### **Član 24.**

##### **(Automatizirano pojedinačno donošenje odluke, uključujući i profiliranje)**

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

**Član 25.**  
**(Ograničenja)**

- (1) Na osnovu posebnog zakona koji se primjenjuje na kontrolora podataka i obrađivača može se ograničiti opseg prava i obaveza iz člana 7., čl. 14. do 24. ovog zakona i člana 36. ovog zakona, ako odredbe tog zakona odgovaraju pravima i obavezama propisanim u čl. 14. do 24. ovog zakona, ako se takvim ograničenjem poštuje suština osnovnih prava i sloboda i ako ono predstavlja neophodnu i proporcionalnu mjeru u demokratskom društvu za zaštitu:
- a) državne sigurnosti;
  - b) odbrane;
  - c) javne sigurnosti;
  - d) sprečavanja, istrage, otkrivanja ili gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
  - e) drugih važnih ciljeva od općeg javnog interesa u Bosni i Hercegovini, a posebno važnog privrednog ili finansijskog interesa, što uključuje monetarna, budžetska i porezna pitanja, javno zdravstvo i socijalnu zaštitu;
  - f) nezavisnosti pravosuđa i sudskih postupaka;
  - g) sprečavanja, istrage, otkrivanja i gonjenja povrede etike u zakonski regulisanim profesijama;
  - h) nadzorne, inspeksijske ili regulatorne funkcije koja je, najmanje povremeno, povezana s izvršavanjem službenih ovlaštenja u slučajevima iz tač. a) do e) i tačke g) ovog stava;
  - i) nosioca podataka ili prava i sloboda drugih;
  - j) ostvarivanja potraživanja u građanskim sporovima.
- (2) Posebni zakon iz stava (1) ovog člana sadrži, po potrebi, posebne odredbe, koje sadrže najmanje sljedeće:
- a) svrhu obrade ili kategoriju obrade;
  - b) kategoriju ličnog podatka;
  - c) opseg uvedenih ograničenja;
  - d) mjere zaštite za sprečavanje zloupotrebe ili nezakonitog pristupa ili prijenosa;
  - e) određivanje kontrolora podataka ili kategoriju kontrolora podataka;
  - f) rok čuvanja i mjere zaštite koje se mogu primijeniti uzimajući u obzir prirodu, opseg i svrhe obrade ili kategorije obrade;
  - g) rizik za prava i slobode nosioca podataka;
  - h) pravo nosioca podataka da bude obaviješten o ograničenju, osim ako to može biti štetno za svrhu tog ograničenja.

**POGLAVLJE III. KONTROLOR PODATAKA I OBRADIVAČ**

**Član 26.**  
**(Obaveza kontrolora podataka)**

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

## **Član 27.**

### **(Tehnička i integrirana zaštita podataka)**

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

## **Član 28.**

### **(Zajednički kontrolori podataka)**

- (1) Ako dva ili više kontrolora podataka zajednički odrede svrhe i načine obrade, smatraju se zajedničkim kontrolorima podataka. Oni na transparentan način, međusobnim sporazumom, određuju odgovornosti svakoga od njih s ciljem izvršavanja obaveza iz ovog zakona, posebno u vezi s ostvarivanjem prava nosioca podataka i dužnostima svakoga od njih u vezi s pružanjem informacija iz čl. 15. i 16. ovog zakona, osim u slučaju da su odgovornosti svakog od kontrolora podataka utvrđene zakonom koji se primjenjuje na kontrolore podataka. Sporazumom se može odrediti kontaktna tačka za nosioca podataka.
- (2) Sporazum iz stava (1) ovog člana mora na odgovarajući način odražavati pojedinačne uloge i odnose zajedničkih kontrolora podataka u odnosu na nosioce podataka. Suština sporazuma mora biti dostupna nosiocu podataka.

- (3) Nezavisno od uvjeta sporazuma iz stava (1) ovog člana, nosilac podataka može ostvarivati svoja prava iz ovog zakona u vezi sa svakim kontrolorom podataka i protiv svakog od njih.

### **Član 29.**

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

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

### **Član 30.**

#### **(Orađivač)**

- (1) Ako se obrada ličnog podatka obavlja u ime kontrolora podataka, kontrolor podataka koristi isključivo obrađivača koji u dovoljnoj mjeri garantuje primjenu odgovarajućih tehničkih i organizacionih mjera tako da obrada bude u skladu sa zahtjevima iz ovog zakona i da se obradom osigurava zaštita prava nosioca podataka.
- (2) Orađivač ne smije angažovati drugog obrađivača bez prethodnog posebnog ili općeg pisanog odobrenja kontrolora podataka. U slučaju općeg pisanog odobrenja, obrađivač obavještava kontrolora podataka o svim planiranim izmjenama u vezi s dodavanjem ili zamjenom drugih obrađivača kako bi time kontroloru podataka omogućio da uloži prigovor na te izmjene.
- (3) Obrada koju obavlja obrađivač uređuje se ugovorom ili drugim pravnim aktom u skladu sa zakonom koji obavezuje obrađivača prema kontroloru podataka, u kojem se navode predmet i trajanje obrade, priroda i svrha obrade, vrsta ličnih podataka i kategorija nosioca podataka, kao i obaveze i prava kontrolora podataka.
- (4) Ugovorom ili drugim pravnim aktom iz stava (3) ovog člana propisuje se da je obrađivač dužan da:
- a) obrađuje lični podatak samo prema dokumentiranim uputstvima kontrolora podataka, između ostalog i u vezi s prijenosom ličnog podatka u drugu državu ili međunarodnu

organizaciju, osim ako je to propisano posebnim zakonom koji se primjenjuje na obrađivača, u tom slučaju, obrađivač obavještava kontrolora podataka o tom pravnom zahtjevu prije obrade, osim ako se tim zakonom zabranjuje takvo obavještavanje zbog važnih razloga od javnog interesa;

- b) osigurava da su se lica ovlaštena za obradu ličnog podatka obavezala na poštovanje povjerljivosti ili da ih na poštovanje povjerljivosti obavezuje odgovarajući zakon;
  - c) preduzima sve potrebne mjere u skladu s članom 34. ovog zakona;
  - d) poštuje uvjete iz st. (2) i (5) ovog člana za angažovanje drugog obrađivača;
  - e) uzimajući u obzir prirodu obrade, pomaže kontroloru podataka putem odgovarajućih tehničkih i organizacionih mjera, koliko je to moguće, da ispuni obavezu kontrolora podataka da odgovori na zahtjeve za ostvarivanje prava nosioca podataka iz poglavlja II. ovog zakona;
  - f) pomaže kontroloru podataka u osiguravanju usklađenosti s obavezama iz čl.34. do 38. ovog zakona, uzimajući u obzir prirodu obrade i informacije koje su dostupne obrađivaču;
  - g) po izboru kontrolora podataka, briše ili vraća kontroloru podataka sve lične podatke nakon završetka pružanja usluga u vezi s obradom i briše postojeće kopije, osim u slučaju da je posebnim zakonom propisana obaveza čuvanja ličnih podataka;
  - h) kontroloru podataka stavlja na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obaveza iz ovog člana i kontroloru podataka ili drugom revizoru kojeg je ovlastio kontrolor podataka omogućava obavljanje revizije, uključujući i inspekcije, i pomaže u njihovom obavljanju;
  - i) u slučaju iz tačke h) ovog stava obrađivač odmah obavještava kontrolora podataka ako prema njegovom mišljenju određeno uputstvo krši ovaj zakon ili druga pravila o zaštiti podataka.
- (5) Ako obrađivač angažuje drugog obrađivača za obavljanje posebnih aktivnosti obrade u ime kontrolora podataka, iste obaveze za zaštitu podataka kao one koje su navedene u ugovoru ili drugom pravnom aktu između kontrolora podataka i obrađivača iz stava (4) ovog člana nameću se tom drugom obrađivaču ugovorom ili drugim pravnim aktom u skladu s posebnim zakonom, a posebno obaveza davanja dovoljnih garancija za primjenu odgovarajućih tehničkih i organizacionih mjera na način kojim se osigurava da obrada zadovoljava zahtjeve iz ovog zakona. Ako taj drugi obrađivač ne ispunjava obaveze zaštite podataka, prvi obrađivač ostaje u potpunosti odgovoran kontroloru podataka za izvršavanje obaveza tog drugog obrađivača.
- (6) Poštovanje odobrenih kodeksa ponašanja od obrađivača, iz člana 42. ovog zakona, ili odobrenog mehanizma certifikacije, iz člana 44. ovog zakona, može služiti kao element za dokazivanje pružanja dovoljnih garancija iz st. (1) i (5) ovog člana.
- (7) Ne dovodeći u pitanje pojedinačni ugovor između kontrolora podataka i obrađivača, ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog člana može se u cjelini ili djelomično zasnivati na standardnim ugovornim klauzulama iz st. (8) i (9) ovog člana, uključujući između ostalog i klauzule koje su dio sertifikata dodijeljenog kontroloru podataka ili obrađivaču u skladu s čl. 44. i 45. ovog zakona.

