



OBAVIJEST O OBRADI OSOBNIH PODATAKA U NEOVISNOM OPERATORU SUSTAVA U BOSNI I HERCEGOVINI

Generalni propis o zaštiti podataka Europske unije (*EU General Data Protection Regulation - GDPR*), odnosno, Opća uredba o zaštiti podataka je Uredba (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/EC, kojom se regulira zaštita podataka i privatnost osoba unutar Europske unije, a donosi i propise vezane za iznošenje podataka u treće zemlje. Glavni ciljevi GDPR-a su vratiti građanima nadzor nad njihovim osobnim podacima i pojednostaviti regulatorno okruženje za međunarodne kompanije ujednačavanjem propisa u cijeloj Uniji. Stupanjem GDPR-a na snagu prestaje važiti Direktiva 95/46/EC, a nakon prijelaznog razdoblja od dvije godine sve zemlje članice EU dužne su od 25.05.2018. primjenjivati ovu uredbu.

U Bosni i Hercegovini, u ovoj oblasti važeće zakonodavstvo čini Zakon o zaštiti osobnih podataka ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11 – ispr.).

Za razliku od važećeg zakonodavstva u Bosni i Hercegovini, Opća uredba o zaštiti podataka ima pristup kojim se želi poboljšati učinkovitost zaštite podataka na način da se posebno nadziru rizične obrade.

Bosna i Hercegovina je Sporazumom o stabilizaciji i pridruživanju preuzela obvezu usklađivanja domaćeg zakonodavstva s pravnom stečevinom Europske unije (za što je krajnji rok 01.06.2021.), tako da se navedena obveza odnosi i na usklađivanje Zakona o zaštiti osobnih podataka sa novim zakonodavstvom EU o zaštiti osobnih podataka.

Imajući u vidu navedeno, kao i široki opseg primjene Uredbe o zaštiti podataka utvrđen u članku 3., Neovisni operator sustava u Bosni i Hercegovini (u daljnjem tekstu: NOSBiH) vodi računa o zaštiti podataka o osobi i u svom poslovanju pridržava se odredbi koje su propisane Općom uredbom o zaštiti podataka i važećim zakonodavstvom, dajući prednost u primjeni Općoj uredbi o zaštiti podataka.

Način na koji se NOSBiH odnosi prema podacima o osobi možete pročitati u nastavku ove obavijesti.

Ova obavijest je općeg karaktera, te je tako treba i shvaćiti.

1. Važni pojmovi

Zakonom o zaštiti ličnih podataka definirani su pojmovi, ali u Općoj uredbi o zaštiti podataka su navedene opsežnije definicije pojmova važnih za privatnost.

Osobni podaci su, prema definiciji iz Uredbe, "svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili posredno, osobito uz pomoć identifikatora kao što su ime, 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 tog pojedinca."

Dakle, pojam *osobni podaci* jako je širok, no jednostavnije rečeno to su: ime i prezime, identifikacijski broj, slika, glas, adresa, broj telefona, IP adresa, ako takvi podaci mogu dovesti do izravnog ili posrednog identificiranja pojedinca. Ističemo da prije prikupljanja osobnih podataka, subjekt koji ih prikuplja, ima obvezu pružanja informacija o tome za koju svrhu se oni prikupljaju, na osnovu kojeg pravnog osnova, kome se podaci otkrivaju, te o pravu pojedinca da svojim podacima pristupi, zahtijeva njihov ispravak ili eventualno brisanje.

Suglasnost ispitanika znači svako dobrovoljno, posebno i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose.

Ako se kao pravna osnova koristi suglasnost, ona mora biti izričita za podatke koji su prikupljeni i cilj korištenja (čl. 7; definirano u čl. 4.). Prema članku 7., na teretu organizacije je da pokaže da su ljudi valjano pristali na obradu svojih podataka. Pristanak se mora dati "slobodnom voljom".

Pseudonimizacija podrazumijeva obradu osobnih podataka na takav način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez upotrebe dodatnih informacija, pod uslovom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da osobni podaci ne mogu biti pripisani pojedincu čiji je identitet utvrđen ili se može utvrditi.

GDPR pseudonimizaciju definira kao postupak obrade podataka na takav način da se više ne mogu pripisati pojedinom ispitaniku bez korištenja dodatnih izvora podataka. Tu je i enkripcija, koja podatke čini nečitljivima za sve neovlaštene osobe bez pristupa ključem za dekripciju. GDPR propisuje da se dodatni podaci (poput ključa za dekripciju) drže podalje od pseudonimiziranih podataka.

