UDK 347.7 / 336.2

Obveze voditelja obrade osobnih podataka

Božo Prelević, dipl. iur.

Do 25. svibnja 2018., dana početka primjene Opće uredbe o zaštiti osobnih podataka, preostalo je još manje od mjesec dana. U ovom kratkom vremenu svi sudionici u procesu zaštite osobnih podataka moraju uskladiti svoje postupanje sa novom uredbom. S time u vezi, autor u članku analizira odredbe Opće uredbe o zaštiti osobnih podataka koje se odnose na prava i obveze voditelja obrade osobnih podataka sa primjerima koji će voditeljima obrade poslužiti u izvršavanju svojih obveza u praksi.

1. Uvod

U prošlim brojevima RiPup-a dali smo analizu nekih odredbi Uredbe (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[1] (u nastavku teksta: Opća uredba)[2], koja je stupila na snagu 24. svibnja 2016., a od 25. svibnja 2018. izravno se primjenjuje u svim državama članicama Europske unije, uključujući i Republiku Hrvatsku. Tako smo već analizirali odredbe koje se odnose na temeljne pojmove u Općoj uredbi te prikupljanje osobnih podatka putem video nadzora[3], kao i prava ispitanika uređena Općom uredbom[4]. Međutim, najveći dio Opće uredbe zapravo se odnosi na obveze voditelja obrade osobnih podataka.

U praksi to znači kako će se najveći dio poduzetnika, znači trgovačkih društava i osoba koje obavljaju samostalnu djelatnost osobnim radom (obrtnika), drugih pravnih osoba (udruga, ustanova, javnih tijela i dr.), naći u ulozi voditelja obrade osobnih podataka kada prikupljaju osobne podatke. Opća uredba pred voditelje obrade osobnih podataka postavlja cijeli niz obveza, pri čemu, kako ćemo vidjeti u nastavku, dobar dio njihovih obveza nije povezan s njihovom veličinom, ili brojem zaposlenih radnika. U nastavku ćemo se najprije upoznati sa poljem primjene Opće uredbe u odnosu na voditelje obrade osobnih podataka odnosno analizirati ćemo na koje se voditelje obrade Opća uredba uopće odnosi.

2. Primjena Opće uredbe na voditelje obrade osobnih podataka

U prvom redu potrebno je podsjetiti se pojma voditelja obrade osobnih podataka.

ističemo...

Općom uredbom je određeno kako se pod pojmom voditelja obrade osobnih podataka podrazumijeva fizička, ili pravna osoba, tijelo javne vlasti, agencija, ili drugo tijelo koje samo, ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.

Kada su svrhe i sredstva takve obrade utvrđeni pravom EU, ili pravom države članice, voditelj obrade, ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom EU, ili pravom države članice[5].

S druge strane, pod pojmom „obrada osobnih podataka" podrazumijeva se svaki postupak, ili skup postupaka koji se obavljaju na osobnim podacima, ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje osobnih podataka[6].

1 SL L 119, 4.5.2016.

2 http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=EN

3 Prelević, Božo, stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)", RiPup br. 3/18, str. 158.

4 Prelević, Božo, stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (II. dio) – prava ispitanika", RiPup br. 4/18, str. 150.

5 Čl. 4. st. 1. t. 7. Opće uredbe.

6 Čl. 4. st. 1. t. 2. Opće uredbe.

2.1. Teritorijalno područje primjene Opće uredbe

ističemo...

Opća uredba se odnosi na obradu osobnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade osobnih podataka u EU, neovisno o tome obavlja li se obrada osobnih podataka u EU, ili ne.

Kako je samom Općom uredbom određeno, ona se primjenjuje na obradu osobnih podataka ispitanika u EU koju obavlja voditelj obrade osobnih podataka bez poslovnog nastana u EU, ako su aktivnosti obrade povezane s[7]:

- nuđenjem robe, ili usluga takvim ispitanicima u EU, neovisno o tome treba li ispitanik izvršiti plaćanje; ili
- praćenjem njihova ponašanja dokle god se njihovo ponašanje odvija unutar EU.

Osim toga, Opća uredba se primjenjuje na obradu osobnih podataka koju obavlja voditelj obrade osobnih podataka koji nema poslovni nastan u EU nego na mjestu gdje se pravo države članice primjenjuje temeljem međunarodnog javnog prava, kao što je to npr. slučaj u diplomatskom, ili konzularnom predstavništvu države članice.

2.2. Primjena Opće uredbe u slučaju kada voditelj obrade nema poslovni nastan u EU

Osim navedenog, postoje i drugi slučajevi u kojima se Opća uredba primjenjuje na obradu osobnih podataka koje obavlja voditelj obrade osobnih podataka koji nema poslovni nastan u EU, o čemu više navodimo u nastavku.

2.2.1. Ponuda robe, ili usluga voditelja obrade iz treće zemlje ispitaniku u EU

ističemo...

Kako bi se osiguralo da pojedincima nije uskraćena zaštita na koju imaju pravo temeljem Opće uredbe na obradu osobnih podataka ispitanika koji se nalaze u EU, a koju obavlja voditelj obrade osobnih podataka bez poslovnog nastana u EU, trebala bi se primjenjivati ova Uredba ako su aktivnosti obrade povezane s ponudom robe, ili usluga takvim ispitanicima, bez obzira na to ima li ta ponuda veze s plaćanjem.

U praksi bi to značilo kako npr., u slučaju da neki voditelj obrade osobnih podataka ima poslovni nastan u Bosni i Hercegovini, a prikuplja, ili obrađuje osobne podatke ispitanika u RH radi ponude robe ili usluga, mora pri obradi njihovih osobnih podataka poštovati odredbe Opće uredbe. Kako bi se utvrdilo nudi li takav voditelj obrade osobnih podatka robu, ili usluge ispitanicima koji se nalaze u EU, trebalo bi utvrditi je li očito da voditelj obrade namjerava ponuditi usluge ispitanicima koji se nalaze u jednoj, ili više država članica EU.

Makar su sama dostupnost internetskih stranica voditelja obrade osobnih podataka, izvršitelja obrade, ili posrednika u EU, ili adrese elektroničke pošte i drugih kontaktnih podataka, ili korištenje jezikom koji je općenito u uporabi u trećoj zemlji u kojoj voditelj obrade ima poslovni nastan nedovoljni za utvrđivanje takve namjere, čimbenici kao što je korištenje jezikom, ili valutom koji su općenito u uporabi u jednoj, ili više država članica s mogućnošću naručivanja robe i usluga na tom drugom jeziku, ili spominjanje kupaca, ili korisnika koji se nalaze u EU, mogu jasno pokazati da voditelj obrade namjerava nuditi robu, ili usluge ispitanicima u EU.

2.2.2. Praćenje ponašanja ispitanika u EU od strane voditelja obrade bez poslovnog nastana u EU

ističemo...

