

NACRT

„EI“

Na temelju članka IV. 4. a) Ustava Bosne i Hercegovine, Parlamentarna skupština Bosne i Hercegovine, na __. sjednici Zastupničkog doma, održanoj _____. godine, i na __. sjednici Doma naroda, održanoj _____. godine, usvojila je

ZAKON

O ZAŠTITI OSOBNIH PODATAKA

DIO PRVI – OPĆE ODREDBE

Članak 1.

(Predmet)

(1) Ovim Zakonom propisuju se:

- a) pravila u vezi sa zaštitom fizičkih osoba u pogledu obrade osobnih podataka i pravila povezana sa slobodnim kretanjem osobnih podataka
- b) nadležnosti Agencije za zaštitu osobnih podataka u Bosni i Hercegovini (u daljnjem tekstu: Agencija), organizacija i upravljanje, kao i druga pitanja značajna za njezin rad i zakonito funkcioniranje
- c) zaštita fizičkih osoba u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprječavanja, istrage i otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela, izvršavanje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje.

(2) Ovim Zakonom vrši se usklađivanje s odredbama Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i odredbama Direktive (EU) 2016/680 Europskog parlamenta i Vijeća o zaštiti pojedinaca u vezi s obradom osobnih podataka od nadležnih tijela s ciljem sprječavanja, istrage i otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela ili izvršavanje kaznenih sankcija i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP.

(3) Navođenje odredbi Uredbe i Direktive iz stavka (2) ovog članka vrši se isključivo s ciljem praćenja i informiranja o preuzimanju pravne stečevine Europske unije u zakonodavstvu Bosne i Hercegovine.

Članak 2.

(Cilj Zakona)

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

Članak 3.

(Uporaba muškog ili ženskog roda)

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

Članak 4.

(Definicije)

Pojedini izrazi upotrijebljeni u ovom Zakonu imaju sljedeća značenja:

- a) „osobni podatak“ je svaki podatak koji se odnosi na fizičku osobu čiji je identitet utvrđen ili se može utvrditi
- b) „nositelj podataka“ je fizička osoba čiji je identitet utvrđen ili čiji se identitet može utvrditi, posredno ili neposredno, posebno s pomoću identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili s pomoću jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili društveni identitet te osobe
- c) „obrada“ je svaki postupak ili skup postupaka koji se vrši na osobnim podacima ili na skupovima osobnih podataka, automatiziranim ili neautomatiziranim sredstvima, kao što su prikupljanje, evidentiranje, organizacija, strukturiranje, čuvanje, prilagođavanje ili izmjena, pronalaženje, vršenje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničenje, brisanje ili uništavanje
- d) „ograničenje obrade“ je obilježavanje čuvanog osobnog podatka s ciljem ograničenja njegove obrade u budućnosti
- e) „izrada profila“ je svaki oblik automatske obrade osobnog podatka koji se sastoji od korištenja osobnog podatka za procjenu određenih osobnih aspekata u vezi s fizičkom osobom, posebno za analizu ili predviđanje aspekata u vezi s radnim rezultatom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanosti, ponašanjem, lokacijom ili kretanjem te fizičke osobe
- f) „pseudonimizacija“ je obrada osobnog podatka tako da se osobni podatak više ne može pripisati određenom nositelju podataka bez korištenja dodatnih informacija, uz uvjet da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podatak ne može pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi

- g) „zbirka osobnih podataka“ je svaki strukturirani skup osobnih podataka koji su dostupni u skladu s posebnim kriterijima, bez obzira na to jesu li centralizirani, decentralizirani ili rasprostranjeni na funkcionalnoj ili zemljopisnoj osnovi
- h) „kontrolor podataka“ je fizička ili pravna osoba, javno tijelo ili nadležno tijelo koje samostalno ili s drugim određuje svrhe i sredstva obrade osobnih podataka. Kada su svrhe i sredstva takve obrade utvrđeni zakonom, kontrolor podataka ili posebni kriteriji za njegovo imenovanje propisuju se zakonom
- i) „javno tijelo“ je svako zakonodavno, izvršno i sudsko tijelo na svim razinama vlasti u Bosni i Hercegovini
- j) „nadležno tijelo“ je tijelo koje je nadležno za sprječavanje, istragu i otkrivanje kaznenih djela, gonjenje počinitelja kaznenih djela ili izvršenje kaznenih sankcija, uključujući i zaštitu i sprječavanje prijetnji javnoj sigurnosti, kao i pravne osobe ako su zakonom ovlaštene za vršenje tih poslova, kao posebna kategorija kontrolora podataka
- k) „obrađivač“ je fizička ili pravna osoba, javno tijelo koje obrađuje osobne podatke u ime kontrolora podataka
- l) „primatelj“ je fizička ili pravna osoba, javno tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li u pitanju treća strana. Javna tijela koja mogu primiti osobne podatke u okviru određene istrage u skladu sa zakonom ne smatraju se primateljima, ali obrada tih podataka mora biti u skladu s važećim pravilima o zaštiti podataka prema svrhama obrade
- m) „treća strana“ znači fizička ili pravna osoba, javno tijelo, Agencija ili drugo tijelo koje nije nositelj podataka, kontrolor podataka, obrađivač ni osobe koje su ovlaštene za obradu osobnih podataka pod neposrednom nadležnošću kontrolora podataka ili obrađivača
- n) „suglasnost“ nositelja podataka je svako dobrovoljno, posebno, informirano i nedvosmisleno izražavanje volje nositelja podataka kada on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose
- o) „povreda osobnog podatka“ je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, čuvani ili na drugi način obrađivani
- p) „genetski podatak“ je osobni podatak koji se odnosi na naslijeđena ili stečena genetska obilježja fizičke osobe koja daju jedinstvene informacije o fiziologiji ili zdravlju te fizičke osobe i koji su dobiveni posebnom analizom biološkog uzorka te fizičke osobe
- r) „biometrijski podatak“ je osobni podatak dobiven posebnom tehničkom obradom u vezi s fizičkim osobinama, fiziološkim obilježjima ili obilježjima ponašanja fizičke osobe koja omogućavaju ili potvrđuju jedinstvenu identifikaciju te fizičke osobe, kao što su fotografije osoba ili daktiloskopski podaci
- s) „podatak koji se odnosi na zdravlje“ je osobni podatak u vezi s fizičkim ili mentalnim zdravljem fizičke osobe, uključujući pružanje zdravstvenih usluga, koji daje informacije o njegovom zdravstvenom stanju
- t) „predstavnik“ je fizička ili pravna osoba s prebivalištem ili boravištem, odnosno sjedištem ili poslovnim nastanom u Bosni i Hercegovini koju je kontrolor podataka ili obrađivač pisanim putem imenovao u skladu s člankom 29. ovog Zakona

- u) „gospodarski subjekt“ je fizička ili pravna osoba koja obavlja gospodarsku djelatnost, bez obzira na pravni oblik te djelatnosti
- v) „skupina gospodarskih subjekata“ je gospodarski subjekt koji ostvaruje kontrolu i gospodarski subjekti koji su pod njegovom kontrolom
- z) „obvezujuće poslovno pravilo“ su politike zaštite osobnih podataka kojih se kontrolor podataka i obrađivač sa sjedištem ili poslovnim nastanom u Bosni i Hercegovini pridržava prilikom prijenosa ili skupova prijenosa osobnih podataka kontroloru podataka ili obrađivaču u jednoj ili više drugih država u okviru skupine gospodarskih subjekata ili skupine gospodarskih subjekata koji se bave zajedničkom gospodarskom djelatnošću
- aa) „usluga informacijskog društva“ je svaka usluga koja se obično pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga, gdje:
 - 1) „na daljinu“ znači da se usluga pruža a da pri tome strane nisu istodobno prisutne
 - 2) „elektroničkim sredstvima“ znači da se usluga na početku šalje i prima na određitu pomoću elektroničke opreme za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radio-vezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima
 - 3) „na osobni zahtjev primatelja usluga“ znači da se usluga pruža prijenosom podataka na osobni zahtjev
- bb) „međunarodna organizacija“ je organizacija sa svojim tijelima uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na temelju sporazuma osnovale dvije ili više zemalja
- cc) „poslovni nastan“ je djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana
- dd) „videonadzor“ je informacijsko-komunikacijski sustav koji ima mogućnost prikupljanja i daljnje obrade osobnih podataka, koji obuhvaća stvaranje snimka koji čini ili je namijenjen da čini dio sustava skladištenja.

Članak 5.

(Glavno područje primjene)

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

Članak 6.

(Teritorijalno područje primjene)

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

DIO DRUGI – OBRADA OSOBNOG PODATKA OD STRANE FIZIČKE OSOBE, PRAVNE OSOBE ILI JAVNOG TIJELA KAO KONTROLORA PODATAKA

POGLAVLJE I. NAČELA OBRADE OSOBNOG PODATKA

Članak 7.

(Načela obrade osobnog podatka)

- (1) Načela obrade osobnog podatka su:
 - a) zakonitost, pravičnost i transparentnost u odnosu na nositelja podataka
 - b) ograničenje svrhe – podaci moraju biti prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama. Daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 56. stavkom (1) ovog Zakona ne smatra se neusklađenom s prvobitnim svrhama
 - c) smanjenje opsega podataka – podaci moraju biti primjereni, relevantni i ograničeni na ono što je neophodno u odnosu na svrhe u koje se obrađuju
 - d) točnost – podaci moraju biti točni i prema potrebi ažurirani. Moraju se poduzeti sve razumne mjere kako bi se osiguralo da osobni podaci, koji nisu točni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni
 - e) ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nositelja podataka, i to ne duže nego što je potrebno u svrhe u koje se osobni podaci obrađuju. Osobni podaci se mogu čuvati na duže razdoblje ako će se osobni podaci

obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 56. stavkom (1) ovog Zakona, što podliježe provođenju primjerenih tehničkih i organizacijskih mjera propisanih ovim Zakonom radi zaštite prava i sloboda nositelja podataka

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

Članak 8.

(Zakonitost obrade osobnog podatka)

- (1) Obrada osobnog podatka je zakonita samo ako je ispunjen najmanje jedan od sljedećih uvjeta:
- a) ako je nositelj podataka dao suglasnost za obradu svojih osobnih podataka u jednu ili više posebnih svrha
 - b) ako je obrada neophodna radi izvršenja ugovora u kojem je nositelj podataka ugovorna strana ili radi poduzimanja radnji na zahtjev nositelja podataka prije zaključenja ugovora
 - c) ako je obrada neophodna radi poštovanja pravnih obveza kontrolora podataka
 - d) obrada je neophodna radi zaštite ključnih interesa nositelja podataka ili druge fizičke osobe
 - e) ako je obrada neophodna za izvršenje zadatka koji se vrši u javnom interesu ili u okviru izvršavanja službenih ovlasti kontrolora podataka
 - f) ako je obrada neophodna zbog legitimnih interesa kontrolora podataka ili treće strane, osim kada nad tim interesima pretežu interesi ili temeljna prava i slobode nositelja podataka, a koji zahtijevaju zaštitu osobnih podataka, posebno ako je nositelj podataka dijete. Ova se točka ne primjenjuje na obradu koju vrše javna tijela pri vršenju svojih poslova.
- (2) Pravni temelj za obradu osobnog podatka iz stavka (1) toč. c) i e) ovog članka utvrđuje se posebnim zakonom, tako da se preciznije propišu posebni uvjeti za obradu te druge mjere za osiguranje zakonite i pravične obrade, među ostalim i za druge posebne obrade kako je to predviđeno u poglavlju V. ovog Zakona.
- (3) Posebnim zakonom, za obradu podatka iz stavka (1) toč. c) i e) ovog članka, propisuje se svrha obrade, koja u pogledu obrade iz stavka (1) točke e) ovog članka mora biti neophodna za izvršenje zadatka koji se obavlja u javnom interesu ili u okviru izvršavanja službenih ovlasti kontrolora podataka. Tim zakonom propisuju se: opći uvjeti kojima se uređuje zakonitost obrade koju vrši kontrolor podataka, vrste podataka koji se obrađuju, kategorije nositelja podataka, subjekti kojima se osobni podaci mogu otkriti i svrhe u koje se podaci mogu otkriti, ograničenje svrhe, rokovi čuvanja te radnje obrade i postupci obrade, uključujući i mjere za osiguranje zakonite i 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 razmjerna zakonitom cilju kojem se teži.

- (4) Ako se obrada vrši u svrhu koja je različita od svrhe u koju su osobni podaci prikupljeni i ne zasniva se na suglasnosti nositelja podataka ili posebnom zakonu koji predstavlja neophodnu i razmjernu mjeru u demokratskom društvu za zaštitu ciljeva iz članka 25. stavka (1) ovog Zakona, kontrolor podataka, s ciljem utvrđivanja je li obrada u drugu svrhu u skladu sa svrhom u koju su osobni podaci prvobitno prikupljeni, uzima u obzir, među ostalim:
- a) svaku vezu između svrha u koje su osobni podaci prikupljeni i svrha namjeravane daljnje obrade
 - b) kontekst u kojem su osobni podaci prikupljeni, posebno u pogledu odnosa između nositelja podataka i kontrolora podataka
 - c) prirodu osobnih podataka, posebno činjenicu obrađuju li se posebne kategorije osobnih podataka u skladu s člankom 11. ovog Zakona ili osobni podaci koji se odnose na kaznenu osuđivanost i kaznena djela u skladu s člankom 12. ovog Zakona
 - d) moguće posljedice namjeravane daljnje obrade za nositelje podataka
 - e) postojanje odgovarajućih mjera zaštite, koje mogu uključivati enkripciju ili pseudonimizaciju.
- (5) Javna i nadležna tijela entiteta i Brčko Distrikta su dužna, 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.

Članak 9.

(Suglasnost)

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

Članak 10.

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

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

Članak 11.

(Obrada posebnih kategorija osobnih podataka)

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

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

Članak 12.

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

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

Članak 13.

(Obrada za koju nije potrebna identifikacija)

- (1) Ako kontrolor podataka obrađuje osobne podatke za čiju svrhu obrade ne zahtijeva ili više ne zahtijeva identificiranje nositelja podataka, kontrolor podataka nije dužan čuvati, pribavljati ili obrađivati dodatne informacije radi identifikacije nositelja podataka samo radi poštovanja ovog Zakona.

- (2) Ako u slučajevima iz stavka (1) ovog članka kontrolor podataka može dokazati da ne može identificirati nositelja podataka, kontrolor podataka o tome, na odgovarajući način, obavještava nositelja podataka, ako je moguće. U tim slučajevima se ne primjenjuju čl. 17. do 22. ovog Zakona, osim u slučaju da nositelj podataka u svrhu ostvarivanja svojih prava iz tih članaka pruži dodatne informacije koje omogućavaju njegovu identifikaciju.

POGLAVLJE II. PRAVA NOSITELJA PODATAKA

Članak 14.

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

- (1) Kontrolor podataka poduzima odgovarajuće mjere kako bi se nositelju podataka pružile sve informacije iz čl. 15. i 16. ovog Zakona i svi vidovi komunikacije za ostvarivanje prava iz čl. 17. do 24. ovog Zakona i članka 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 elektronički oblik kada je primjereno. Ako nositelj podataka zahtijeva, informacije se mogu pružiti usmeno, uz uvjet da je identitet nositelja podataka utvrđen drugim sredstvima.
- (2) Kontrolor podataka olakšava ostvarivanje prava nositelja podataka iz čl. 17. do 24. ovog Zakona. U slučajevima iz članka 13. stavka (1) ovog Zakona kontrolor podataka ne smije odbiti postupiti po zahtjevu nositelja podataka za ostvarivanje njegovih prava iz čl. 17. do 24. ovog Zakona, osim ako kontrolor podataka dokaže da ne može utvrditi identitet nositelja podataka.
- (3) Kontrolor podataka nositelju podataka na njegov zahtjev pruža informacije o poduzetim radnjama iz čl. 17. 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 nositelja podataka o svakom takvom produženju u roku od 30 dana od dana zaprimanja zahtjeva, pri čemu navodi razloge za odgađanje. Ako nositelj podataka podnese zahtjev elektroničkim putem, informacije se pružaju elektroničkim putem ako je to moguće, osim u slučaju kada nositelj podataka zahtijeva drugačije.
- (4) Ako kontrolor podataka ne postupi po zahtjevu nositelja podataka, dužan je bez odgađanja, a najkasnije 30 dana od dana zaprimanja zahtjeva, obavijestiti nositelja 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 članka 36. ovog Zakona pružaju se bez naknade. Ako su zahtjevi nositelja podataka očito neutemeljeni ili pretjerani, posebice zbog učestalog ponavljanja, kontrolor podataka može:

- a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi 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 neutemeljenosti ili pretjeranosti zahtjeva je na kontroloru podataka.
- (7) Ako kontrolor podataka ima opravdane sumnje u pogledu identiteta fizičke osobe koja podnosi zahtjev iz čl. 17. do 23. ovog Zakona, on može, ne dovodeći u pitanje članak 13. ovog Zakona, zatražiti dodatne informacije neophodne za potvrđivanje identiteta nositelja podataka.
- (8) Informacije koje moraju biti pružene nositeljima podataka, u skladu s čl. 15. i 16. ovog Zakona, mogu se pružiti u kombinaciji sa standardiziranim simbolima, kako bi se na lako vidljiv, razumljiv i jasno čitljiv način pružio logičan pregled namjeravane obrade. Ako su simboli prikazani elektronički, moraju biti strojno čitljivi.
- (9) Agencija je ovlaštena donijeti propise u svrhu određivanja informacija koje se prikazuju simbolima i postupke za utvrđivanje standardiziranih simbola.

