

Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka

Sadržaj

- I. OPĆE ODREDBE
- II. NAČELA
- III. PRAVA ISPITANIKA
- IV. VODITELJ OBRADJE I IZVRŠITELJ OBRADJE
- V. PRIJENOSI OSOBNIH PODATAKA TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA
- VI. NADZOR
- VII. PRIGOVORI I PRAVNA ZAŠTITA
- VIII. PREKRŠAJNE ODREDBE
- IX. PRIJELAZNE I ZAVRŠNE ODREDBE

I. OPĆE ODREDBE

Članak 1.

Ovim Zakonom utvrđuju se pravila zaštite fizičkih osoba u vezi s obradom i razmjenom osobnih podataka od strane nadležnih tijela u svrhu sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i sprječavanje takvih prijetnji.

Članak 2.

Ovim Zakonom u hrvatsko zakonodavstvo preuzima se Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprječavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119/89, od 4. 5. 2016.).

Članak 3.

(1) Ovaj Zakon primjenjuje se na obradu osobnih podataka od strane nadležnih tijela za svrhe utvrđene u članku 1. ovoga Zakona automatiziranu u cijelosti ili djelomično te na neautomatiziranu obradu osobnih podataka, a koja čini ili će činiti dio sustava pohrane.

(2) Odredbe ovoga Zakona ne primjenjuju se na obradu i razmjenu osobnih podataka tijekom djelatnosti koje u području nacionalne sigurnosti obavljaju tijela sigurnosno-obavještajnog sustava, djelatnosti u vezi s pitanjima iz područja nacionalne sigurnosti koje obavljaju tijela obrambenog sustava, kao i na obradu i razmjenu osobnih podataka pri obavljanju djelatnosti obuhvaćenih glavom V. poglavljem 2. Ugovora o Europskoj uniji.

Članak 4.

(1) Pojedini pojmovi u smislu ovoga Zakona imaju sljedeće značenje:

1) osobni podatak je svaka informacija koja se odnosi na fizičku osobu čiji je identitet utvrđen ili se može utvrditi

2) ispitanik je fizička osoba čiji se identitet može utvrditi izravno ili neizravno uz pomoć identifikatora, kao što su ime i prezime, osobni identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet

3) obrada osobnih podataka je postupak ili skup postupaka koji se provode nad osobnim podacima ili skupovima osobnih podataka, bilo automatiziranim ili neautomatiziranim sredstvima, kao što je prikupljanje, bilježenje, organiziranje, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom i širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje

4) ograničavanje obrade je označavanje pohranjenih osobnih podataka radi ograničavanja njihove obrade u budućnosti

5) izrada profila je svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s ispitanikom, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem fizičke osobe

6) pseudonimizacija je obrada osobnih podataka na način da se podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati ispitaniku čiji je identitet utvrđen ili se može utvrditi

7) sustav pohrane je svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi

- 8) nadležno tijelo je tijelo javne vlasti nadležno za sprječavanje, istraživanje, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i sprječavanje takvih prijetnji
- 9) voditelj obrade je nadležno tijelo koje samostalno ili zajednički s drugim tijelima određuje svrhe i sredstva obrade osobnih podataka
- 10) zajednički voditelji obrade su voditelji obrade dva ili više nadležnih tijela koja imaju zajednički definiranu svrhu i način obrade
- 11) izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti ili drugo tijelo koje obrađuje osobne podatke po zahtjevu voditelja obrade
- 12) primatelj je fizička ili pravna osoba, tijelo javne vlasti ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Tijela javne vlasti koja mogu primiti osobne podatke u okviru provođenja kriminalističkih istraživanja kaznenog djela i kaznenog postupka ne smatraju se primateljima, a obrada takvih podataka mora biti u skladu s pravilima o zaštiti podataka.
- 13) povreda osobnih podataka je kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani
- 14) genetski podatak podrazumijeva sve osobne podatke, osobito one dobivene analizom biološkog uzorka, a koji se odnose na naslijeđena ili stečena genetska obilježja fizičke osobe koja daju jedinstvenu informaciju o fiziologiji ili zdravlju te fizičke osobe
- 15) biometrijski podatak podrazumijeva osobne podatke dobivene posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja fizičke osobe koja omogućuju ili potvrđuju jedinstvenu identifikaciju
- 16) zdravstveni podatak podrazumijeva osobne podatke povezane s fizičkim ili mentalnim zdravljem fizičke osobe
- 17) nadzorno tijelo je neovisno tijelo javne vlasti propisano ovim Zakonom
- 18) međunarodna organizacija je organizacija i njezina tijela uređena međunarodnim javnim pravom ili bilo koje drugo tijelo koje su sporazumom ili na osnovi sporazuma osnovale dvije ili više zemalja.
- (2) Odredbe ovoga Zakona kojima se propisuje prijenos podataka u države članice Europske unije primjenjuju se i na Republiku Island, Kraljevinu Norvešku, Švicarsku Konfederaciju i Kneževinu Lihtenštajn.
- (3) Ostali pojmovi koji se koriste u ovome Zakonu, a značenje im nije propisano u stavku 1. ovoga članka, imaju značenje kako je propisano Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (u daljnjem tekstu: Uredba (EU) 2016/679).

Članak 5.

Izrazi koji se koriste u ovome Zakonu, a imaju rodno značenje, odnose se jednako na muški i ženski rod.

II. NAČELA

Članak 6.

Načela obrade osobnih podataka

- (1) Osobni podaci moraju se obrađivati pošteno i zakonito.

- (2) Obrada se može provoditi samo ako je nužna i samo u onoj mjeri u kojoj je to potrebno radi postizanja svrhe navedene u članku 1. ovoga Zakona i pod uvjetima propisanim ovim Zakonom
- (3) Osobni podaci prikupljaju se i obrađuju u svrhu koja je izričito navedena i u skladu sa zakonom.
- (4) Osobni podaci ne smiju se prikupljati u većem opsegu nego što je to nužno za postizanje svrhe prikupljanja.
- (5) Osobni podaci moraju biti točni, potpuni i prema potrebi ažurni.
- (6) Voditelj obrade ili izvršitelj obrade mora poduzeti razumne mjere da se podaci koji nisu točni, uzimajući u obzir svrhu u koju se obrađuju, bez odgode isprave ili brišu.
- (7) Osobni podaci moraju se čuvati u obliku koji dopušta identifikaciju ispitanika, ne duže nego je to potrebno za svrhu u koju se podaci obrađuju.
- (8) Osobni podaci se obrađuju na način kojim se osigurava sigurnost osobnih podataka, primjenom odgovarajućih tehničkih ili organizacijskih mjera.
- (9) Obrada osobnih podataka, različita od svrhe iz članka 1. ovoga Zakona, dopuštena je ako je:
- voditelj obrade posebnim propisom ovlašten za obradu takvih osobnih podataka
 - obrada nužna i proporcionalna drugoj zakonitoj svrsi.
- (10) Obrada osobnih podataka koju obavlja voditelj obrade može uključivati i arhiviranje podataka kada je to potrebno radi javnog interesa, znanstvenih, statističkih ili povijesnih svrha te potrebe iz članka 1. ovoga Zakona, pri čemu se primjenjuju odgovarajuće mjere radi zaštite prava i sloboda ispitanika.
- (11) Voditelj obrade odgovoran je za usklađenost svoga postupanja s odredbama stavaka 1. – 10. ovoga članka te je mora biti u mogućnosti dokazati.

Članak 7.

Rokovi za pohranu i preispitivanje

Nadležna tijela koja obrađuju osobne podatke u svrhu iz članka 1. ovoga Zakona postupaju u skladu s posebnim propisima u primjeni odgovarajućih rokova za njihovo brisanje ili za periodično preispitivanje potrebe za pohranom osobnih podataka.

Članak 8.