Na obradu osobnih podataka ispitanika koji se nalaze u EU, koju obavlja voditelj obrade osobnih podataka bez poslovnog nastana u EU, također bi se trebala primjenjivati Opća uredba kada se odnosi na praćenje ponašanja takvih ispitanika ako se njihovo ponašanje odvija unutar EU.

Kako bi se odredilo može li se aktivnost obrade smatrati praćenjem ponašanja ispitanika, trebalo bi utvrditi prati li se pojedince na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova.

Podsjećamo, pod pojmom „izrade profila" u Općoj uredbi se podrazumijeva svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu, ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom, ili kretanjem tog pojedinca[8].

2.2.3. Imenovanje predstavnika voditelja obrade osobnih podataka bez poslovnog nastana u EU

U slučaju da voditelj obrade koji nema poslovni nastan u EU obrađuje osobne podatke ispitanika u EU čije su aktivnosti obrade povezane s ponudom robe, ili usluga, bez obzira na to je li potrebno plaćanje ispitanika, za takve bi ispitanike u EU, ili za praćenje njihova ponašanja dok se ono odvija unutar EU, voditelj obrade osobnih podatka, ili izvršitelj obrade, mora imenovati predstavnika, osim ako:

- se obrada osobnih podataka obavlja samo povremeno, ne uključuje opsežnu obradu posebnih kategorija osobnih podataka, ili je obrada osobnih podataka povezana s kaznenim presudama i kažnjivim djelima te vjerojatno neće dovesti do rizika za prava i slobode pojedinaca, uzimajući u obzir prirodu, kontekst, opseg i svrhe obrade; ili
- je voditelj obrade tijelo javne vlasti, ili javno tijelo.

Sukladno Općoj uredbi, „predstavnik" znači fizičku, ili pravnu osobu s poslovnim nastanom u državi članici EU, u kojoj se nalaze ispitanici čiji se osobni podaci obrađuju u vezi s robom ili uslugama koje im se nude, ili čije se ponašanje prati, koju je voditelj obrade osobnih podataka, ili izvršitelj obrade imenovao pisanim putem sukladno čl. 27. Opće uredbe, koja predstavlja voditelja obrade osobnih podataka, ili izvršitelja obrade, u pogledu njihovih obveza temeljem Opće uredbe[9]. Predstavnik bi trebao djelovati u ime voditelja obrade osobnih podataka i može mu se obratiti svako nadzorno tijelo.

7 Čl. 3. st. 2. Opće uredbe.

8 Čl. 4. st. 1. t. 4. Opće uredbe.

9 Čl. 4. st. 1. t. 17. Opće uredbe.

ističemo...

Voditelj obrade osobnih podataka mora izričito, pisanim ovlaštenjem imenovati predstavnika da djeluje u njegovo ime s obzirom na obveze voditelja obrade temeljem Opće uredbe.

Imenovanje takvog predstavnika ne utječe na dužnost, ili odgovornost voditelja obrade osobnih podataka temeljem Opće uredbe. Voditelj obrade osobnih podataka ovlašćuje predstavnika kako bi se, uz obraćanje voditelju obrade osobnih podataka, ili izvršitelju obrade, ili umjesto obraćanja njima, njemu obraćali osobito nadzorna tijela i ispitanici u pogledu svih pitanja u vezi s obradom za potrebe osiguravanja sukladnosti s Općom Uredbom[10].

U slučaju da voditelj obrade osobnih podataka postupa protivno Općoj uredbi, odgovoran je predstavnik voditelaj obrade. Međutim, sukladno čl. 27. st. 5. Opće uredbe, imenovanje predstavnika voditelja obrade osobnih podataka, ili izvršitelja obrade, ne utječe na pravne zahtjeve koji bi mogle biti postavljeni i protiv samog voditelja obrade.

2.3. Obrada od strane fizičkih osoba u okviru osobne, ili kućne aktivnosti

ističemo...

Opća uredba se ne primjenjuje na obradu osobnih podataka koju fizičke osobe obavljaju u okviru isključivo osobne, ili kućne aktivnosti te stoga nije povezana s profesionalnom, ili komercijalnom djelatnošću.

Međutim, Opća uredba se primjenjuje na voditelje obrade, ili izvršitelje obrade osobnih podataka, koji pružaju sredstva za obradu osobnih podataka za takve osobne, ili kućne aktivnosti.

3. Obveze voditelja obrade osobnih podataka

ističemo...

Voditelj obrade osobnih podataka u prvom redu mora osigurati obradu osobnih podataka sukladno odredbama Opće uredbe, pridržavajući se pri tome njenih temeljnih načela.

Sukladno čl. 5. Opće uredbe, osobni podaci moraju biti:

- zakonito, pošteno i transparentno obrađivani s obzirom na ispitanika („zakonitost, poštenost transparentnost");
- prikupljeni u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije sukladan tim svrhama, s time da se daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog, ili povijesnog istraživanja, ili u statističke svrhe, sukladno čl. 89. st. 1. Opće uredbe, ne smatra neusklađenom s prvotnim svrhama („ograničavanje svrhe");
- primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju („smanjenje količine podataka");
- točni i prema potrebi ažurni, što znači kako se mora poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe u koje se obrađuju, bez odlaganja izbrišu, ili isprave („točnost");
- čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju, s time da se osobni podaci mogu pohraniti na dulja razdoblja ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog, ili povijesnog istraživanja, ili u statističke svrhe sukladno čl. 89. st. 1. Opće uredbe, što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih Općom uredbom radi zaštite prava i sloboda ispitanika („ograničenje pohrane");
- obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene, ili nezakonite obrade te od slučajnog gubitka, uništenja, ili oštećenja primjenom odgovarajućih tehničkih, ili organizacijskih mjera („cjelovitost i povjerljivost").

Voditelj obrade osobnih podataka odgovoran je za usklađenost sa ovim načelima Opće uredbe i tu usklađenost mora biti u mogućnosti dokazati („pouzdanost"). To će u praksi značiti kako ispunjavanje ovih temeljnih načela prikupljanja osobnih podataka mora biti dokumentirano, odnosno uobličeno u dokument (npr. interni akt o zaštiti osobnih podataka), ili više dokumenata u pisanom obliku (uključujući i elektronski oblik).

3.1. Opće obveze voditelja obrade osobnih podataka

Kod svakog voditelja obrade osobnih podataka trebalo bi uspostaviti dužnosti i odgovornosti voditelja obrade za svaku obradu osobnih podataka koju provodi on sam, ili izvršitelj obrade osobnih podataka u njegovo ime.

ističemo...

Voditelj obrade osobnih podataka ima obvezu provođenja odgovarajućih i djelotvornih mjera radi usklađivanja sa Općom uredbom, pri čemu mora biti u mogućnosti to i dokazati, što znači da provedba tih mjera mora biti dokumentirana u pisanom obliku (uključujući i elektronski oblik).