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

### **Član 31.**

#### **(Obrada ličnog podatka pod kontrolom kontrolora podataka ili obrađivača)**

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

### **Član 32.**

#### **(Evidencija o obradi ličnog podatka)**

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

organizacije i u slučaju prijenosa iz člana 51. stava (2) ovog zakona, dokumentaciju o odgovarajućim zaštitnim mjerama;

- d) ako je moguće, opći opis tehničkih i organizacionih sigurnosnih mjera iz člana 34. stava (1) ovog zakona.
- (3) Evidencija iz st. (1) i (2) ovog člana mora biti u pisanom obliku, što uključuje i elektronski oblik.
- (4) Kontrolor podataka ili obrađivač te predstavnik kontrolora podataka ili obrađivača, ako je primjenjivo, na zahtjev Agencije omogućavaju uvid u evidenciju.
- (5) Obaveze iz st. (1) i (2) ovog člana ne primjenjuju se na privredni subjekat ili organizaciju u kojoj je zaposleno manje od 250 lica, osim kada postoji vjerovatnoća da će obrada koju obavlja predstavljati visok rizik za prava i slobode nosioca podataka, ako obrada nije povremena ili ako obrada obuhvata posebne kategorije podataka iz člana 11. stava (1) ovog zakona, ili su u pitanju lični podaci koji se odnose na krivičnu osuđivanost i krivična djela.

### **Član 33.**

#### **(Saradnja s Agencijom)**

Kontrolor podataka i obrađivač te ako su određeni njihovi predstavnici, dužni su, na zahtjev, saradivati s Agencijom u obavljanju njenih zadataka.

### **Član 34.**

#### **(Sigurnost obrade ličnog podatka)**

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

- (4) Kontrolor podataka i obrađivač preduzimaju mjere kako bi osigurali da svako fizičko lice koje djeluje pod nadležnošću kontrolora podataka ili obrađivača, a koje ima pristup ličnom podatku, ne obrađuje taj podatak ako to nije prema uputstvima kontrolora podataka, osim u slučajevima kada je to propisano posebnim zakonom.

### **Član 35.**

#### **(Izvještavanje Agencije o povredi ličnog podatka)**

- (1) Kontrolor podataka dužan je o povredi ličnog podatka bez nepotrebnog odgađanja i, ako je moguće, a najkasnije u roku od 72 sata nakon saznanja za tu povredu obavijestiti Agenciju o povredi ličnog podatka, osim u slučaju ako je vjerovatno da ta povreda neće ugroziti prava i slobode fizičkog lica. Ako izvještavanje nije izvršeno u roku od 72 sata, kontrolor podataka dužan je Agenciji navesti razloge za kašnjenje.
- (2) Obradivač je dužan, po saznanju za povredu ličnog podatka, bez nepotrebnog odgađanja o tome obavijestiti kontrolora podataka.
- (3) Izvještaj iz stava (1) ovog člana sadrži najmanje sljedeće:
- a) opis prirode povrede ličnih podataka, i ako je moguće, s navedenim kategorijama i približnim brojem nosilaca podataka, kao i kategorijama i približnim brojem evidencija ličnih podataka;
  - b) ime i prezime te kontaktne podatke službenika za zaštitu podataka ili druge kontaktne tačke od koje se može dobiti još informacija;
  - c) opis moguće posljedice povrede ličnog podatka;
  - d) opis mjera koje je kontrolor podataka preduzeo ili čije je preduzimanje predložio radi rješavanja problema povrede ličnog podatka, uključujući prema potrebi i mjere za ublažavanje njenih mogućih štetnih posljedica.
- (4) Ako i u mjeri u kojoj nije moguće istovremeno dostaviti informacije, informacije se mogu dostavljati u dijelovima, bez nepotrebnog daljnjeg odgađanja.
- (5) Kontrolor podataka dokumentira svaku povredu ličnog podatka, uključujući i činjenice u vezi s povredom ličnog podatka, njene posljedice i mjere preduzete za otklanjanje štete. Dokumentacija iz ovog stava omogućava Agenciji postupanje po ovom članu.

### **Član 36.**

#### **(Obavještavanje nosioca podataka o povredi ličnog podatka)**

- (1) Kontrolor podataka dužan je bez odgađanja pisanim putem obavijestiti nosioca podataka o povredi ličnog podatka, ako je vjerovatno da će povreda ličnog podatka prouzrokovati visok rizik za prava i slobode fizičkog lica.
- (2) Kontrolor podataka u obavještenju iz stava (1) ovog člana, jasnim i jednostavnim jezikom, opisuje prirodu povrede ličnog podatka te se najmanje navode informacije i mjere iz člana 35. stava (3) tač. b), c) i d) ovog zakona.
- (3) Obavještavanje iz stava (1) ovog člana nosioca podataka nije obavezno ako je ispunjen jedan od sljedećih uvjeta:

- a) ako je kontrolor podataka preduzeo odgovarajuće tehničke i organizacione zaštitne mjere i te mjere su primijenjene na lični podatak u vezi s kojim je došlo do povrede ličnog podatka, a prije svega mjere koje lični podatak čine nerazumljivim licu koje nije ovlašteno da mu pristupi, kao što je enkripcija;
  - b) ako je kontrolor podataka preduzeo naknadne mjere kojima se osigurava da više nije moguće da će doći do visokog rizika za prava i slobode nosioca podataka iz stava (1) ovog člana;
  - c) ako bi to zahtijevalo neproporcionalan napor, mora se objaviti javno saopćenje ili se preduzima slična mjera kojom se nosioci podataka obavještavaju na jednako djelotvoran način.
- (4) Ako kontrolor podataka nije obavijestio nosioca podataka o povredi ličnog podatka, Agencija, nakon razmatranja stepena vjerovatnoće da će povreda ličnog podatka prouzrokovati visok rizik za prava i slobode fizičkih lica, može od kontrolora podataka zahtijevati da to učini, ako nije ispunjen neki od uvjeta iz stava (3) ovog člana.

### **Član 37.**

#### **(Procjena uticaja obrade na zaštitu ličnog podatka)**

- (1) Ako je vjerovatno da će neka vrsta obrade, posebno posredstvom novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica, kontrolor podataka prije obrade provodi procjenu uticaja predviđenih obrada na zaštitu ličnog podatka.
- (2) Pri provođenju procjene uticaja obrade na zaštitu ličnog podatka, kontrolor podataka traži savjet od službenika za zaštitu ličnih podataka, ako je imenovan.
- (3) Procjena uticaja obrade na zaštitu ličnog podatka iz stava (1) ovog člana obavezna je posebno u slučaju:
  - a) systemske i obimne procjene ličnih aspekata u vezi s fizičkim licima koja se zasniva na automatiziranoj obradi, uključujući profiliranje, i koja je osnov za donošenje odluka koje proizvode pravni učinak u odnosu na fizičko lice ili na sličan način značajno utiču na fizičko lice;
  - b) obimne obrade posebnih kategorija ličnih podataka iz člana 11. stava (1) ovog zakona ili podataka koji se odnose na krivičnu osuđivanost i krivična djela iz člana 12. ovog zakona ili
  - c) sistemskog praćenja javno dostupnog područja u velikoj mjeri.
- (4) Agencija uspostavlja i javno objavljuje popis vrsta postupaka obrade na koje se primjenjuje obaveza vršenja procjene uticaja na zaštitu ličnih podataka, u skladu sa stavom (1) ovog člana.
- (5) Agencija može da uspostavi i javno objavi popis vrsta postupaka obrade za koje nije potrebna procjena uticaja na zaštitu ličnog podatka.
- (6) Procjena uticaja obuhvata najmanje:
  - a) sistemski opis predviđenih obrada i svrha obrade, uključujući, ako je primjenjivo, legitiman interes kontrolora podataka;
  - b) procjenu nužnosti i proporcionalnosti obrada povezanih s njihovim svrhama;