Razlika između različitih kategorija ispitanika

Prilikom obrade osobnih podataka, prema potrebi i koliko je god to moguće, nadležno tijelo mora osigurati jasnu razliku između osobnih podataka različitih kategorija ispitanika, kao što su:

1. osobe za koje postoji sumnja da su počinile ili će počiniti kazneno djelo
2. osobe pravomoćno osuđene za kazneno djelo
3. žrtve kaznenog djela
4. osobe koje imaju saznanja o počinjenom kaznenom djelu.

Članak 9.

Razlika između osobnih podataka i provjera kvalitete osobnih podataka

(1) Nadležna tijela osiguravaju da se osobni podaci koji su netočni, nepotpuni ili neažurni ne prenose niti ne stavljaju na raspolaganje te da se osobni podaci utemeljeni na činjenicama razlikuju od osobnih podataka utemeljenih na osobnim procjenama ili prikupljenih tehničkim uređajima.

(2) Nadležno tijelo provjerava kvalitetu osobnih podataka prije njihova prenošenja ili stavljanja na raspolaganje.

(3) Pri prenošenju osobnih podataka dodaju se nužne informacije koje primatelju omogućavaju procjenu stupnja točnosti, potpunosti, pouzdanosti i ažurnosti osobnih podataka.

(4) Kada se utvrdi da su preneseni osobni podaci netočni ili da su preneseni nezakonito, primatelj mora biti obaviješten bez odgode.

(5) U slučaju iz stavka 4. ovoga članka, osobni podaci moraju se ispraviti, brisati ili se obradu mora ograničiti u skladu s člankom 17. stavkom 4. ovoga Zakona.

Članak 10.

Posebni uvjeti obrade

(1) Osobni podaci koje nadležna tijela prikupljaju za svrhe utvrđene u članku 1. ovoga Zakona mogu se obrađivati i u svrhe koje nisu propisane u članku 1. ovoga Zakona, ako je to propisano posebnim propisom, a na takvu obradu podataka primjenjuje se Uredba (EU) 2016/679.

(2) Ako je nadležnim tijelima povjereno obavljanje zadaća drukčijih od onih koje se obavljaju u svrhe iz članka 1. ovoga Zakona, na obradu podataka za takve svrhe primjenjuje se Uredba (EU) 2016/679, uključujući i za arhiviranje u javnom interesu ili u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe.

(3) Ako nadležno tijelo koje prenosi podatke predviđa posebne uvjete za njihovu obradu, nadležno tijelo koje prenosi takve osobne podatke će obavijestiti i upozoriti primatelja kojemu ih prenosi o tim uvjetima i zahtjevu za poštivanje tih uvjeta.

(4) Nadležno tijelo koje prenosi podatke ne primjenjuje uvjete iz stavka 3. ovoga članka na primatelje u drugim državama članicama ili na agencije, urede i tijela osnovane u skladu s glavom V. poglavljima 4. i 5. Ugovora o funkcioniranju Europske unije, različite od onih koji su primjenjivi na slične prijenose podataka drugih nadležnih tijela u smislu ovoga Zakona.

Članak 11.

Obrada posebnih kategorija osobnih podataka

(1) Zabranjena je obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, religijska ili filozofska uvjerenja ili sindikalno članstvo te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije ispitanika ili podataka koji se odnose na zdravlje, spolni život ili seksualnu orijentaciju ispitanika.

(2) Dopuštena je obrada podataka iz stavka 1. ovoga članka ako je:

- obrada osobnih podataka potrebna u svrhu izvršavanja prava i obveza koje ima voditelj obrade na temelju ovoga Zakona ili posebnih propisa
- obrada osobnih podataka nužna radi zaštite života ili tjelesnog integriteta ispitanika ili druge osobe
- ispitanik sam objavio osobne podatke.

(3) U slučaju iz stavka 2. ovoga članka, obrada podataka mora biti posebno označena i zaštićena.

Članak 12.

Automatizirano pojedinačno donošenje odluka

- (1) Odluka koja proizvodi pravni učinak za ispitanika ne može se temeljiti samo na automatiziranoj obradi.
- (2) Iznimno od stavka 1. ovoga članka, donošenje odluke koja proizvodi ili utječe na pravni učinak na ispitanika, a temelji se isključivo na automatiziranoj obradi osobnih podataka i na izradi profila namijenjenih procjeni određenih osobnih aspekata ispitanika, dopuštena je samo ako je donošenje takve odluke predviđeno ovim Zakonom ili drugim propisima kojima se osigurava odgovarajuća zaštita prava ispitanika.
- (3) Odluke iz stavaka 1. i 2. ovoga članka ne smiju se temeljiti na posebnim kategorijama osobnih podataka iz članka 11. ovoga Zakona, osim ako su uspostavljene odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika.
- (4) Zabranjuje se izrada profila koja dovodi do diskriminacije ispitanika na temelju posebnih kategorija osobnih podataka iz članka 11. ovoga Zakona.

III. PRAVA ISPITANIKA

Članak 13.

Obavještavanje i način obavještavanja ispitanika

- (1) Voditelj obrade dužan je osigurati da se ispitaniku pruže sve informacije određene odredbama ovoga Zakona.
- (2) Informacije iz stavka 1. ovoga članka pružaju se odgovarajućim sredstvom.
- (3) U pravilu, voditelj obrade pruža informacije u istom obliku u kojem je zaprimio zahtjev ispitanika.
- (4) Voditelj obrade dužan je u roku od 30 dana od dana zaprimanja zahtjeva pisano obavijestiti podnositelja zahtjeva o radnjama koje su poduzete u vezi s njegovim zahtjevom.
- (5) Informacije se stavljaju na raspolaganje ili daju ispitaniku bez naknade.
- (6) Iznimno od odredbe stavka 5. ovoga članka, kod neutemeljenih ili pretjeranih zahtjeva ispitanika, osobito zbog njihovog učestalog ponavljanja, voditelj obrade može naplatiti naknadu sukladno posebnom propisu, uzimajući u obzir administrativne troškove za pružanje informacija ili obavijesti ili za poduzimanje traženih mjera ili može odbiti postupiti po zahtjevu.
- (7) Voditelj obrade obrazlaže neutemeljenost ili pretjeranost zahtjeva te o tome u pisanom obliku izvješćuje podnositelja zahtjeva.
- (8) Kada postoji sumnja u identitet podnositelja zahtjeva, voditelj obrade može tražiti pružanje dodatnih informacija potrebnih za potvrđivanje identiteta.
- (9) Ako podnositelj zahtjeva ne dokaže svoj identitet, voditelj obrade odbit će postupiti po zahtjevu.

Članak 14.

Informacije koje su dostupne ili se daju ispitaniku

- (1) Voditelj obrade učinit će dostupnim ispitaniku sljedeće informacije:
 1. naziv, sjedište i kontaktne podatke voditelja obrade
 2. kontaktne podatke službenika za zaštitu osobnih podataka
 3. svrhu obrade za koje su ti osobni podaci namijenjeni

4. obavijest o pravu na podnošenje prigovora nadzornom tijelu i naziv, sjedište i kontaktne podatke nadzornog tijela
5. obavijest da ima pravo od voditelja obrade zatražiti pristup osobnim podacima, njihov ispravak ili brisanje, ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika.

(2) Osim informacija iz stavka 1. ovoga članka, ispitaniku se, radi ostvarivanja njegovih prava, mogu učiniti dostupnim i informacije o:

1. pravnom temelju obrade podataka
2. razdoblju u kojem će se osobni podaci pohranjivati ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja
3. kategorijama primatelja osobnih podataka, uključujući treće zemlje ili međunarodne organizacije.

(3) Ako se osobni podaci prikupljaju bez znanja ispitanika, radi ostvarivanja njegovih prava, u određenim slučajevima prema potrebi i procjeni, mogu mu se učiniti dostupnim i druge dodatne informacije.

Članak 15.