Mjerama koje provodi radi usklađivanja s Općom uredbom trebalo bi u obzir uzeti prirodu, opseg, kontekst i svrhe obrade te rizik za prava i slobode pojedinaca.

Općenito, voditelj obrade osobnih podataka ima, između ostalog, sljedeće obveze:

- procjena usklađenosti politika zaštite osobnih podataka sa Općom uredbom, zakonom i podzakonskim propisima;
- uvođenje internih politika zaštite osobnih podataka;
- edukacija zaposlenika o propisima i internim politikama zaštite osobnih podataka
- usklađivanje internih politika zaštite osobnih podataka s odredbama Opće uredbe, zakona i podzakonskih propisa iz područja zaštite osobnih podataka;
- poštivanje temeljnih načela Opće uredbe;
- provedba mjera koje ispunjavaju načela tehničke i integrirane zaštite podataka;
- poštivanje odobrenih kodeksa ponašanja;
- vođenje evidencija aktivnosti obrade;
- suradnja s nadzornim tijelom;

10 Čl. 27. st. 4. Opće uredbe.

- provedba odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala odgovarajuća razinu sigurnosti obrade osobnih podataka;
- izvješćivanje nadzornog tijela i ispitanika o povredi osobnih podataka;
- obavještavanje ispitanika o povredi osobnih podataka;
- procjena učinka obrade na zaštitu osobnih podataka;
- prethodno savjetovanje s nadzornim tijelom;
- poštivanje kodeksa ponašanja;
- imenovanje službenika za zaštitu osobnih podataka kada je to određeno Općom uredbom;
- traženje privole od ispitanika kada je to potrebno radi provedbe načela zakonitosti obrade;
- poštivanje prava ispitanika (poštivanje prava na brisanje podataka, informiranje o točki kontakta radi provjere stanja obrade osobnih podataka ispitanika, informiranje ispitanika o njegovim pravima i obvezama voditelja obrade putem pravila privatnosti;
- imenovanje predstavnika voditelja obrade osobnih podataka s poslovnim nastanom izvan EU, koji obrađuju podatke ispitanika u EU;
- izmjena ugovora o radu koji se sklapaju sa vlastitim radnicima radi ustupanja obrade njihovih osobnih podataka izvršiteljima obrade;
- sklapanje ugovora sa izvršiteljem obrade osobnih podataka i dr.

Voditelj obrade osobnih podataka mora dokumentirati na koji način ispunjava navedene obveze, što znači da mora izraditi i čuvati niz akata u pisanom obliku (uključujući i elektronski oblik), o čemu više navodimo u nastavku[11].

3.1.1. Procjena usklađenosti s Općom uredbom

ističemo...

Svaki voditelj obrade osobnih podataka bi u postupku primjene Opće uredbe najprije trebao provesti procjenu usklađenosti svojih politika zaštite osobnih podataka sa Općom uredbom.

Od ove procjene zapravo ovisi daljnje postupanje voditelja obrade osobnih podataka u primjeni Opće uredbe. Procjenu voditelj obrade osobnih podataka može, između ostalog, izvršiti i ispunjavanjem upitnika koji sadrži pitanja o stupnju usklađenosti njegovih politika zaštite osobnih podataka s Općom uredbom.

Primjer: procjena usklađenosti s Općom uredbom

Aktivnost	DA	NE
Napravljena analiza o obvezi imenovanja službenika za zaštitu osobnih podataka		
Imenovanje službenika za zaštitu osobnih podataka		
Postojanje sukoba interesa kod službenika za zaštitu osobnih podataka		
Postojanje grupe za usklađivanje sa Općom uredbom		
Edukacija radnika o novim pravilima zaštite osobnih podataka		
Obveza vođenja evidencija obrade		
Utvrđeni su osobni podaci koji se prikupljaju i obrađuju		
Utvrđena je obrada posebnih kategorija podataka		
Utvrđeno je postojanje prijenosa osobnih podataka		
Osigurane organizacijske i tehničke mjere za zaštitu osobnih podataka		
Utvrđene politike i postupci u slučaju povrede osobnih podataka		
Postojanje registra povreda osobnih podataka		
Postojanje internih politika (akta) za zaštitu osobnih podataka		
Postojanje pravila privatnosti		
Usklađenost privola s Općom uredbom		
Postojanje registra privola		
Usklađenost ugovora s izvršiteljima obrade sukladno Općoj uredbi		
Upoznavanje ispitanika s pravima temeljem Opće uredbe		
Kontrola usklađenosti s Općom uredbom		

3.1.2. Uvođenje internih politika i provedba mjera tehničke i integrirane zaštite

ističemo...

Ovisno o rezultatima procjene usklađenosti politika voditelja obrade osobnih podataka sa Općom uredbom, voditelj obrade bi radi dokazivanja usklađenosti s Općom uredbom trebao uvesti interne politike i provesti mjere koje osobito ispunjavaju načela tehničke zaštite podataka i integrirane zaštite podataka.

Takve mjere mogle bi se, među ostalim, sastojati od smanjenja količine obrade osobnih podataka, pseudonimizacije osobnih podataka što je prije moguće, transparentnosti u vezi s funkcijama i obradom osobnih podataka, omogućavanja ispitaniku da prati obradu podataka, omogućavanja voditelju obrade da stvara i poboljšava sigurnosne značajke.

ističemo...

Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade mora provesti odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom, koje se prema potrebi preispituju i ažuriraju.

U slučaju da su navedene mjere razmjerne u odnosu na aktivnosti obrade, one uključuju provedbu odgovarajućih politika zaštite podataka od strane voditelja obrade. Pri tome se poštivanje odobrenih kodeksa ponašanja iz čl. 40. Opće uredbe[12], ili odobrenih mehanizama certificiranja iz čl. 42. Opće uredbe može iskoristiti kao element za dokazivanje sukladnosti s obvezama voditelja obrade.

Voditelj obrade osobnih podataka, uzimajući u obzir najnovija dostignuća, trošak provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade podataka, u vrijeme određivanja sredstava obrade i u vrijeme same obrade, mora provesti odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka, kao što je smanjenje količine podataka, te uključenje zaštitnih mjera u obradu kako bi se ispunili zahtjevi iz Opće uredbe i zaštitila prava ispitanika.

11 Vidjeti pod 3.8.

12 Vidjeti pod 3.5.

ističemo...

Podsjećamo kako pod pojmom „pseudonimizacija", u smislu čl. 4. st. 1. t. 5. Opće uredbe, podrazumijevamo obradu osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen, ili se može utvrditi.

Voditelj obrade mora provesti odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade.