Još jedan od pristupa jest i tokenizacija, što je nematematički pristup obradi podataka u kojem se osjetljivi podaci zamjenjuju neosjetljivim zamjenama pod nazivom tokeni. Tokeni nemaju važnost niti vrijednost kao podaci. Njima se ne mijenja vrsta niti dužina podataka, što znači da ih mogu obrađivati sustavi kao baze podataka koje brinu o vrstama i dužini podataka. Tim se pristupom zahtijeva manje procesorskih resursa za obradu i zauzima manje mjesta za pohranu u bazama podataka u usporedbi s podacima enkriptiranim na tradicionalni način. To je omogućeno držanjem određenih podataka potpuno ili djelomično vidljivima za obradu i analitiku, dok se osjetljivi podaci skrivaju.

Pseudonimizacija se preporučuje kao metoda za smanjenje rizika po ispitanike, ali i kao način da voditelji odnosno izvršitelji obrade ispune svoje obveze vezane za zaštitu podataka (Uvodna odredba 28.).

Iako GDPR potiče korištenje pseudonimizacije u cilju smanjenja rizika po ispitanike, pseudonimizirani se podaci i dalje smatraju osobnima (Uvodna odredba br. 28.) te tako i dalje spadaju pod nadzor GDPR-a.

Obavijest o kršenju/povredi podataka - Povreda osobnih podataka znači 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.

Ispitanike nije potrebno obavijestiti o povredi ako je voditelj obrade poduzeo odgovarajuće tehničke i organizacijske mjere zaštite podataka, osobito one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja nije ovlaštena da im pristupi, kao što je enkripcija (čl. 34.).

Sustav pohrane znači svaki strukturirani skup osobnih podataka dostupnih prema posebnim kriterijima, bilo da su centralizirani, decentralizirani ili raspršeni na funkcionalnoj ili zemljopisnoj osnovi.

2. Principi obrade podataka o osobi

Principi obrade podataka o osobi u skladu s Općom uredbom o zaštiti podataka su:

- **zakonitost, poštenost i transparentnost obrade** – što znači da obrada podataka treba biti u skladu s određenim pravnim osnovom, da je pojedinac informiran o postupku obrade i njegovim ciljevima, jer je voditelj obrade obavezan ispitaniku pružiti sve dodatne informacije neophodne za poštenu i transparentnu obradu, uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka; ispitanik bi trebao biti informiran o postupku izrade profila i posljedicama takve izrade profila
- **ograničavanje svrhe** – što znači da podaci trebaju biti prikupljeni u posebne, izričite i zakonite svrhe te da se dalje ne smiju obrađivati na način koji nije u skladu s tim ciljevima; a moguća je daljnja obrada u svrhu arhiviranja u javnom interesu, znanstvenog ili historijskog istraživanja ili u statističke svrhe
- **smanjenje količine podataka** – što znači da podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhu za koju se obrađuju
- **točnost** – što znači da podaci moraju biti točni i prema potrebi ažurni; mora se poduzeti svaka razumna mjera u cilju osiguranja da se osobni podaci koji nisu točni, uzimajući u obzir svrhu za koju se obrađuju, bez odlaganja izbrišu ili isprave
- **ograničenje pohrane** – što znači da podaci moraju biti pohranjeni u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo, koliko je potrebno za svrhu za koju se osobni podaci obrađuju; na dulje periode, njihovo čuvanje je moguće samo ako će se osobni podaci obrađivati isključivo u svrhu arhiviranja u javnom interesu, znanstvenog ili historijskog istraživanja ili u statističke svrhe, uz provođenje primjerenih mjera zaštite propisanih Uredbom
- **cjelovitost i povjerljivost** – što znači da podaci moraju biti obrađivani tako da bude zadovoljena odgovarajuća razina sigurnosti, uključujući zaštitu od neovlaštene ili nezakonite obrade te slučajnog gubitka, uništenja ili oštećenja
- **pouzdanost** – što znači da je voditelj obrade odgovoran za poštovanje principa i da je teret dokaza na njemu.

3. Pravne osnove za obradu osobnih podataka

Obrada osobnih podataka obuhvaća radnje kao što su njihovo prikupljanje, evidentiranje, čuvanje, uvid, otkrivanje, prenošenje ili uništavanje.

Prema Općoj uredbi o zaštiti podataka podaci se ne smiju obrađivati osim ako za to postoji barem jedna od sljedećih pravnih osnova (čl. 6. st. 1.):

- Ispitanik je dao suglasnost za obradu podataka za jednu ili više posebnih svrha.
- Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se, na zahtjev ispitanika, poduzele odgovarajuće radnje prije sklapanja ugovora.
- Obrada je nužna radi poštivanja pravnih obveza voditelja obrade.
- Obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe.
- Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade.
- Obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili osnovna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

4. Prava osobe čiji se podaci obrađuju

U skladu s Općom uredbom o zaštiti podataka, osobe čiji se podaci obrađuju u NOSBiH-u mogu ostvariti sljedeća prav:,