- c) procjenu rizika za prava i slobode nosioca podataka;
  - d) predviđene mjere za rješavanje rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguranje zaštite ličnih podataka i dokazivanje usklađenosti s ovim zakonom, uzimajući u obzir prava i legitimne interese nosioca podataka i drugih uključenih lica.
- (7) Usklađenost odobrenih kodeksa ponašanja iz člana 42. ovog zakona od kontrolora podataka ili obrađivača uzima se u obzir prilikom procjene uticaja obrade koje primjenjuju ti kontrolori podataka ili obrađivači, posebno u svrhe procjene uticaja na zaštitu ličnih podataka.
- (8) Kontrolor podataka prema potrebi od nosioca podataka ili njegovog predstavnika traži mišljenje o namjeravanoj obradi, ne dovodeći u pitanje komercijalne ili javne interese ili sigurnost postupka obrade.
- (9) Ako obrada u skladu s članom 8. stavom (1) tač. c) ili e) ovog zakona ima pravni osnov u posebnom zakonu koji se primjenjuje na kontrolora podataka, ako su tim zakonom uređene posebne obrade ili skup predmetnih radnji i ako je procjena uticaja na zaštitu ličnih podataka već provedena kao dio opće procjene uticaja u kontekstu donošenja pravnog osnova, st. (1) do (6) ovog člana se ne primjenjuju, osim ako je posebnim propisom utvrđeno da je potrebno provesti takvu procjenu prije obrade.
- (10) Kontrolor podataka prema potrebi preispituje da li je obrada izvršena u skladu s procjenom uticaja na zaštitu ličnih podataka, i to najmanje kada dođe do promjene u nivou rizika koji predstavljaju postupci obrade.

### **Član 38.**

#### **(Prethodno savjetovanje kontrolora podataka s Agencijom)**

- (1) Kontrolor obrade savjetuje se s Agencijom prije obrade ako je procjena uticaja na zaštitu ličnih podataka iz člana 37. ovog zakona pokazala da bi obrada podataka prouzrokovala visok rizik za prava i slobode pojedinaca, u slučaju da kontrolor podataka ne donese mjere za ublažavanje rizika.
- (2) Ako Agencija utvrdi da bi se namjeravanom obradom iz stava (1) ovog člana kršio ovaj zakon, posebno ako kontrolor podataka nije u dovoljnoj mjeri utvrdio ili umanjio rizik za prava i slobode pojedinaca, Agencija u roku od najviše 56 dana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje kontrolora podataka, a prema potrebi i obrađivača, i pri tom može koristiti ovlaštenja iz člana 103. ovog zakona.
- (3) Rok iz stava (2) ovog člana, po potrebi, može se produžiti za 42 dana, u zavisnosti od složenosti namjeravane obrade.
- (4) Agencija, u roku od 30 dana od zaprimanja zahtjeva, obavještava kontrolora podataka, a prema potrebi i obrađivača, o produženju roka iz stava (3) ovog člana i o razlozima odgađanja.
- (5) Proticanje rokova iz st. (2) i (3) može biti privremeno obustavljeno dok Agencija ne dobije informacije koje je zahtijevala za potrebe savjetovanja.
- (6) Pri savjetovanju kontrolor podataka Agenciji dostavlja:

- a) ako je primjenjivo, odgovarajuće odgovornosti kontrolora podataka, zajedničkih kontrolora podataka i obrađivača koji učestvuju u obradi, posebno u slučaju obrade unutar grupe privrednih subjekata;
  - b) svrhu i sredstva namjeravane obrade;
  - c) zaštitne mjere i druge mjere za zaštitu prava i sloboda nosioca podataka na osnovu ovog zakona;
  - d) kontaktne podatke službenika za zaštitu podataka, ako je primjenjivo;
  - e) procjenu uticaja na zaštitu podataka kako je propisano članom 37. ovog zakona;
  - f) sve druge informacije koje Agencija zatraži.
- (7) O prijedlogu zakona kojim se reguliše obrada ličnih podataka, prije njegovog upućivanja u parlamentarnu proceduru, predlagač se može prethodno savjetovati sa Agencijom.
- (8) Nezavisno od stava (1) ovog člana, posebnim zakonom se može propisati obaveza kontroloru podataka da se savjetuje s Agencijom i da od nje pribavi prethodno odobrenje u vezi s obradom koju obavlja za izvršenje zadataka u javnom interesu, uključujući i obradu u vezi sa socijalnom i zdravstvenom zaštitom.

### **Član 39.**

#### **(Imenovanje službenika za zaštitu ličnih podataka)**

- (1) Kontrolor podataka i obrađivač dužni su imenovati službenika za zaštitu ličnih podataka u slučajevima:
- a) ako obradu vrši javni organ, osim sudova koji postupaju u okviru sudske nadležnosti;
  - b) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od postupaka obrade koje zbog svoje prirode, opsega i/ili svrhe zahtijevaju redovno i sistemsko praćenje nosioca podataka u velikom broju ili
  - c) ako se osnovne djelatnosti kontrolora podataka ili obrađivača sastoje od opsežne obrade posebnih kategorija podataka na osnovu člana 11. ovog zakona i ličnih podataka u vezi s krivičnom osuđivanosti i krivičnim djelima iz člana 12. ovog zakona.
- (2) Grupa privrednih subjekata može imenovati jednog službenika za zaštitu ličnih podataka uz uvjet da je službenik za zaštitu ličnih podataka lako dostupan iz svakog sjedišta ili poslovnog nastana.
- (3) Ako je kontrolor podataka ili obrađivač javni organ, za više takvih organa može se imenovati jedan službenik za zaštitu ličnih podataka, uzimajući u obzir njihovu organizacionu strukturu i veličinu.
- (4) U slučajevima koji nisu navedeni u stavu (1) ovog člana, kontrolor podataka ili obrađivač ili udruženje i drugi organ koji predstavlja kategoriju kontrolora podataka ili obrađivača mogu, odnosno u slučajevima kada je to propisano posebnim zakonom moraju imenovati službenika za zaštitu ličnih podataka. Službenik za zaštitu ličnih podataka može obavljati poslove u ime tih udruženja i drugih organa koji predstavljaju kontrolore podataka ili obrađivače.

- (5) Službenik za zaštitu ličnih podataka imenuje se na osnovu njegovih stručnih kvalifikacija, a posebno stručnog znanja o pravu i praksi u oblasti zaštite ličnih podataka i sposobnosti obavljanja zadataka iz člana 41. ovog zakona.
- (6) Službenik za zaštitu ličnih podataka može biti zaposlen kod kontrolora podataka ili obrađivača ili može obavljati poslove na osnovu ugovora o djelu.
- (7) Kontrolor podataka ili obrađivač objavljuje kontaktne podatke službenika za zaštitu ličnih podataka i dostavlja ih Agenciji.

#### **Član 40.**

##### **(Status službenika za zaštitu ličnih podataka)**

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

#### **Član 41.**

##### **(Zadatak službenika za zaštitu ličnih podataka)**

- (1) Službenik za zaštitu ličnih podataka obavlja sljedeće zadatke:
  - a) informisanje i savjetovanje kontrolora podataka ili obrađivača i zaposlenih koji vrše obradu o njihovim obavezama iz ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka;
  - b) praćenje poštovanja ovog zakona i drugih zakona kojima se propisuje zaštita ličnih podataka, kao i politika kontrolora podataka ili obrađivača u vezi sa zaštitom ličnih

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

## **Član 42.**

### **(Kodeks ponašanja)**

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

- (4) Udruženja i subjekt iz stava (2) ovog člana koji namjeravaju izraditi kodeks ponašanja ili izmijeniti i proširiti postojeći kodeks ponašanja, nacrt kodeksa ponašanja, odnosno izmjene ili proširenje kodeksa ponašanja, dostavljaju Agenciji.
- (5) Agencija daje mišljenje o tome da li je nacrt kodeksa u skladu s ovim zakonom te odobrava nacrt kodeksa ako ocijeni da osigurava dovoljno adekvatne zaštitne mjere.
- (6) Ako Agencija odobri nacrt kodeksa ponašanja, odnosno izmjene ili dopune kodeksa ponašanja, u skladu sa stavom (5) ovog člana, Agencija registruje i objavljuje kodeks ponašanja.
- (7) Kontrolor podataka ili obrađivač, na koje se ovaj zakon ne primjenjuje u skladu s članom 6. ovog zakona, mogu primjenjivati kodeks ponašanja koji je odobren, u skladu sa stavom (5) ovog člana, kako bi osigurali odgovarajuće zaštitne mjere u okviru prijenosa ličnih podataka drugoj državi ili međunarodnoj organizaciji, uz uvjete iz člana 48. stava (2), tačke d) ovog zakona.
- (8) Kontrolor podataka ili obrađivač iz stava (7) ovog člana, putem ugovornih ili drugih pravno obavezujućih instrumenata, preuzima obavezujuće i provedive obaveze za primjenu zaštitnih mjera, uključujući i mjere u vezi s pravima nosioca podataka.