Ova se obveza primjenjuje na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane i njihovu dostupnost. Takvim se mjerama osigurava da osobni podaci nisu automatski, bez intervencije pojedinca, dostupni neograničenom broju pojedinca[13]. Treba istaknuti kako se odobreni mehanizam certificiranja sukladno čl. 42. Opće uredbe, može iskoristiti kao element za dokazivanje sukladnosti sa navedenim zahtjevima Opće uredbe za osiguravanje tehničke i integrirane zaštite osobnih podataka od strane voditelja obrade.

3.1.3. Zajednički voditelji obrade osobnih podataka

Općom uredbom je predviđena i mogućnost obrađivanja osobnih podataka putem zajedničkog voditelja obrade od strane više voditelja obrade.

ističemo...

Naime, sukladno čl. 29. Opće uredbe, u slučaju da dvoje, ili više voditelja obrade zajednički odrede svrhe i načine obrade, oni su zajednički voditelji obrade.

Oni na transparentan način određuju svoje odgovornosti za poštovanje obveza iz Opće uredbe, posebno s obzirom na ostvarivanje prava ispitanika i svojih dužnosti u pogledu pružanja informacija iz čl. 13. i 14. Opće uredbe (informacije koje se trebaju dostaviti ako se osobni podaci prikupljaju od ispitanika te informacije koje se trebaju pružiti ako osobni podaci nisu dobiveni od ispitanika)[14], te to čine međusobnim dogovorom, osim ako su odgovornosti voditeljâ obrade utvrđene pravom EU, ili pravom države članice kojem voditelji obrade podliježu i u mjeri u kojoj su one utvrđene.

Međusobnim dogovorom se može odrediti i kontaktna točka (osoba, broj telefona) za ispitanike. Ovaj dogovor mora odražavati pojedinačne uloge i odnose zajedničkih voditelja obrade u odnosu na ispitanike. Bit dogovora mora biti dostupna ispitaniku.

Bez obzira na uvjete ovog dogovora ispitanik može ostvarivati svoja prava iz Opće uredbe u vezi sa svakim voditeljem obrade, kao i protiv svakog od njih. Svakako treba naglasiti kako zajedničko vođenje obrade osobnih podataka sukladno odredbama Opće uredbe predstavlja samo mogućnost, a ne i obvezu.

13 Čl. 25. st. 2. Opće uredbe.

14 Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (II. dio) – prava ispitanika", RiPup br. 4/18, str. 156.

3.1.4. Evidencija aktivnosti obrade

Općom uredbom je predviđeno da svaki voditelj obrade i predstavnik voditelja obrade te ako je primjenjivo, vodi evidenciju aktivnosti obrade za koje je odgovoran[15]. Ova evidencija sadržava sve sljedeće informacije:

- ime i kontaktne podatke voditelja obrade osobnih podataka te ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;
- svrhu obrade;
- opis kategorija ispitanika i kategorija osobnih podataka;
- kategorije primatelja kojima su osobni podaci otkriveni, ili će im biti otkriveni, uključujući primatelje u trećim zemljama, ili međunarodne organizacije;
- ako je primjenjivo, prijenose osobnih podataka u treću zemlju, ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje, ili međunarodne organizacije te, u slučaju prijenosa iz čl. 49. st. 1. podstavka 2. Opće uredbe, dokumentaciju o odgovarajućim zaštitnim mjerama;
- ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;
- ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz čl. 32. st. 1. Opće uredbe[16].

ističemo...

Evidencija aktivnosti obrade mora biti u pisanom obliku, uključujući i elektronski oblik.

Voditelj obrade te njegov predstavnik, ako je primjenjivo, na zahtjev daju nadzornom tijelu uvid u evidenciju.

Važno je istaknuti kako se navedena obveza vođenja evidencija obrade osobnih podataka ne primjenjuje na poduzeće, ili organizaciju u kojoj je zaposleno manje od 250 osoba, osim ako:

- će obrada koju provodi vjerojatno prouzročiti visok rizik za prava i slobode ispitanika;
- obrada nije povremena, ili;
- obrada uključuje posebne kategorije podataka iz čl. 9. st. 1. Opće uredbe, ili;
- je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima iz čl. 10. Opće uredbe[17].

Opća uredba, naime, načelno sadržava odstupanja za organizacije u kojima je zaposleno manje od 250 osoba s obzirom na vođenje evidencije, radi uzimanja u obzir posebnih situacija mikropoduzeća, malih i srednjih poduzeća. Ipak, u slučaju da su ispunjeni navedeni posebni uvjeti, pravilo da poduzeća, ili organizacije sa manje od zaposlenih 250 osoba ne moraju voditi evidenciju obrade podataka neće se primijeniti.

Podsjećamo kako se pod pojmom „poduzeće", u smislu odredbi Opće uredbe podrazumijeva fizička, ili pravna osoba koja se bavi gospodarskom djelatnošću, bez obzira na pravni oblik te djelatnosti, uključujući partnerstva, ili udruženja koja se redovno bave gospodarskom djelatnošću[18]. Voditelj obrade osobnih podataka trebao bi voditi evidenciju o aktivnostima obrade pod svojom odgovornošću radi dokazivanja sukladnosti s Općom uredbom. Osim toga, svaki voditelj obrade osobnih podataka, koji mora voditi evidenciju obrade

15 Čl. 30. st. 1. Opće uredbe.

16 Vidjeti pod 3.2.

17 Detaljnije o odredbama čl. 9. i 10. Opće uredbe u stručnom članku, Prelević, B., „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)", RiPup br. 3/18, str. 162-164.

18 Čl. 4. st. 1. t. 18. Opće uredbe.

trebao bi imati obvezu surađivati s nadzornim tijelom i omogućiti mu na zahtjev uvid u tu evidenciju kako bi mu mogla poslužiti za praćenje postupaka obrade.

Primjer: Evidencija aktivnosti obrade – voditelj obrade – čl. 30. st. 1. Opće uredbe

Voditelj obrade		Službenik za zaštitu osobnih podataka	
Naziv	CCC d.o.o.	Ime i prezime	Veronika Nikić
Adresa	Velika avenija 1c	Adresa	Plava cesta 23a
Telefon	9999-9991	Telefon	9199-9999
E-pošta	ccc@net.com	E-pošta	vnikic@ccc.net.bc

Svrha obrade	Kategorija ispitanika	Kategorija osobnih podataka	Kategorija primatelja	Prijenos u 3. zemlje / MO*	Zaštitne mjere za prijenos podataka	Rokovi brisanja/ čuvanja podataka	Opis zaštitnih mjera	Pravna osnova
plaća	radnik	kontakt podaci	služba financija	ne	–	trajno	zaključani ormari, enkripcija	Ugovor o radu
evidencija o radnicima	radnik	kontakt podaci	pravna služba	ne	–	6	zaključani ormari enkripcija	PSNVER**

3.1.5. Suradnja s nadzornim tijelom

Voditelj obrade, ako je to primjenjivo, njihovi predstavnici, na zahtjev moraju surađivati s nadzornim tijelom, odnosno Agencijom za zaštitu osobnih podataka (u nastavku teksta: Agencija) u ispunjavanju njegovih zadaća.