Pravo ispitanika na pristup

(1) Voditelj obrade dužan je ispitaniku najkasnije u roku od 30 dana od zaprimanja zahtjeva izdati potvrdu o tome obrađuju li se njegovi osobni podaci, a ako se obrađuju, dozvoliti pristup takvim osobnim podacima i sljedećim informacijama:

1. svrhama obrade i pravnom temelju obrade
2. kategorijama osobnih podataka
3. primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama
4. predviđenom razdoblju u kojem će se osobni podaci pohranjivati ili kriterijima korištenima za utvrđivanje tog razdoblja
5. postojanju prava da se od voditelja obrade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika
6. o pravu na podnošenje prigovora nadzornom tijelu i kontaktne podatke nadzornog tijela
7. o obavješćivanju o osobnim podacima koji se obrađuju i o svim dostupnim informacijama o njihovu izvoru.

(2) Zahtjev iz stavka 1. ovoga članka mora sadržavati osobne podatke podnositelja zahtjeva, dokaz o identitetu, datum podnošenja zahtjeva i potpis.

Članak 16.

Ograničenja prava pristupa i informacija koje se stavljaju na raspolaganje ili daju ispitaniku

(1) Voditelj obrade će ispitaniku u cijelosti ili djelomično ograničiti pravo iz članka 14. stavaka 2. i 3. i članka 15. ovoga Zakona u onoj mjeri i u onom trajanju u kojem takvo djelomično ili potpuno ograničavanje čini neophodnu i proporcionalnu mjeru uz poštivanje temeljnih prava i zakonitih interesa ispitanika kako bi se:

1. izbjeglo ometanje istraživanja kaznenih djela i vođenje kaznenog postupka
2. izbjeglo ometanje istražnih i nadzornih postupaka koje provode tijela javne vlasti sukladno posebnim propisima

3. izbjeglo ometanje izvršavanja kaznenih sankcija

4. zaštitila javna sigurnost

5. zaštitila nacionalna sigurnost

6. zaštitila prava i slobode drugih.

(2) Voditelj obrade pisanim putem dostavlja obavijest ispitaniku o odbijanju ili ograničavanju pristupa i o razlozima koji su doveli do odbijanja ili ograničavanja, osim ako bi davanje takvih informacija dovelo u pitanje neku od svrha iz stavka 1. ovoga članka.

(3) Voditelj obrade upućuje ispitanika o pravu na podnošenje prigovora nadzornom tijelu ili ostvarivanje prava pristupa podnošenjem pravnog lijeka.

(4) Voditelj obrade dužan je na primjeren način zabilježiti činjenične ili pravne razloge na kojima se temelji njegova odluka.

(5) Podaci iz stavka 4. ovoga članka se na zahtjev stavljaju nadzornom tijelu na raspolaganje.

(6) U slučaju podnošenja prigovora iz stavka 3. ovoga članka, nadzorno tijelo zatražit će od Ureda Vijeća za nacionalnu sigurnost mišljenje o osnovanosti razloga ograničenja ako je odluka voditelja obrade o ograničenju prava ispitanika donesena iz razloga navedenog u stavku 1. točki 5. ovoga članka te će u tu svrhu Uredu Vijeća za nacionalnu sigurnost dostaviti odluku voditelja obrade i zabilježene činjenične ili pravne razloge na kojima se ona temelji, a koje nadzornom tijelu nije obvezujuće.

(7) Ured Vijeća za nacionalnu sigurnost će mišljenje o osnovanosti ograničenja prava ispitanika utvrditi u suradnji s nadležnom sigurnosno-obavještajnom agencijom.

Članak 17.

Pravo na ispravak ili brisanje osobnih podataka i ograničenje obrade

(1) Ispitanik može od voditelja obrade ishoditi ispravak netočnih odnosno nadopunu nepotpunih osobnih podataka na temelju pisanog zahtjeva, među ostalim i davanjem dodatne izjave.

(2) Zahtjev iz stavka 1. ovoga članka, osim podataka iz članka 15. stavka 2. ovoga Zakona, mora sadržavati i obrazloženje zahtjeva i dodatna pojašnjenja vezano uz zahtjev.

(3) Voditelj obrade će izbrisati osobne podatke bez odgode ako se krše odredbe članka 6. ili članka 11. ovoga Zakona ili kada se osobni podaci moraju brisati radi poštivanja pravne obveze kojoj podliježe voditelj obrade.

(4) Voditelj obrade će umjesto brisanja ograničiti obradu ako:

1. ispitanik osporava točnost osobnih podataka, a njihovu točnost nije moguće utvrditi

2. osobni podaci moraju biti sačuvani u obliku u kojem su prikupljeni i pohranjeni radi korištenja u kaznenom postupku.

(5) Ako je obrada ograničena na temelju stavka 4. točke 1. ovoga članka, voditelj obrade pisanim putem obavještava ispitanika prije uklanjanja ograničenja obrade te o svakom odbijanju ispravka ili brisanja osobnih podataka ili ograničavanja obrade, kao i razlozima odbijanja.

(6) Voditelj obrade može primijeniti razloge iz članka 16. stavka 1. točaka 1. – 5. ovoga Zakona kojima se u cijelosti ili djelomično ograničava obveza pružanja takvih informacija u onoj mjeri u kojoj takvo ograničavanje čini nužnu i proporcionalnu mjeru uz dužno poštovanje temeljnih prava i legitimnih interesa ispitanika.

(7) Voditelj obrade dužan je obavijestiti ispitanika o mogućnosti podnošenja prigovora nadzornom tijelu ili o pravu na podnošenje pravnog lijeka.

(8) Voditelj obrade o ispravku netočnih osobnih podataka dostavlja obavijest nadležnom tijelu od kojeg je zaprimio netočne podatke.

(9) Ako su osobni podaci bili ispravljani ili brisani ili je obrada bila ograničena na temelju stavka 4. ovoga članka, voditelj obrade dužan je obavijestiti primatelje kojima su podaci preneseni da isprave ili brišu osobne podatke ili ograniče obradu osobnih podataka u okviru svoje nadležnosti i odgovornosti.

Članak 18.

Ostvarivanje prava ispitanika i provjera nadzornog tijela

(1) U slučajevima iz članka 16. stavka 3. i članka 17. stavka 7. ovoga Zakona, prava ispitanika mogu se ostvariti i putem nadzornog tijela.

(2) Voditelj obrade dužan je obavijestiti i uputiti ispitanika o mogućnosti ostvarivanja njegovih prava putem nadzornog tijela.

(3) Kada ispitanik ostvaruje pravo iz stavka 1. ovoga članka, nadzorno tijelo obavještava ispitanika o tome da je provelo sve potrebne provjere ili preispitivanje te o pravu ispitanika na pravni lijek.

Članak 19.

Prava ispitanika u kaznenim istragama, istraživanjima i postupcima

Ako su osobni podaci sadržani u odluci suda ili drugog neovisnog pravosudnog tijela, evidenciji ili spisu predmeta obrađenom tijekom istraživanja, istrage i postupka, ispitanik prava iz članaka 14., 15. i 17. ovoga Zakona ostvaruje u skladu s posebnim propisima.

IV. VODITELJ OBRADJE I IZVRŠITELJ OBRADJE

Članak 20.

Obveze voditelja obrade

(1) Voditelj obrade, uzimajući u obzir sadržaj, opseg i svrhu obrade, kao i mogućnost nastupanja ugroza za prava i slobode ispitanika, provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s odredbama ovoga Zakona.

(2) Mjere iz stavka 1. ovoga članka se prema potrebi preispituju i ažuriraju.

(3) Mjere iz stavka 1. ovoga članka podrazumijevaju i provedbu odgovarajućih postupaka koje imaju za cilj zaštitu podataka od strane voditelja obrade.

Članak 21.

Tehnička i integrirana zaštita podataka

(1) Voditelj obrade u vrijeme određivanja sredstava obrade i u vrijeme same obrade provodi odgovarajuće tehničke i organizacijske mjere za omogućivanje učinkovite primjene načela zaštite podataka kako bi se ispunili zahtjevi iz ovoga Zakona i zaštitila prava ispitanika te kako bi se osiguralo da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade.