### **Član 43.**

#### **(Praćenje odobrenog kodeksa ponašanja)**

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

## **Član 44.**

### **(Certifikacija)**

- (1) Agencija preporučuje uspostavljanje postupka certifikacije zaštite ličnih podataka, pečata i oznaka za zaštitu podataka s ciljem dokazivanja poštovanja odredbi ovog zakona, posebno uzimajući u obzir potrebe mikro, malih i srednjih pravnih lica.
- (2) Postupak certifikacije zaštite ličnih podataka, pečata i oznaka može biti uspostavljen i radi dokazivanja postojanja odgovarajućih zaštitnih mjera koje osiguravaju kontrolor podataka i obrađivač na koje se ovaj zakon u skladu s članom 6. ovog zakona ne odnosi, u okviru prijenosa ličnih podataka drugoj državi ili međunarodnoj organizaciji, uz uvjete iz člana 48. stava (2) tačke d) ovog zakona.
- (3) Kontrolori podataka ili obrađivači, iz stava (2) ovog člana, putem ugovornih ili drugih pravno obavezujućih instrumenata prihvataju primjenu odgovarajućih zaštitnih mjera, uključujući i mjere u vezi s nosiocem podataka.
- (4) Certifikacija je dobrovoljna i dostupna putem procesa koji je transparentan.
- (5) Certifikacija, u skladu s ovim članom, ne umanjuje odgovornost kontrolora podataka ili obrađivača za poštovanje ovog zakona i ne dovodi u pitanje nadležnosti Agencije.
- (6) Certifikaciju, u skladu s ovim članom, izdaje certifikacioni organ iz člana 45. ovog zakona na osnovu kriterija koje je odobrila Agencija.
- (7) Kontrolor podataka ili obrađivač, u postupku certifikacije, certifikacionom organu pruža sve informacije i omogućava pristup aktivnostima obrade koje su potrebne za postupak certifikacije.
- (8) Certifikat se kontroloru podataka ili obrađivaču izdaje na najviše tri godine i može se obnoviti uz iste uvjete.
- (9) Certifikacioni organ oduzima certifikat kontroloru ili obrađivaču ako više ne ispunjava uvjete za izdavanje certifikata.
- (10) Agencija postupak certifikacije zaštite ličnih podataka, pečata i oznake unosi u evidenciju i javno objavljuje.

## **Član 45.**

### **(Certifikacioni organ)**

- (1) Akreditaciju certifikacionog organa, s odgovarajućim stepenom stručnosti iz oblasti zaštite ličnih podataka, vrši Agencija.
- (2) Certifikacioni organ obavještava Agenciju o odluci o izdavanju i obnavljanju certifikata kako bi Agencija mogla obavljati ovlaštenja iz člana 103. stava (2) tačke h) ovog zakona.
- (3) Certifikacioni organ može biti akreditiran samo ako:
  - a) Agenciji na zadovoljavajući način dokaže svoju nezavisnost i stručnost u predmetu certifikacije;
  - b) se obaveže da će poštovati kriterije iz člana 44. stava (6) ovog zakona;

- c) uspostavi postupke za izdavanje, periodično preispitivanje i povlačenje certifikacije, pečata i oznaka za zaštitu podataka;
  - d) uspostavi postupke i strukture za rješavanje pritužbe na kršenja certifikacije ili način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio certifikaciju i učini te postupke i strukture transparentnim nosiocima podataka i javnosti;
  - e) Agenciji dokaže da njegovi zadaci i dužnosti ne dovode do sukoba interesa.
- (4) Akreditacija certifikacionog organa provodi se na osnovu kriterija koje je propisala Agencija.
  - (5) Akreditacija se izdaje na najviše pet godina i može se obnoviti uz iste uvjete ako certifikacioni organ i dalje ispunjava zahtjeve iz ovog člana.
  - (6) Ne dovodeći u pitanje DIO ČETVRTI ovog zakona, Agencija povlači akreditaciju certifikacionog organa ako se uvjeti iz stava (3) ovog člana ne ispune ili više nisu ispunjeni, ili ako se radnjama koje preduzima certifikacioni organ krši ovaj zakon.
  - (7) Certifikacioni organ odgovoran je za pravilnu procjenu koja dovodi do certifikacije ili oduzimanja certifikata, ne dovodeći u pitanje odgovornost kontrolora podataka ili obrađivača za poštovanje ovog zakona.
  - (8) Certifikacioni organ u pisanoj formi obavještava Agenciju o razlozima za izdavanje ili oduzimanje certifikata.
  - (9) Agencija javno objavljuje kriterije iz člana 44. stava (6) ovog zakona.

#### **POGLAVLJE IV. PRIENOS LIČNOG PODATKA U DRUGU DRŽAVU ILI MEĐUNARODNU ORGANIZACIJU**

##### **Član 46.**

##### **(Opća načela prijenosa)**

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

##### **Član 47.**

##### **(Prijenos na osnovu adekvatnosti nivoa zaštite ličnog podatka)**

- (1) Prijenos ličnog podatka u drugu državu, na dio njene teritorije, ili u jedan ili više sektora u toj državi ili međunarodnu organizaciju može se obavljati ako je utvrđeno da ta druga država, dio njene teritorije, ili jedan ili više sektora u toj državi ili ta međunarodna organizacija osigurava adekvatan nivo zaštite ličnog podatka.
- (2) Smatra se da je adekvatan nivo zaštite iz stava (1) ovog člana osiguran u državi, dijelovima njene teritorije, ili jednom ili više sektora u toj državi ili međunarodnoj organizaciji, za koje je od Evropske unije utvrđeno da osiguravaju adekvatan nivo zaštite ličnog podatka.

- (3) Odluku o adekvatnosti nivoa zaštite ličnog podatka iz stava (1) ovog člana donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stava (3) ovog člana, uzimajući u obzir:
- a) načelo vladavine prava, poštovanje ljudskih prava i osnovnih sloboda, sektorsko zakonodavstvo, uključujući zakonodavstvo o javnoj sigurnosti, odbrani, državnoj sigurnosti, krivičnom pravu i pristupu javnih organa ličnim podacima, kao i primjenu tih propisa, pravila o zaštiti ličnih podataka, pravila struke i mjere osiguranja zaštite ličnih podataka, uključujući pravila o daljnjem prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, koja se primjenjuju u praksi sudova i drugih organa vlasti u drugoj državi ili međunarodnoj organizaciji, kao i djelotvornost ostvarivanja prava nosioca ličnog podatka, a posebno djelotvornost upravnih i sudskih postupaka zaštite prava nosioca ličnog podatka;
  - b) postojanje i efikasnost rada nadzornog organa u drugoj državi ili organa koji je nadležan za međunarodnu organizaciju u ovoj oblasti, s ovlaštenjem da osigura primjenu pravila o zaštiti ličnog podatka i pokrene postupke zaštite ličnog podatka u slučaju njihovog nepoštovanja, pruži pomoć i savjetuje nosioce ličnih podataka u ostvarivanju njihovih prava, kao i da saraduje s nadzornim organima drugih država;
  - c) međunarodne obaveze koje je druga država ili međunarodna organizacija preuzela, ili druge obaveze koje proizlaze iz pravno obavezujućih međunarodnih ugovora ili drugih pravnih instrumenata, kao i iz članstva u multilateralnim ili regionalnim organizacijama, a posebno u vezi sa zaštitom ličnih podataka.
- (5) Agencija kontinuirano prati stanje u oblasti zaštite ličnih podataka u drugoj državi, dijelu njene teritorije, jednom ili više sektora unutar te države ili međunarodnoj organizaciji i o tome po potrebi izvještava Vijeće ministara Bosne i Hercegovine.
- (6) Izvještaj iz stava (5) ovog člana uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija, koje su od značaja za preispitivanje postojanja adekvatnog nivoa zaštite ličnog podatka, na osnovu čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stava (3) ovog člana.
- (7) Odluka donesena na osnovu stava (3) ovog člana ne dovodi u pitanje prijenos ličnog podatka u drugu državu, na teritoriju ili u jedan ili više određenih sektora unutar te druge države ili međunarodnu organizaciju u skladu s čl. 48. do 51. ovog zakona.
- (8) Lista država, dio njihovih teritorija, jedan ili više sektora unutar države i međunarodnih organizacija, u vezi s kojim je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju adekvatan nivo zaštite ličnih podataka, objavljuju se u „Službenom glasniku BiH“ i na službenoj internet stranici Agencije.