3.2. Sigurnost osobnih podataka

Važna obveza voditelja obrade osobnih podataka odnosi se na osiguravanje sigurnosti osobnih podataka, o čemu detaljnije navodimo u nastavku.

3.2.1. Sigurnost obrade

Sukladno čl. 32. Opće uredbe, voditelj obrade, uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

- pseudonimizaciju i enkripciju (šifriranje) osobnih podataka;
- sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;
- sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog, ili tehničkog incidenta;
- proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog, ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka, ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni, ili na drugi način obrađivani. Poštivanje odobrenog kodeksa ponašanja, ili odobrenog mehanizma certificiranja iz čl. 42. Opće uredbe, može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima za osiguranje sigurnosti obrade od strane voditelja obrade osobnih podataka.

Voditelj obrade osobnih podataka mora poduzeti mjere kako bi osigurao da svaki pojedinac koji djeluje pod odgovornošću voditelja obrade, a koji ima pristup osobnim podacima, ne obrađuje te podatke ako to nije prema uputama voditelja obrade, osim ako je to obvezan učiniti prema pravu EU, ili pravu države članice. Možemo rezimirati kako voditelj obrade osobnih podataka, kao i izvršitelj obrade, mora osigurati primjerenu sigurnost obrade osobnih podataka.

3.2.2. Izvješćivanje nadzornog tijela o povredi osobnih podataka

ističemo...

Voditelj obrade osobnih podataka mora u slučaju povrede osobnih podataka, bez nepotrebnog odgađanja te ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvjestiti nadzorno tijelo iz čl. 55. Opće uredbe, odnosno Agenciju, o toj povredi osobnih podataka, osim ako može dokazati u skladu s načelom odgovornosti kako nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca[19].

Ako izvješćivanje nije učinjeno unutar 72 sata, mora biti popraćeno razlozima za kašnjenje. Izvršitelj obrade bez nepotrebnog odgađanja izvješćuje voditelja obrade nakon što sazna za povredu osobnih podataka.

U izvješćivanju o povredi mora se barem:

- opisati priroda povrede osobnih podataka, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;

19 Čl. 33. st. 1. Opće uredbe.

- navesti ime i kontaktne podatke službenika za zaštitu podataka, ili druge kontaktne točke od koje se može dobiti još informacija;
- opisati vjerojatne posljedice povrede osobnih podataka;
- opisati mjere koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje problema povrede osobnih podataka, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

U slučaju da voditelj obrade osobnih podataka ne može odmah pružiti navedene informacije, mora ih pružati postupno, bez nepotrebnog daljnjeg odgađanja. Voditelj obrade dokumentira sve povrede osobnih podataka, uključujući činjenice vezane zapovredu osobnih podataka, njezine posljedice i mjere poduzete za popravljanje štete. Takva dokumentacija nadzornom tijelu omogućuje provjeru navedenih odredbi Opće uredbe.

3.2.3. Obavješćivanje ispitanika o povredi osobnih podataka

ističemo...

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja mora obavijestiti ispitanika o povredi osobnih podataka, kako bi on mogao poduzeti potrebne mjere opreza[20].

Ova obavijest bi se ispitanicima trebala pružiti što je prije, u razumnim granicama, izvedivo i u bliskoj suradnji s nadzornim tijelom (Agencijom), poštujući njegove upute, ili upute drugih relevantnih tijela vlasti. Tako bi npr. o potrebi za umanjivanjem neposrednog rizika od štete bilo bi potrebno odmah obavijestiti ispitanike, dok potreba za provedbom odgovarajućih mjera protiv daljnje, ili slične povrede osobnih podataka može opravdati duži rok za obavijest.

U obavijesti dostavljenoj ispitaniku se opisuje se priroda povrede osobnih podataka uporabom jasnog i jednostavnog jezika te ona sadržava barem informacije i mjere iz čl. 33. st. 3. t. (b), (c) i (d) Opće uredbe[21]. Sukladno čl. 34. st. 3. Opće uredbe, obavješćivanje ispitanika ipak neće biti obvezno ako je ispunjen bilo koji od sljedećih uvjeta:

- voditelj obrade poduzeo je odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom osobnih podataka, posebno one koje osobne podatke čine nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti, kao što je enkripcija;
- voditelj obrade poduzeo je naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika iz čl. 34. st. 1. Opće uredbe;
- time bi se zahtijevao nerazmjeran napor, s time da u takvom slučaju mora postojati javno obavješćivanje, ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način.

U slučaju da voditelj obrade nije do tog trenutka obavijestio ispitanika o povredi osobnih podataka, nakon razmatranja razine vjerojatnosti da će povreda osobnih podataka prouzročiti visok rizik, nadzorno tijelo (Agencija) može od njega zahtijevati da to učini, ili može zaključiti da je ispunjen neki od uvjeta navedenih u čl. 34. st. 3. Opće uredbe.

20 Čl. 34. st. 1. Opće uredbe.

21 Vidjeti pod 3.2.2.

3.3. Procjena učinka obrade na zaštitu osobnih podataka

Jedna od važnih obveza voditelja obrade osobnih podataka jest i izrada procjene učinka obrade na zaštitu podataka (u nastavku teksta: procjena učinka).

ističemo...

Procjena učinka mora biti dokumentirana u pisanom obliku (uključujući i elektronski oblik).

Općom uredbom je predviđeno kako u slučaju da je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade prije obrade osobnih podataka mora provesti procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka[22].

Ishod procjene učinka trebao bi se uzeti u obzir pri utvrđivanju odgovarajućih mjera radi dokazivanja da je obrada osobnih podataka od strane voditelja obrade sukladna s Općom uredbom.

ističemo...

U slučaju da se u procjeni učinka pokaže kako postupci obrade osobnih podataka uključuju visok rizik koji voditelj obrade ne može umanjiti odgovarajućim mjerama u smislu dostupne tehnologije i troškova provedbe, voditelj obrade se prije obrade osobnih podataka mora savjetovati s nadzornim tijelom.

Takav visok rizik vjerojatno će proizaći iz određenih vrsta obrade i opsega i učestalosti obrade, što može također prouzročiti štetu, ili ometanje prava i slobode ispitanika.

Nadzorno tijelo trebalo bi odgovoriti na zahtjev za savjetovanje u određenom vremenskom roku. Međutim, izostanak reakcije nadzornog tijela u tom roku ne bi smio utjecati na bilo koju intervenciju nadzornog tijela sukladno njegovim zadaćama i ovlastima iz Opće uredbe, uključujući ovlast da zabrani postupke obrade. Rezultat procjene učinka na zaštitu podataka koja je provedena u vezi s dotičnom obradom može se kao dio tog postupka savjetovanja dostaviti nadzornom tijelu, a osobito mjere predviđene za umanjivanje rizika za prava i slobode pojedinaca.