(2) Mjere iz stavka 1. ovoga članka odnose se na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost, čime se osigurava da osobni podaci bez intervencije fizičke osobe ne mogu biti dostupni neograničenom broju osoba.

Članak 22.

Zajednički voditelji obrade

(1) Zajednički voditelji obrade sporazumno određuju svoje odgovornosti i obveze tijekom obrade osobnih podataka, osobito u pogledu ostvarivanja prava ispitanika i svojih dužnosti pružanja informacija ispitaniku iz članka 14. ovoga Zakona.

(2) Zajednički voditelji obrade određuju jedinstvenu kontaktnu točku za ostvarivanje prava ispitanika.

Članak 23.

Izvršitelj obrade

(1) Voditelj obrade koristi usluge samo onog izvršitelja obrade koji može u dovoljnoj mjeri jamčiti provedbu odgovarajućih tehničkih i organizacijskih mjera propisanih odredbama ovoga Zakona.

(2) Korištenje usluga izvršitelja obrade od strane voditelja obrade uređuje se ugovorom ili drugim pravnim aktom kojim se uređuje predmet i trajanje obrade, opseg, sadržaj i svrha obrade, vrsta osobnih podataka, kategorije ispitanika te obveze i prava voditelja obrade, kao i da izvršitelj obrade:

1. djeluje samo prema uputama voditelja obrade

2. osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim odredbama o povjerljivosti

3. bilo kojim odgovarajućim sredstvom pomaže voditelju obrade osigurati usklađenost s odredbama o pravima ispitanika

4. prema izboru voditelja obrade, briše ili vraća voditelju obrade sve osobne podatke nakon dovršetka pružanja usluge obrade podataka te briše postojeće kopije, osim ako prema nekoj zakonskoj odredbi ne postoji obveza pohrane osobnih podataka

5. voditelju obrade stavlja na raspolaganje sve informacije potrebne za pridržavanje odredbi ovoga članka

6. poštuje odredbe stavka 3. ovoga članka za angažiranje drugog izvršitelja obrade.

(3) Izvršitelj obrade ne može koristiti usluge drugog izvršitelja obrade bez prethodnog pisanog odobrenja voditelja obrade.

(4) Po zaprimanju odobrenja izvršitelj obrade dužan je obavijestiti voditelja obrade o svim planiranim izmjenama u vezi s korištenjem drugih izvršitelja obrade.

(5) Voditelj obrade može uskratiti suglasnost izvršitelju obrade na korištenje usluga drugog izvršitelja obrade.

(6) Ako izvršitelj obrade utvrđuje svrhe i načine obrade kršeći odredbe ovoga Zakona, taj se izvršitelj obrade smatra voditeljem obrade u pogledu obrade koja mu je povjerena.

Članak 24.

Obrada pod vodstvom voditelja obrade ili izvršitelja obrade

Izvršitelj obrade i bilo koja osoba koja djeluje pod vodstvom voditelja obrade ili izvršitelja obrade, a koja ima pristup osobnim podacima, obrađuje samo one podatke koje od nje zatraži voditelj obrade, osim ako je to drugačije određeno posebnim propisom.

Članak 25.

Evidencija aktivnosti obrade

(1) Voditelj obrade u okviru svoje odgovornosti vodi evidenciju svih kategorija aktivnosti obrade koja sadržava sljedeće informacije:

1. naziv zbirke
2. ime i kontaktne podatke voditelja obrade i bilo kojeg zajedničkog voditelja obrade te službenika za zaštitu osobnih podataka
3. svrhe obrade
4. kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodnim organizacijama
5. opis kategorija ispitanika i kategorija osobnih podataka
6. upotreba izrade profila kada je to moguće s obzirom na svrhu obrade
7. kategorije prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju kada se podaci prenose
8. pravni temelj za postupak obrade, uključujući prijenose, kojem su osobni podaci namijenjeni
9. predviđene rokove za brisanje različitih kategorija osobnih podataka
10. opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 30. stavka 1. ovoga Zakona.

(2) Svaki izvršitelj obrade vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju u ime voditelja obrade, a koja sadržava:

1. ime i kontaktne podatke jednog ili više izvršitelja obrade i svakog voditelja obrade u čije ime izvršitelj obrade djeluje te službenika za zaštitu osobnih podataka
2. kategorije obrade koje se provode za svakog voditelja obrade
3. podatke o trećoj zemlji ili međunarodnoj organizaciji kojoj su prenijeti osobni podaci kada je za to postojala izričita uputa voditelja obrade
4. opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 30. stavka 1. ovoga Zakona.

(3) Evidencije iz stavaka 1. i 2. ovoga članka moraju biti u pisanom obliku, što uključuje i elektronički oblik.

(4) Voditelj obrade i izvršitelj obrade stavljaju evidenciju na raspolaganje nadzornom tijelu na njegov zahtjev.

Članak 26.

Zapisivanje

(1) U automatiziranim sustavima obrade podataka voditelj i izvršitelj obrade osiguravaju bilježenje postupaka obrade osobnih podataka.

- (2) Bilježenje postupaka obrade odnosi se i na datum i vrijeme obrade podataka te, ako je moguće, identitet osobe koja je obavila uvid ili otkrila osobne podatke, kao i identitet primatelja takvih osobnih podataka.
- (3) Zapisi se upotrebljavaju samo u svrhe provjere zakonitosti obrade, nadzora procesa i osiguravanja cjelovitosti i sigurnosti osobnih podataka.
- (4) Voditelj obrade i izvršitelj obrade na zahtjev stavljaju zapise na raspolaganje nadzornom tijelu.

Članak 27.

Suradnja s nadzornim tijelom

Voditelj obrade i izvršitelj obrade pružaju i daju na uvid sve potrebne informacije nadzornom tijelu radi obavljanja poslova iz njegove nadležnosti propisanih ovim Zakonom.

Članak 28.

Procjena učinka na zaštitu podataka

- (1) Voditelj obrade je prije poduzimanja obrade dužan provesti procjenu učinka planirane obrade na zaštitu osobnih podataka kada je vjerojatno da će neka obrada prouzročiti visoki rizik za prava i slobode fizičke osobe.
- (2) Procjena iz stavka 1. ovoga članka sadržava općeniti opis predviđenih postupaka obrade, procjenu rizika za prava i slobode ispitanika, predviđene mjere za rizike, zaštitne i sigurnosne mjere i mehanizme kako bi se osigurala zaštita osobnih podataka ispitanika i drugih uključenih osoba.

Članak 29.

Prethodno savjetovanje s nadzornim tijelom

(1) Voditelj obrade ili izvršitelj obrade dužan je provesti savjetovanje s nadzornim tijelom prije nove obrade osobnih podataka koji će biti uključeni u novi sustav pohrane koji se treba uspostaviti, ako:

1. procjena učinka na zaštitu podataka iz članka 28. ovoga Zakona upućuje na to da bi obrada mogla rezultirati visokim rizikom ako voditelj obrade ne poduzme mjere kako bi umanjio rizik
2. vrsta obrade predstavlja visok rizik za prava i slobode ispitanika.

(2) Savjetovanje s nadzornim tijelom provodi se tijekom izrade prijedloga zakona ili prijedloga drugih propisa koji se odnose na obradu osobnih podataka.

(3) Nadzorno tijelo utvrdit će i javno objaviti popis postupaka obrade za koje je potrebno obaviti prethodno savjetovanje u skladu sa stavkom 1. ovoga članka.

(4) Voditelj obrade nadzornom tijelu dostavlja procjenu učinka na zaštitu podataka na temelju članka 28. ovoga Zakona samostalno ili na temelju zahtjeva te pruža sve ostale informacije na temelju kojih će nadzorno tijelo moći procijeniti usklađenost obrade, a posebno rizike za zaštitu osobnih podataka ispitanika i povezane zaštitne mjere.

