NN 68/2018 (27.7.2018.), Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija

HRVATSKI SABOR

1391

Na temelju članka 89. Ustava Republike Hrvatske, donosim

ODLUKU

O PROGLAŠENJU ZAKONA O ZAŠTITI FIZIČKIH OSOBA U VEZI S OBRADOM I RAZMJENOM OSOBNIH PODATAKA U SVRHE SPRJEČAVANJA, ISTRAŽIVANJA, OTKRIVANJA ILI PROGONA KAZNENIH DJELA ILI IZVRŠAVANJA KAZNENIH SANKCIJA

Proglašavam Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, koji je Hrvatski sabor donio na sjednici 13. srpnja 2018.

Klasa: 011-01/18-01/97
Urbroj: 71-06-01/1-18-2
Zagreb, 19. srpnja 2018.

Predsjednica
Republike Hrvatske
Kolinda Grabar-Kitarović, v. r.

ZAKON

O ZAŠTITI FIZIČKIH OSOBA U VEZI S OBRADOM I RAZMJENOM OSOBNIH PODATAKA U SVRHE SPRJEČAVANJA, ISTRAŽIVANJA, OTKRIVANJA ILI PROGONA KAZNENIH DJELA ILI IZVRŠAVANJA KAZNENIH SANKCIJA

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

Načela obrade osobnih podataka

Članak 6.

(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.

Rokovi za pohranu i preispitivanje

Članak 7.

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.

Razlika između različitih kategorija ispitanika

Članak 8.

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.

Razlika između osobnih podataka i provjera kvalitete osobnih podataka

Članak 9.

(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.

Posebni uvjeti obrade

Članak 10.

(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.

Obrada posebnih kategorija osobnih podataka

Članak 11.

(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.

Automatizirano pojedinačno donošenje odluka

Članak 12.

(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

Obavještavanje i način obavještavanja ispitanika

Članak 13.

(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.

Informacije koje su dostupne ili se daju ispitaniku

Članak 14.

(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.

Pravo ispitanika na pristup

Članak 15.

(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.

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

Članak 16.