Jedna procjena učinka može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike. Pri provođenju procjene učinka na zaštitu podataka voditelj obrade mora tražiti savjet od službenika za zaštitu podataka, ako je on imenovan. Procjena učinka na zaštitu podataka obvezna je osobito u slučaju:

- sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca, ili na sličan način značajno utječu na pojedinca;
- opsežne obrade posebnih kategorija osobnih podataka iz čl. 9. st. 1. Opće uredbe, ili podataka u vezi s kaznenim osudama i kažnjivim djelima iz čl. 10. Opće uredbe; ili
- sustavnog praćenja javno dostupnog područja u velikoj mjeri.

Općom uredbom je predviđeno da nadzorno tijelo uspostavlja i javno objavljuje popis vrsta postupaka obrade koje podliježu zahtjevu

22 Čl. 35. st. 1. Opće uredbe.

za procjenu učinka sukladno čl. 35. st. 1. Opće uredbe. Ove popise nadzorno tijelo priopćuje te Odboru iz čl. 68. Opće uredbe.

Nadzorno tijelo može također uspostaviti i javno objaviti popis vrsta postupaka obrade za koje nije potrebna procjena učinka, koje također priopćuje Odboru. Prije usvajanja ovih popisa nadležno nadzorno tijelo primjenjuje mehanizam konzistentnosti iz čl. 63. Opće uredbe, kada takvi popisi obuhvaćaju aktivnosti obrade koje su povezane s ponudom robe, ili usluga ispitanicima, ili s praćenjem njihova ponašanja u nekoliko država članica, ili koje mogu znatno utjecati na slobodno kretanje osobnih podataka unutar EU.

Procjena učinka sadrži barem[23]:

- sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes voditelja obrade;
- procjenu nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama;
- procjenu rizika za prava i slobode ispitanika iz čl. 35. st. 1. Opće uredbe; i
- mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s Općom uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba.

Poštivanje odobrenih kodeksa ponašanja iz čl. 40. Opće uredbe od strane relevantnih voditelja obrade osobnih podataka, ili izvršitelja obrade uzima se u obzir pri procjeni učinka postupaka obrade koje provode ti voditelji obrade, ili izvršitelji obrade, posebno u svrhe procjene učinka. Prema potrebi voditelj obrade osobnih podataka od ispitanika, ili njihovih predstavnika traži mišljenje o namjeravanoj obradi, ne dovodeći u pitanje komercijalne, ili javne interese, ili sigurnost postupka obrade.

U slučaju da obrada sukladno čl. 6. st. 1. t. (c), ili (e) Opće uredbe, ima pravnu osnovu u pravu EU, ili pravu države članice kojem voditelj obrade podliježe, ako su tim pravom uređuju posebni postupci obrade, ili skupina dotičnih postupaka te je procjena učinka na zaštitu podataka već provedena kao dio opće procjene učinka u kontekstu donošenja pravne osnove, odredbe čl. 35. st. 1.-7. se ne primjenjuju, osim ako države članice smatraju da je potrebnoprovesti takvu procjenu prije aktivnosti obrade. Voditelj obrade osobnih podataka prema potrebi provodi preispitivanje kako bi procijenio je li obrada provedena sukladno procjeni učinka barem onda kada postoji promjena u razini rizika koji predstavljaju postupci obrade.

3.3.1. Izrada procjene rizika

Sastavni dio sadržaja procjene učinka iz čl. 35. st. 7. Opće uredbe, kako smo naveli[24], jest i procjena rizika za prava i slobode ispitanika iz čl. 35. st. 1. Opće uredbe. To znači kako voditelj obrade osobnih podataka mora procijeniti rizike povezane s obradom i provesti mjere za njihovo umanjivanje, kao što je enkripcija. Ovim bi se mjerama trebala osigurati odgovarajuća razina zaštite uključujući povjerljivost, uzimajući u obzir najnovija dostignuća i troškove provedbe u odnosu na rizike i prirodu osobnih podataka koji se trebaju zaštititi.

Prilikom procjene rizika za sigurnost podataka u obzir bi trebalo uzeti rizike koje predstavlja obrada osobnih podataka poput slučajnog, ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog odavanja, ili pristupa osobnim podacima koji su preneseni, pohranjeni, ili na drugi način obrađivani, a što osobito može dovesti do fizičke, materijalne, ili nematerijalne štete. Rizične vrste postupaka obrade mogu biti osobito one koje uključuju upotrebu novih tehnologija, ili one koje su nove vrste i s obzirom na koje voditelj obrade još nije proveo procjenu učinka, ili za koje je procjena učinka postala potrebna obzirom na vrijeme koje je proteklo od prvotne obrade.

ističemo...

Procjena rizika, budući je sastavni dio procjene učinka, također mora biti dokumentirana u pisanom obliku (uključujući i elektronski oblik).

3.4. Prethodno savjetovanje

U krug obveza voditelja obrade osobnih podataka spada i obveza prethodnog savjetovanja s nadzornim tijelom (Agencijom).

ističemo...

Naime, sukladno čl. 36. st. 1. Opće uredbe, voditelj obrade osobnih podataka mora se savjetovati s nadzornim tijelom prije obrade ako se procjenom učinka na zaštitu podataka iz čl. 35. Opće uredbe pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika[25].

U slučaju da nadzorno tijelo smatra da bi se namjeravanom obradom kršila Opća uredba, osobito ako voditelj obrade nije u dovoljnoj mjeri utvrdio, ili umanjio rizik, nadzorno tijelo u roku od najviše osam tjedana od zaprimanja zahtjeva za savjetovanje pisanim putem savjetuje voditelja obrade i, prema potrebi, izvršitelja obrade, te može iskoristiti bilo koju od svojih ovlasti iz čl. 58. Opće uredbe[26].

Taj se rok može prema potrebi produžiti za šest tjedana, uzimajući u obzir složenost namjeravane obrade. Nadzorno tijelo u roku od mjesec dana od zaprimanja zahtjeva obavješćuje voditelja obrade, i, prema potrebi, izvršitelja obrade o svakom takvom produljenju i o razlozima odgode. Ti se rokovi mogu suspendirati sve dok nadzorno tijelo ne dobije informacije koje je moglo zatražiti u svrhe savjetovanja.

Prilikom savjetovanja s nadzornim tijelom sukladno navedenoj odredbi čl. 36. st. 1. Opće uredbe, voditelj obrade osobnih podataka nadzornom tijelu dostavlja:

- ako je primjenjivo, odgovarajuće odgovornosti voditelja obrade, zajedničkih voditelja obrade i izvršitelja obrade uključenih u obradu, osobito za obrade unutar grupe poduzetnika;
- svrhu i i sredstva namjeravane obrade;
- zaštitne mjere i druge mjere za zaštitu prava i sloboda ispitanika određene Općom uredbom;
- ako je primjenjivo, kontaktne podatke službenika za zaštitu podataka;
- procjenu učinka na zaštitu podataka kako je predviđena u čl. 35. Opće uredbe; i
- sve druge informacije koje nadzorno tijelo zatraži.