Članak 15.

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

- (1) Ako se osobni podatak prikuplja od nositelja podataka, kontrolor podataka u trenutku prikupljanja osobnog podatka nositelju podataka pruža sljedeće informacije:
- 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 temelj za obradu te svrhu obrade osobnog podatka
 - d) legitimni interes kontrolora podataka ili treće osobe, ako je obrada utemeljena u članku 8. stavku (1) točki f) ovog Zakona
 - e) o primatelju ili kategoriji primatelja osobnih podataka, ako ih ima
 - f) činjenicu da kontrolor podataka namjerava prenijeti osobne 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 članka 51. stavka (2) ovog Zakona, upućivanje na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove preslike ili mjesto na kojem su stavljene na raspolaganje, ako je primjenjivo.
- (2) Osim informacija iz stavka (1) ovog članka, kontrolor podataka u trenutku prikupljanja osobnog podatka, pruža nositelju podataka sljedeće dodatne informacije, ako je to neophodno da bi se osigurala pravična i transparentna obrada:
- a) o roku u kojem će se osobni 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 osobnom podatku, ispravka ili brisanje osobnog podatka ili ograničenje obrade u vezi s nositeljem podataka ili prava na ulaganje prigovora na obradu takvog podatka, te prava na prenosivost podatka
 - c) o pravu da se suglasnost povuče u bilo kojem trenutku, bez utjecaja na zakonitost obrade koja se zasnivala na suglasnosti prije njezinog povlačenja, ako je obrada zasnovana na članku 8. stavku (1) točki a) ovog Zakona ili članku 11. stavku (2) točki a) ovog Zakona
 - d) o pravu na podnošenje pritužbe Agenciji ili tužbe nadležnom sudu
 - e) informacije o tome je li davanje osobnog podatka zakonska ili ugovorna obveza ili neophodan uvjet za zaključenje ugovora, kao i ima li nositelj podataka obvezu dati osobni podatak i koje su moguće posljedice ako se takav podatak ne pruži
 - f) o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz članka 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 nositelja podataka.
- (3) Ako kontrolor podataka namjerava dodatno obrađivati osobne podatke u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade nositelju podataka pruža informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stavka (2) ovog članka.
- (4) Kontrolor podataka nije dužan pružiti informacije nositelju podataka iz st. (1), (2) i (3) ovog članka u onoj mjeri u kojoj nositelj podataka već raspolaže tim informacijama.

Članak 16.

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

- (1) Ako osobni podatak nije dobiven od nositelja podataka, kontrolor podataka pruža nositelju podataka sljedeće informacije:
- 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 temelju za obradu i svrhe obrade kojoj su namijenjeni osobni podaci
 - d) o kategorijama osobnih podataka koji se obrađuju
 - e) o primatelju ili kategorijama primatelja osobnih podataka, prema potrebi
 - f) o činjenicama da kontrolor podataka namjerava osobne podatke prenijeti primatelju u drugoj državi ili međunarodnoj organizaciji i postojanju ili nepostojanju odluke Vijeća ministara Bosne i Hercegovine o adekvatnosti iz članka 47. stavka (3) ovog Zakona ili u slučaju prijenosa osobnih podataka iz čl. 48. ili 49. ovog Zakona ili članka 51. stavka (2) ovog Zakona, upućivanje na primjerene ili odgovarajuće zaštitne mjere i načine dobivanja njihove preslike ili mjesta na kojem su stavljene na raspolaganje, ako je primjenjivo.
- (2) Osim informacija iz stavka (1) ovog članka, kontrolor podataka pruža nositelju podataka sljedeće informacije ako je to neophodno da bi se osigurala pravična i transparentna obrada u odnosu na nositelja podataka:

- a) o roku u kojem će se osobni podatak čuvati ili, ako to nije moguće, kriterije koji se koriste za određivanje tog roka
 - b) o legitimnim interesima kontrolora podataka ili treće osobe ako je obrada utemeljena na članku 8. stavku (1) točki f) ovog Zakona
 - c) o pravu da se od kontrolora podataka zatraži pristup osobnim podacima, ispravka ili brisanje osobnih podataka ili ograničenje obrade u vezi s nositeljem podataka i pravu na prigovor na obradu, kao i pravu na prenosivost podataka
 - d) o pravu da se suglasnost povuče u bilo kojem trenutku, bez utjecaja na zakonitost obrade zasnovane na suglasnosti prije povlačenja, ako je obrada zasnovana na članku 8. stavku (1) točki a) ovog Zakona ili članku 11. stavku (2) točki a) ovog Zakona
 - e) o pravu na podnošenje pritužbe Agenciji ili tužbe nadležnom sudu
 - f) o izvoru osobnih podataka i, prema potrebi, dolaze li iz javno dostupnih izvora
 - g) o postojanju automatiziranog donošenja odluka, uključujući i izradu profila iz članka 24. st. (1) i (4) ovog Zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nositelja podataka.
- (3) Kontrolor podataka pruža informacije iz st. (1) i (2) ovog članka:
- a) u razumnom roku nakon dobivanja osobnih podataka, a najkasnije u roku od 30 dana, uzimajući u obzir posebne okolnosti obrade osobnog podatka
 - b) ako se osobni podatak koristi za komunikaciju s nositeljem podataka, najkasnije prilikom prve komunikacije ili
 - c) ako je predviđeno otkrivanje podataka drugom primatelju, najkasnije u trenutku kada je osobni podatak prvi put otkriven.
- (4) Ako kontrolor podataka namjerava dodatno obrađivati osobni podatak u svrhu koja se razlikuje od svrhe za koju su podaci prikupljeni, on prije te dodatne obrade pruža nositelju podataka informacije o toj drugoj svrsi i sve dodatne relevantne informacije iz stavka (2) ovog članka.
- (5) Stavci (1) do (4) ovog članka ne primjenjuju se ako i u mjeri u kojoj:
- a) nositelj podataka već posjeduje informacije
 - b) pružanje takvih informacija je nemoguće ili bi zahtijevalo nerazmjerne napore, posebno za obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s uvjetima i mjerama zaštite iz članka 56. stavka (1) ovog Zakona ili u mjeri u kojoj je vjerojatno da se obvezom iz stavka (1) ovog članka može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade. U takvim slučajevima, kontrolor podataka poduzima odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nositelja podataka, između ostalog i stavljanjem informacija na raspolaganje javnosti
 - c) dobivanje ili otkrivanje podataka je izričito propisano posebnim zakonom koji se primjenjuje na nositelja podataka, a koji predviđa odgovarajuće mjere za zaštitu legitimnih interesa nositelja podataka ili
 - d) osobni podatak mora ostati povjerljiv u skladu s obvezom čuvanja profesionalne tajne koju propisuje posebni zakon, uključujući i druge zakonske obveze čuvanja tajne.

Članak 17.

(Pravo nositelja podataka na pristup osobnom podatku)

- (1) Nositelj podataka ima pravo dobiti potvrdu od kontrolora podataka o tome obrađuju li se njegovi osobni podaci i, ako se obrađuju, pristup osobnim podacima i sljedećim informacijama:
 - a) svrsi obrade
 - b) kategoriji osobnog podatka koji se obrađuje
 - c) primatelju ili kategorijama primatelja kojima je osobni podatak otkriven ili će im biti otkriven, a posebno primatelju u drugoj državi ili međunarodnoj organizaciji
 - d) predviđenom roku u kojem se osobni podaci čuvaju, ako je to moguće ili ako to nije moguće, kriterijima korištenim za određivanje tog roka
 - e) pravu da se od kontrolora podataka zatraži ispravka ili brisanje osobnog podatka ili ograničavanje obrade osobnog podatka koji se odnosi na nositelja podataka ili pravo na prigovor na takvu obradu
 - f) pravu na podnošenje pritužbe Agenciji ili tužbe nadležnom sudu
 - g) ako se osobni podatak ne prikuplja od nositelja podataka, svakoj dostupnoj informaciji o njegovom izvoru
 - h) postojanju automatiziranog donošenja odluka, uključujući i profiliranje iz članka 24. st. (1) i (4) ovog Zakona te, najmanje u tim slučajevima, razumne informacije o kriteriju koji se koristi, kao i značaju i predviđenim posljedicama takve obrade za nositelja podataka.
- (2) Ako se osobni podatak prenosi u drugu državu ili međunarodnu organizaciju, nositelj podataka ima pravo biti informiran o odgovarajućim mjerama zaštite u skladu s člankom 48. ovog Zakona koje se odnose na prijenos podataka.
- (3) Kontrolor podataka osigurava presliku osobnog podatka koji se obrađuje. Za sve dodatne preslike koje zatraži nositelj podataka, kontrolor podataka može naplatiti opravdanu naknadu na temelju administrativnih troškova. Ako nositelj podataka podnese zahtjev elektroničkim putem, osim ako nositelj podataka ne zahtijeva drugačije, informacije se pružaju u uobičajenom elektroničkom obliku.
- (4) Pravo na dobivanje preslike iz stavka (3) ovog članka ne smije negativno utjecati na prava i slobode drugih.

Članak 18.

(Pravo na ispravku)

- (1) Nositelj podataka ima pravo da mu kontrolor podataka omogući ispravku netočnog osobnog podatka, bez nepotrebnog odgađanja.
- (2) Uzimajući u obzir svrhu obrade, nositelj podataka ima pravo dopuniti nepotpun osobni podatak, među ostalim i davanjem dodatne izjave.

Članak 19.

(Pravo na brisanje)

- (1) Nositelj podataka ima pravo da mu kontrolor podataka omogući brisanje osobnog podatka koji se na njega odnosi, a kontrolor podataka ima obvezu obrisati osobni podatak, bez nepotrebnog odgađanja, ako je ispunjen jedan od sljedećih uvjeta:
- a) osobni podatak više nije neophodan za svrhe u koje je prikupljen ili na drugi način obrađen
 - b) nositelj podataka povukao je suglasnost na kojoj je obrada zasnovana u skladu s člankom 8. stavkom (1) točkom a) ovog Zakona ili člankom 11. stavkom (2) točkom a) ovog Zakona i ako ne postoji drugi pravni temelj za obradu
 - c) nositelj podataka uložio je prigovor na obradu u skladu s člankom 23. stavkom (1) ovog Zakona i ne postoje zakonski razlozi za obradu ili je nositelj podataka uložio prigovor na obradu u skladu s člankom 23. stavkom (2) ovog Zakona
 - d) osobni podatak je nezakonito obrađen
 - e) osobni podatak mora biti obrisani radi postupanja u skladu sa zakonskom obvezom kojoj podliježe kontrolor podataka
 - f) osobni podatak je prikupljen u vezi s ponudom usluga informacijskog društva iz članka 10. stavka (1) ovog Zakona.
- (2) Ako je kontrolor podataka javno objavio osobni podatak, a dužan je u skladu sa stavkom (1) ovog članka taj osobni podatak brisati, uzimajući u obzir dostupnu tehnologiju i troškove provođenja, kontrolor podataka poduzima razumne mjere, uključujući i tehničke mjere, da bi obavijestio kontrolore podataka koji obrađuju osobni podatak da je nositelj podataka zatražio od tih kontrolora podataka da brišu sve poveznice do njega ili presliku ili rekonstrukciju tog osobnog podatka.
- (3) Stavke (1) i (2) ovog članka ne primjenjuju se u mjeri u kojoj je obrada neophodna:
- a) radi ostvarivanja prava na slobodu izražavanja i informiranja
 - b) radi poštovanja zakonske obveze kojom se zahtijeva obrada propisana posebnim zakonom, a koja se primjenjuje na kontrolora podataka ili radi izvršenja zadatka koji se vrši u javnom interesu ili u okviru izvršavanja službenih ovlasti dodijeljenih kontroloru podataka
 - c) radi javnog interesa u području javnog zdravlja u skladu s člankom 11. stavkom (2) toč. h) i i) ovog članka, kao i člankom 11. stavkom (3) ovog Zakona
 - d) u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s člankom 56. stavkom (1) ovog Zakona u mjeri u kojoj je vjerojatno da se pravom iz stavka (1) ovog članka može onemogućiti ili ozbiljno ugroziti ostvarivanje ciljeva te obrade ili
 - e) radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Članak 20.

(Pravo na ograničenje obrade)

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

Članak 21.

(Obveza obavještavanja o ispravci ili brisanju osobnog podatka ili ograničenju obrade)

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

Članak 22.

(Pravo na prenosivost osobnog podatka)

- (1) Nositelj podataka ima pravo preuzeti osobni podatak, koji se odnosi na njega a koji je dao kontroloru podataka, u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, te ima pravo prenositi taj podatak drugom kontroloru podataka bez ometanja od kontrolora podataka kojem je osobni podatak dan, ako:
 - a) se obrada vrši u skladu s člankom 8. stavkom (1) točkom a) ovog Zakona ili člankom 11. stavkom (2) točkom a) ovog Zakona ili na temelju ugovora u skladu s člankom 8. stavkom (1) točkom b) ovog Zakona
 - b) se obrada vrši automatski.
- (2) Pri ostvarivanju svojeg prava na prenosivost podatka, u skladu sa stavkom (1) ovog članka, nositelj podatka ima pravo na neposredni prijenos od jednog kontrolora podataka drugom kontroloru podataka, ako je to tehnički izvodljivo.

- (3) Ostvarivanjem prava na prenosivost podataka iz stavka (1) ovog članka ne dovodi se u pitanje članak 19. ovog Zakona. To se pravo ne primjenjuje na obradu neophodnu za izvršenje zadatka koji se vrši u javnom interesu ili u okviru službenih ovlasti dodijeljenih kontroloru podataka.
- (4) Pravo na prenosivost podatka iz stavka (1) ovog članka ne smije negativno utjecati na prava i slobode drugih.

Članak 23.

(Pravo na prigovor)

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

Članak 24.

(Automatizirano pojedinačno donošenje odluke, uključujući i profiliranje)

- (1) Nositelj podataka ima pravo da se na njega ne primjenjuje odluka utemeljena isključivo na automatiziranoj obradi, uključujući i profiliranje, koja proizvodi pravni učinak koji se na njega odnosi ili na sličan način značajno na njega utječe.
- (2) Stavak (1) ovoga članka ne primjenjuje se ako je odluka:
 - a) potrebna za zaključivanje ili izvršenje ugovora između nositelja 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 nositelja podataka ili
 - c) utemeljena na izričitoj suglasnosti nositelja podataka.
- (3) U slučajevima iz stavka (2) toč. a) i c) ovog članka, kontrolor podataka poduzima odgovarajuće mjere za zaštitu prava i sloboda te legitimnih interesa nositelja podataka, najmanje prava na sudjelovanje fizičke osobe u donošenju odluke, prava izražavanja vlastitog stajališta i prava na osporavanje odluke.
- (4) Odluka iz stavka (2) ovog članka ne smije biti utemeljena na posebnim kategorijama osobnih podataka iz članka 11. stavka (1) ovog Zakona, osim ako se primjenjuje članak 11. stavak (2) toč. a) ili g) ovog Zakona te ako su uspostavljene odgovarajuće mjere za zaštitu prava i sloboda i legitimnih interesa nositelja podataka.

Članak 25.

(Ograničenja)

- (1) Na temelju posebnog zakona koji se primjenjuje na kontrolora podataka i obrađivača može se ograničiti opseg prava i obveza iz članka 7., čl.14. do 24. ovog Zakona i članka 36. ovog Zakona, ako odredbe tog zakona odgovaraju pravima i obvezama propisanim u čl. 14. do 24. ovog Zakona, ako se takvim ograničenjem poštuje suština temeljnih prava i sloboda i ako ono predstavlja neophodnu i razmjernu mjeru u demokratskom društvu za zaštitu:
- a) državne sigurnosti
 - b) obrane
 - c) javne sigurnosti
 - d) sprječavanja, istrage, otkrivanja ili gonjenja kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprječavanje
 - e) drugih važnih ciljeva od općeg javnog interesa u Bosni i Hercegovini, a posebice važnog gospodarskog ili finansijskog interesa, što uključuje monetarna, proračunska i porezna pitanja, javno zdravstvo i socijalnu skrb
 - f) neovisnosti pravosuđa i sudskih postupaka
 - g) sprječavanja, istrage, otkrivanja i gonjenja povrede etike u zakonski reguliranim profesijama
 - h) nadzorne, inspeksijske ili regulatorne funkcije koja je, najmanje povremeno, povezana s izvršavanjem službenih ovlasti u slučajevima iz toč. a) do e) i točke g) ovog stavka
 - i) nositelja podataka ili prava i sloboda drugih
 - j) ostvarivanja potraživanja u građanskim sporovima.
- (2) Posebni zakon iz stavka (1) ovog članka sadrži, po potrebi, posebne odredbe, koje sadrže najmanje sljedeće:
- a) svrhu obrade ili kategoriju obrade
 - b) kategoriju osobnog podatka
 - c) opseg uvedenih ograničenja

- d) mjere zaštite za sprječavanje 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 nositelja podataka
- h) pravo nositelja podataka da bude obaviješten o ograničenju, osim ako to može biti štetno za svrhu tog ograničenja.