#### **Član 48.**

##### **(Prijenos na koji se primjenjuju odgovarajuće zaštitne mjere)**

- (1) Kontrolor podataka ili obrađivač može prenijeti lične podatke u drugu državu, na dio njene teritorije, jedan ili više sektora unutar te države ili u međunarodnu organizaciju za koju listom iz člana 47. stava (8) ovog zakona nije utvrđeno postojanje adekvatnog nivoa zaštite ličnih podataka samo ako je kontrolor podataka ili obrađivač osigurao odgovarajuće

zaštitne mjere tih podataka i ako su nosiocu ličnih podataka osigurana provediva prava i djelotvorna sudska zaštita.

- (2) Odgovarajuće zaštitne mjere iz stava (1) ovog člana mogu se, bez posebnog odobrenja Agencije, osigurati:
- a) pravno obavezujućim aktom sačinjenim između javnih organa;
  - b) obavezujućim poslovnim pravilima u skladu s članom 49. ovog zakona;
  - c) odobrenim kodeksom ponašanja u skladu s članom 42. ovog zakona s obavezujućim i izvršnim obavezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, između ostalog i u vezi s pravom nosioca podataka ili
  - d) odobrenim postupkom certifikacije u skladu s članom 44. ovog zakona s obavezujućim i izvršnim obavezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, između ostalog i u vezi s pravima nosioca podataka.
- (3) Odgovarajuće zaštitne mjere iz stava (1) ovog člana mogu se osigurati standardnim ugovornim klauzulama o zaštiti podataka koje donosi Agencija.
- (4) Uz uvjet da to odobri Agencija, odgovarajuće zaštitne mjere iz stava (1) ovog člana također mogu biti osigurane posebno:
- a) ugovorom između kontrolora podataka ili obrađivača i kontrolora podataka, obrađivača ili primaoca ličnih podataka u drugoj državi ili međunarodnoj organizaciji ili
  - b) odredbama koje se unose u sporazume između javnih organa i koje sadrže provediva i djelotvorna prava nosioca podataka.

#### **Član 49.**

##### **(Obavezujuća poslovna pravila)**

- (1) Obavezujuća poslovna pravila određuju najmanje:
- a) strukturu i podatke za kontakt-grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost i svakog od njihovih članova;
  - b) prijenose podataka ili skupove prijenosa, uz navođenje kategorije ličnih podataka, vrste obrade i njene svrhe, kategorije nosilaca podataka i određenja druge države ili država o kojima se radi;
  - c) njihovu pravno obavezujuću prirodu;
  - d) primjenu načela zaštite podataka, a posebno ograničenja svrhe, smanjenja količine podataka, ograničenja roka čuvanja, kvaliteta podataka, tehničke i integrirane zaštite podataka, pravnog osnova obrade, obrade posebnih kategorija ličnih podataka, mjera za postizanje sigurnosti podataka i uvjeta u vezi s daljnjim prijenosom organima koji nisu obavezani obavezujućim poslovnim pravilima;
  - e) prava nosilaca podataka u vezi s obradom i načine za ostvarenje tih prava, uključujući i pravo da se na njih ne primjenjuju odluke koje se zasnivaju isključivo na automatskoj obradi, što uključuje i izradu profila u skladu s članom 24. ovog zakona, pravo na pritužbu Agenciji i pravo na sudska zaštitu, u skladu s članom 110. ovog zakona, a u odgovarajućim slučajevima i pravo na naknadu štete za kršenje obavezujućih poslovnih pravila;

- f) da kontrolor podataka ili obrađivač sa sjedištem poslovnim nastanom na teritoriji Bosne i Hercegovine prihvata odgovornost za sva kršenja obavezujućih poslovnih pravila od bilo kojeg člana koji nema sjedište ili poslovni nastan u Bosni i Hercegovini ili je kontrolor podataka ili obrađivač u cjelini ili djelomično izuzet od odgovornosti ako dokaže da taj član grupe privrednih subjekata nije djelomično odgovoran za događaj koji je prouzrokovao štetu;
  - g) na koji način se nosiocima podataka, osim informacija iz čl. 15. i 16. ovog zakona, pružaju informacije o obavezujućim poslovnim pravilima, posebno o odredbama iz tač. d), e) i f) ovog stava;
  - h) zadatke svakog službenika za zaštitu podataka imenovanog u skladu s članom 39. ovog zakona ili bilo kojeg drugog lica ili subjekta odgovornog za praćenje usklađenosti s obavezujućim poslovnim pravilima u grupi privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kao i praćenje osposobljenosti i rješavanje pritužbi;
  - i) postupke povodom pritužbi;
  - j) mehanizme unutar grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, kojima se osigurava provjera poštovanja obavezujućih poslovnih pravila, koji uključuju reviziju zaštite podataka i metode za osiguravanje korektivnih mjera za zaštitu prava nosioca podataka. Rezultate takve provjere potrebno je saopćiti licu ili subjektu iz tačke h) ovog stava i upravljačkom organu grupe privrednih subjekata koji vrše zajedničku privrednu djelatnost, a na zahtjev ih je potrebno staviti na raspolaganje Agenciji;
  - k) mehanizme za izvještavanje i vođenje evidencije o promjenama pravila i izvještavanje Agencije o tim promjenama;
  - l) mehanizam saradnje s Agencijom radi osiguravanja usklađenosti svakog člana grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, prije svega tako što se Agenciji stave na raspolaganje rezultati provjera mjera iz tačke j) ovog stava;
  - m) mehanizme za izvještavanje Agenciji o bilo kakvim pravnim obavezama koje se odnose na člana grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost i primjenjuju se u drugoj državi, a koje bi mogle imati značajan negativan uticaj na garancije sadržane u obavezujućim poslovnim pravilima;
  - n) odgovarajuće osposobljavanje iz oblasti zaštite ličnih podataka za osoblje koje ima stalni ili redovni pristup ličnim podacima.
- (2) Agencija odobrava obavezujuća poslovna pravila uz uvjet da:
- a) su pravno obavezujuća i da se primjenjuju na svakog zainteresovanog člana određene grupe privrednih subjekata koji obavljaju zajedničku privrednu djelatnost, što uključuje i njihove zaposlene, te da ih oni izvršavaju;
  - b) nosiocima podataka izričito daju provediva prava u vezi s obradom njihovih ličnih podataka;
  - c) ispunjavaju uvjete iz stava (1) ovog člana.
- (3) Agencija može odrediti format i postupke razmjene informacija između kontrolora podataka, obrađivača i Agencije za obavezujuća poslovna pravila u smislu ovog člana.