(5) Kada nadzorno tijelo smatra da bi se obradom iz stavka 1. ovoga članka kršile odredbe ovoga Zakona, osobito ako voditelj obrade nije u dovoljnoj mjeri utvrdio ili umanjio rizik, nadzorno tijelo u roku od najviše 45 dana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje voditelja obrade i, prema potrebi, izvršitelja obrade te može iskoristiti bilo koju od svojih ovlasti iz članka 44. ovoga Zakona.

(6) Rok iz stavka 5. ovoga članka može se prema potrebi produljiti za 30 dana, uzimajući u obzir složenost planirane obrade.

(7) Nadzorno tijelo u roku od 30 dana od zaprimanja zahtjeva obavještava voditelja obrade i, prema potrebi, izvršitelja obrade o svakom takvom produljenju te o razlozima odgode.

Članak 30.

Sigurnost obrade

(1) Voditelj obrade i izvršitelj obrade, uzimajući u obzir najnovija dostignuća i troškove provedbe te opseg, sadržaj i svrhe obrade, kao i rizik različite vjerojatnosti i ozbiljnosti za prava i slobode fizičkih osoba, provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, osobito u pogledu obrade posebnih kategorija osobnih podataka iz članka 11. ovoga Zakona.

(2) U pogledu automatizirane obrade voditelj obrade ili izvršitelj obrade nakon procjene rizika provode mjere čija je svrha sljedeće:

1. neovlaštenim osobama onemogućiti pristup opremi za obradu koja se upotrebljava za obradu
2. spriječiti neovlašteno čitanje, kopiranje, mijenjanje ili uklanjanje nosača podataka
3. spriječiti neovlašteno unošenje osobnih podataka te neovlašteno pregledavanje, mijenjanje ili brisanje pohranjenih osobnih podataka
4. spriječiti upotrebu sustava automatizirane obrade neovlaštenim osobama koje se koriste opremom za podatkovnu komunikaciju
5. osigurati da osobe koje su ovlaštene za upotrebu sustava automatizirane obrade imaju pristup samo osobnim podacima koji su predviđeni njihovim odobrenjem za pristup
6. osigurati mogućnost provjere i utvrđivanja tijela kojima su osobni podaci preneseni ili bi mogli biti preneseni ili stavljeni na raspolaganje upotrebom opreme za podatkovnu komunikaciju
7. osigurati mogućnost naknadne provjere i utvrđivanja osobnih podataka koji su uneseni u sustave automatizirane obrade te vremena unosa i osoba koje su ih unijeli
8. spriječiti neovlašteno čitanje, kopiranje, mijenjanje ili brisanje osobnih podataka tijekom prijenosa osobnih podataka ili prijenosa nosača podataka
9. osigurati mogućnost ponovne uspostave instaliranih sustava u slučaju prekida
10. osigurati pouzdanost funkcioniranja sustava i prijave grešaka u funkcioniranju sustava te onemogućavanje ugroze cjelovitosti osobnih podataka zbog nedostataka u funkcioniranju sustava.

Članak 31.

Izvješćivanje nadzornog tijela o povredi osobnih podataka

(1) O povredi osobnih podataka voditelj obrade dužan je bez odgode, a najkasnije u roku od 72 sata od saznanja za povredu, izvijestiti nadzorno tijelo, osim ako povreda neće rezultirati rizikom za prava i slobode ispitanika.

(2) Ako izvješćivanje nadzornog tijela nije učinjeno u roku od 72 sata od saznanja za povredu, voditelj obrade mora izraditi pisano obrazloženje s navođenjem razloga kašnjenja.

(3) Izvršitelj obrade dužan je bez odgode obavijestiti voditelja obrade nakon saznanja o povredi osobnih podataka.

(4) Izvješće o povredi osobnih podataka iz stavka 1. ovoga članka sadržava:

1. prirodu povrede osobnih podataka, uključujući kategorije i približan broj ispitanika te kategorije i približan broj evidencija osobnih podataka o kojima je riječ
2. ime i kontaktne podatke službenika za zaštitu osobnih podataka ili druge kontaktne točke od koje se mogu dobiti dodatne informacije

3. vjerojatne posljedice povrede osobnih podataka

4. mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

(5) Kada nije moguće istodobno pružiti sve informacije o povredi, informacije se mogu pružati i postupno.

(6) Voditelj obrade evidentira svaku povredu osobnih podataka iz stavka 1. ovoga članka, uključujući činjenice povezane s povredom osobnih podataka, njezine posljedice i mjere poduzete za ispravljanje utvrđenih nedostataka.

(7) Kada se radi o povredi osobnih podataka među kojima su i osobni podaci preneseni od strane voditelja obrade druge države obavijest o povredi dostavlja se voditelju obrade te države bez nepotrebnog odgađanja.

Članak 32.

Obavijest ispitaniku o povredi osobnih podataka

(1) Kada je vjerojatno da će povreda osobnih podataka prouzročiti visok rizik za prava i slobode ispitanika, voditelj obrade će bez odgode o povredi obavijestiti ispitanika.

(2) U obavijesti ispitaniku iz stavka 1. ovoga članka navodi se priroda povrede osobnih podataka te informacije o poduzetim mjerama iz članka 31. stavka 4. točaka 2., 3. i 4. ovoga Zakona.

(3) Obavijest ispitaniku iz stavka 1. ovoga članka nije obvezna ako je:

1. voditelj obrade proveo odgovarajuće tehničke i organizacijske mjere zaštite koje su primijenjene na povrijeđene osobne podatke, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti

2. voditelj obrade poduzeo naknadne mjere kojima se osigurava da pojava visokog rizika za prava i slobode ispitanika iz stavka 1. ovoga članka više nije vjerojatna

3. zbog nerazmjernog napora nužno javno obavješćivanje ili slična mjera kojom se ispitanici izvješćuju na jednako djelotvoran način.

(4) Kada voditelj obrade ne obavijesti ispitanika o povredi osobnih podataka, nadzorno tijelo, nakon što utvrdi vjerojatnost da bi povreda osobnih podataka mogla prouzročiti visok rizik, može od voditelja obrade zahtijevati da obavijesti ispitanika ili zaključiti da je ispunjen neki od uvjeta iz stavka 3. ovoga članka.

(5) Obavijest ispitaniku iz stavka 1. ovoga članka može se odgoditi, ograničiti ili uskratiti na temelju postojanja razloga iz članka 16. ovoga Zakona.

Članak 33.

Imenovanje službenika za zaštitu osobnih podataka

(1) Voditelj obrade imenuje službenika za zaštitu osobnih podataka.

(2) Od obaveze imenovanja službenika za zaštitu osobnih podataka izuzeti su sudovi i druga neovisna pravosudna tijela kada postupaju u okviru svoje pravosudne nadležnosti.

(3) Službenik za zaštitu osobnih podataka imenuje se na temelju njegovih stručnih kvaliteta, a posebno njegovog stručnog znanja o pravu i praksi u području zaštite osobnih podataka te sposobnosti izvršavanja zadaća iz članka 35. ovoga Zakona.

(4) Kada to dozvoljava organizacijska struktura i veličina nadležnih tijela, za sva ta tijela može se imenovati jedan službenik za zaštitu osobnih podataka.

(5) Voditelj obrade dužan je o imenovanju službenika za zaštitu osobnih podataka izvijestiti nadzorno tijelo u roku od 30 dana od dana donošenja odluke o imenovanju te je dužan njegove službene kontakt podatke učiniti javno dostupnim na svojim mrežnim stranicama ili na drugi odgovarajući način.

Članak 34.

Položaj službenika za zaštitu osobnih podataka

(1) Voditelj obrade osigurava primjerenu i pravodobnu uključenost službenika za zaštitu osobnih podataka u sva pitanja povezana sa zaštitom osobnih podataka.