POGLAVLJE III. KONTROLOR PODATAKA I OBRAĐIVAČ

Članak 26.

(Obveza kontrolora podataka)

- (1) Kontrolor podataka dužan je primijeniti odgovarajuće tehničke i organizacijske mjere imajući u vidu prirodu, opseg, okolnosti i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode fizičkih osoba, 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 stavka (1) ovog članka, ako su razmjerne u odnosu na aktivnosti obrade, uključuju provođenje odgovarajućih politika zaštite podataka od kontrolora podataka.
- (3) Poštovanje odobrenih kodeksa ponašanja iz članka 42. ovog Zakona ili odobrenih mehanizama certifikacije iz članka 44. ovog Zakona može služiti kao element za dokazivanje usklađenosti s obvezama kontrolora podataka.

Članak 27.

(Tehnička i integrirana zaštita podataka)

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

- (3) Odobreni mehanizam certifikacije iz članka 44. ovog Zakona može služiti kao element za dokazivanje usklađenosti sa zahtjevima iz st. (1) i (2) ovog članka.

Članak 28.

(Zajednički kontrolori podataka)

- (1) Ako dva ili više kontrolora podataka zajednički odrede svrhe i načine obrade, smatraju se zajedničkim kontrolorima podataka. Oni na transparentan način, međusobnim sporazumom, određuju odgovornosti svakoga od njih s ciljem izvršavanja obveza iz ovog Zakona, posebno u vezi s ostvarivanjem prava nositelja podataka i dužnostima svakoga od njih u pogledu pružanja informacija iz čl. 15. i 16. ovog Zakona, osim u slučaju da su odgovornosti svakog od kontrolora podataka utvrđene zakonom koji se primjenjuje na kontrolore podataka. Sporazumom se može odrediti kontaktna točka za nositelje podataka.
- (2) Sporazum iz stavka (1) ovog članka mora na odgovarajući način odražavati pojedinačne uloge i odnose zajedničkih kontrolora podataka u odnosu na nositelje podataka. Suština sporazuma mora biti dostupna nositelju podataka.
- (3) Neovisno o uvjetima sporazuma iz stavka (1) ovog članka, nositelj podataka može ostvarivati svoja prava iz ovog Zakona u odnosu sa svakim kontrolorom podataka i protiv svakog od njih.

Članak 29.

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

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

Članak 30.

(Obrađivač)

- (1) Ako se obrada osobnog podatka vrši u ime kontrolora podataka, kontrolor podataka koristi isključivo obrađivača koji u dovoljnoj mjeri jamči primjenu odgovarajućih tehničkih i organizacijskih mjera tako da obrada bude u skladu sa zahtjevima iz ovog Zakona i da se obradom osigurava zaštita prava nositelja podataka.
- (2) Obrada ne smije angažirati 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 vrši obrađivač uređuje se ugovorom ili drugim pravnim aktom u skladu sa zakonom koji obvezuje obrađivača prema kontroloru podataka, u kojem se navode predmet i trajanje obrade, priroda i svrha obrade, vrsta osobnih podataka i kategorija nositelja podataka, kao i obveze i prava kontrolora podataka.
- (4) Ugovorom ili drugim pravnim aktom iz stavka (3) ovog članka propisuje se da je obrađivač dužan:
 - a) obrađivati osobni podatak samo prema dokumentiranim uputama kontrolora podataka, među ostalim i u pogledu prijenosa osobnog 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) osiguravati da su se osobe ovlaštene za obradu osobnog podatka obvezale na poštovanje povjerljivosti ili da ih na poštovanje povjerljivosti obvezuje odgovarajući zakon
 - c) poduzimati sve potrebne mjere u skladu s člankom 34. ovog Zakona
 - d) poštovati uvjete iz st. (2) i (5) ovog članka za angažiranje drugog obrađivača
 - e) uzimajući u obzir prirodu obrade, pomagati kontroloru podataka putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu kontrolora podataka da odgovori na zahtjeve za ostvarivanje prava nositelja podataka iz poglavlja II. ovog Zakona
 - f) pomagati kontroloru podataka u osiguravanju usklađenosti s obvezama iz čl. 34. do 38. ovog Zakona, uzimajući u obzir prirodu obrade i informacije koje su dostupne obrađivaču
 - g) po izboru kontrolora podataka, brisati ili vraćati kontroloru podataka sve osobne podatke nakon završetka pružanja usluga vezanih za obradu i brisati postojeće preslike, osim u slučaju da je posebnim zakonom propisana obveza čuvanja osobnih podataka
 - h) kontroloru podataka stavljati na raspolaganje sve informacije koje su neophodne za dokazivanje poštovanja obveza iz ovog članka i kontroloru podataka ili drugom revizoru kojeg ovlasti kontrolor podataka omogućavati vršenje revizije, uključujući i inspekcije, i pomagati u njihovom vršenju
 - i) u slučaju iz točke h) ovog stavka obrađivač odmah obavještava kontrolora podataka ako prema njegovom mišljenju određena uputa krši ovaj Zakon ili druga pravila o zaštiti podataka.

- (5) Ako obrađivač angažira drugog obrađivača za vršenje posebnih aktivnosti obrade u ime kontrolora podataka, iste obveze za zaštitu podataka kao one koje su navedene u ugovoru ili drugom pravnom aktu između kontrolora podataka i obrađivača iz stavka (4) ovog članka nameću se tom drugom obrađivaču ugovorom ili drugim pravnim aktom u skladu s posebnim zakonom, a posebno obveza davanja dovoljnih jamstava za primjenu odgovarajućih tehničkih i organizacijskih mjera na način kojim se osigurava da obrada zadovoljava zahtjeve iz ovog Zakona. Ako taj drugi obrađivač ne ispunjava obveze zaštite podataka, prvi obrađivač ostaje u potpunosti odgovoran kontroloru podataka za izvršavanje obveza tog drugog obrađivača.
- (6) Poštovanje odobrenih kodeksa ponašanja od obrađivača, iz članka 42. ovog Zakona, ili odobrenog mehanizma certifikacije, iz članka 44. ovog Zakona, može služiti kao element za dokazivanje pružanja dovoljnih jamstava iz st. (1) i (5) ovog članka.
- (7) Ne dovodeći u pitanje pojedinačni ugovor između kontrolora podataka i obrađivača, ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog članka može se u cjelini ili djelomično zasnivati na standardnim ugovornim klauzulama iz st. (8) i (9) ovog članka, uključujući, među ostalim, i klauzule koje su dio certifikata dodijeljenog kontroloru podataka ili obrađivaču u skladu s čl. 44. i 45. ovog Zakona.
- (8) Agencija može donijeti standardne ugovorne klauzule za pitanja iz st. (3), (4) i (5) ovog članka s ciljem dosljedne primjene ovog Zakona.
- (9) Ugovor ili drugi pravni akt iz st. (3), (4) i (5) ovog članka mora biti u pisanom obliku, što uključuje i elektronički oblik.
- (10) Ne dovodeći u pitanje čl. 112., 113., 114. i 115. ovog Zakona, ako obrađivač krši ovaj Zakon time što određuje svrhu i načine obrade podataka, obrađivač se smatra kontrolorom podataka u vezi s tom obradom.

Članak 31.

(Obrada osobnog podatka pod kontrolom kontrolora podataka ili obrađivača)

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

Članak 32.

(Evidencija o obradi osobnog 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 nositelja podataka i kategorija osobnih podataka

- d) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući i primatelje u drugim državama ili međunarodnim organizacijama
 - e) ako je primjenjivo, o prijenosu osobnih podataka u drugu državu ili međunarodnu organizaciju, uključujući identifikaciju druge države ili međunarodne organizacije i, u slučaju prijenosa iz članka 51. stavka (2) ovog Zakona, dokumentaciju o odgovarajućim zaštitnim mjerama
 - f) ako je moguće, predviđene rokove za brisanje različitih kategorija podataka
 - g) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 34. stavka (1) ovog Zakona.
- (2) Svaki obrađivač i predstavnik obrađivača, ako je primjenjivo, vodi evidenciju o svim aktivnostima obrade koje se vrše 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 osobnih podataka u drugu državu ili međunarodnu organizaciju, s identifikacijom te druge države ili međunarodne organizacije i u slučaju prijenosa iz članka 51. stavka (2) ovog Zakona, dokumentaciju o odgovarajućim zaštitnim mjerama
 - d) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 34. stavka (1) ovog Zakona.
- (3) Evidencija iz st. (1) i (2) ovog članka mora biti u pisanom obliku, što uključuje i elektronički oblik.
- (4) Kontrolor podataka ili obrađivač te predstavnik kontrolora podataka ili obrađivača, ako je primjenjivo, na zahtjev Agencije omogućavaju uvid u evidenciju.
- (5) Obveze iz st. (1) i (2) ovog članka ne primjenjuju se na gospodarski subjekt ili organizaciju u kojoj je zaposleno manje od 250 osoba, osim kada je vjerojatno da će obrada koju vrši predstavljati visok rizik za prava i slobode nositelja podataka, ako obrada nije povremena ili ako obrada obuhvaća posebne kategorije podataka iz članka 11. stavka (1) ovog Zakona, ili su u pitanju osobni podaci koji se odnose na kaznenu osuđivanost i kaznena djela.

Članak 33.

(Suradnja s Agencijom)

Kontrolor podataka i obrađivač te ako su određeni njihovi predstavnici dužni su, na zahtjev, surađivati s Agencijom u vršenju njezinih zadataka.

Članak 34.

(Sigurnost obrade osobnog podatka)

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

Članak 35.

(Izvještavanje Agencije o povredi osobnog podatka)

- (1) Kontrolor podataka dužan je o povredi osobnog podatka bez nepotrebnog odgađanja i, ako je moguće, najkasnije u roku od 72 sata nakon saznanja za tu povredu izvijestiti Agenciju o povredi osobnog podatka, osim u slučaju ako je vjerojatno da ta povreda neće ugroziti prava i slobode fizičke osobe. Ako 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 osobnog podatka, bez nepotrebnog odgađanja o tome izvijestiti kontrolora podataka.
- (3) Izvješće iz stavka (1) ovog članka sadrži najmanje sljedeće:
 - a) opis prirode povrede osobnih podataka, i ako je moguće, s navedenim kategorijama i približnim brojem nositelja podataka, kao i kategorijama i približnim brojem evidencija osobnih podataka
 - b) ime i prezime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija
 - c) opis vjerojatne posljedice povrede osobnog podatka

- d) opis mjera koje je kontrolor podataka poduzeo ili čije je poduzimanje predložio radi rješavanja problema povrede osobnog podatka, uključujući prema potrebi i mjere za ublažavanje njezinih 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 osobnog podatka, uključujući i činjenice u vezi s povredom osobnog podatka, njezine posljedice i mjere poduzete za otklanjanje štete. Dokumentacija iz ovog stavka omogućava Agenciji postupanje po ovom članku.

Članak 36.

(Obavješćavanje nositelja podataka o povredi osobnog podatka)

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

Članak 37.

(Procjena utjecaja obrade na zaštitu osobnog podatka)

- (1) Ako je vjerojatno da će neka vrsta obrade, osobito posredstvom novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode fizičkih osoba, kontrolor podataka prije obrade provodi procjenu utjecaja predviđenih obrada na zaštitu osobnog podatka.

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

Članak 38.

(Prethodno savjetovanje kontrolora podataka s Agencijom)

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

Članak 39.

(Imenovanje službenika za zaštitu osobnih podataka)

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

Članak 40.

(Status službenika za zaštitu osobnih podataka)

- (1) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu osobnih podataka bude na odgovarajući način i pravodobno uključen u sva pitanja koja se tiču zaštite osobnih podataka.
- (2) Kontrolor podataka i obrađivač podržavaju službenika za zaštitu osobnih podataka u izvršavanju zadataka iz članka 41. ovog Zakona, pružajući mu potrebna sredstva za izvršavanje tih zadataka i ostvarivanje pristupa osobnim podacima i postupcima obrade, kao i za održavanje njegovog stručnog znanja.
- (3) Kontrolor podataka i obrađivač osiguravaju da službenik za zaštitu osobnih podataka ne prima nikakve instrukcije pri vršenju tih zadataka. Kontrolor podataka ili obrađivač ne može ga razriješiti dužnosti ili kazniti zbog toga što vrši svoje zadatke. Službenik za zaštitu osobnih podataka odgovara neposredno najvišoj razini rukovodstva kontrolora podataka ili obrađivača.

- (4) Nositelj podataka može se obratiti službeniku za zaštitu osobnih podataka za sva pitanja koja se tiču obrade njegovih osobnih podataka i ostvarivanja njegovih prava iz ovog Zakona.
- (5) Službenik za zaštitu osobnih podataka, u vezi s obavljanjem svojih zadataka, dužan je sve podatke do kojih dođe u postupku obrade podataka čuvati kao službenu tajnu u skladu sa zakonom.
- (6) Službenik za zaštitu osobnih podataka može vršiti i druge zadatke i dužnosti. Kontrolor podataka ili obrađivač osigurava da ti zadaci i dužnosti ne dovedu do sukoba interesa.

Članak 41.

(Zadatak službenika za zaštitu osobnih podataka)

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

Članak 42.

(Kodeks ponašanja)

- (1) Agencija izdaje preporuku za izradu kodeksa ponašanja s ciljem pravilne primjene ovog Zakona, uzimajući u obzir specifičnost različitih sektora obrade i posebne potrebe mikro, malih i srednjih gospodarskih subjekata.
- (2) Udruga i drugi subjekt koji predstavlja kategorije kontrolora podataka ili obrađivača mogu izraditi kodekse ponašanja, 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 osobnih podataka
 - d) pseudonimizaciju osobnih podataka

- e) informiranje javnosti i nositelja podataka
 - f) ostvarivanje prava nositelja podataka
 - g) informiranje i zaštitu djece i način pribavljanja suglasnosti nositelja roditeljskog prava nad djetetom
 - h) mjere i postupke iz čl. 26. i 27. ovog Zakona kao i mjere za postizanje sigurnosti obrade iz članka 34. ovog Zakona
 - i) izvještavanje Agencije o povredama osobnih podataka i obavještanje nositelja podataka o takvim povredama
 - j) prijenos osobnih podataka drugim državama ili međunarodnim organizacijama ili
 - k) izvansudske postupke i druge postupke za rješavanje sporova između kontrolora podataka i nositelja podataka u vezi s obradom, ne dovodeći u pitanje prava nositelja podataka na temelju čl. 108. i 110. ovog Zakona.
- (3) Kodeks ponašanja iz stavka (2) ovog članka obvezno sadrži odredbe koje pravnoj osobi iz članka 43. stavka (1) ovog Zakona omogućavaju da provodi obvezno praćenje usklađenosti kontrolora podataka ili obrađivača koji su se obvezali na njegovu primjenu, ne dovodeći u pitanje nadležnosti Agencije.
- (4) Udruga i subjekt iz stavka (2) ovog članka koji namjeravaju izraditi kodeks ponašanja ili izmijeniti i proširiti postojeći kodeks ponašanja, nacrt kodeksa ponašanja, odnosno izmjene ili proširenje kodeksa ponašanja, dostavljaju Agenciji.
- (5) Agencija daje mišljenje o tome je li 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 stavkom (5) ovog članka, Agencija registrira i objavljuje kodeks ponašanja.
- (7) Kontrolor podataka ili obrađivač, na koje se ovaj Zakon ne primjenjuje u skladu s člankom 6. ovog Zakona, mogu primjenjivati kodeks ponašanja koji je odobren, u skladu sa stavkom (5) ovog članka, kako bi osigurali odgovarajuće zaštitne mjere u okviru prijenosa osobnih podataka drugoj državi ili međunarodnoj organizaciji, uz uvjete iz članka 48. stavka (2), točke d) ovog Zakona.
- (8) Kontrolor podataka ili obrađivač iz stavka (7) ovog članka, putem ugovornih ili drugih pravno obvezujućih instrumenata, preuzima obvezujuće i provedive obveze za primjenu zaštitnih mjera, uključujući i mjere vezane za prava nositelja podataka.

Članak 43.

(Praćenje odobrenog kodeksa ponašanja)

- (1) Pravna osoba s odgovarajućim stupnjem stručnosti za predmet kodeksa ponašanja može vršiti praćenje usklađenosti s kodeksom ponašanja, ako ju je u tu svrhu akreditirala agencija.
- (2) Pravna osoba iz stavka (1) ovog članka može biti akreditirana za praćenje usklađenosti s kodeksom ponašanja ako je:
- a) Agenciji dokazala svoju neovisnost i stručnost za predmet kodeksa ponašanja

- b) uspostavila postupke koji joj omogućavaju da ocjenjuje kvalificiranost kontrolora podataka i obrađivača za primjenu kodeksa ponašanja, da prati njihovu primjenu odredbi kodeksa ponašanja te da periodično preispituje njegovo funkcioniranje
 - c) uspostavila postupke i strukture za rješavanje prigovora na kršenja kodeksa ponašanja ili na način na koji kontrolor podataka ili obrađivač primjenjuju ili je primijenio kodeks ponašanja i učinio te postupke i strukture transparentnim nositeljima podataka i javnosti i
 - d) Agenciji dokazala da njezini zadaci i dužnosti ne dovode do sukoba interesa.
- (3) Pravna osoba iz stavka (1) ovog članka, uz primjenu odgovarajućih zaštitnih mjera, poduzima odgovarajuće radnje u slučajevima kršenja kodeksa ponašanja od kontrolora podataka ili obrađivača, što uključuje suspendiranje ili isključenje iz kodeksa ponašanja.
 - (4) Pravna osoba iz stavka (1) ovog članka dužna je obavijestiti Agenciju o radnjama i razlozima iz stavka (3) ovog članka.
 - (5) Agencija oduzima akreditaciju pravnoj osobi koja više ne ispunjava uvjete za akreditaciju ili ako pravna osoba krši odredbe ovog Zakona.
 - (6) Ovaj se članak ne primjenjuje na obradu osobnih podataka koju obavlja javno tijelo.