## Član 50.

### **(Prijenos ili otkrivanje podataka koji nisu dopušteni)**

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

### **Član 51.**

#### **(Odstupanje u posebnim slučajevima)**

- (1) Prijenos ili skup prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, ako ne postoji odluka o adekvatnosti, u skladu s članom 47. stavom (3) ovog zakona ili odgovarajuće zaštitne mjere u skladu s članom 48. ovog zakona, uključujući i obavezujuća poslovna pravila iz člana 49. ovog zakona, obavlja se samo uz jedan od sljedećih uvjeta:
  - a) nosilac podataka je izričito saglasan s predloženim prijenosom, nakon što je upoznat s mogućim rizicima takvih prijenosa zbog nepostojanja odluke o adekvatnosti i odgovarajućih zaštitnih mjera iz člana 48. ovog zakona;
  - b) prijenos je neophodan za izvršenje ugovora između nosioca podataka i kontrolora podataka ili provođenje predugovornih mjera na zahtjev nosioca podataka;
  - c) prijenos je neophodan radi sklapanja ili izvršenja ugovora sklopljenog u interesu nosioca podataka između kontrolora podataka i drugog fizičkog ili pravnog lica;
  - d) prijenos je neophodan iz važnih razloga javnog interesa;
  - e) prijenos je neophodan za postavljanje, ostvarivanje ili odbranu pravnih zahtjeva;
  - f) prijenos je neophodan za zaštitu ključnih interesa nosioca podataka ili drugih lica ako nosilac podataka fizički ili pravno nije sposoban dati saglasnost;
  - g) prijenos se vrši iz registra, koji prema pravnim propisima u Bosni i Hercegovini služi za pružanje informacija javnosti i koji je dostupan na uvid javnosti ili bilo kojem licu koje može dokazati postojanje legitimnog interesa, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani posebnim zakonom za uvid u tom posebnom slučaju.
- (2) Prijenos ili skup prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, u slučaju kada osnov za prijenos ne može biti čl. 47. ili 48. ovog zakona, uključujući i obavezujuća poslovna pravila iz člana 49. ovog zakona, i kada se ne primjenjuje nijedno odstupanje u posebnim slučajevima iz stava (1) ovog člana, može se izvršiti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničen broj nosilaca podataka i ako je neophodan za potrebe važnih, legitimnih interesa kontrolora podataka nad kojima ne prevladavaju interesi ili prava i slobode nosioca podataka, a kontrolor podataka je procijenio sve okolnosti prijenosa podataka i na osnovu te procjene je predvidio odgovarajuće zaštitne mjere u vezi sa zaštitom ličnih podataka. Kontrolor podataka o prijenosu obavještava Agenciju. Uz informacije iz čl. 15. i 16. ovog zakona, kontrolor podataka obavještava nosioca podataka o prijenosu i o važnim legitimnim interesima.
- (3) Prijenos na osnovu stava (1) tačke g) ovog člana ne uključuje lične podatke u cjelini ni cijele kategorije ličnih podataka sadržanih u registru. Kada je registar namijenjen uvidu

licima koja imaju legitiman interes, prijenos se vrši samo ako to zahtijevaju ta lica ili ako su oni primaoci.

- (4) Na aktivnosti koje obavljaju javni organi prilikom izvršavanja svojih javnih ovlaštenja ne primjenjuju se stav (1) tač. a), b) i c) i stav (2) ovog člana.
- (5) Javni interes iz stava (1) tačke d) ovog člana mora biti propisan zakonom koji se primjenjuje na kontrolora podataka.
- (6) Ako nije donesena odluka o adekvatnosti, iz važnih razloga javnog interesa posebnim propisom mogu biti izričito propisana ograničenja prijenosa određenih kategorija ličnih podataka drugoj državi ili međunarodnoj organizaciji.
- (7) Kontrolor podataka ili obrađivač dokumentuje procjenu, kao i odgovarajuće zaštitne mjere iz st. (1) i (2) ovog člana, u evidencijama iz člana 32. ovog zakona.

## **POGLAVLJE V. POSEBNI SLUČAJEVI OBRADJE**

### **Član 52.**

#### **(Obrada ličnog podatka i sloboda izražavanja i informisanja)**

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

### **Član 53.**

#### **(Obrada ličnog podatka i javni pristup službenim dokumentima)**

- (1) Javni organ i nadležni organ, u skladu sa zakonom koji se primjenjuje na taj organ, mogu u javnom interesu otkriti lične podatke iz službenih dokumenata kojima raspolažu, kako bi se javni pristup službenim dokumentima uskladio s pravom na zaštitu ličnih podataka u skladu s ovim zakonom.
- (2) Odredbe ovog zakona uzimaju se u obzir prilikom primjene propisa o slobodi pristupa informacijama u Bosni i Hercegovini.

### **Član 54.**

#### **(Obrada jedinstvenog matičnog broja fizičkog lica)**

- (1) Posebni uvjeti za obradu jedinstvenog matičnog broja fizičkog lica ili bilo kojeg drugog identifikatora opće primjene propisuju se posebnim zakonom.

- (2) Jedinstveni matični broj fizičkog lica ili bilo koji drugi identifikator opće primjene iz stava (1) ovog člana obrađuje se samo uz primjenu odgovarajućih zaštitnih mjera u vezi s pravima i slobodama nosioca podataka u skladu s ovim zakonom.

#### **Član 55.**

##### **(Obrada ličnih podataka u kontekstu zaposlenja)**

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

#### **Član 56.**

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

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

## **Član 57.**

### **(Videonadzor)**

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

## **Član 58.**

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

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

## **Član 59.**

### **(Obaveza čuvanja profesionalne tajne)**

- (1) Posebnim propisom može se utvrditi ograničenje Agencije iz člana 103. stava (1) tač. (f) i (g) u vezi s kontrolorom podataka ili obrađivačem koji, na osnovu posebnog

propisa koji je donio nadležni organ, podliježu obavezi profesionalne tajne i drugim jednakovrijednim obavezama tajnosti, ako je to nužno i razmjerno kako bi se uskladilo pravo na zaštitu ličnih podataka s obavezom tajnosti.

- (2) Posebni propis iz stava (1) ovog člana primjenjuje se samo na lične podatke koje je kontrolor podataka ili obrađivač dobio kao rezultat ili primio tokom aktivnosti koja je obuhvaćena obavezom tajnosti.

## **DIO TREĆI – OBRADA LIČNOG PODATKA OD NADLEŽNOG ORGANA KAO KONTROLORA PODATAKA**

### **Član 60.**

#### **(Načela obrade ličnih podataka od nadležnog organa)**

- (1) Načela obrade ličnih podataka od nadležnog organa su:
  - a) zakonitost i pravičnost;
  - b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama;
  - c) smanjenje opsega podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u svrhe u koje se obrađuju;
  - d) tačnost – podaci moraju biti tačni i prema potrebi ažurirani, moraju se preduzeti sve razumne mjere kako bi se osiguralo da lični podaci koji nisu tačni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljani;
  - e) ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nosioca podataka, i to ne duže nego što je potrebno u svrhe u koje se podaci obrađuju;
  - f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigura odgovarajuća sigurnost ličnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacionih mjera.
- (2) Obrada koju vrši isti ili neki drugi nadležni organ u svrhu iz člana 1. stava (1) tačke c) ovog zakona različitu od one za koju su lični podaci prikupljeni dopuštena je:
  - a) ako je nadležni organ ovlašten za obradu takvih ličnih podataka u takvu svrhu u skladu s posebnim propisom ili
  - b) ako je obrada neophodna i proporcionalna drugoj zakonitoj svrsi.
- (3) Obrada koju vrši isti ili neki drugi nadležni organ može uključivati arhiviranje u javnom interesu, u naučne, statističke ili historijske svrhe, za svrhe iz člana 1. stava (1) tačke c) ovog zakona, uz preduzimanje odgovarajućih zaštitnih mjera u vezi s pravima i slobodama nosioca podataka.
- (4) Nadležni organ odgovoran je za usklađenost sa st. (1), (2) i (3) ovog člana i mora biti u mogućnosti dokazati tu usklađenost.

### **Član 61.**

### **(Rok za čuvanje i brisanje ličnog podatka)**

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

### **Član 62.**

#### **(Razlika između različitih kategorija nosilaca podataka)**

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

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

### **Član 63.**

#### **(Razlika između ličnih podataka i provjera kvaliteta ličnih podataka)**

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

### **Član 64.**

#### **(Zakonitost obrade ličnog podatka od nadležnog organa)**

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

## **Član 65.**

### **(Posebni uvjeti obrade)**

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

## **Član 66.**

### **(Obrada posebnih kategorija ličnih podataka od nadležnog organa)**

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

## **Član 67.**

### **(Automatizirano pojedinačno donošenje odluke od nadležnog organa)**

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

## **Član 68.**

### **(Obavještanje i način ostvarivanja prava nosilaca podataka)**

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

#### **Član 69.**

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

- (1) Nadležni organ dužan je nosiocu podataka staviti na raspolaganje kao minimum sljedeće informacije:
  - a) identitet i kontaktne podatke nadležnog organa;
  - b) kontaktne podatke službenika za zaštitu ličnih podataka, ako je primjenjivo;
  - c) svrhu obrade ličnih podataka;
  - d) o pravu na podnošenje pritužbe Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu;
  - e) o postojanju prava da od nadležnog organa zatraži pristup svojim ličnim podacima, njihovu ispravku ili brisanje, ili ograničenje obrade ličnih podataka.
- (2) Osim informacija iz stava (1) ovog člana, radi ostvarivanja njegovih prava, nadležni organ nosiocu podataka daje sljedeće dodatne informacije:
  - a) pravni osnov obrade ličnih podataka;

- b) rok u kojem će se lični podaci čuvati ili, ako to nije moguće, o kriterijima korištenim za utvrđivanje tog roka;
  - c) o kategorijama primalaca ličnih podataka, uključujući druge države ili međunarodne organizacije, ako je primjenjivo;
  - d) prema potrebi i dodatne informacije ako se lični podaci prikupljaju bez znanja nosioca podataka.
- (3) Posebnim zakonom mogu se propisati mjere za odgađanje, ograničenje ili uskraćivanje pružanja informacija iz stava (2) ovog člana nosiocu podataka u onoj mjeri i u onom trajanju u kojem takva mjera predstavlja potrebnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje osnovnih prava i legitimnih interesa nosioca podataka, s ciljem da se:
- a) spriječi ometanje službenog i zakonom uređenog prikupljanja informacija, istraga ili postupaka;
  - b) izbjegne ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinitelja krivičnih djela ili izvršavanja krivičnih sankcija;
  - c) zaštititi javna sigurnost;
  - d) zaštititi državna sigurnost;
  - e) zaštite prava i slobode drugih.
- (4) Posebnim zakonom mogu se propisati kategorije obrade koje mogu u cjelini ili djelomično biti obuhvaćene bilo kojom od tačaka iz stava (3) ovog člana.