(2) Voditelj obrade službeniku za zaštitu osobnih podataka osigurava uvjete i sredstva neophodna za izvršavanje njegovih zadaća iz članka 35. ovoga Zakona te pristup osobnim podacima i postupcima obrade.

(3) Voditelj obrade osigurava službeniku za zaštitu osobnih podataka potrebne uvjete za stručno osposobljavanje i usavršavanje u području zaštite osobnih podataka.

Članak 35.

Zadaće službenika za zaštitu osobnih podataka

Zadaće službenika za zaštitu osobnih podataka su:

1. informiranje i savjetovanje voditelja obrade te zaposlenika koji obavljaju obradu podataka o njihovim obvezama propisanim ovim Zakonom i drugim propisima o zaštiti podataka
2. praćenje primjene ovoga Zakona i drugih propisa o zaštiti podataka u odnosu na zaštitu osobnih podataka, uključujući i raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoba koje sudjeluju u postupcima obrade i povezanim revizijama
3. pružanje savjeta, kada je to zatraženo, po pitanju procjene učinka na zaštitu podataka i praćenje njezina izvršavanja na temelju članka 28. ovoga Zakona
4. suradnja s nadzornim tijelom
5. djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima povezanim s obradom, što uključuje i prethodno savjetovanje iz članka 29. ovoga Zakona te savjetovanje, prema potrebi, u pogledu svih drugih pitanja.

V. PRIJENOSI OSOBNIH PODATAKA TREĆIM ZEMLJAMA ILI MEĐUNARODNIM ORGANIZACIJAMA

Članak 36.

Opća načela za prijenose osobnih podataka

(1) Osobni podaci mogu se prenositi trećoj zemlji ili međunarodnoj organizaciji, uključujući daljnje prijenose još jednoj trećoj zemlji ili međunarodnoj organizaciji, ako su ispunjeni sljedeći uvjeti:

1. prijenos je nužan u svrhe utvrđene u članku 1. ovoga Zakona
2. osobni podaci prenose se voditelju obrade u trećoj zemlji ili međunarodnoj organizaciji koji predstavlja javno tijelo nadležno za prikupljanje i obradu podataka u svrhe iz članka 1. ovoga Zakona
3. ako su osobni podaci preneseni ili stavljeni na raspolaganje iz druge države članice Europske unije koja je dala prethodno odobrenje za prijenos

4. kada su ispunjeni uvjeti iz članka 37., 38. i 39. ovoga Zakona

5. u slučaju daljnjeg prijenosa u još jednu treću zemlju ili međunarodnu organizaciju, nadležno tijelo koje je izvršilo prvotni prijenos ili drugo nadležno tijelo iste države članice, nakon što je uzelo u obzir ozbiljnost kaznenog djela, svrhu s kojom su osobni podaci prvotno preneseni i razinu zaštite osobnih podataka u trećoj zemlji ili međunarodnoj organizaciji kojoj su dalje preneseni osobni podaci, odobrava daljnji prijenos.

(2) Prijenosi bez prethodnog odobrenja druge države članice Europske unije u skladu sa stavkom 1. točkom 3. ovoga članka dopušteni su samo ako je prijenos osobnih podataka potreban za sprječavanje neposredne i ozbiljne prijetnje javnoj sigurnosti ili drugim bitnim interesima druge zemlje, a prethodno se odobrenje ne može pravodobno dobiti.

(3) Nadležno tijelo odgovorno za izdavanje prethodnog odobrenja obavještava se bez odgađanja.

Članak 37.

Prijenosi na temelju odluke o primjerenosti

(1) Prijenos osobnih podataka u treću zemlju ili međunarodnu organizaciju može se izvršiti kada Europska komisija utvrdi da treća zemlja, teritorij ili jedan ili više određenih sektora u trećoj zemlji, ili međunarodna organizacija osigurava odgovarajuću razinu zaštite.

(2) Prijenos osobnih podataka iz stavka 1. ovoga članka ne zahtijeva posebno odobrenje.

Članak 38.

Prijenosi koji podliježu odgovarajućim zaštitnim mjerama

(1) Kada ne postoji odluka na temelju članka 37. ovoga Zakona, prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji može se ostvariti:

1. ako su odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka predviđene u pravno obvezujućem instrumentu

2. ako je voditelj obrade procijenio sve okolnosti u vezi s prijenosom osobnih podataka i zaključio da postoje odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.

(2) Voditelj obrade dostavlja obavijest nadzornom tijelu o prijenosima izvršenim u skladu sa stavkom 1. točkom 2. ovoga članka.

(3) Kada se prijenos temelji na stavku 1. točki 2. ovoga članka, takav se prijenos mora dokumentirati.

(4) Dokumentiranje prijenosa uključuje datum i vrijeme prijenosa, informacije o nadležnom tijelu kojem se podaci prenose, obrazloženje prijenosa i navođenje kategorije i vrste prenesenih osobnih podataka.

(5) Dokumentacija se na zahtjev stavlja na raspolaganje nadzornom tijelu.

Članak 39.

Odstupanja za posebne situacije

(1) Kada ne postoji odluka iz članka 37. ili nisu ispunjeni uvjeti iz članka 38. ovoga Zakona, prijenos ili kategorija prijenosa osobnih podataka u treću zemlju ili međunarodnu organizaciju se može ostvariti samo pod uvjetom da je prijenos nužan:

1. radi zaštite života ili tjelesnog integriteta ispitanika ili druge osobe

2. radi zaštite interesa ispitanika, ako je tako predviđeno pravom države članice koja obavlja prijenos osobnih podataka

3. kako bi se spriječila neposredna i ozbiljna prijetnja javnoj sigurnosti države članice ili treće zemlje
 4. u pojedinačnim slučajevima u svrhe navedene u članku 1. ovoga Zakona
 5. u pojedinačnom slučaju radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva u vezi sa svrhama navedenima u članku 1. ovoga Zakona.
- (2) Osobni podaci ne smiju se prenositi ako nadležno tijelo koje obavlja prijenos utvrdi da temeljna prava i slobode ispitanika na koga se odnosi prijenos podataka imaju prednost pred javnim interesom u pogledu prijenosa iz stavka 1. točaka 4. i 5. ovoga članka.
- (3) Kada se prijenos temelji na stavku 1. ovoga članka, takav se prijenos mora dokumentirati.
- (4) Dokumentiranje prijenosa uključuje datum i vrijeme prijenosa, informacije o nadležnom tijelu kojem se podaci prenose, obrazloženje prijenosa i navođenje kategorije i vrste prenesenih osobnih podataka.
- (5) Dokumentacija se na zahtjev stavlja na raspolaganje nadzornom tijelu.

Članak 40.

Prijenosi osobnih podataka primateljima s poslovnim nastanom u trećim zemljama

- (1) Nadležna tijela mogu, ne dovodeći u pitanje niti jedan međunarodni sporazum iz stavka 2. ovoga članka, iako nisu ispunjeni uvjeti iz članka 36. stavka 1. točke 2. ovoga Zakona, u svakom pojedinačnom slučaju, prenijeti osobne podatke izravno primateljima s poslovnim nastanom u trećim zemljama samo ako se poštuju druge odredbe ovoga Zakona i ako su ispunjeni sljedeći uvjeti:
1. prijenos je nužan za obavljanje zadaće nadležnog tijela koje obavlja prijenos u svrhe navedene u članku 1. ovoga Zakona
 2. kada nadležno tijelo koje obavlja prijenos utvrdi da temeljna prava i slobode ispitanika čiji osobni podaci se prenose nemaju prednost nad javnim interesom
 3. kada nadležno tijelo koje obavlja prijenos smatra da je prijenos tijelu nadležnom u svrhe iz članka 1. ovoga Zakona u trećoj zemlji neučinkovit ili neprimjeren, posebno iz razloga što se ne može pravodobno ostvariti
 4. kada je tijelo koje je u trećoj zemlji nadležno za obradu osobnih podataka u svrhe iz članka 1. ovoga Zakona obaviješteno bez odgode, osim ako je neučinkovito ili neprimjereno
 5. kada nadležno tijelo koje obavlja prijenos obavijesti primatelja o određenoj svrsi ili svrhama u koje primatelj može obrađivati osobne podatke samo ako je takva obrada nužna.
- (2) Međunarodni sporazum iz stavka 1. ovoga članka svaki je bilateralni ili multilateralni međunarodni sporazum koji je na snazi između Republike Hrvatske i trećih zemalja u području pravosudne suradnje u kaznenim stvarima i policijske suradnje.
- (3) Nadležno tijelo koje obavlja prijenos dostavlja obavijest nadzornom tijelu o prijenosima u skladu s ovim člankom.
- (4) Kada se prijenos temelji na stavku 1. ovoga članka, takav se prijenos mora dokumentirati.