Članak 44.

(Certifikacija)

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

- (9) Certifikacijsko tijelo oduzima certifikat kontroloru ili obrađivaču ako više ne ispunjava uvjete za izdavanje certifikata.
- (10) Agencija postupak certifikacije zaštite osobnih podataka, pečata i oznake unosi u evidenciju i javno objavljuje.

Članak 45.

(Certifikacijsko tijelo)

- (1) Akreditaciju certifikacijskog tijela, s odgovarajućim stupnjem stručnosti iz područja zaštite osobnih podataka, vrši Agencija.
- (2) Certifikacijsko tijelo obavještava Agenciju o odluci o izdavanju i obnavljanju certifikata kako bi Agencija mogla vršiti ovlasti iz članka 103. stavka (2) točke h) ovog Zakona.
- (3) Certifikacijsko tijelo može biti akreditirano samo ako:
 - a) Agenciji na zadovoljavajući način dokaže svoju neovisnost i stručnost u predmetu certifikacije
 - b) se obveže da će poštovati kriterije iz članka 44. stavka (6) ovog Zakona
 - c) uspostavi postupke za izdavanje, periodično preispitivanje i povlačenje certifikacije, pečata i oznaka za zaštitu podataka
 - d) uspostavi postupke i strukture za rješavanje pritužbe na kršenje certifikacije ili način na koji kontrolor podataka ili obrađivač primjenjuje ili je primijenio certifikaciju, i učini te postupke i strukture transparentnim nositeljima podataka i javnosti
 - e) Agenciji dokaže da njegovi zadaci i dužnosti ne dovode do sukoba interesa.
- (4) Akreditacija certifikacijskog tijela provodi se na temelju kriterija koje je propisala Agencija.
- (5) Akreditacija se izdaje na najviše pet godina i može se obnoviti uz iste uvjete ako certifikacijsko tijelo i dalje ispunjava zahtjeve iz ovog članka.
- (6) Ne dovodeći u pitanje DIO ČETVRTI ovog Zakona, Agencija povlači akreditaciju certifikacijskog tijela ako se uvjeti iz stavka (3) ovog članka ne ispune ili više nisu ispunjeni, ili ako se radnjama koje poduzima certifikacijsko tijelo krši ovaj Zakon.
- (7) Certifikacijsko tijelo odgovorno je za pravilnu procjenu koja dovodi do certifikacije ili oduzimanja certifikata, ne dovodeći u pitanje odgovornost kontrolora podataka ili obrađivača za poštovanje ovog Zakona.
- (8) Certifikacijsko tijelo u pisanoj formi obavještava Agenciju o razlozima za izdavanje ili oduzimanje certifikata.
- (9) Agencija javno objavljuje kriterije iz članka 44. stavka (6) ovog Zakona.

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

Članak 46.
(Opća načela prijenosa)

Svaki prijenos osobnog podatka čija je obrada u tijeku 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 obuhvaća i daljnji prijenos osobnog podatka iz druge države ili međunarodne organizacije u još jednu drugu državu ili međunarodnu organizaciju.

Članak 47.
(Prijenos na temelju adekvatnosti razine zaštite osobnog podatka)

- (1) Prijenos osobnog podatka u drugu državu, na dio njezina teritorija, ili u jedan ili više sektora u toj državi ili međunarodnu organizaciju može se vršiti ako je utvrđeno da ta druga država, dio njezina teritorija, ili jedan ili više sektora u toj državi ili ta međunarodna organizacija osiguravaju adekvatnu razinu zaštite osobnog podatka.
- (2) Smatra se da je adekvatna razina zaštite iz stavka (1) ovog članka osigurana u državi, dijelovima njezina teritorija, ili jednom ili više sektora u toj državi, ili međunarodnoj organizaciji, za koje je od Europske unije utvrđeno da osiguravaju adekvatnu razinu zaštite osobnog podatka.
- (3) Odluku o adekvatnosti razine zaštite osobnog podatka iz stavka (1) ovog članka donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stavka (3) ovog članka, uzimajući u obzir:
 - a) načelo vladavine prava, poštovanje ljudskih prava i temeljnih sloboda, sektorsko zakonodavstvo, uključujući zakonodavstvo o javnoj sigurnosti, obrani, državnoj sigurnosti, kaznenom pravu i pristupu javnih tijela osobnim podacima, kao i primjenu tih propisa, pravila o zaštiti osobnih podataka, pravila struke i mjere osiguranja zaštite osobnog podatka, uključujući pravila o daljnjem prijenosu osobnog podatka u drugu državu ili međunarodnu organizaciju, koja se primjenjuju u praksi sudova i drugih tijela vlasti u drugoj državi ili međunarodnoj organizaciji, kao i djelotvornost ostvarivanja prava nositelja osobnih podataka, a posebno djelotvornost upravnih i sudskih postupaka zaštite prava nositelja osobnih podataka
 - b) postojanje i efikasnost rada nadzornog tijela u drugoj državi ili tijela koje je nadležno za međunarodnu organizaciju u ovom području, s ovlašću da osigura primjenu pravila o zaštiti osobnih podataka i pokrene postupke zaštite osobnih podataka u slučaju njihovog nepoštovanja, pruži pomoć i savjetuje nositelje osobnih podataka u ostvarivanju njihovih prava, kao i da surađuje s nadzornim tijelima drugih država
 - c) međunarodne obveze koje je druga država ili međunarodna organizacija preuzela, ili druge obveze koje proizlaze iz pravno obvezujućih međunarodnih ugovora ili drugih pravnih instrumenata, kao i iz članstva u multilateralnim ili regionalnim organizacijama, a posebno u vezi sa zaštitom osobnih podataka.

- (5) Agencija kontinuirano prati stanje u području zaštite osobnog podatka u drugoj državi, dijelu njezina teritorija, jednom ili više sektora unutar te države ili međunarodnoj organizaciji i o tome po potrebi izvještava Vijeće ministara Bosne i Hercegovine.
- (6) Izvješće iz stavka (5) ovog članka uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija, koje su od značaja za preispitivanje postojanja adekvatne razine zaštite osobnih podataka, na temelju čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stavka (3) ovog članka.
- (7) Odluka donesena na temelju stavka (3) ovog članka ne dovodi u pitanje prijenos osobnih podataka u drugu državu, na teritorij 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, glede kojih je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju adekvatnu razinu zaštite osobnih podataka, objavljuje se u „Službenom glasniku BiH“ i na službenoj internet stranici Agencije.

Članak 48.

(Prijenos na koji se primjenjuju odgovarajuće zaštitne mjere)

- (1) Kontrolor podataka ili obrađivač može prenijeti osobne podatke u drugu državu, na dio njezina teritorija, jedan ili više sektora unutar te države ili u međunarodnu organizaciju za koju listom iz članka 47. stavka (8) ovog Zakona nije utvrđeno postojanje adekvatne razine zaštite osobnih podataka samo ako je kontrolor podataka ili obrađivač osigurao odgovarajuće zaštitne mjere tih podataka i ako su nositelju osobnih podataka osigurana provediva prava i djelotvorna sudska zaštita.
- (2) Odgovarajuće zaštitne mjere iz stavka (1) ovog članka mogu se, bez posebnog odobrenja Agencije, osigurati:
 - a) pravno obvezujućim aktom sačinjenim između javnih tijela
 - b) obvezujućim poslovnim pravilima u skladu s člankom 49. ovog Zakona
 - c) odobrenim kodeksom ponašanja u skladu s člankom 42. ovog Zakona s obvezujućim i izvršnim obvezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, među ostalim i u pogledu prava nositelja podataka ili
 - d) odobrenim postupkom certifikacije u skladu s člankom 44. ovog Zakona s obvezujućim i izvršnim obvezama kontrolora podataka ili obrađivača u drugoj državi za primjenu odgovarajućih zaštitnih mjera, među ostalim i u pogledu prava nositelja podataka.
- (3) Odgovarajuće zaštitne mjere iz stavka (1) ovog članka mogu se osigurati standardnim ugovornim klauzulama o zaštiti podataka koje donosi Agencija.
- (4) Uz uvjet da to odobri Agencija, odgovarajuće zaštitne mjere iz stavka (1) ovog članka također mogu biti osigurane posebno:
 - a) ugovorom između kontrolora podataka ili obrađivača i kontrolora podataka, obrađivača ili primatelja osobnih podataka u drugoj državi ili međunarodnoj organizaciji ili
 - b) odredbama koje se unose u sporazume između javnih tijela i koji sadrže provediva i djelotvorna prava nositelja podataka.

Članak 49.

(Obvezujuća poslovna pravila)

(1) Obvezujuća poslovna pravila određuju najmanje:

- a) strukturu i podatke za kontakt skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost i svakog od njihovih članova
- b) prijenose podataka ili skupove prijenosa, uz navođenje kategorije osobnih podataka, vrste obrade i njezine svrhe, kategorije nositelja podataka i određenja druge države ili država o kojima se radi
- c) njihovu pravno obvezujuću prirodu
- d) primjenu načela zaštite podataka, a posebice ograničenja svrhe, smanjenja količine podataka, ograničenja roka čuvanja, kvalitete podataka, tehničke i integrirane zaštite podataka, pravnog temelja obrade, obrade posebnih kategorija osobnih podataka, mjera za postizanje sigurnosti podataka i uvjeta u vezi s daljnjim prijenosom tijelima koja nisu obvezana obvezujućim poslovnim pravilima
- e) prava nositelja podataka u vezi s obradom i načine za ostvarenje tih prava, uključujući i pravo da se na njih ne primjenjuju odluke koje se temelje isključivo na automatskoj obradi, što uključuje i izradu profila u skladu s člankom 24. ovog Zakona, pravo na pritužbu Agenciji i pravo na sudsku zaštitu, u skladu s člankom 110. ovog Zakona, a u odgovarajućim slučajevima i pravo na naknadu štete za kršenje obvezujućih poslovnih pravila
- f) da kontrolor podataka ili obrađivač sa sjedištem ili poslovnim nastanom na teritoriju Bosne i Hercegovine prihvaća odgovornost za sva kršenja obvezujućih poslovnih pravila od bilo kojeg člana koji nema sjedište ili poslovni nastan u Bosni i Hercegovini ili je kontrolor podataka ili obrađivač u cjelini ili djelomično izuzet od odgovornosti ako dokaže da taj član skupine gospodarskih subjekata nije odgovoran za događaj koji je prouzročio štetu
- g) na koji način se nositeljima podataka, osim informacija iz čl. 15. i 16. ovog Zakona, pružaju informacije o obvezujućim poslovnim pravilima, posebice o odredbama iz toč. d), e) i f) ovog stavka
- h) zadatke svakog službenika za zaštitu podataka imenovanog u skladu s člankom 39. ovog Zakona ili bilo koje druge osobe ili subjekta odgovornog za praćenje usklađenosti s obvezujućim poslovnim pravilima u skupini gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, kao i praćenje osposobljenosti i rješavanje pritužbi
- i) postupke u povodu pritužbi
- j) mehanizme unutar skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, kojima se osigurava provjera poštovanja obvezujućih poslovnih pravila, koji uključuju reviziju zaštite podataka i metode za osiguravanje korektivnih mjera za zaštitu prava nositelja podataka. Rezultate takve provjere potrebno je priopćiti osobi ili subjektu iz točke h) ovog stavka i upravljačkom tijelu skupine gospodarskih subjekata koji vrše zajedničku gospodarsku 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 suradnje s Agencijom radi osiguravanja usklađenosti svakog člana skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, prije svega tako što se Agenciji stave na raspolaganje rezultati provjera mjera iz točke j) ovog stavka
 - m) mehanizme za izvještavanje Agencije o bilo kakvim pravnim obvezama koje se odnose na člana skupine gospodarskih subjekata koji vrše zajedničku gospodarsku djelatnost i primjenjuju se u drugoj državi, a koji bi mogli imati značajan negativan utjecaj na jamstva sadržana u obvezujućim poslovnim pravilima
 - n) odgovarajuće osposobljavanje iz područja zaštite osobnih podataka za osoblje koje ima stalan ili redovit pristup osobnim podacima.
- (2) Agencija odobrava obvezujuća poslovna pravila uz uvjet da:
- a) su pravno obvezujuća i da se primjenjuju na svakog zainteresiranog člana određene skupine gospodarskih subjekata koji obavljaju zajedničku gospodarsku djelatnost, što uključuje i njihove zaposlene, te da ih oni izvršavaju
 - b) nositeljima podataka izričito daju provediva prava u vezi s obradom njihovih osobnih podataka
 - c) ispunjavaju uvjete iz stavka (1) ovog članka.
- (3) Agencija može odrediti format i postupke razmjene informacija između kontrolora podataka, obrađivača i Agencije za obvezujuća poslovna pravila u smislu ovog članka.

Članak 50.

(Prijenos ili otkrivanje podataka koji nisu dopušteni)

Svaka presuda suda, tribunala ili odluka upravnog tijela druge države kojom se od kontrolora podataka ili obrađivača zahtijeva prijenos ili otkrivanje osobnih podataka može biti priznata ili izvršena samo ako se temelji 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.

Članak 51.

(Odstupanje u posebnim slučajevima)

- (1) Prijenos ili skup prijenosa osobnih podataka u drugu državu ili međunarodnu organizaciju, ako ne postoji odluka o adekvatnosti, u skladu s člankom 47. stavkom (3) ovog Zakona ili odgovarajuće zaštitne mjere u skladu s člankom 48. ovog Zakona, uključujući i obvezujuća poslovna pravila iz članka 49. ovog Zakona, vrši se samo uz jedan od sljedećih uvjeta:
- a) nositelj podataka je izričito suglasan s predloženim prijenosom, nakon što je upoznat s mogućim rizicima takvih prijenosa zbog nepostojanja odluke o adekvatnosti i odgovarajućih zaštitnih mjera iz članka 48. ovog Zakona
 - b) prijenos je neophodan za izvršenje ugovora između nositelja podataka i kontrolora podataka ili provođenje predugovornih mjera na zahtjev nositelja podataka
 - c) prijenos je neophodan radi sklapanja ili izvršenja ugovora sklopljenog u interesu nositelja podataka između kontrolora podataka i druge fizičke ili pravne osobe

- d) prijenos je neophodan iz važnih razloga javnog interesa
 - e) prijenos je neophodan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva
 - f) prijenos je neophodan za zaštitu ključnih interesa nositelja podataka ili drugih osoba ako nositelj podataka fizički ili pravno nije sposoban dati suglasnost
 - 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 kojoj osobi koja može dokazati postojanje legitimnog interesa, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani posebnim zakonom za uvid u tom posebnom slučaju.
- (2) Prijenos ili skup prijenosa osobnih podataka u drugu državu ili međunarodnu organizaciju, u slučaju kada temelj za prijenos ne može biti čl. 47. ili 48. ovog Zakona, uključujući i obvezujuća poslovna pravila iz članka 49. ovog Zakona, i kada se ne primjenjuje nijedno odstupanje u posebnim slučajevima iz stavka (1) ovog članka, može se izvršiti samo ako se prijenos ne ponavlja, ako se odnosi samo na ograničeni broj nositelja podataka i ako je neophodan za potrebe važnih, legitimnih interesa kontrolora podataka nad kojima ne prevladavaju interesi ili prava i slobode nositelja podataka, a kontrolor podataka je procijenio sve okolnosti prijenosa podataka i na temelju te procjene je predvidio odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka. Kontrolor podataka o prijenosu obavještava Agenciju. Uz informacije iz čl. 15. i 16. ovog Zakona, kontrolor podataka obavještava nositelja podataka o prijenosu i o važnim legitimnim interesima.
- (3) Prijenos na temelju stavka (1) točke g) ovog članka ne uključuje osobne podatke u cjelini ni cijele kategorije osobnih podataka sadržanih u registru. Kada je registar namijenjen uvidu osobama koje imaju legitiman interes, prijenos se vrši samo ako to zahtijevaju te osobe ili ako su one primatelji.
- (4) Na aktivnosti koje obavljaju javna tijela prilikom izvršavanja svojih javnih ovlasti ne primjenjuju se stavak (1) toč. a), b) i c) i stavak (2) ovog članka.
- (5) Javni interes iz stavka (1) točke d) ovog članka mora biti propisan zakonom koji se primjenjuje na kontrolora podataka.
- (6) Ako nije donesena odluka o adekvatnosti, iz važnih razloga javnog interesa posebnim propisom mogu biti izričito propisana ograničenja prijenosa određenih kategorija osobnih podataka drugoj državi ili međunarodnoj organizaciji.
- (7) Kontrolor podataka ili obrađivač dokumentira procjenu, kao i odgovarajuće zaštitne mjere iz st. (1) i (2) ovog članka, u evidencije iz članka 32. ovog Zakona.