Općom uredbom je predviđeno kako se neovisno o navedenoj odredbi čl. 36. st. 2. Opće uredbe, od voditelja obrade osobnih podataka pravom države članice, znači i pravom RH, može zahtijevati da se savjetuju s nadzornim tijelom i od njega dobiju prethodno odobrenje u pogledu obrade koju obavlja voditelj obrade za izvršenje zadaće

23 Čl. 35. st. 7. Opće uredbe.
24 Vidjeti pod 3.3.
25 Vidjeti pod 3.3.
26 Čl. 36. st. 2. Opće uredbe.

koju voditelj obrade provodi u javnom interesu, uključujući i obradu u vezi sa socijalnom zaštitom i javnim zdravljem.

3.5. Kodeksi ponašanja

Jedna od obveza za voditelje obrade osobnih podataka previđena Općom uredbom jest i postupanje sukladno kodeksima ponašanja koji ih obvezuju. Naime, Općom uredbom je predviđena mogućnost izrade kodeksa ponašanja koji su namijenjeni pružanju doprinosa ispravnoj primjeni Opće uredbe, uzimajući u obzir posebna obilježja različitih sektora obrade i posebne potrebe mikro, malih i srednjih poduzeća. To zapravo znači kako udruženja (npr. Hrvatska gospodarska komora) i druga tijela koja predstavljaju kategorije voditelja obrade osobnih podataka mogu izraditi kodekse ponašanja, ili izmijeniti ili proširiti takve kodekse radi preciziranja primjene Opće uredbe, u pogledu[27]:

- poštene i transparetne obrade osobnih podataka;
- legitimnih interesa voditelja obrade u posebnim kontekstima;
- prikupljanja osobnih podataka;
- pseudonimizacije osobnih podataka;
- informiranja javnosti i ispitanika;
- ostvarivanja prava ispitanika;
- informiranja i zaštite djece te načina pribavljanja privole nositelja roditeljske odgovornosti nad djetetom;
- mjera i postupaka iz čl. 24. i 25. Opće uredbe[28] te mjera za osiguravanje sigurnosti obrade iz čl. 32. Opće uredbe[29];
- izvješćivanja nadzornih tijela o povredama osobnih podataka i obavješćivanja ispitanika o takvim povredama;
- prijenosa osobnih podataka trećim zemljama ili međunarodnim organizacijama; ili
- izvansudskih postupaka i drugih postupaka za rješavanje sporova između voditelja obrade i ispitanika s obzirom na obradu, ne dovodeći u pitanje prava ispitanika temeljem čl. 77. i 79. Opće uredbe.

Osim voditelja obrade osobnih podataka koji moraju poštivati odredbe kodeksa ponašanja koji su odobreni sukladno čl. 40. st. 5. Opće uredbe i koji imaju opću valjanost sukladno čl. 40. st. 4. Opće uredbe, kodekse ponašanja moraju poštivati i voditelji obrade osobnih podataka koji ne podliježu ovoj Uredbi temeljem čl. 3. Opće uredbe[30], kako bi osigurali odgovarajuće zaštitne mjere u okviru prijenosa osobnih podataka trećim zemljama, ili međunarodnim organizacijama pod uvjetima iz čl. 46. st. 2. t. (e) Opće uredbe. Takvi voditelji obrade putem ugovornih, ili drugih pravno obvezujućih instrumenata preuzimaju obvezujuće i provedive obveze za primjenu tih odgovarajućih zaštitnih mjera, među ostalim s obzirom na prava ispitanika. Kodeks ponašanja sadržava mehanizme koji tijelu iz čl. 41. st. 1. Opće uredbe[31] omogućuju da provodi obvezno praćenje sukladnosti voditeljâ obrade, ili izvršiteljâ obrade koji su se obvezali na njegovu primjenu, ne dovodeći u pitanje zadaće i ovlasti nadzornih tijela koja su nadležna temeljem čl. 55., ili čl. 56. Opće uredbe.

3.5.1. Praćenje odobrenih kodeksa ponašanja

Sukladno čl. 41. st. 1. Opće uredbe, tijelo s odgovarajućim stupnjem stručnosti za predmet kodeksa i koje je u tu svrhu akreditiralo nadležno nadzorno tijelo, uz primjenu prikladnih zaštitnih mjera, poduzima odgovarajuće radnje u slučajevima u kojima voditelj obrade osobnih podataka, ili izvršitelj obrade krše kodeks, što uključuje suspendiranje, ili isključivanje dotičnog voditelja obrade, ili izvršitelja obrade iz kodeksa. Ono izvješćuje nadležno nadzorno tijelo o takvim radnjama i razlozima za njihovo poduzimanje. Ova odredba se ne primjenjuje na obradu obavljaju tijela javne vlasti i javna tijela.

3.6. Imenovanje službenika za zaštitu osobnih podataka

Voditelj obrade osobnih podataka imenuje službenika za zaštitu podataka u svakom slučaju u kojem[32]:

- obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti;
- osnovne djelatnosti voditelja obrade, ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri,ili
- osnovne djelatnosti voditelja obrade, ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka temeljem čl. 9. i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz čl. 10. Opće uredbe.

Kada se radi o najvećem broju poduzetnika, oni će, kao voditelji obrade osobnih podataka, ili izvršitelji obrade, morati imenovati službenika za zaštitu osobnih podataka kada se osnovne djelatnosti voditelja obrade, ili izvršitelja obrade, sastoje od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri.

ističemo...

Službenik za zaštitu podataka imenuje se temeljem stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz čl. 39. Opće uredbe.

Međutim, ovo ne znači da navedene poslove mogu isključivo obavljati pravnici, ili stručnjaci informacijske tehnologije nego i osobe drugih kvalifikacija koje raspolažu potrebnim stručnim znanjem. Za poslove službenika za zaštitu osobnih podataka, mišljenja smo, može se:

- sklopiti ugovor o radu;
- sklopiti dodatak (aneks) ugovora o radu sa radnikom s kojim voditelj obrade osobnih podataka već ima sklopljen ugovor o radu;
- sklopiti ugovor o djelu sa osobom koja nije u radnom odnosu kod voditelja obrade osobnih podataka.

Član uprave, voditelj pravnog odjela ili odjela informacijske tehnologije, ili direktor odjela ne bi mogao biti službenik za zaštitu osobnih podataka. Naime, službenik za zaštitu osobnih podataka mora biti neovisan u svojem radu. S time u vezi otvara se pitanje angažiranja vanjskog službenika za zaštitu osobnih podataka temeljem ugovora o djelu za poduzetnike koji imaju zaposlenog samo direktora trgovačkog društva, ili kod obrtnika.