VI. NADZOR

Članak 41.

Nadzorno tijelo

(1) Nadzor nad obradom osobnih podataka za svrhe iz članka 1. ovoga Zakona obavlja nadzorno tijelo osnovano posebnim zakonom kojim se uređuje zaštita osobnih podataka koje je neovisno i samostalno u svom radu (u daljnjem tekstu: nadzorno tijelo).

(2) Nadzorno tijelo predstavlja Republiku Hrvatsku pred Europskim odborom za zaštitu podataka u smislu provedbe ovoga Zakona.

Članak 42.

Izuzeće od nadležnosti nadzornog tijela

Postupak nadzora obrade osobnih podataka koju u okviru svoje pravosudne nadležnosti provode sudovi i druga neovisna pravosudna tijela i odgovornost za povrede odredbi ovoga Zakona od strane sudova i drugih neovisnih pravosudnih tijela kada postupaju u okviru svoje pravosudne nadležnosti propisuju se posebnim zakonom.

Članak 43.

Zadaće nadzornog tijela

(1) Nadzorno tijelo u okviru svojih nadležnosti:

1. prati i nadzire primjenu odredaba ovoga Zakona te njihovo poštivanje
2. promiče javnu svijest i shvaćanje o rizicima, pravilima, zaštitnim mjerama i pravima koja se odnose na obradu i postupanje s osobnim podacima
3. savjetuje Hrvatski sabor, Vladu Republike Hrvatske i druge institucije i tijela javne vlasti u pitanjima zakonodavnih i administrativnih mjera koje se odnose na obradu i postupanje s osobnim podacima
4. podiže svijest nadležnih tijela, voditelja obrade i izvršitelja obrade odgovornih za obradu osobnih podataka o njihovim obvezama koje proizlaze iz odredbi ovoga Zakona
5. na zahtjev pruža svakom ispitaniku podatke i saznanja o ostvarivanju njegovih prava prema ovom Zakonu, prema potrebi u tu svrhu surađuju s nadzornim tijelima u drugim državama
6. postupa i rješava po prigovorima koje podnese ispitanik, nevladina organizacija ili udruga sukladno članku 51. ovoga Zakona, provjerava navode prigovora te u razumnom roku izvješćuje podnositelja prigovora o napretku i ishodu postupanja, posebice ako je potrebno poduzimanje dodatnih provjera
7. nadzire zakonitost obrade sukladno članku 18. ovoga Zakona i u razumnom roku dostavlja obavijest ispitaniku o provedenom nadzoru sukladno članku 18. stavku 3. ovoga Zakona ili razlozima zbog kojih nadzor nije proveden
8. surađuje s nadzornim tijelima drugih država članica radi pružanja uzajamne pomoći u svrhu provedbe ovoga Zakona
9. postupa na temelju zahtjeva tijela javne vlasti, a koje se odnose na provjeru zakonitosti obrade i postupanja s osobnim podacima
10. prati i izučava problematiku povezanu s područjem obrade osobnih podataka i njihov utjecaj na njihovu zaštitu, posebice razvoj informacijskih i komunikacijskih tehnologija
11. provodi postupke savjetovanja u vezi s postupcima obrade osobnih podataka sukladno članku 27. ovoga Zakona.

(2) Nadzorno tijelo je dužno, radi osiguranja jednostavnosti i ostvarivanja prava svakog ispitanika na podnošenje prigovora sukladno stavku 1. točki 6. ovoga članka, izraditi obrazac za podnošenje prigovora ispitanika nadzornom tijelu koje ne smije biti ograničeno samo na jedno sredstvo komunikacije.

(3) Izvršavanje zadaća nadzornog tijela u odnosu na ispitanika i službenika za zaštitu osobnih podataka oslobođeno je upravne pristojbe.

(4) Iznimno od odredbe stavka 3. ovoga članka, kada je prigovor ispitanika neutemeljen ili pretjeran, osobito zbog njegovog učestalog ponavljanja, nadzorno tijelo može naplatiti naknadu na temelju posebnog propisa ili može odbiti postupiti po zahtjevu.

(5) Teret dokazivanja da je prigovor očito neutemeljen ili pretjeran je na nadzornom tijelu.

Članak 44.

Ovlasti nadzornog tijela

(1) Nadzorno tijelo ima ovlast od voditelja obrade i izvršitelja obrade ishoditi pristup svim osobnim podacima te svim informacijama potrebnim za obavljanje svojih zadaća.

(2) Nadzorno tijelo ima sljedeće korektivne ovlasti:

1. izdavati upozorenja voditelju obrade ili izvršitelju obrade o tome da namjeravani postupci obrade mogu prouzročiti kršenje odredaba ovoga Zakona

2. zahtijevati od voditelja obrade ili izvršitelja obrade da, prema potrebi, postupke obrade uskladi s odredbama ovoga Zakona, na određeni način i u određenom roku, posebno na način da zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade sukladno članku 17. ovoga Zakona

3. privremeno ili trajno ograničiti ili zabraniti obradu.

(3) Nadzorno tijelo ima ovlasti savjetovati voditelja obrade sukladno članku 29. ovoga Zakona i davati mišljenja na vlastitu inicijativu ili na zahtjev o svakom pitanju u svezi sa zaštitom osobnih podataka.

(4) O izrečenim mjerama iz stavka 2. točaka 2. i 3. ovoga članka nadzorno tijelo donosi rješenje protiv kojeg nije dopuštena žalba, već se može pokrenuti upravni spor.

(5) Po izvršnosti rješenja iz stavka 4. ovoga članka nadzorno tijelo će provesti kontrolni nadzor.

(6) Nadzorno tijelo je ovlašteno obavijestiti nadležna pravosudna tijela o kršenjima odredaba ovoga Zakona i sudjelovati u pravnim postupcima koji se vode u vezi s provođenjem odredbi ovoga Zakona.

(7) Nadzorno tijelo može pokrenuti i ima pravo sudjelovati u prekršajnim postupcima za prekršaje propisane ovim Zakonom.

(8) Nadzorno tijelo je u tijeku prekršajnog postupka ovlašteno poduzimati sve radnje na koje je po posebnom zakonu ovlašten putem osobe koju za to ovlasti kao svog predstavnika.

Članak 45.

Javno objavljivanje odluke

(1) Nadzorno tijelo će na svojim mrežnim stranicama objaviti pravomoćno rješenje iz članka 44. stavka 4. ovoga Zakona koje će biti anonimizirano u odnosu na osobne podatke ispitanika.

(2) Ako se protiv rješenja nadzornog tijela iz članka 44. stavka 4. ovoga Zakona vodio upravni spor pred nadležnim upravnim sudom Republike Hrvatske te je tužitelj upravni spor izgubio, tada će nadzorno tijelo na svojim mrežnim stranicama objaviti pravomoćnu presudu nadležnog upravnog suda koja će biti anonimizirana u odnosu na osobne podatke ispitanika.

Članak 46.

Izvjescivanje o povredama

(1) Sva nadležna tijela dužna su omogućiti uspostavu učinkovitog mehanizma za poticanje povjerljivog izvješćivanja o povredama odredbi ovoga Zakona.