POGLAVLJE V. POSEBNI SLUČAJEVI OBRADJE

Članak 52.

(Obrada osobnog podatka i sloboda izražavanja i informiranja)

- (1) Obrada osobnih podataka prilikom korištenja prava na slobodu izražavanja i informiranja, što uključuje obradu isključivo u novinarske svrhe, u svrhe akademskog, umjetničkog ili književnog izražavanja, vrši se u skladu s posebnim propisima.
- (2) Posebnim propisima iz stavka (1) ovog članka 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 takve iznimke ili odstupanja potrebni da se uskladi pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja.

Članak 53.

(Obrada osobnog podatka i javni pristup službenim dokumentima)

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

Članak 54.

(Obrada jedinstvenog matičnog broja fizičke osobe)

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

Članak 55.

(Obrada osobnih podataka u kontekstu zaposlenja)

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

Članak 56.

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

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

Članak 57.

(Videonadzor)

- (1) Praćenje određenog prostora putem videonadzora dopušteno je samo ako je to nužno za zaštitu osoba i imovine i ako ne prevladaju interesi nositelja podataka.
- (2) Videonadzorom mogu biti obuhvaćeni samo prostori ili dijelovi prostora čiji je nadzor nužan radi postizanja svrhe iz stavka (1) ovog članka.
- (3) Uspostavljanje videonadzora javno dostupnih objekata velikih površina, kao što su sportski objekti, zabavni centri, trgovački centri ili parkirališta, ili vozila javnog prijevoza, dopušteno je isključivo u cilju zaštite života, zdravlja i slobode osobe te imovine.
- (4) Kontrolor podataka koji vrši videonadzor dužan je donijeti odluku koja će sadržavati pravila obrade s ciljem poštivanja prava na zaštitu privatnosti i osobnog života nositelja podataka, ako videonadzor nije propisan zakonom.
- (5) Kontrolor podataka ili obrađivač dužan je na vidnom mjestu istaknuti oznaku o vršenju videonadzora. Oznaka o videonadzoru sadrži sljedeće informacije: da je prostor pod videonadzorom, podatke o kontroloru podataka, odnosno obrađivaču i kontaktne podatke putem kojih nositelj podataka može ostvariti svoja prava. Oznaka treba biti vidljiva najkasnije prilikom ulaska u vidokrug snimanja.
- (6) Kontrolor podataka ili obrađivač dužan je da, kod sustava videonadzora javno dostupnih objekata iz stavka 3. ovog članka, bilježi zapise o uporabi sustava i da ih čuva najmanje 12

mjeseci. Zapisu omogućavaju da se utvrdi datum i vrijeme, te identitet osobe koja je izvršila uvid u sustav videonadzora.

- (7) Za uspostavu videonadzora u stambenim, odnosno poslovno-stambenim zgradama potrebna je suglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova. Videonadzorom 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 članka 1. stavka (1) točke c) ovog Zakona dopušteno je samo ako je to propisano posebnim zakonom.

Članak 58.

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

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

Članak 59.

(Obveza čuvanja profesionalne tajne)

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

DIO TREĆI – OBRADA OSOBNOG PODATKA OD NADLEŽNOG TIJELA KAO KONTROLORA PODATAKA

Članak 60.

(Načela obrade osobnih podataka od nadležnog tijela)

- (1) Načela obrade osobnih podataka od nadležnog tijela 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) točnost – podaci moraju biti točni i prema potrebi ažurirani, moraju se poduzeti sve razumne mjere kako bi se osiguralo da osobni podaci koji nisu točni, imajući u vidu svrhe u koje se obrađuju, budu bez odgađanja izbrisani ili ispravljeni
 - e) ograničenje čuvanja – podaci moraju biti čuvani u obliku koji omogućava identifikaciju nositelja podataka, i to ne duže nego što je potrebno u svrhe u koje se podaci obrađuju
 - f) cjelovitost i povjerljivost – podaci moraju biti obrađivani tako da se osigura odgovarajuća sigurnost osobnih podataka, uključujući i zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.
- (2) Obrada koju vrši isto ili neko drugo nadležno tijelo u svrhu iz članka 1. stavka (1) točke c) ovog Zakona različitu od one za koju su osobni podaci prikupljeni dopuštena je:
- a) ako je nadležno tijelo ovlašteno za obradu takvih osobnih podataka u takvu svrhu u skladu s posebnim propisom ili
 - b) ako je obrada neophodna i proporcionalna drugoj zakonitoj svrsi.
- (3) Obrada koju vrši isto ili neko drugo nadležno tijelo može uključivati arhiviranje u javnom interesu, u znanstvene, statističke ili povijesne svrhe, za svrhe iz članka 1. stavka (1) točke c) ovog Zakona, uz poduzimanje odgovarajućih zaštitnih mjera u pogledu prava i sloboda nositelja podataka.
- (4) Nadležno tijelo odgovorno je za usklađenost sa st. (1), (2) i (3) ovog članka i mora biti u mogućnosti dokazati tu usklađenost.

Članak 61.

(Rok za čuvanje i brisanje osobnog podatka)

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

Članak 62.

(Razlika između različitih kategorija nositelja podataka)

Nadležno tijelo dužno je, prema potrebi i ako je to moguće, napraviti jasnu razliku između osobnih podataka različitih kategorija nositelja podataka, kao što je:

- a) osoba za koju postoji osnova sumnje da je izvršila ili namjerava izvršiti kazneno djelo
- b) osoba osuđena za kaznena djela
- c) osoba koja je žrtva kaznenog djela ili osoba u pogledu koje postoje određene činjenice koje daju osnovu za sumnju da bi ta osoba mogla biti žrtva kaznenog djela
- d) osoba koja se dovodi u vezu s kaznenim djelom, kao što je osoba koja se može pozvati da svjedoči u istragama ili naknadnom kaznenom postupku, osoba koja može dati informacije o kaznenim djelima ili osoba za kontakt ili suradnici osoba iz toč. a) i b) ovog stavka.

Članak 63.

(Razlika između osobnih podataka i provjera kvalitete osobnih podataka)

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

Članak 64.

(Zakonitost obrade osobnog podatka od nadležnog tijela)

- (1) Obrada osobnih podataka koju vrši nadležno tijelo zakonita je samo ako je nužna i samo u onoj mjeri u kojoj je nužna za vršenje poslova nadležnog tijela u svrhe iz članka 1. stavka (1) točke c) ovog Zakona i ako je propisana posebnim zakonom.
- (2) Posebni zakon iz stavka (1) ovog članka propisuje najmanje ciljeve obrade, osobne podatke koji se obrađuju i svrhe obrade.

Članak 65.

(Posebni uvjeti obrade)

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

Članak 66.

(Obrada posebnih kategorija osobnih podataka od nadležnog tijela)

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

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

Članak 67.

(Automatizirano pojedinačno donošenje odluke od nadležnog tijela)

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

Članak 68.

(Obavješćavanje i način ostvarivanja prava nositelja podataka)

- (1) Nadležno tijelo dužno je poduzeti sve odgovarajuće mjere kako bi se nositelju podataka pružile sve informacije iz članka 69. ovog Zakona te dale sve obavijesti u pogledu članka 67., čl. 70. do 74. i članka 87. ovog Zakona u vezi s obradom.
- (2) Informacije iz stavka (1) ovog članka daju se u sažetom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika.
- (3) Informacije iz stavka (1) ovog članka pružaju se nositelju podataka u obliku u kojem je zahtjev podnesen ili na način koji je istaknut u zahtjevu, u roku od 30 dana od dana podnošenja zahtjeva.
- (4) Nadležno tijelo dužno je olakšati ostvarivanje prava nositelja podataka iz članka 67., čl. 70. do 74. ovog Zakona.
- (5) Nadležno tijelo dužno je nositelja podataka pisanim putem obavijestiti o daljnjim radnjama u vezi s njegovim zahtjevom, bez odgađanja.
- (6) Nadležno tijelo dužno je, bez naknade, pružiti informacije, odnosno poduzeti mjere, na temelju članka 69. ovog Zakona, te sve obavijesti pružene ili mjere poduzete na temelju članka 67., čl. 70. do 74. ovog Zakona i članka 87. ovog Zakona.
- (7) Ako je zahtjev nositelja podataka očito neutemeljen ili pretjeran, posebice zbog njegovog učestalog ponavljanja, nadležno tijelo može:

- a) naplatiti naknadu stvarnih administrativnih troškova, kao što su troškovi umnožavanja, skeniranja ili troškovi nosača podataka, kao i naknadu troškova dostave ili poduzimanja traženih mjera ili
 - b) odbiti postupiti po zahtjevu.
- (8) Teret dokazivanja očite neutemeljenosti ili pretjeranosti zahtjeva iz stavka (7) ovog članka je na nadležnom tijelu.
- (9) Ako nadležno tijelo ima opravdanu sumnju u pogledu identiteta fizičke osobe koja podnosi zahtjev iz čl. 70. ili 72. ovog Zakona, nadležno tijelo može zatražiti dodatne informacije neophodne za potvrđivanje identiteta nositelja podataka.

Članak 69.

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

- (1) Nadležno tijelo dužno je nositelju podataka staviti na raspolaganje kao minimum sljedeće informacije:
- a) identitet i kontaktne podatke nadležnog tijela
 - b) kontaktne podatke službenika za zaštitu osobnih podataka, ako je primjenjivo
 - c) svrhu obrade osobnih podataka
 - d) o pravu na podnošenje pritužbe Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu
 - e) o postojanju prava da od nadležnog tijela zatraži pristup svojim osobnim podacima, njihovu ispravku ili brisanje, ili ograničenje obrade osobnih podataka.
- (2) Osim informacija iz stavka (1) ovog članka, radi ostvarivanja njegovih prava, nadležno tijelo nositelju podataka daje sljedeće dodatne informacije:
- a) pravni temelj obrade osobnih podataka
 - b) rok u kojem će se osobni podaci čuvati ili, ako to nije moguće, o kriterijima korištenim za utvrđivanje tog roka
 - c) o kategorijama primatelja osobnih podataka, uključujući druge države ili međunarodne organizacije, ako je primjenjivo
 - d) prema potrebi i dodatne informacije ako se osobni podaci prikupljaju bez znanja nositelja podataka.
- (3) Posebnim zakonom mogu se propisati mjere za odgađanje, ograničenje ili uskraćivanje pružanja informacija iz stavka (2) ovog članka nositelju podataka u onoj mjeri i u onom trajanju u kojem takva mjera predstavlja potrebnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje temeljnih prava i legitimnih interesa nositelja podataka, s ciljem da se:
- a) spriječi ometanje službenog i zakonom uređenog prikupljanja informacija, istraga ili postupaka
 - b) izbjegne ometanje sprječavanja, istrage i otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela ili izvršavanja kaznenih 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 točaka iz stavka (3) ovog članka.

Članak 70.

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

- (1) Nadležno tijelo dužno je, u roku od 30 dana od dana zaprimanja zahtjeva za pristup osobnim podacima, nositelju podataka izdati potvrdu o tome obrađuje li njegove osobne podatke te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacijama o:
 - a) svrsi obrade i pravnom temelju obrade
 - b) kategoriji osobnih podataka koji se obrađuju
 - c) primatelju ili kategoriji primatelja kojemu su osobni podaci otkriveni, posebno primatelju u drugoj državi ili međunarodnoj organizaciji
 - d) predviđenom roku u kojem će se osobni podaci čuvati, ako je to moguće, ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog roka
 - e) postojanju prava da od nadležnog tijela zatraži ispravku ili brisanje svojih osobnih podataka ili ograničenje obrade osobnih podataka
 - f) pravu na podnošenje pritužbe Agenciji i kontaktnim podacima Agencije ili tužbe nadležnom sudu
 - g) osobnim podacima koji se obrađuju i o svim dostupnim informacijama o izvoru osobnih podataka.
- (2) Potvrda iz stavka (1) ovog članka izdaje se u skladu s odredbama članka 71. ovog Zakona.

Članak 71.

(Ograničenja prava pristupa osobnom podatku)

- (1) Posebnim zakonom koji se odnosi na nadležno tijelo može se nositelju podataka u cjelini ili djelomično ograničiti pravo pristupa osobnom podatku u onoj mjeri i u onom trajanju u kojem takvo djelomično ili potpuno ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje temeljnih prava i legitimnih interesa nositelja podataka, kako bi se:
 - a) spriječilo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka
 - b) izbjeglo ometanje sprječavanja, istrage i otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela ili izvršavanja kaznenih sankcija
 - c) zaštitila javna sigurnost
 - d) zaštitila državna sigurnost
 - e) zaštitila prava i slobode drugih.
- (2) Posebnim zakonom mogu se odrediti kategorije obrade koje mogu u cjelini ili djelomično biti obuhvaćene bilo kojom točkom iz stavka (1) ovog članka.

- (3) U slučajevima iz st. (1) i (2) ovog članka, nadležno tijelo dužno je, bez odgađanja, pisanim putem obavijestiti nositelja podataka o svakom odbijanju ili ograničenju pristupa osobnim podacima te o razlozima odbijanja ili ograničenja, osim ako bi pružanje takvih informacija dovelo u pitanje neku od svrha iz stavka (1) ovog članka.
- (4) Nadležno tijelo dužno je obavijestiti nositelja podataka o mogućnosti podnošenja pritužbe Agenciji ili tužbe nadležnom sudu.
- (5) Nadležno tijelo dužno je dokumentirati činjenične ili pravne razloge na kojima se temelji odluka.
- (6) Dokumentacija iz stavka (5) ovog članka stavlja se Agenciji na raspolaganje.

Članak 72.

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

- (1) Nadležno tijelo dužno je:
 - a) bez nepotrebnog odgađanja, nositelju podataka omogućiti ispravku netočnih osobnih podataka koji se na njega odnose. Uzimajući u obzir svrhe obrade podataka, nositelj podataka ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave
 - b) nositelju podataka omogućiti brisanje osobnih podataka, bez nepotrebnog odgađanja, ako se obradom krše odredbe čl. 60., 64. ili 66. ovog Zakona, ili ako se osobni podaci moraju brisati radi poštovanja pravne obveze iz posebnog zakona
 - c) ograničiti obradu ako:
 - 1) nositelj podataka osporava točnost osobnih podataka, a njihovu točnost ili netočnost nije moguće utvrditi ili
 - 2) osobni podaci moraju biti sačuvani kao dokaz
 - d) obavijestiti nositelja podataka prije uklanjanja ograničenja obrade ako je obrada ograničena na temelju točke c) alineje 1) ovog stavka
 - e) pisanim putem obavijestiti nositelja podataka o svakom odbijanju ispravke ili brisanja osobnih podataka ili ograničenja obrade te o razlozima odbijanja. Posebnim zakonom koji se odnosi na nadležno tijelo može se nositelju podataka potpuno ili djelomično ograničiti pravo pristupa u onoj mjeri i u onom trajanju u kojem takvo potpuno ili djelomično ograničenje čini neophodnu i proporcionalnu mjeru u demokratskom društvu, uz poštovanje temeljnih prava i legitimnih interesa nositelja podataka, kako bi se:
 - 1) izbjeglo ometanje službenog ili zakonom uređenog prikupljanja informacija, istraga ili postupaka
 - 2) izbjeglo ometanje sprječavanja, istrage i otkrivanja kaznenih djela ili gonjenja počinitelja kaznenih djela ili izvršavanja kaznenih sankcija
 - 3) zaštitila javna sigurnost
 - 4) zaštitila državna sigurnost
 - 5) zaštitila prava i slobode drugih
 - f) obavijestiti nositelja podataka o mogućnosti podnošenja pritužbe Agenciji ili tužbe nadležnom sudu
 - g) o ispravci netočnih osobnih podataka obavijestiti nadležno tijelo od kojeg potiču netočni podaci.

- (2) Nadležno tijelo dužno je, ako su osobni podaci ispravljani ili brisani, ili je obrada bila ograničena na temelju stavka (1) toč. a), b) ili c) ovog članka, obavijestiti primatelje, a primatelji su dužni ispraviti ili obrisati osobne podatke ili ograničiti obradu osobnih podataka u okviru svoje odgovornosti.

Članak 73.

(Ostvarivanje prava nositelja podataka i provjera Agencije)

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

Članak 74.

(Prava nositelja podataka u kaznenim istragama i postupcima)

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

Članak 75.

(Obveza nadležnog tijela)

- (1) Nadležno tijelo dužno je primijeniti odgovarajuće tehničke i organizacijske mjere imajući u vidu prirodu, opseg, okolnosti i svrhe obrade, kao i rizike različitih razina vjerojatnoće i ozbiljnosti za prava i slobode fizičkih osoba, kako bi osiguralo da se obrada vrši u skladu s ovim Zakonom i kako bi to moglo dokazati. Te mjere se prema potrebi preispituju i ažuriraju.
- (2) Mjere iz stavka (1) ovog članka, ako su razmjerne u odnosu na aktivnosti obrade, uključuju provođenje odgovarajućih politika zaštite podataka od nadležnog tijela.

Članak 76.

(Tehnička i integrirana zaštita osobnog podatka od nadležnog tijela)

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

podaci nisu automatski, bez intervencije fizičke osobe, dostupni neograničenom broju osoba.

Članak 77.

(Nadležno tijelo kao zajednički kontrolor podataka)

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

Članak 78.