## **Član 70.**

### **(Pravo nosioca podataka na pristup ličnom podatku kod nadležnog organa)**

- (1) Nadležni organ dužan je, u roku od 30 dana od dana zaprimanja zahtjeva za pristup ličnim podacima, nosiocu podataka izdati potvrdu o tome obrađuje li njegove lične podatke te ako se takvi lični podaci obrađuju, pristup ličnim podacima i informacijama o:
- a) svrsi obrade i pravnom osnovu obrade;
  - b) kategoriji ličnih podataka koji se obrađuju;
  - c) primaocu ili kategoriji primaoca kojem su lični podaci otkriveni, posebno primaocu u drugoj državi ili međunarodnoj organizaciji;
  - d) predviđenom roku u kojem će se lični podaci čuvati, ako je to moguće, ili, ako to nije moguće, kriterijima korištenim za utvrđivanje tog roka;
  - e) postojanju prava da od nadležnog organa zatraži ispravku ili brisanje svojih ličnih podataka ili ograničenje obrade ličnih podataka;
  - f) pravu na podnošenje pritužbe Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu;
  - g) ličnim podacima koji se obrađuju i o svim dostupnim informacijama o izvoru ličnih podataka.
- (2) Potvrda iz stava (1) ovog člana izdaje se u skladu s odredbama člana 71. ovog zakona.

## **Član 71.**

### **(Ograničenja prava pristupa ličnom podatku)**

- (1) Posebnim zakonom koji se odnosi na nadležni organ može se nosiocu podataka u cjelini ili djelomično ograničiti pravo pristupa ličnom podatku u onoj mjeri i u onom trajanju u kojem takvo djelomično ili potpuno ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje osnovnih prava i legitimnih interesa nosioca podataka, kako bi se:
  - a) spriječilo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka;
  - b) izbjeglo ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca krivičnih djela ili izvršavanja krivičnih sankcija;
  - c) zaštitila javna sigurnost;
  - d) zaštitila državna sigurnost;
  - e) zaštitila prava i slobode drugih.
- (2) Posebnim zakonom mogu se odrediti kategorije obrade koje mogu u cjelini ili djelomično biti obuhvaćene bilo kojom tačkom iz stava (1) ovog člana.
- (3) U slučajevima iz st. (1) i (2) ovog člana, nadležni organ dužan je, bez odgađanja, pisanim putem obavijestiti nosioca podataka o svakom odbijanju ili ograničenju pristupa ličnim podacima te o razlozima odbijanja ili ograničenja, osim ako bi pružanje takvih informacija dovelo u pitanje neku od svrha iz stava (1) ovog člana.
- (4) Nadležni organ dužan je obavijestiti nosioca podataka o mogućnosti podnošenja pritužbe Agenciji ili tužbe nadležnom sudu.
- (5) Nadležni organ dužan je dokumentirati činjenične ili pravne razloge na kojima se zasniva odluka.
- (6) Dokumentacija iz stava (5) ovog člana stavlja se Agenciji na raspolaganje.

## **Član 72.**

### **(Pravo na ispravku ili brisanje ličnog podatka i ograničenje obrade od nadležnog organa)**

- (1) Nadležni organ dužan je:
  - a) bez nepotrebnog odgađanja, nosiocu podataka omogućiti ispravku netačnih ličnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade podataka, nosilac podataka ima pravo dopuniti nepotpune lične podatke, između ostalog i davanjem dodatne izjave;
  - b) nosiocu podataka omogućiti brisanje ličnih podataka, bez nepotrebnog odgađanja, ako se obradom krše odredbe čl. 60., 64. ili 66. ovog zakona, ili ako se lični podaci moraju brisati radi poštovanja pravne obaveze iz posebnog zakona;
  - c) ograničiti obradu ako:
    - 1) nosilac podataka osporava tačnost ličnih podataka, a njihovu tačnost ili netačnost nije moguće utvrditi ili
    - 2) lični podaci moraju biti sačuvani kao dokaz;
  - d) obavijestiti nosioca podataka prije uklanjanja ograničenja obrade ako je obrada ograničena na osnovu tačke c) alineje 1) ovog stava;

- e) pisanim putem obavijestiti nosioca podataka o svakom odbijanju ispravke ili brisanja ličnih podataka ili ograničenja obrade te o razlozima odbijanja. Posebnim zakonom koji se odnosi na nadležni organ može se nosiocu podataka potpuno ili djelomično ograničiti pravo pristupa u onoj mjeri i u onom trajanju u kojem takvo potpuno ili djelomično ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje osnovnih prava i legitimnih interesa nosioca podataka, kako bi se:
- 1) izbjeglo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka,
  - 2) izbjeglo ometanje sprečavanja, istrage i otkrivanja krivičnih djela ili gonjenja počinioca djela ili izvršavanja krivičnih sankcija,
  - 3) zaštitila javna sigurnost,
  - 4) zaštitila državna sigurnost i
  - 5) zaštitila prava i slobode drugih;
- f) obavijestiti nosioca podataka o mogućnosti podnošenja pritužbe Agenciji ili tužbe nadležnom sudu;
- g) o ispravci netačnih ličnih podataka obavijestiti nadležni organ od kojeg potiču netačni podaci.
- (2) Nadležni organ dužan je, ako su lični podaci ispravljani ili brisani, ili je obrada bila ograničena na osnovu stava (1) tač. a), b) ili c) ovog člana, obavijestiti primaoca, a primaoci su dužni ispraviti ili obrisati lične podatke ili ograničiti obradu ličnih podataka u okviru svoje odgovornosti.

### **Član 73.**

#### **(Ostvarivanje prava nosilaca podataka i provjera Agencije)**

- (1) Nadležni organ dužan je obavijestiti nosioca podataka o mogućnosti ostvarivanja prava putem pritužbe Agenciji ili tužbe nadležnom sudu.
- (2) Ako je nosilac podataka nezadovoljan postupkom nadležnog organa, može podnijeti pritužbu Agenciji ili tužbu nadležnom sudu, u slučajevima iz člana 69. stava (3), člana 71. stava (3) i člana 72. stava (1) tačke d) ovog zakona.
- (3) U slučaju iz stava (1) ovog člana, Agencija je dužna obavijestiti nosioca podataka o tome da su izvršene provjere i nadzor kao i o pravu na pravni lijek.

### **Član 74.**

#### **(Prava nosioca podataka u krivičnim istragama i postupcima)**

Nosilac podataka ostvaruje prava iz čl. 69., 70. i 72. ovog zakona u skladu sa zakonima o krivičnim postupcima, ako su lični podaci sadržani u sudskoj odluci ili evidenciji ili spisu predmeta obrađeni tokom krivičnih istraga i postupaka.

### **Član 75.**

#### **(Obaveza nadležnog organa)**

- (1) Nadležni organ dužan je da primijeni odgovarajuće tehničke i organizacione mjere imajući u vidu prirodu, opseg, okolnosti i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode fizičkih lica, kako bi osigurao da se obrada vrši u skladu s

ovim zakonom i kako bi to mogao dokazati. Te mjere se prema potrebi preispituju i ažuriraju.

- (2) Mjere iz stava (1) ovog člana, ako su proporcionalne u odnosu na aktivnosti obrade, uključuju provođenje odgovarajućih politika zaštite podataka od nadležnog organa.

