



OBAVJEŠTENJE O OBRADI LIČNIH PODATAKA U NEZAVISNOM OPERATORU SISTEMA U BOSNI I HERCEGOVINI

Generalni propis o zaštiti podataka Evropske unije (*EU General Data Protection Regulation - GDPR*), odnosno Opća uredba o zaštiti podataka je Uredba (EU) 2016/679 Evropskog parlamenta i Vijeća od 27. aprila 2016. o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka, te o stavljanju izvan snage Direktive 95/46/EC, kojom se reguliše zaštita podataka i privatnost lica unutar Evropske unije, a donosi i propise vezane za iznošenje podataka u treće zemlje. Glavni ciljevi GDPR-a su vratiti građanima nadzor nad njihovim ličnim 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 ličnih 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 efektivnost zaštite podataka na način da se posebno nadziru rizične obrade.

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

Imajući u vidu navedeno, kao i široki obim primjene Uredbe o zaštiti podataka utvrđen u članu 3., Nezavisni operator sistema u Bosni i Hercegovini (u daljem tekstu: NOSBiH) vodi računa o zaštiti podataka o ličnosti 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 ličnosti možete pročitati u nastavku ovog obavještenja.

Ovo obavještenje je općeg karaktera, te ga tako treba i shvatiti.

1. Važni pojmovi

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

Lični 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 lice koje se može identifikovati direktno ili indirektno, naročito uz pomoć identifikatora kao što su ime, identifikacioni broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više faktora svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca."

Dakle, pojam *lični podaci* jako je širok, no jednostavnije rečeno to su: ime i prezime, identifikacioni broj, slika, glas, adresa, broj telefona, IP adresa, ako takvi podaci mogu dovesti do direktnog ili indirektnog identificiranja pojedinca. Ističemo da prije prikupljanja ličnih podataka, subjekt koji ih prikuplja, ima obavezu 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.

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

Ako se kao pravna osnova koristi saglasnost, ona mora biti izričita za podatke koji su prikupljeni i svrhu za koje se koriste (čl. 7; definisano u čl. 4.). Prema članu 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 ličnih podataka na takav način da se lični 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 organizacionim mjerama kako bi se osiguralo da se lični podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi.

GDPR pseudonimizaciju definiše 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 sva neovlaštena lica bez pristupa ključu za dekrpciju. GDPR propisuje da se dodatni podaci (poput ključa za dekrpciju) 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 sistemi 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 uporedbi s podacima enkriptiranim na tradicionalni način. To se omogućuje držanjem određenih podataka potpuno ili djelimično vidljivima za obradu i analitiku, dok se osjetljivi podaci skrivaju.

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

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

Obavijest o kršenju/povredi podataka - Povreda ličnih podataka znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa ličnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

Ispitanike nije potrebno obavijestiti o povredi ako je voditelj obrade preduzeo odgovarajuće tehničke i organizacione mjere zaštite podataka, naročito one koje lične podatke čine nerazumljivima bilo kom licu koje nije ovlašteno da im pristupi, kao što je enkripcija (čl. 34.).

Sistem pohrane znači svaki strukturirani skup ličnih podataka dostupnih prema posebnim kriterijumima, bilo da su centralizovani, decentralizovani ili raspršeni na funkcionalnoj ili geografskoj osnovi.

2. Principi obrade podataka o ličnosti

Principi obrade podataka o ličnosti u skladu sa 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 informisan o postupku obrade i njegovoj svrsi, jer je voditelj obrade obavezan ispitaniku pružiti sve dodatne informacije neophodne za poštenu i transparentnu obradu, uzimajući u obzir posebne okolnosti i kontekst obrade ličnih podataka; ispitanik bi trebao biti informisan 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 određenom svrhom; a moguća je daljnja obrada u cilju arhiviranja u javnom interesu, naučnog 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
- **tačnost** – što znači da podaci moraju biti tačni i prema potrebi ažurni; mora se preduzeti svaka razumna mjera u cilju osiguranja da se lični podaci koji nisu tačni, 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 svrhe radi kojih se lični podaci obrađuju; na dulje periode, njihovo čuvanje je moguće samo ako će se lični podaci obrađivati isključivo u svrhu arhiviranja u javnom interesu, naučnog 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 zadovoljen odgovarajući nivo 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 ličnih podataka

Obrada osobnih podataka podrazumijeva radnje kao što su njihovo prikupljanje, evidentiranje, čuvanje, stavljanje na 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 saglasnost 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, preduzele odgovarajuće radnje prije sklapanja ugovora.
- Obrada je nužna radi poštivanja pravnih obaveza voditelja obrade.
- Obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili drugog fizičkog lica.
- Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službenog ovlaštenja 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 ličnih podataka, osobito ako je ispitanik dijete.

4. Prava lica čiji se podaci obrađuju

U skladu sa Općom uredbom o zaštiti podataka, lica čiji se podaci obrađuju u NOSBiH-u mogu ostvariti sljedeća prava:

- **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, svrsi obrade i pravnoj osnovi za obradu podataka, primaocima, iznošenju u treće zemlje, periodu pohrane, mogućnosti povlačenja saglasnosti, itd.
- **pravo pristupa podacima** (čl. 15) koje pripada ispitanicima

To im pravo omogućuje pristup ličnim 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 netačnih ličnih podataka koji se na njega odnose, a uzimajući u obzir svrhu obrade, ispitanik ima pravo i dopuniti nepotpune lične podatke, među ostalim i davanjem dodatne izjave
- **brisanje („pravo na zaborav“)** (čl. 17) – što podrazumijeva da ispitanik od voditelja obrade ima pravo ishoditi brisanje ličnih podataka koji se na njega odnose bez nepotrebnog odgađanja ako, među ostalim, lični podaci više nisu neophodni u odnosu na svrhu obrade
- **pravo na ograničenje obrade** (čl. 18) – što podrazumijeva da u pojedinim situacijama npr. kada je tačnost podataka osporavana ispitanik ima pravo zahtijevati

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

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

Ispitanici, takođe, imaju pravo svoje lične podatke prenijeti iz jednog sistema 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 identifikovati 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 ličnih 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 lične 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 direktnog marketinga, lični 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 utiču, 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 saglasnosti ispitanika.

5. Podaci o licu za zaštitu podataka o ličnosti

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

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

6. Prava koja pripadaju licu u slučaju nedozvoljene obrade

U slučaju nedozvoljene obrade njegovih podataka, tom licu pripadaju sva prava iz Opće uredbe o zaštiti podataka kao i pravo podnošenje žalbe nadležnom nadzornom tijelu.