(Korištenje usluge obrađivača od nadležnog tijela)

- (1) Nadležno tijelo koristi uslugu samo onog obrađivača koji može u dovoljnoj mjeri osigurati provođenje odgovarajućih tehničkih i organizacijskih mjera propisanih ovim Zakonom.
- (2) Korištenje usluge obrađivača od nadležnog tijela uređuje se ugovorom ili drugim pravnim aktom kojim se uređuju predmet, tehničke i organizacijske mjere propisane ovim Zakonom, trajanje obrade, opseg, sadržaj i svrha obrade, vrsta osobnih podataka, kategorije nositelja podataka te obveze i prava nadležnog tijela, kao i da obrađivač:
 - a) djeluje samo prema uputama nadležnog tijela
 - b) osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim odredbama o povjerljivosti
 - c) bilo kojim odgovarajućim sredstvom pomaže nadležnom tijelu osigurati usklađenost s odredbama o pravima nositelja podataka
 - d) prema izboru nadležnog tijela, briše ili vraća nadležnom tijelu sve osobne podatke nakon završetka pružanja usluge obrade podataka te briše postojeće preslike, osim ako prema nekoj zakonskoj odredbi ne postoji obveza čuvanja osobnih podataka
 - e) nadležnom tijelu stavlja na raspolaganje sve informacije potrebne za pridržavanje odredbi ovoga članka
 - f) poštuje odredbe stavka (3) ovoga članka za angažiranje drugog obrađivača.
- (3) Obradač ne može koristiti uslugu drugog obrađivača bez prethodnog pisanog odobrenja nadležnog tijela.
- (4) Po zaprimanju odobrenja obrađivač je dužan obavijestiti nadležno tijelo o svim planiranim izmjenama u vezi s korištenjem usluge drugih obrađivača.

osobnih podataka u drugoj državi ili međunarodnoj organizaciji, odobriti daljnji prijenos.

- (2) Nadležnom tijelu dopušten je prijenos, bez prethodnog odobrenja druge države, u skladu sa stavkom (1) točkom c) ovog članka, izuzetno, ako je prijenos osobnih podataka potreban za sprječavanje neposredne i ozbiljne prijetnje javnoj sigurnosti Bosne i Hercegovine ili druge države ili bitnim interesima Bosne i Hercegovine, a prethodno odobrenje se ne može pravodobno dobiti.
- (3) Nadležno tijelo dužno je obavijestiti tijelo u drugoj državi, odgovorno za izdavanje prethodnog odobrenja, o slučaju iz stavka (2) ovog članka.
- (4) Sve odredbe u vezi s prijenosom osobnih podataka u drugu državu ili međunarodnu organizaciju primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite fizičkih osoba koja je zajamčena ovim dijelom Zakona.

Članak 92.

(Prijenos od nadležnog tijela na temelju odluke o adekvatnosti)

- (1) Prijenos osobnih podataka u drugu državu ili međunarodnu organizaciju može se vršiti ako Vijeće ministara Bosne i Hercegovine odluči da druga država, teritorij, ili jedan ili više konkretnih sektora unutar te druge države, ili međunarodna organizacija osigurava adekvatnu razinu zaštite, u kojem slučaju takav prijenos ne zahtijeva posebno odobrenje.
- (2) Smatra se da je adekvatna razina zaštite iz stavka (1) ovog članka osigurana u državi, dijelovima njezina teritorija, ili jednom ili više sektora u toj državi, međunarodnoj organizaciji, za koje je od Europske unije utvrđeno da osiguravaju adekvatnu razinu zaštite osobnih podataka.
- (3) Odluku o adekvatnosti razine zaštite osobnih podataka iz stavka (1) ovog članka donosi Vijeće ministara Bosne i Hercegovine na prijedlog Agencije.
- (4) Agencija priprema prijedlog odluke iz stavka (3) ovog članka uzimajući u obzir:
 - a) vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno opće i sektorsko zakonodavstvo, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, državnoj sigurnosti, kazneno pravo i pristup javnih tijela osobnim podacima, kao i primjenu tog zakonodavstva, pravila o zaštiti osobnih podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos osobnih podataka u još jednu drugu državu ili međunarodnu organizaciju, koja se poštuju u toj drugoj državi ili međunarodnoj organizaciji, sudsku praksu, kao i postojanje djelotvornih i provedivih prava nositelja podataka i efikasnu upravnu i sudsku zaštitu nositelja podataka
 - b) postojanje i efikasno funkcioniranje jednog ili više neovisnih nadzornih tijela u drugoj državi ili tijela kojem podliježe međunarodna organizacija, odgovornih za osiguravanje i provođenje poštovanja pravila o zaštiti podataka, što uključuje adekvatne izvršne ovlasti za pružanje pomoći nositeljima podataka u ostvarivanju njihovih prava, kao i za suradnju s Agencijom
 - c) međunarodne obveze koje je druga država ili međunarodna organizacija preuzela ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezinog sudjelovanja u multilateralnim ili regionalnim organizacijama, posebice u vezi sa zaštitom osobnih podataka.

- (5) Agencija kontinuirano prati stanje u području zaštite osobnih podataka u drugoj državi, dijelu njezinog teritorija, jednom ili više sektora unutar te države ili međunarodnoj organizaciji i o tome po potrebi izvještava Vijeće ministara Bosne i Hercegovine.
- (6) Izvješće iz stavka (5) ovog članka uključuje dostupne informacije i informacije prikupljene od međunarodnih organizacija, koje su od značaja za preispitivanje postojanja adekvatne razine zaštite osobnih podataka, na temelju čega Vijeće ministara Bosne i Hercegovine donosi odluku iz stavka (3) ovog članka.
- (7) Odluka donesena na temelju stavka (3) ovog članka ne dovodi u pitanje prijenos osobnih podataka u drugu državu, na teritorij ili u jedan ili više određenih sektora unutar te druge države ili međunarodnu organizaciju, u skladu s čl. 93. i 94. ovog Zakona.
- (8) Lista država, dijela njihovih teritorija, jedan ili više sektora unutar tih država i međunarodnih organizacija glede kojih je Vijeće ministara Bosne i Hercegovine donijelo odluku da ne osiguravaju ili da više ne osiguravaju adekvatnu razinu zaštite osobnih podataka objavljuje se u „Službenom glasniku BiH“ i na službenoj internetskoj stranici Agencije.

Članak 93.

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

- (1) Nadležno tijelo može izvršiti prijenos osobnih podataka u drugu državu ili međunarodnu organizaciju, ako nije donesena odluka na temelju članka 92. stavka (3) ovog Zakona, uz sljedeće uvjete:
 - a) ako su odgovarajuće zaštitne mjere glede zaštite osobnih podataka predviđene u pravno obvezujućem instrumentu ili
 - b) ako je nadležno tijelo procijenilo sve okolnosti u vezi s prijenosom osobnih podataka i zaključilo da postoje odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.
- (2) Nadležno tijelo dužno je obavijestiti Agenciju o kategorijama prijenosa u skladu sa stavkom (1) točkom b) ovog članka.
- (3) Kada se prijenos osobnih podataka temelji na stavku (1) točki b) ovog članka, nadležno tijelo dužno je takav prijenos dokumentirati, a dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje je dobilo podatke, obrazloženje prijenosa i koji su osobni podaci preneseni.

Članak 94.

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

- (1) Ako ne postoji odluka o adekvatnosti iz članka 92. stavka (3) ovog Zakona ili odgovarajuće zaštitne mjere iz članka 93. ovog Zakona, prijenos ili skup prijenosa osobnih podataka u drugu državu ili međunarodnu organizaciju vrši se samo ako je prijenos neophodan i ako ispunjava jedan od sljedećih uvjeta:
 - a) kako bi se zaštitili ključni interesi nositelja podataka ili druge osobe
 - b) kako bi se zaštitili legitimni interesi nositelja podataka, ako je to predviđeno posebnim zakonom

- (5) Nadležno tijelo može uskratiti suglasnost obrađivaču za korištenje usluge drugog obrađivača.
- (6) Ako obrađivač utvrđuje svrhe i načine obrade kršeći odredbe ovoga Zakona, taj se obrađivač smatra nadležnim tijelom glede obrade koja mu je povjerena.

Članak 79.

(Obrada pod kontrolom nadležnog tijela)

Osoba koja djeluje pod kontrolom nadležnog tijela ili obrađivača, a ima pristup osobnim podacima, ne smije obrađivati te podatke bez naloga kontrolora podataka, osim kada je to propisano posebnim zakonom.

Članak 80.

(Evidencija o obradi od nadležnog tijela)

- (1) Nadležno tijelo vodi evidenciju obrade za koju je odgovorno. Ta evidencija sadrži sljedeće informacije:
 - a) naziv i kontaktne podatke nadležnog tijela, zajedničkog nadležnog tijela i službenika za zaštitu osobnih podataka
 - b) svrhu obrade
 - c) kategoriju primatelja kojem su osobni podaci otkriveni ili će mu biti otkriveni, uključujući primatelja u drugoj državi ili međunarodnoj organizaciji
 - d) opis kategorije nositelja podataka i kategorije osobnih podataka
 - e) uporabu izrade profila, ako je primjenjivo
 - f) kategoriju prijenosa osobnih podataka u drugu državu ili međunarodnu organizaciju, ako je primjenjivo
 - g) pravni temelj za postupak obrade, uključujući prijenose, kojem su osobni podaci namijenjeni
 - h) predviđeni rokovi za brisanje različitih kategorija osobnih podataka, ako je moguće
 - i) opći opis tehničkih i organizacijsko-sigurnosnih mjera iz članka 85. stavka (1) ovog Zakona, ako je moguće.
- (2) Nadležno tijelo 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 osobnih podataka u drugu državu ili međunarodnu organizaciju, ako za to postoji izričita uputa kontrolora podataka, uključujući identifikaciju te druge države ili međunarodne organizacije
 - d) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 85. stavka (1).

- (3) Evidencija iz stavka (1) ovog članka mora biti u pisanom obliku, što uključuje elektronički oblik.
- (4) Nadležno tijelo na zahtjev Agencije, prilikom nadzora, stavlja evidenciju na uvid.

Članak 81.

(Zapisivanje)

- (1) Nadležno tijelo dužno je, kod automatiziranog sustava obrade osobnih podataka, uspostaviti pristup sustavu 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 osobe koja je izvršila uvid ili otkrila osobne podatke i identitet primatelja takvih osobnih podataka.
- (2) Zapis se upotrebljava samo u svrhe provjere zakonitosti obrade, samopraćenja i osiguranja cjelovitosti i sigurnosti osobnih podataka te za kaznene postupke.
- (3) Nadležno tijelo na zahtjev Agencije, prilikom nadzora, stavlja zapise na uvid.

Članak 82.

(Suradnja nadležnog tijela i obrađivača s Agencijom)

Nadležno tijelo i obrađivač dužni su surađivati s Agencijom, na zahtjev, pri izvršavanju njezine nadležnosti.

Članak 83.

(Procjena utjecaja na zaštitu osobnog podatka od nadležnog tijela)

- (1) Nadležno tijelo prije obrade vrši procjenu utjecaja predviđenih postupaka obrade na zaštitu osobnih podataka, ako je vjerojatno da će neka vrsta obrade, posebno primjenom novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe te obrade, prouzročiti visoki rizik za prava i slobode osoba.
- (2) Procjena iz stavka (1) ovog članka mora sadržavati najmanje opći opis predviđenih postupaka obrade, procjenu rizika za prava i slobode nositelja podataka, predviđene mjere za rizike, zaštitne i sigurnosne mjere i mehanizme kako bi se osigurala zaštita osobnih podataka i dokazala usklađenost s ovim Zakonom, uzimajući u obzir prava i legitimne interese nositelja podataka i drugih uključenih osoba.

Članak 84.

(Prethodno savjetovanje nadležnog tijela s Agencijom)

- (1) Nadležno tijelo ili obrađivač dužno je savjetovati se s Agencijom prije obrade osobnih podataka koji će biti uključeni u novu zbirku osobnih podataka, ako:
 - a) procjena utjecaja na zaštitu podataka, kako je predviđeno člankom 83. ovog Zakona, upućuje na to da bi obrada mogla prouzročiti visok rizik ako nadležno tijelo ne poduzme mjere kako bi umanjilo rizik ili
 - b) vrsta obrade, posebice ako se upotrebljavaju nove tehnologije, mehanizmi ili postupci, predstavlja visok rizik za prava i slobode nositelja podataka.

- (2) Agencija može uspostaviti popis postupaka obrade za koje je potrebno obaviti prethodno savjetovanje u skladu sa stavkom (1) ovog članka.
- (3) Nadležno tijelo dužno je Agenciji dostaviti procjenu utjecaja na zaštitu podataka na temelju članka 83. ovog Zakona i na njegov zahtjev pružiti sve ostale informacije s pomoću kojih će Agencija moći procijeniti usklađenost obrade te posebice rizike za zaštitu osobnih podataka nositelja podataka i povezane zaštitne mjere.
- (4) Agencija će u roku od 42 dana od zaprimanja pisanog zahtjeva iz stavka (1) ovog članka pisanim putem dati savjet nadležnom tijelu, te može iskoristiti bilo koju od svojih ovlasti, ako smatra da bi se namjeravanom obradom iz stavka (1) ovog članka kršile odredbe ovog Zakona, posebice ako nadležno tijelo nije u dovoljnoj mjeri utvrdilo ili umanjilo rizik.
- (5) Rok iz stavka (4) ovog članka može se prema potrebi produžiti za 30 dana, uzimajući u obzir složenost namjeravane obrade.
- (6) Agencija u roku od 30 dana od zaprimanja zahtjeva obavještava nadležno tijelo i, prema potrebi, obrađivača o svakom produženju i razlozima odgađanja.
- (7) O prijedlogu zakona kojim se regulira obrada osobnih podataka, prije njegovog upućivanja u parlamentarnu proceduru, predlagač se može prethodno savjetovati sa Agencijom.

Članak 85.

(Sigurnost obrade od nadležnog tijela i obrađivača)

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

- j) održava ispravna funkcija sustava, da se pojava pogrešaka u funkcioniranju sustava prijavi i da se čuvani osobni podaci ne mogu ugroziti zbog nedostataka u funkcioniranju sustava.

Članak 86.

(Obavješćavanje Agencije o povredi osobnog podatka od nadležnog tijela)

- (1) Nadležno tijelo dužno je u slučaju povrede osobnih podataka, bez odgađanja, a najkasnije 72 sata nakon saznanja za povredu, obavijestiti Agenciju o povredi osobnih podataka, osim ako povreda osobnih podataka ne ugrožava prava i slobode fizičke osobe.
- (2) Obradivač je dužan u slučaju povrede osobnih podataka, bez odgađanja, obavijestiti nadležno tijelo, nakon što sazna za povredu osobnih podataka.
- (3) Ako obavješćavanje Agencije iz stavka (1) ovog članka nije izvršeno u roku od 72 sata, mora se sačiniti pisano obrazloženje s navođenjem razloga za kašnjenje.
- (4) Obavijest iz stavka (1) ovog članka sadrži najmanje sljedeće informacije:
 - a) opis povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj nositelja podataka, kao i kategorije i približan broj evidencija osobnih podataka o kojima je riječ
 - b) ime i prezime te kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija
 - c) opis vjerojatne posljedice povrede osobnih podataka
 - d) opis mjera koje je nadležno tijelo poduzelo ili čije je poduzimanje predložilo radi rješavanja problema povrede osobnih 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) Nadležno tijelo dokumentira svaku povredu osobnih podataka iz stavka (1) ovog članka, uključujući i činjenice u vezi s povredom osobnih podataka, njezine posljedice i mjere poduzete za popravljivanje situacije.
- (7) Dokumentacija iz stavka (4) ovog članka mora biti dostupna Agenciji s ciljem provjere primjene ovog članka.
- (8) Nadležno tijelo osigurava da se u slučaju povrede osobnih podataka koja uključuje osobne podatke koje je prenio kontrolor podataka druge države ili koji su preneseni njemu, informacije iz stavka (4) prenose kontroloru podataka te države bez nepotrebnog odgađanja.

Članak 87.

(Obavješćavanje nositelja podatka o povredi osobnog podatka)

- (1) Ako je vjerojatno da će povreda osobnih podataka prouzročiti visok rizik za prava i slobode fizičke osobe, nadležno tijelo, bez odgađanja, obavještava nositelja podataka o povredi osobnih podataka.

- (2) U obavijesti iz stavka (1) ovog članka jasnim i jednostavnim jezikom opisuje se priroda povrede osobnih podataka te se navode najmanje informacije i mjere iz članka 86. stavka (4) toč. b), c) i d) ovog Zakona.
- (3) Obavješćavanje nositelja podataka nije obvezno ako je ispunjen jedan od sljedećih uvjeta:
- a) ako je nadležno tijelo poduzelo odgovarajuće tehničke i organizacijske mjere zaštite i te mjere su primijenjene na osobne podatke u vezi s kojima je došlo do povrede osobnih podataka, a prije svega mjere koje osobne podatke čine nerazumljivim osobi koja nije ovlaštena pristupiti im, kao što je enkripcija
 - b) ako je kontrolor podataka poduzeo naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode nositelja podataka
 - c) ako bi to zahtijevalo nerazmjeran napor. U tom slučaju se objavljuje javna obavijest ili se poduzima slična mjera kojom se nositelji podataka obavješćavaju na jednako djelotvoran način.
- (4) Ako nadležno tijelo do tog trenutka nije obavijestilo nositelja podataka o povredi osobnih podataka, Agencija, nakon razmatranja stupnja vjerojatnoće da će povreda osobnih podataka prouzročiti visok rizik, može od njega zahtijevati da to učini ili može zaključiti da je ispunjen neki od uvjeta iz stavka (3) ovog članka.
- (5) Obavješćavanje nositelja podataka može se odgoditi, ograničiti ili uskratiti u skladu s uvjetima i na temelju razloga iz članka 69. stavka (3) ovog Zakona.