- **transparentnost** (čl. 12-14) – što podrazumijeva pružanje informacija prilikom prikupljanja podataka kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o svom identitetu te kontakt podacima, ciljevima obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, periodu pohrane, mogućnosti povlačenja suglasnosti, itd.
- **pravo pristupa podacima** (čl. 15) koje pripada ispitanicima

To im pravo omogućuje pristup osobnim podacima i podacima o načinu njihove obrade. Voditelj obrade dužan je, na zahtjev, pružiti pregled kategorija podataka koji se obrađuju kao i kopiju stvarnih podataka. Nadalje, voditelj obrade ispitanika mora obavijestiti o detaljima obrade poput svrhe, eventualnim primateljima podataka i načinu na koji je voditelj stekao te podatke.

- **pravo na ispravak** (čl. 16) – što podrazumijeva da ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhu obrade, ispitanik ima pravo i dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave
- **brisanje („pravo na zaborav“)** (čl. 17) – što podrazumijeva da ispitanik od voditelja obrade ima pravo ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja ako, među ostalim, osobni podaci više nisu neophodni u odnosu na svrhu obrade
- **pravo na ograničenje obrade** (čl. 18) – što podrazumijeva da u pojedinim situacijama npr. kada je točnost podataka osporavana ispitanik ima pravo zahtijevati

ograničavanje obrade njegovih osobnih podataka, uz iznimku pohrane i nekih drugih vrsta obrade

- **pravo na prenosivost** (čl. 20) – što podrazumijeva da ispitanik ima pravo dobiti svoje osobne podatke, koje je prethodno pružio voditelju obrade, u strukturiranom obliku, te u uobičajeno upotrebljavanom i strojno čitljivom format, te da ima pravo te podatke prenijeti drugom voditelju obrade bez ometanja voditelja obrade kojem su osobni podaci prethodno pruženi, ako se obrada provodi automatizovanim putem i zasniva na suglasnosti ili ugovoru

Ispitanici, također, imaju pravo svoje osobne podatke prenijeti iz jednog sustava elektronske obrade u drugi, a da ih u tome ne sputava voditelj obrade. Ovim pravom nisu obuhvaćeni na odgovarajući način anonimizirani podaci, ali jesu podaci koji ne sadrže identifikatore, pomoću kojih se pojedinca može identificirati uz dodatne podatke, obuhvaćeni ovim pravom. Ovo pravo podrazumijeva podatke koje je ispitanik 'dao' i podatke koji su nastali 'praćenjem', poput ponašanja ispitanika. Nadalje, voditelj obrade podatke mora pružiti u strukturiranom, uobičajeno korištenom formatu (čl. 20.).

- **pravo na prigovor** (čl. 21) – što podrazumijeva da ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ona zasniva na zadaćama od javnog interesa, na izvršavanje službenih ovlasti voditelja obrade ili legitimne interese voditelja obrade (uključujući i profiliranje), kada voditelj obrade ne smije više obrađivati osobne podatke ispitanika osim ako dokaže da njegovi legitimni razlozi za obradu nadilaze interese ispitanika, te radi zaštite pravnih zahtjeva, također ako se ispitanik protivi obradi za potrebe izravnog marketinga, osobni podaci više se ne smiju obrađivati
- **pravo protivljenja donošenju automatizovanih pojedinačnih odluka (profiliranje)** (čl. 22) – što podrazumijeva da ispitanik ima pravo na to da se na njega ne odnosi odluka koja se zasniva isključivo na automatizovanoj obradi, uključujući izradu profila, koja proizvodi pravne efekte koji se na njega odnose ili na sličan način na njega značajno utječu, osim ako je takva odluka potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka, ako je dopuštena pravom EU-a ili nacionalnim pravom kojim se propisuju odgovarajuće mjere zaštite prava i sloboda, te legitimnih interesa ispitanika ili je zasnovana na izričitoj suglasnosti ispitanika.

5. Podaci o osobi za zaštitu podataka o osobi

U okviru primjene standarda zaštite podataka o osobi, NOSBiH, kao voditelj obrade podataka o osobi, odredio je zaposlenika čija je dužnost zaštita osobnih podataka, kojem se možete obratiti u vezi sa svim pitanjima i zahtjevima koji se odnose na obradu Vaših osobnih podataka na sljedeće adrese:

- E mail: info@nosbih.ba
- Pošta: Neovisni operator sustava u Bosni i Hercegovini, Hifzi Bjelevca 17, Sarajevo, Bosna i Hercegovina

6. Prava koja pripadaju osobi u slučaju nedozvoljene obrade

U slučaju nedozvoljene obrade njenih podataka, osobi pripadaju sva prava iz Opće uredbe o zaštiti podataka kao i pravo podnošenja žalbe nadležnom nadzornom tijelu.