#### **Član 76.**

##### **(Tehnička i integrirana zaštita ličnog podatka od nadležnog organa)**

- (1) Nadležni organ dužan je, uzimajući u obzir najnovija dostignuća i trošak provođenja kao i prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih nivoa vjerovatnoće i ozbiljnosti za prava i slobode lica koji proizlaze iz obrade podataka, i u vrijeme određivanja sredstava obrade i u vrijeme same obrade, primijeniti odgovarajuće tehničke i organizacione mjere, poput pseudonimizacije, za omogućavanje djelotvorne primjene načela zaštite podataka, kao što je smanjenje količine podataka te uključivanje zaštitnih mjera u obradu, kako bi se ispunili zahtjevi iz ovog zakona i zaštitila prava nosioca podataka.
- (2) Mjere iz stava (1) ovog člana odnose se na količinu prikupljenih ličnih podataka, opseg njihove obrade, rok njihovog čuvanja i njihovu dostupnost, čime se osigurava da lični podaci nisu automatski, bez intervencije fizičkog lica, dostupni neograničenom broju lica.

#### **Član 77.**

##### **(Nadležni organ kao zajednički kontrolor podataka)**

- (1) Ako dva ili više nadležnih organa odrede svrhe i načine obrade ličnih podataka, smatra se da su zajednički kontrolori podataka. Oni na transparentan način međusobnim sporazumom određuju odgovornosti svakoga od njih s ciljem izvršavanja obaveza iz ovog zakona, posebno u vezi s ostvarivanjem prava nosilaca podataka i dužnostima svakoga od njih u vezi s pružanjem informacija iz člana 69. ovog zakona, osim ako su odgovornosti nadležnih organa utvrđene zakonom koji se primjenjuje na te nadležne organe. Sporazumom se određuje kontaktna tačka za nosioca podataka. Zakonom se može odrediti koji od zajedničkih kontrolora podataka može djelovati kao jedinstvena kontaktna tačka za ostvarivanje prava nosioca podataka.
- (2) Nezavisno od uvjeta sporazuma iz stava (1) ovog člana, nosilac podataka može ostvarivati svoja prava iz ovog zakona u odnosu sa svakim nadležnim organom i protiv svakog od njih.

#### **Član 78.**

##### **(Korištenje usluge obrađivača od nadležnog organa)**

- (1) Nadležni organ koristi uslugu samo onog obrađivača koji može u dovoljnoj mjeri osigurati provođenje odgovarajućih tehničkih i organizacionih mjera propisanih ovim zakonom.
- (2) Korištenje usluge obrađivača od nadležnog organa uređuje se ugovorom ili drugim pravnim aktom kojim se uređuju predmet, tehničke i organizacione mjere propisane ovim zakonom, trajanje obrade, opseg, sadržaj i svrha obrade, vrsta ličnih podataka, kategorije nosilaca podataka te obaveze i prava nadležnog organa, kao i da obrađivač:
  - a) djeluje samo prema uputstvima nadležnog organa;
  - b) osigurava da su se lica ovlaštena za obradu ličnih podataka obavezala na poštovanje povjerljivosti ili da podliježu zakonskim odredbama o povjerljivosti;

- c) bilo kojim odgovarajućim sredstvom pomaže nadležnom organu osigurati usklađenost s odredbama o pravima nosioca podataka;
  - d) prema izboru nadležnog organa, briše ili vraća nadležnom organu sve lične podatke nakon završetka pružanja usluge obrade podataka te briše postojeće kopije, osim ako prema nekoj zakonskoj odredbi ne postoji obaveza čuvanja ličnih podataka;
  - e) nadležnom organu stavlja na raspolaganje sve informacije potrebne za pridržavanje odredbi ovoga člana;
  - f) poštuje odredbe stava (3) ovoga člana za angažovanje drugog obrađivača.
- (3) Obradivač ne može koristiti uslugu drugog obrađivača bez prethodnog pisanog odobrenja nadležnog organa.
- (4) Po zaprimanju odobrenja obrađivač je dužan obavijestiti nadležni organ o svim planiranim izmjenama u vezi s korištenjem usluge drugih obrađivača.
- (5) Nadležni organ može uskratiti saglasnost obrađivaču za korištenje usluge drugog obrađivača.
- (6) Ako obrađivač utvrđuje svrhe i načine obrade kršeći odredbe ovoga zakona, taj se obrađivač smatra nadležnim organom u vezi s obradom koja mu je povjerena.

#### **Član 79.**

##### **(Obrada pod kontrolom nadležnog organa)**

Lice koje djeluje pod kontrolom nadležnog organa ili obrađivača, a ima pristup ličnim podacima, ne smije obrađivati te podatke bez naloga kontrolora podataka, osim kada je to propisano posebnim zakonom.

#### **Član 80.**

##### **(Evidencija o obradi od nadležnog organa)**

- (1) Nadležni organ vodi evidenciju obrade za koju je odgovoran. Ta evidencija sadrži sljedeće informacije:
- a) naziv i kontaktne podatke nadležnog organa, zajedničkog nadležnog organa i službenika za zaštitu ličnih podataka;
  - b) svrhu obrade;
  - c) kategoriju primaoca kome su lični podaci otkriveni ili će mu biti otkriveni, uključujući primaoca u drugoj državi ili međunarodnoj organizaciji;
  - d) opis kategorije nosioca podataka i kategorije ličnih podataka;
  - e) upotrebu izrade profila, ako je primjenjivo;
  - f) kategoriju prijenosa ličnih podataka u drugu državu ili međunarodnu organizaciju, ako je primjenjivo;
  - g) pravni osnov za postupak obrade, uključujući prijenose, kojem su lični podaci namijenjeni;
  - h) predviđene rokove za brisanje različitih kategorija ličnih podataka, ako je moguće;
  - i) opći opis tehničkih i organizaciono-sigurnosnih mjera iz člana 85. stava (1) ovog zakona, ako je moguće.

(2) Nadležni organ osigurava da svaki obrađivač vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju u ime kontrolora podataka, a koja sadrži:

- a) ime i kontaktne podatke jednog ili više obrađivača i svakog kontrolora podataka u čije ime obrađivač djeluje te službenika za zaštitu podataka, ako je primjenjivo;
- b) kategoriju obrade koja se provodi za svakog kontrolora podataka;
- c) ako je primjenjivo, podatke o prijenosu ličnih podataka u drugu državu ili međunarodnu organizaciju, ako za to postoji izričito uputstvo kontrolora podataka, uključujući identifikaciju te druge države ili međunarodne organizacije;
- d) ako je moguće, opći opis tehničkih i organizaciono-sigurnosnih mjera iz člana 85. stava (1).

(3) Evidencija iz stava (1) ovog člana mora biti u pisanom obliku, što uključuje elektronski oblik.

(4) Nadležni organ na zahtjev Agencije, prilikom nadzora, stavlja evidenciju na uvid.

### **Član 81.**

#### **(Zapisivanje)**

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

### **Član 82.**

#### **(Saradnja nadležnog organa i obrađivača s Agencijom)**

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

### **Član 83.**

#### **(Procjena uticaja na zaštitu ličnog podatka od nadležnog organa)**

- (1) Nadležni organ prije obrade vrši procjenu uticaja predviđenih postupaka obrade na zaštitu ličnih podataka ako je vjerovatno da će neka vrsta obrade, posebno primjenom novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe te obrade, prouzrokovati visoki rizik za prava i slobode lica.
- (2) Procjena iz stava (1) ovog člana mora sadržavati najmanje opći opis predviđenih postupaka obrade, procjenu rizika za prava i slobode nosioca podataka, predviđene mjere za rizike, zaštitne i sigurnosne mjere i mehanizme kako bi se osigurala zaštita ličnih podataka i dokazala usklađenost s ovim zakonom, uzimajući u obzir prava i legitimne interese nosioca podataka i drugih uključenih lica.

## **Član 84.**

### **(Prethodno savjetovanje nadležnog organa s Agencijom)**

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

## **Član 85.**

### **(Sigurnost obrade od nadležnog organa i obrađivača)**

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

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

## **Član 86.**

### **(Obavješćavanje Agencije o povredi ličnog podatka od nadležnog organa)**

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

## **Član 87.**

### **(Obavještavanje nosioca podatka o povredi ličnog podatka)**

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

## **Član 88.**

### **(Imenovanje službenika za zaštitu ličnih podataka od nadležnog organa)**

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