Članak 88.

(Imenovanje službenika za zaštitu osobnih podataka od nadležnog tijela)

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

Članak 89.

(Radno mjesto službenika za zaštitu osobnih podataka nadležnog tijela)

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

Članak 90.

(Zadaci službenika za zaštitu osobnih podataka nadležnog tijela)

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

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

Članak 91.

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

- (1) Nadležno tijelo dužno je svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u drugu državu ili međunarodnu organizaciju, uključujući daljnji prijenos u još jednu drugu državu ili međunarodnu organizaciju, izvršavati pridržavajući se odredbi ovog dijela Zakona, samo ako su ispunjeni sljedeći uvjeti, i to:
 - a) prijenos je neophodan u svrhe utvrđene u članku 1. stavku (1) točki c) ovog Zakona
 - b) osobni podaci prenose se nadležnom tijelu u drugoj državi ili međunarodnoj organizaciji, koji predstavlja javno tijelo nadležno za potrebe iz članka 1. stavka (1) točka c) ovog Zakona
 - c) ako su osobni podaci preneseni ili stavljeni na raspolaganje iz druge države, ta je država dala prethodno odobrenje za prijenos u skladu sa svojim pravom
 - d) ako je Vijeće ministara Bosne i Hercegovine, na prijedlog Agencije, donijelo odluku o adekvatnosti iz članka 92. stavka (3) ovog Zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o adekvatnosti iz članka 92. stavka (3) ovog Zakona, moraju biti osigurane ili postoje odgovarajuće zaštitne mjere iz članka 93. ovog Zakona ili ako Vijeće ministara Bosne i Hercegovine nije donijelo odluku o adekvatnosti iz članka 92. stavka (3) ovog Zakona i nisu osigurane ili ne postoje odgovarajuće zaštitne mjere iz članka 93. ovog Zakona, primjenjuju se odstupanja za posebne situacije iz članka 94. ovog Zakona
 - e) u slučaju daljnjeg prijenosa u još jednu drugu državu ili međunarodnu organizaciju, nadležno tijelo koje je izvršilo prvi prijenos ili drugo nadležno tijelo u Bosni i Hercegovini može, nakon što je uzelo u obzir sve relevantne činjenice, uključujući ozbiljnost kaznenog djela, svrhu u koju su osobni podaci prvo preneseni i razinu zaštite

- c) kako bi se spriječila neposredna i ozbiljna prijetnja javnoj sigurnosti na teritoriju Bosne i Hercegovine ili druge države
 - d) u pojedinačnim slučajevima u svrhe navedene u članku 1. stavku (1) točki c) ovog Zakona ili
 - e) u pojedinačnom slučaju radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva u vezi sa svrhama navedenim u članku 1. stavku (1) točki c) ovog Zakona.
- (2) Osobni podaci ne smiju se prenositi ako nadležno tijelo koje vrši prijenos utvrdi da temeljna prava i slobode odnosnog nositelja podataka imaju prednost pred javnim interesom glede prijenosa iz stavka (1) toč. d) i e) ovog članka.
- (3) Ako se prijenos vrši na temelju stavka (1) ovog članka, nadležno tijelo dužno je takav prijenos dokumentirati i dokumentaciju, po zahtjevu, staviti na raspolaganje Agenciji, uključujući datum i vrijeme prijenosa, informacije o nadležnom tijelu koje je dobilo podatke, obrazloženje prijenosa i koji su osobni podaci preneseni.

Članak 95.

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

- (1) Nadležno tijelo može u skladu s posebnim zakonom, odstupajući od članka 91. stavka (1) točke b) ovog Zakona i ne dovodeći u pitanje nijedan međunarodni sporazum iz stavka (2) ovog članka, u pojedinačnim i posebnim slučajevima, prenijeti osobne podatke izravno primateljima sa sjedištem ili poslovnim nastanom u drugoj državi samo ako se pridržavaju odredbi ovog dijela Zakona i ako su ispunjeni sljedeći uvjeti:
- a) prijenos je isključivo neophodan za obavljanje zadatka nadležnog tijela koje obavlja prijenos kako je predviđeno posebnim zakonom u svrhe navedene u članku 1. stavku (1) točki c) ovog Zakona
 - b) nadležno tijelo koje vrši prijenos utvrdi da temeljna prava i slobode dotičnog nositelja podataka nemaju prednost nad javnim interesom koji iziskuje prijenos u predmetnom slučaju
 - c) nadležno tijelo koje vrši prijenos smatra da je prijenos tijelu nadležnom za postupanje u svrhu iz članka 1. stavka (1) točke c) ovog Zakona u drugu državu nedjelotvoran ili neprimjeren, posebno zato što se prijenos ne može pravodobno ostvariti
 - d) tijelo koje je u drugoj državi nadležno za postupanje u svrhu iz članka 1. stavka (1) točke c) ovog Zakona obaviješteno je bez odgađanja, osim ako je to nedjelotvorno ili neprimjereno
 - e) nadležno tijelo koje vrši prijenos obavijesti primatelja o određenoj svrsi ili svrhama u koje taj primatelj isključivo može obrađivati osobne podatke, samo ako je takva obrada neophodna.
- (2) Međunarodni sporazum iz stavka (1) ovog članka je svaki bilateralni ili multilateralni međunarodni sporazum na snazi između Bosne i Hercegovine i druge države u području pravosudne suradnje u kaznenim stvarima i policijske suradnje.
- (3) Nadležno tijelo koje vrši prijenos dužno je obavijestiti Agenciju o prijenosima u skladu s ovim člankom.
- (4) Nadležno tijelo koje vrši prijenos osobnih podataka na temelju stavka (1) ovog članka dužno je takav prijenos dokumentirati.

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

Članak 96.

(Agencija)

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

Članak 97.

(Neovisnost Agencije)

- (1) Agencija djeluje potpuno neovisno pri obavljanju svojih nadležnosti u skladu s ovim Zakonom.
- (2) Ravnatelj, zamjenik ravnatelja i zaposleni u Agenciji, pri obavljanju svojih dužnosti i vršenju svojih ovlasti u skladu s ovim Zakonom, ne smiju biti izloženi neposrednom ili posrednom vanjskom utjecaju i ne smiju ni od koga tražiti ili primiti instrukcije.
- (3) Ravnatelj, zamjenik ravnatelja i zaposleni u Agenciji moraju se suzdržavati od svih radnji koje nisu u skladu s njihovim dužnostima i tijekom svog mandata i zaposlenja ne smiju se baviti nespojivom djelatnošću, bez obzira na to je li ona plaćena ili ne.
- (4) Agencija mora imati ljudske, tehničke i financijske resurse, prostorije i infrastrukturu potrebne za efikasno vršenje svojih nadležnosti, uključujući i ovlasti koje se odnose na međunarodnu uzajamnu pomoć i suradnju.
- (5) Zaposleni u Agenciji su državni službenici i zaposlenici i na njih se primjenjuju Zakon o državnoj službi u institucijama Bosne i Hercegovine i Zakon o radu u institucijama Bosne i Hercegovine.
- (6) Pravilnik o unutarnjem ustrojstvu Agencije donosi ravnatelj Agencije uz prethodnu suglasnost Vijeća ministara Bosne i Hercegovine.
- (7) Sredstva potrebna za rad Agencije osiguravaju se iz proračuna institucija Bosne i Hercegovine i međunarodnih obveza Bosne i Hercegovine.
- (8) Agencija podliježe financijskoj kontroli u skladu s propisima o financijskoj kontroli.

Članak 98.

(Rukovođenje Agencijom)

- (1) Agencijom rukovodi ravnatelj.

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

Članak 99.

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

- (1) Ravnatelja i zamjenika ravnatelja imenuje Parlamentarna skupština Bosne i Hercegovine (u daljnjem tekstu: Parlamentarna skupština) na temelju javnog natječaja.
- (2) Ravnatelj i zamjenik ravnatelja imenuju se na razdoblje od šest godina uz mogućnost još jednog ponovnog imenovanja.
- (3) Uvjeti za imenovanje ravnatelja i zamjenika ravnatelja su:
 - a) da je stariji od 18 godina
 - b) da je državljanin Bosne i Hercegovine u skladu sa Zakonom o državljanstvu Bosne i Hercegovine
 - c) da nije osuđivan i da se protiv njega ne vodi kazneni postupak
 - d) da nije obuhvaćen odredbom članka IX. 1. Ustava Bosne i Hercegovine
 - e) da je zdravstveno sposoban
 - f) završen fakultet društvenog smjera, VSS/VII stupanj ili visoko obrazovanje bolonjskog sustava studiranja s najmanje 240 ECTS bodova
 - g) da ima najmanje 10 godina radnog iskustva u struci, od čega najmanje pet godina radnog iskustva na poslovima rukovođenja
 - h) da ima stručna znanja i iskustva iz područja zaštite osobnih podataka
 - i) da nije član političke stranke.
- (4) Parlamentarna skupština može privremeno suspendirati ravnatelja i zamjenika ravnatelja ako se otkrije teška povreda službene dužnosti. Privremena suspenzija traje dok se teška povreda službene dužnosti ne utvrdi konačnom odlukom.
- (5) Parlamentarna skupština može razriješiti ravnatelja i zamjenika ravnatelja prije isteka mandata:
 - a) na njegov zahtjev
 - b) ako se utvrdi teška povreda službene dužnosti ili
 - c) ako više ne ispunjava uvjete potrebne za imenovanje.

Članak 100.

(Nespojivost funkcije i obveza čuvanja profesionalne tajne)

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

Članak 101.

(Nadležnosti Agencije)

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

Članak 102.

(Zadaci Agencije)

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

- i) donosi standardne ugovorne klauzule iz članka 30. stavka (8) i članka 48. stavka (3) ovog Zakona
 - j) utvrđuje i vodi popis obrada u vezi s obvezom vršenja procjene utjecaja na zaštitu podataka u skladu s člankom 37. stavkom (4) ovog Zakona
 - k) daje savjete o postupku obrade osobnih podataka iz članka 38. stavka (2) ovog Zakona i članka 84. stavka (4) ovog Zakona
 - l) potiče izradu kodeksa ponašanja i daje mišljenje i odobrava takve kodekse ponašanja koji pružaju dovoljne zaštitne mjere u skladu s člankom 42. stavkom (5) ovog Zakona
 - m) potiče uspostavu mehanizama certifikacije zaštite podataka, kao i pečata i oznaka za zaštitu podataka u skladu s člankom 44. stavkom (1) ovog Zakona i odobrava kriterije certifikacije u skladu s člankom 44. stavkom (6) ovog Zakona
 - n) u određenim slučajevima vrši periodično preispitivanje izdanih certifikata u skladu s člankom 44. st. (8) i (9) ovog Zakona
 - o) sačinjava i objavljuje kriterije za akreditaciju tijela za praćenje kodeksa ponašanja u skladu s člankom 43. ovog Zakona i akreditaciju certifikacijskog tijela u skladu s člankom 45. ovog Zakona
 - p) vrši akreditaciju tijela za praćenje kodeksa ponašanja u skladu s člankom 43. ovog Zakona i akreditaciju certifikacijskog tijela u skladu s člankom 45. ovog Zakona
 - r) odobrava odgovarajuće zaštitne mjere iz članka 48. stavka (4) ovog Zakona
 - s) odobrava obvezujuća poslovna pravila u skladu s člankom 49. ovog Zakona
 - t) vodi internu evidenciju o kršenjima ovog Zakona i mjerama koje su poduzete u skladu s člankom 103. stavkom (2) ovog Zakona
 - u) daje mišljenje na prijedlog zakona institucijama na razini Bosne i Hercegovine, koji se odnosi na obradu osobnih podataka
 - v) izvršava sve ostale zadatke u vezi sa zaštitom osobnih podataka.
- (2) Agencija propisuje izgled i sadržaj obrasca za podnošenje pritužbe.
 - (3) Agencija obavlja zadatke besplatno za nositelje podataka i ako je to primjenjivo, i za službenike za zaštitu osobnih podataka.
 - (4) Agencija obavlja zadatke besplatno za nositelje podataka i za službenike za zaštitu osobnih podataka iz DIJELA TREĆEG ovog Zakona.
 - (5) Ako su zahtjevi nositelja podataka očito neutemeljeni ili pretjerani, posebice zbog učestalog ponavljanja, Agencija može naplatiti naknadu stvarnih administrativnih troškova ili odbiti postupiti po zahtjevu, pri čemu Agencija snosi teret dokazivanja očite neutemeljenosti ili pretjeranosti zahtjeva.
 - (6) Agencija naplaćuje naknadu za izdavanje akreditacije certifikacijskom tijelu.
 - (7) Agencija naplaćuje naknadu za davanje mišljenja i drugih usluga, poslovnim subjektima u svrhu obavljanja njihove redovite djelatnosti.
 - (8) Kriterije za određivanje visine naknade iz st. (5), (6) i (7) ovog članka utvrđuje Agencija uz prethodnu suglasnost Vijeća ministara Bosne i Hercegovine i oni se objavljuju u „Službenom glasniku BiH“.
 - (9) Naknada se uplaćuje na Jedinstveni račun trezora institucija Bosne i Hercegovine.

Članak 103.
(Ovlasti Agencije)

(1) Agencija ima sljedeće ovlasti:

- a) vršiti preispitivanje certifikata izdanih u skladu s člankom 44. st. (8) i (9) ovog Zakona
- b) vršiti inspekcijske nadzore
- c) vršiti reviziju zaštite podataka
- d) naložiti kontroloru podataka i obrađivaču, a prema potrebi i predstavniku kontrolora podataka ili obrađivača, dostavljanje svih informacija potrebnih za obavljanje njezinih zadataka
- e) obavijestiti kontrolora podataka ili obrađivača o navodnom kršenju ovog Zakona
- f) ostvariti pristup svim osobnim podacima i svim informacijama u posjedu kontrolora podataka i obrađivača, koje su potrebne za obavljanje njezinih zadataka
- g) ostvariti pristup svim prostorijama kontrolora podataka i obrađivača, u kojima se vrši obrada osobnih podataka, uključujući svu opremu i sredstva za obradu podataka.

(2) Agencija ima sljedeće korektivne ovlasti:

- a) izreći upozorenje kontroloru podataka ili obrađivaču da bi namjeravane obrade mogle lako predstavljati kršenje ovog Zakona
- b) izreći opomenu kontroloru podataka ili obrađivaču ako se obradom krši ovaj Zakon
- c) naložiti kontroloru podataka ili obrađivaču da postupi po zahtjevu nositelja podataka za ostvarivanje njegovih prava u skladu s ovim Zakonom
- d) naložiti kontroloru podataka ili obrađivaču da obrade, ako je potrebno, uskladi s odredbama ovog Zakona na točno određen način i u točno zadanom roku
- e) naložiti kontroloru podataka da nositelja podataka obavijesti o povredi osobnih podataka
- f) privremeno ili trajno ograničiti ili zabraniti obradu
- g) naložiti ispravljanje ili brisanje osobnih podataka ili ograničenje obrade i obavješćavanje o takvim radnjama primatelja kojima su osobni podaci otkriveni
- h) oduzeti certifikat izdan u skladu s čl. 44. i 45. ovog Zakona ili certifikacijskom tijelu naložiti da ne izda certifikat ako zahtjevi za certifikaciju nisu ispunjeni ili da povuče certifikat ako zahtjevi više nisu ispunjeni
- i) izdati prekršajni nalog u okviru prekršajnog postupka ili podnijeti zahtjev za pokretanje prekršajnog postupka u skladu sa ovim Zakonom
- j) naložiti privremeno obustavljanje prijenosa podataka primatelju u drugoj državi ili međunarodnoj organizaciji.