(2) Službenicima nadležnih tijela koji odgovornim osobama ili nadležnim tijelima podnesu prijavu o povredama ovoga Zakona jamči se zaštita anonimnosti te zaštita od bilo kojeg oblika zlostavljanja.

Članak 47.

Izvjescivanje o aktivnostima

Godišnje izvješće o radu koje nadzorno tijelo podnosi Hrvatskom saboru u skladu s posebnim propisom mora sadržavati i podatke o praćenju provedbe ovoga Zakona strukturirane u skladu s odredbama posebnog zakona kojima je propisan sadržaj toga godišnjeg izvješća.

Članak 48.

Obavješćivanje Europske komisije

Nadzorno tijelo će na zahtjev Europske komisije dostaviti godišnje izvješće o provođenju ovoga Zakona Europskoj komisiji i Europskom odboru za zaštitu podataka.

Članak 49.

Međunarodna suradnja i uzajamna pomoć nadzornih tijela

(1) Nadzorno tijelo na zahtjev nadzornog tijela druge države članice pruža informacije i uzajamnu pomoć radi provedbe odredaba ovoga Zakona te uspostavlja mjere za učinkovitu uzajamnu suradnju. Uzajamna pomoć obuhvaća zahtjeve za informacijama i mjerama nadzora, kao što su zahtjevi za provedbom savjetovanja, nadzora i istraživanja.

(2) Nadzorno tijelo je dužno u razumnom roku, a najkasnije u roku od 30 dana, odgovoriti na zahtjev.

(3) Zahtjev za uzajamnu pomoć mora sadržavati obrazloženu svrhu i razloge traženja informacija.

(4) Nadzorno tijelo zahtjev ne može odbiti osim ako:

1. nije nadležno za predmet zahtjeva ili za mjere koje treba poduzeti na temelju zahtjeva

2. bi udovoljavanje zahtjevu kršilo odredbe ovoga Zakona.

(5) Kada nadzorno tijelo zaprimi zahtjev, dužno je podnositelja zahtjeva, sukladno stavku 2. ovoga članka, obavijestiti o rezultatima, napretku ili poduzetim mjerama odnosno o razlozima odbijanja zahtjeva na temelju stavka 4. ovoga članka.

(6) Nadzorno tijelo u pravilu elektroničkim putem pruža informacije koje drugo nadzorno tijelo zatraži, koristeći se standardiziranim formatom.

(7) Postupanje po zahtjevu za uzajamnu pomoć ne podliježe naplati naknada.

VII. PRIGOVORI I PRAVNA ZAŠTITA

Članak 50.

Pravo na podnošenje prigovora nadzornom tijelu i pravo na učinkoviti pravni lijek protiv odluke nadzornog tijela

- (1) Ispitanik ili osoba koje ga je ovlaštena zastupati može u roku od 30 dana od dana saznanja za moguću povredu nadzornom tijelu podnijeti prigovor ako smatra da mu je povrijeđeno neko pravo utvrđeno ovim Zakonom.
- (2) Postupajući po prigovoru nadzorno tijelo će provesti odgovarajući postupak i izvijestiti ispitanika o napretku i ishodu.
- (3) O prigovoru iz stavka 1. ovoga članka nadzorno tijelo odlučuje rješenjem.
- (4) Protiv rješenja nadzornog tijela nije dopuštena žalba, ali se može pokrenuti upravni spor.

Članak 51.

Zastupanje ispitanika

Ispitanik može ovlastiti neprofitno tijelo, organizaciju ili udruženje, koje je osnovano sukladno posebnim propisima, a u čijem Statutu se navode ciljevi od javnog interesa te koje je aktivno u području zaštite prava i sloboda ispitanika s obzirom na zaštitu njegovih osobnih podataka, da u njegovo ime podnese prigovor nadzornom tijelu i da u njegovo ime ostvaruje prava iz članka 50. ovoga Zakona.

Članak 52.

Pravo na naknadu štete

Svaka osoba koja je pretrpjela štetu zbog postupka nezakonite obrade ili bilo koje radnje kojom se krše odredbe ovoga Zakona ima pravo na naknadu štete od voditelja obrade sukladno općim pravilima o naknadi štete.

VIII. PREKRŠAJNE ODREDBE

Članak 53.

(1) Novčanom kaznom u iznosu od 5000,00 do 20.000,00 kuna kaznit će se izvršitelj obrade pravna osoba, koja nije tijelo javne vlasti, ako:

1. ne poduzme razumne mjere da se podaci koji nisu točni, uzimajući u obzir svrhu obrade, bez odgode isprave ili izbrišu (članak 6. stavak 6.)
2. koristi usluge drugog izvršitelja bez prethodnog pisanog odobrenja voditelja obrade (članak 23. stavak 3.)
3. po zaprimanju odobrenja ne obavijesti voditelja obrade o svim planiranim izmjenama u vezi s korištenjem drugih izvršitelja obrade (članak 23. stavak 4.)
4. ne vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju u ime voditelja obrade prema članku 25. stavku 2.
5. ne vodi evidenciju svih kategorija aktivnosti obrade koje se obavljaju u ime voditelja obrade u pisanom i elektronskom obliku (članak 25. stavak 3.)
6. na zahtjev nadzornog tijela ne stavi evidenciju na raspolaganje (članak 25. stavak 4.)
7. u automatiziranim sustavima obrade podataka ne osigura bilježenje postupaka obrade osobnih podataka (članak 26. stavak 1.)
8. na zahtjev nadzornog tijela ne stavi zapis na raspolaganje (članak 26. stavak 4.)
9. na zahtjev nadzornog tijela ne pruža i ne daje na uvid sve potrebne informacije (članak 27.)

10. ne provede savjetovanje s nadzornim tijelom prije nove obrade osobnih podataka koji će biti uključeni u novi sustav pohrane koji se treba uspostaviti (članak 29. stavak 1.)

11. ne provodi tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti s obzirom na rizik, osobito u pogledu obrade posebnih kategorija osobnih podataka (članak 30. stavak 1.)

12. u pogledu automatizirane obrade, nakon procjene rizika, ne provede mjere prema članku 30. stavku 2.

13. bez odgode, a nakon saznanja o povredi osobnih podataka, ne obavijesti voditelja obrade (članak 31. stavak 3.).

(2) Za prekršaje iz stavka 1. ovoga članka novčanom kaznom od 2000,00 do 10.000,00 kuna kaznit će se i odgovorna osoba u pravnoj osobi izvršitelja obrade koje nije tijelo javne vlasti.

Članak 54.

Ako je postupanjem iz članka 44. stavka 5. ovoga Zakona utvrđeno da voditelj obrade ili izvršitelj obrade koji je tijelo javne vlasti nije postupio u skladu s izvršnim rješenjem iz članka 44. stavka 4. ovoga Zakona, odgovorna osoba voditelja obrade ili izvršitelja obrade kaznit će se novčanom kaznom u iznosu od 2000,00 do 10.000,00 kuna.

IX. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 55.

Prijenos

Automatizirani sustavi obrade podataka uspostavljeni prije stupanja na snagu ovoga Zakona moraju se u potpunosti uskladiti s člankom 26. stavkom 1. ovoga Zakona najkasnije do 6. svibnja 2023.

Članak 56.

Odnos s prethodno sklopljenim međunarodnim sporazumima u području pravosudne suradnje u kaznenim stvarima i policijske suradnje

Međunarodni sporazumi koji uključuju prijenos osobnih podataka trećim zemljama ili međunarodnim organizacijama koje je sklopila Republika Hrvatska prije 6. svibnja 2016., a koji su u skladu s pravom Europske unije primjenjivim prije tog datuma, ostaju na snazi dok ih se ne izmjeni ili stavi izvan snage.

Članak 57.

Stupanje na snagu

Ovaj Zakon stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 022-03/18-01/74

Zagreb, 13. srpnja 2018.

HRVATSKI SABOR