(3) Agencija ima sljedeće ovlasti u vezi s odobravanjem i savjetovanjem:

- a) savjetovati kontrolora podataka u skladu s postupkom prethodnog savjetovanja iz čl. 38. i 84. ovog Zakona
- b) davati mišljenja o svim pitanjima koja se tiču zaštite osobnih podataka, na vlastitu inicijativu ili na zahtjev zakonodavnih tijela, vlada ili, u slučajevima kada je to posebnim zakonom propisano, drugim institucijama i tijelima, kao i javnosti

- c) odobriti obradu iz članka 38. stavka (8) ovog Zakona ako je posebnim zakonom propisano takvo prethodno odobrenje
 - d) davati mišljenja i odobravati nacрте kodeksa ponašanja u skladu s člankom 42. stavkom (5) ovog Zakona
 - e) akreditirati certifikacijska tijela u skladu s člankom 45. ovog Zakona
 - f) odobravati kriterije certifikacije u skladu s člankom 44. stavkom (6) ovog Zakona
 - g) usvajati standardne klauzule o zaštiti podataka iz članka 30. stavka (8) i članka 48. stavka (3) ovog Zakona
 - h) odobriti odgovarajuće zaštitne mjere iz članka 48. stavka (4) točke a) ovog Zakona
 - i) odobriti odgovarajuće zaštitne mjere iz članka 48. stavka (4) točke b) ovog Zakona
 - j) odobriti obvezujuća poslovna pravila u skladu s člankom 49. ovog Zakona.
- (4) Odluka Agencije je konačna u upravnom postupku i protiv nje nije dopuštena žalba, ali se može pokrenuti upravni spor pred Sudom Bosne i Hercegovine.
- (5) Agencija u postupku odlučivanja primjenjuje pravila upravnog postupka, osim ako ovim Zakonom nije drugačije propisano.
- (6) Agencija je ovlaštena da po potrebi obavijesti nadležna istražna tijela o povredama ovog Zakona ili pokrene pravne postupke, ili u tim postupcima na drugi način sudjeluje kako bi se proveo ovaj Zakon.
- (7) Svaka obrada osobnih podataka koji imaju određen stupanj tajnosti na temelju posebnog zakona, provodi se u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.
- (8) Obradu osobnih podataka iz stavka (7) ovog članka provode službenici Agencije koji imaju dozvolu za pristup tajnim podacima, u skladu sa zakonom kojim se uređuje zaštita tajnih podataka.

Članak 104.

(Međunarodna suradnja radi zaštite osobnih podataka)

Agencija poduzima odgovarajuće mjere u vezi s drugim državama i međunarodnim organizacijama radi:

- a) razvoja mehanizama međunarodne suradnje za olakšavanje efikasnog provođenja zakonodavstva o zaštiti osobnih podataka
- b) osiguravanja uzajamne međunarodne pomoći u provođenju zakonodavstva o zaštiti osobnih podataka, što podrazumijeva obavješćavanje, upućivanje pritužbe, pružanje pomoći u istragama i razmjenu informacija, u skladu s odgovarajućim mjerama za zaštitu osobnih podataka i drugim temeljnim pravima i slobodama
- c) uključivanja relevantnih interesnih skupina u raspravu i aktivnosti čiji je cilj unapređenje međunarodne suradnje na provođenju zakonodavstva o zaštiti osobnih podataka
- d) promoviranja razmjene i dokumentiranja zakonodavstva i prakse u vezi sa zaštitom osobnih podataka, uključujući i sporove oko nadležnosti s drugim državama.

Članak 105.
(Povjerljivo prijavljivanje povreda Zakona)

- (1) Nadležno tijelo koje obrađuje osobne podatke u svrhe iz članka 1. stavka (1) točke c) ovog Zakona dužno je osigurati primjenu efikasnih mehanizama za povjerljivo prijavljivanje slučajeva povrede ovog Zakona.
- (2) Mehanizmi koji se primjenjuju u skladu sa stavkom (1) ovog članka moraju osigurati da se povreda može prijaviti nadležnom tijelu ili Agenciji.
- (3) Ovi mehanizmi uključuju podizanje svijesti o zaštiti osobnih podataka i mjere o zaštiti osoba koje prijavljuju povrede.

Članak 106.
(Izvješća Agencije)

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

Članak 107.
(Inspekcijski nadzor)

- (1) Inspekcijski nadzor nad provođenjem ovog Zakona obavlja inspektor Agencije.
- (2) Inspektor svoj identitet, svojstvo i ovlaštenje dokazuje legitimacijom inspektora.
- (3) Inspekcijskim nadzorom ostvaruje se neposredan uvid u zakonitost rada i postupanje kontrolora podataka i obrađivača s ciljem provjere usklađenosti njegovog rada sa ovim Zakonom i drugim propisima koji se odnose na zaštitu osobnih podataka.
- (4) Inspekcijski nadzor može biti redoviti, izvanredni i revizijski.
- (5) Redoviti inspekcijski nadzor se provodi na temelju godišnjeg i mjesečnog plana inspekcijskog nadzora, koji se donosi na razini Agencije.
- (6) Rješenje iz redovitog inspekcijskog nadzora donosi inspektor, protiv kojeg je dozvoljena žalba ravnatelju Agencije u roku od 15 dana od dana prijema rješenja.
- (7) Izvanredni inspekcijski nadzor se provodi na temelju pritužbe ili postupanja po službenoj dužnosti kada je, u odnosu na konkretni slučaj, potrebno izvršiti inspekcijski nadzor.
- (8) Zapisnik iz izvanrednog inspekcijskog nadzora je dokazno sredstvo u postupku po pritužbi ili po službenoj dužnosti, koji provodi i rješava Agencija.
- (9) Revizijski inspekcijski nadzor se provodi nakon redovitog ili izvanrednog inspekcijskog nadzora s ciljem provjere izvršenja naloženih upravnih mjera.
- (10) Rješenje u postupku nakon izvršenog izvanrednog i revizijskog inspekcijskog nadzora, donosi ravnatelj Agencije i isto je konačno u upravnom postupku.
- (11) Nakon provedenog inspekcijskog nadzora, inspektor sastavlja zapisnik o utvrđenom činjeničnom stanju, koji potpisuju inspektor i ovlaštena osoba kontrolora podataka ili obrađivača.
- (12) Inspektor ima pravo pregledati sve poslovne prostorije i objekte u kojima se vrši obrada osobnih podataka, proces rada, uređaje, isprave i dokumentaciju, kao i obavljati druge radnje u vezi sa svrhom inspekcijskog nadzora, u skladu s člankom 103. stavkom (1) toč. f) i g) i člankom 103. st. (7) i (8) ovog Zakona.

- (13) Kontrolor podataka i obrađivač dužni su inspektoru omogućiti nesmetano vršenje inspekcijskog nadzora.
- (14) Ako se inspektoru u tijeku inspekcijskog nadzora, onemogućava vršenje nadzora ili pruži fizički otpor ili ako se taj otpor osnovano očekuje, inspektor može zatražiti pomoć policije.
- (15) O izvršenom inspekcijskom nadzoru inspektor vodi evidenciju.

DIO PETI – PRAVNA SREDSTVA, ODGOVORNOST I KAZNE

Članak 108.

(Pravo na pritužbu Agenciji)

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

Članak 109.

(Pravo na djelotvorno pravno sredstvo protiv odluka Agencije)

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

Članak 110.

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

- (1) Nositelj podataka ima pravo na sudsku zaštitu protiv kontrolora podataka ili obrađivača ako smatra da su zbog obrade osobnih podataka prekršena njegova prava iz ovoga Zakona i ako nije koristio pravo na pritužbu Agenciji iz članka 108. stavak (1) ovog Zakona.
- (2) Postupak sudske zaštite iz stavka (1) ovog članka, vodi se u skladu sa zakonima kojima se uređuje parnični postupak.

Članak 111.

(Zastupanje nositelja podataka)

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

Članak 112.

(Pravo na naknadu štete i odgovornost)

- (1) Svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja ovog Zakona ima pravo na naknadu za pretrpljenu štetu od kontrolora podataka ili obrađivača.
- (2) Svaki kontrolor podataka odgovoran je za štetu prouzročenu obradom kojom se krši ovaj Zakon. Obradivač je odgovoran za štetu prouzročenu obradom samo ako nije poštovao obveze iz ovog Zakona koje su posebno propisane za obrađivače ili ako je prekoračio zakonite instrukcije kontrolora podataka ili je postupio protivno njima.
- (3) Kontrolor podataka ili obrađivač izuzet je od odgovornosti ako dokaže da nije ni na koji način odgovoran za događaj koji je prouzročio štetu.
- (4) Ako je u istu obradu uključeno više od jednog kontrolora podataka ili obrađivača ili su u istu obradu uključeni i kontrolor podataka i obrađivač i ako su odgovorni za štetu prouzročenu obradom, svaki kontrolor podataka ili obrađivač odgovoran je za cjelokupnu štetu.
- (5) Ako je kontrolor podataka ili obrađivač platio punu odštetu u skladu sa stavkom (4) ovog članka, taj kontrolor podataka ili obrađivač ima pravo od drugih kontrolora podataka ili obrađivača, koji su uključeni u istu obradu, zahtijevati povrat dijela odštete koji odgovara njihovom udjelu u odgovornosti za štetu.
- (6) Pravo na naknadu štete ostvaruje se u sudskom postupku, a mjesna nadležnost utvrđuje se u skladu s člankom 110. stavkom (2) ovog Zakona.

Članak 113.

(Opći uvjeti za izricanje novčane kazne)

- (1) Agencija osigurava da je izricanje novčane kazne, u skladu s ovim člankom i u vezi s povredama ovog Zakona, u svakom pojedinačnom slučaju djelotvorno, razmjerno i odvraćajuće.
- (2) Agencija izdaje prekršajni nalog ili podnosi zahtjev za pokretanje prekršajnog postupka nadležnom sudu, pored mjera iz članka 103. stavka (2) toč. a) do h) i točke j) ovog Zakona, u ovisnosti o okolnostima svakog pojedinačnog slučaja. Prilikom odlučivanja o novčanoj kazni i iznosu kazne u svakom pojedinačnom slučaju u obzir se uzima posebno:
 - a) priroda, težina i trajanje povrede, imajući u vidu prirodu, opseg i svrhu predmetne obrade, kao i broj nositelja podataka i stupanj štete koju su pretrpjeli
 - b) ima li povreda obilježje namjere ili nepažnje

- c) svaka radnja koju je kontrolor podataka ili obrađivač poduzeo kako bi ublažio štetu koju su pretrpjeli nositelji podataka
 - d) stupanj odgovornosti kontrolora podataka ili obrađivača, pri čemu se uzimaju u obzir tehničke i organizacijske mjere koje su primijenili, u skladu s čl. 27. i 34. ovog Zakona
 - e) sve utvrđene prethodne povrede od kontrolora podataka ili obrađivača
 - f) stupanj suradnje s Agencijom na otklanjanju povrede i ublažavanju mogućih štetnih posljedica povrede
 - g) kategorija osobnih podataka na koje povreda utječe
 - h) način na koji je Agencija saznala za povredu, a posebno je li i u kojem opsegu kontrolor podataka ili obrađivač izvijestio o povredi
 - i) ako su protiv kontrolora podataka ili obrađivača u vezi s istim predmetom prethodno izrečene mjere iz članka 103. stavka (2) ovog Zakona, i poštovanje tih mjera
 - j) poštovanje odobrenih kodeksa ponašanja, u skladu sa člankom 42. ovog Zakona ili odobrenih mehanizama certifikacije, u skladu sa člankom 44. ovog Zakona
 - k) sve ostale otežavajuće ili olakšavajuće okolnosti, kao što su financijska dobit ostvarena kršenjem ili izbjegnuti gubici, izravno ili neizravno, tim kršenjem.
- (3) Ako kontrolor podataka ili obrađivač za istu ili povezane obrade namjerno ili iz nepažnje prekrši više odredbi ovog Zakona, ukupan iznos novčane kazne ne smije biti veći od iznosa utvrđenog za najtežu povredu.
- (4) Novčanom kaznom u iznosu od 10.000 KM do 20.000.000 KM kažnjava se:
- a) kontrolor podataka i obrađivač za obradu osobnih podataka izvršenu suprotno čl. 10. i 13., čl. 27. do 41., te čl. 44. i 45. ovog Zakona
 - b) certifikacijsko tijelo koje postupi suprotno čl. 44. i 45. ovog Zakona
 - c) tijelo za praćenje odobrenih kodeksa ponašanja ako postupi suprotno članku 43. stavku (3) ovog Zakona.
- (5) Novčanom kaznom u iznosu od 20.000 KM do 40.000.000 KM kaznit će se:
- a) tko vrši obradu osobnih podataka suprotno čl. 7., 8., 9. i 11. ovog Zakona
 - b) tko krši prava nositelja podataka iz čl. 14. do 24. ovog Zakona
 - c) tko prenese osobne podatke primatelju u drugu državu ili međunarodnu organizaciju suprotno čl. 46. do 51. ovog Zakona
 - d) tko postupi suprotno obvezama iz posebnih zakona donesenih na temelju DIJELA DRUGOG Poglavlja V. ovog Zakona
 - e) tko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenom obustavljanju prijenosa podataka u skladu s člankom 103. stavkom (2) ovog Zakona ili uskrati pristup suprotno članku 103. stavku (1) ovog Zakona.
- (6) Za nepostupanje po nalogu Agencije iz članka 103. stavka (2) ovog Zakona u skladu sa stavkom (2) ovog članka izriče se novčana kazna u iznosu od 20.000 KM do 40.000.000 KM.
- (7) Za povredu iz st. (4), (5) i (6) ovoga članka novčanom kaznom u iznosu od 5.000 KM do 70.000 KM kaznit će se odgovorna osoba, a novčanom kaznom od 500 KM do 5.000 KM kaznit će se zaposlena osoba kod kontrolora podataka ili obrađivača.

- (8) Novčanom kaznom u iznosu od 5.000 KM do 70.000 KM, kaznit će se odgovorna osoba, a novčanom kaznom u iznosu od 500 KM do 5.000 KM kaznit će se zaposlena osoba u javnom i nadležnom tijelu za prekršaj:
- a) iz čl. 7. do 11., članka 13., čl. 14. do 24., čl. 27. do 41., čl. 44. i 45., čl. 52. do 59., članka 60., članka 64., članka 66., čl. 67. do 73., čl. 76. i 77. i čl. 79. do 90. ovog Zakona
 - b) tko prenese osobne podatke primatelju u drugu državu ili međunarodnu organizaciju suprotno čl. 46. do 51., te čl. 91. do 95. ovog Zakona
 - c) tko ne postupi po nalogu Agencije ili privremenom ili trajnom ograničenju obrade ili privremenom obustavljanju prijenosa podataka u skladu s člankom 103. stavkom (2) ovog Zakona ili uskrati pristup suprotno članku 103. stavku (1) ovog Zakona.
- (9) Zastarijevanje izricanja novčane kazne nastupa nakon proteka razdoblja od pet godina od dana kada je povreda izvršena.
- (10) Ne dovodeći u pitanje nadležnosti i ovlasti Agencije, novčane kazne ne mogu se izreći javnom tijelu i nadležnom tijelu za povrede ovoga Zakona, osim odgovornoj i zaposlenoj osobi iz stavka (8) ovog članka.
- (11) Na postupak izricanja novčane kazne iz ovog članka primjenjuju se odredbe Zakona o prekršajima Bosne i Hercegovine, a iznosi novčanih kazni propisani su ovim Zakonom.
- (12) Izuzetno od odredbe stavka (11) ovoga članka, prihod ostvaren na temelju naplate novčanih kazni, dijeli se na način propisan člankom 114. ovoga Zakona.

Članak 114.

(Izvršenje i naplata novčane kazne)

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

- a) ako je sjedište ili poslovni nastan pravne osobe ili prebivalište fizičke osobe u Bosni i Hercegovini, sredstva sa Jedinstvenog računa trezora institucija Bosne i Hercegovine se uplaćuju na račun entiteta ili Brčko distrikta Bosne i Hercegovine, ovisno od sjedišta ili poslovnog nastana pravne osobe ili prebivališta fizičke osobe
- b) ako je sjedište ili poslovni nastan pravne osobe ili prebivalište fizičke osobe izvan Bosne i Hercegovine, sredstva sa Jedinstvenog računa trezora institucija Bosne i Hercegovine raspoređuju se prema Odluci o utvrđivanju privremenih koeficijenata za raspodjelu sredstava s Jedinstvenog računa. U Federaciji Bosne i Hercegovine sredstva se raspoređuju između županija i općina u skladu sa Zakonom o pripadnosti javnih prihoda u Federaciji Bosne i Hercegovine.

Članak 115.

(Kazne)

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

DIO ŠESTI – PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 116.

(Mjere u prijelaznom razdoblju)

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

Članak 117.

(Podzakonski akti)

Svi podzakonski akti propisani ovim Zakonom donijet će se u roku od 210 dana od dana stupanja na snagu ovoga Zakona.

Članak 118.

(Odnos s prethodno sklopljenim sporazumima)

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

Članak 119.

(Prestanak važenja)

- (1) Početkom primjene ovog Zakona prestaje važiti Zakon o zaštiti osobnih podataka („Službeni glasnik BiH“, br. 49/06, 76/11 i 89/11).
- (2) Početkom primjene ovog Zakona prestaju važiti podzakonski akti doneseni na temelju Zakona iz stavka (1) ovog članka: Pravilnik o postupku po prigovoru nositelja osobnih podataka u Agenciji za zaštitu osobnih podataka u Bosni i Hercegovini („Službeni glasnik BiH“, broj 51/09), Pravilnik o inspekcijskom nadzoru u području zaštite osobnih podataka („Službeni glasnik BiH“, broj 51/09), Instrukcija o načinu provjere obrade osobnih

podataka prije uspostave zbirke osobnih podataka („Službeni glasnik BiH”, broj 51/09), Pravilnik o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka („Službeni glasnik BiH”, broj 52/09) i Pravilnik o načinu čuvanja i posebnim mjerama tehničke zaštite osobnih podataka („Službeni glasnik BiH”, broj 67/09).

Članak 120.

(Stupanje na snagu i primjena)

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

PS BiH broj /24
2024. godine
Sarajevo

Predsjedatelj
Doma naroda
Parlamentarne skupštine BiH

Predsjedatelj
Zastupničkog doma
Parlamentarne skupštine BiH