Očekuje se da će Agencija u vezi navedenog s vremenom dati odgovarajuće mišljenje. O problematici obavljanja poslova službenika za zaštitu osobnih podataka detaljnije ćemo pisati u jednom od sljedećih brojeva RiPup-a.

27 Čl. 40. st. 2. Opće uredbe.
28 Vidjeti pod 3.1. i 3.1.2.
29 Vidjeti pod 3.2.1.
30 Vidjeti pod 2.1.
31 Vidjeti pod 3.5.1.
32 Čl. 37. st. 1. Opće uredbe.

3.7. Traženje privole od ispitanika

Makar smo o zakonitosti obrade osobnih podataka već pisali u prethodnim člancima o Općoj uredbi[33], budući da se u praksi pokazuje kao nejasno pitanje kada voditelj obrade mora od ispitanika tražiti privolu radi obrade njegovih osobnih podataka, podsjećamo na odredbu čl. 6. Opće uredbe kojim je određeno kada je obrada osobnih podataka zakonita. Obrada osobnih podataka je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno najmanje jedno od sljedećeg:

- ispitanik je dao privolu za obradu svojih osobnih podataka u jednu, ili više posebnih svrha;
- obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- obrada je nužna radi poštovanja 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 temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete, pri čemu se navedeno ne odnosi na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća.

ističemo...

Iz navedenog slijedi kako voditelj obrade mora tražiti privolu ispitanika uvijek kada nije ispunjen niti jedan od drugih navedenih uvjeta za zakonitost obrade osobnih podataka ispitanika.

Primjer: Privola

PRIVOLA

Potpisom ove izjave dajem privolu trgovačkom društvu DDD d.o.o. iz Splita, Nova ulica 10 (u nastavku teksta: voditelj obrade osobnih podataka) da prikuplja moje osobne podatke – telefonski broj 1999-9999 i adresu elektronske pošte nikokoni@bepe.hr (u nastavku teksta: osobni podaci) te da ih obrađuje na način da me na navedeni telefonski broj i adresu elektronske pošte obavještava o svojim izdanjima stručne literature. Navedeni osobni podaci mogu se koristiti samo za navedene svrhe.

Mojim osobnim podacima pristup mogu imati ovlaštene osobe iz odjela marketinga voditelja obrade osobnih podataka samo za svrhu koja je gore navedena. Voditelj obrade osobnih podataka poduzima sve tehničke i organizacijske mjere za zaštitu osobnih podataka. Voditelj obrade osobnih podataka će čuvati moje osobne podatke sve dok postoji pravni temelj za obradu podataka (privola) te će moje osobne podatke predati svojim izvršiteljima obrade koji rade na analizi ekonomske opravdanosti pojedinih stručnih izdanja, a koji mogu obrađivati osobne podatke samo sukladno uputama Voditelja obrade osobnih podataka.

Predmetnu privolu dajem dobrovoljno te njenim potpisom potvrđujem kako sam upoznat da u bilo koje vrijeme mogu povući privolu bez bilo kakvih negativnih posljedica. Također sam upoznat da, sukladno Općoj uredbi o zaštiti podataka, mogu pod određenim uvjetima, koristiti svoja prava da dobijem potvrdu o obradi, izvršiti uvid u svoje osobne podatke, ispraviti ili dopuniti moje osobne podatke, prigovoriti daljnjoj, ili prekomjernoj obradi, blokirati nezakonitu obradu, zatražiti brisanje mojih osobnih podataka te zaprimiti preslik osobnih podataka radi prijenosa drugom voditelju obrade.

Potvrđujem da sam od strane voditelja osobnih podataka upoznat kako sve ostale informacije vezano za obradu mojih osobnih podataka mogu provjeriti u pravilima privatnosti na www.aaa.hr.gov.net te se mogu u pisanom obliku obratiti na adresu Voditelja obrade osobnih podataka: Mala cesta 101, 10000 Zagreb, tel. 1999-9991, aaainfo@pebe.hr. Upoznat sam kako u vezi povrede mojih prava mogu podnijeti pritužbu Agenciji za zaštitu osobnih podataka, Martićeva 14, Zagreb.

DATUM: _____
IME I PREZIME: _____
POTPIS: _____

3.8. Pisani akti koje bi trebao imati voditelj obrade osobnih podataka

U ostvarivanju svojih obveza iz Opće uredbe, voditelj obrade osobnih podataka mora izraditi niz akata koje navodimo u nastavku, u pisanom obliku (uključujući i elektronski oblik):

- procjenu usklađenosti s Općom uredbom;
- dokumentiranu i obrazloženu analiza potrebe angažiranja službenika za zaštitu osobnih podataka;
- ugovor o radu/ugovor o djelu sa službenikom za zaštitu osobnih podataka ako se imenuje;
- interne politike zaštite osobnih podataka (interni akt);
- interne politike tehničke zaštite osobnih podataka;
- dokumentaciju o provedenom obrazovanju (edukaciji) zaposlenika o propisima i internim politikama zaštite osobnih podataka
- procjenu učinka zaštite osobnih podataka sa procjenom rizika za slobode ispitanika koji proizlaze iz obrade njihovih podataka;
- izvješće nadzornom tijelu o povredi osobnih podataka;
- obavijest ispitaniku o povredi osobnih podataka;
- postupke brisanja osobnih podataka;
- privolu za prikupljanje osobnih podataka;
- izjavu o povjerljivosti;
- politiku privatnosti;
- evidencije sukladno Općoj uredbi (o povredi osobnih podataka, o prikupljenim privolama, o brisanim osobnim podacima, aktivnosti obrade voditelja obrade);
- ugovor sa izvršiteljem obrade osobnih podataka;
- korporativna pravila za zaštitu osobnih podataka i dr.

Neki od ovih akata mogu biti po prirodi stvari objedinjeni u jednom, kao što je npr. interni akt o politikama zaštite osobnih podataka, dok će neki po prirodi stvari morati egzistirati u samostalnom obliku.

3.9. Angažiranje izvršitelja obrade osobnih podataka

U praksi će se često događati slučajevi da voditelj obrade osobnih podataka angažira izvršitelja obrade, koji će u njegovo ime obrađivati osobne podatke koje je prikupio voditelj obrade. Kako bi se osiguralo poštivanje zahtjeva iz Opće uredbe u vezi s obradom koju provodi

33 Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)“, RiPup br. 3/18, str. 161.

izvršitelj obrade u ime voditelja obrade, pri povjeravanju aktivnosti obrade izvršitelju obrade, voditelj obrade trebao bi angažirati samo izvršitelje obrade koji u zadovoljavajućoj mjeri jamče, osobito u pogledu stručnog znanja, pouzdanosti i resursa, provedbu tehničkih i organizacijskih mjera koje udovoljavaju zahtjevima iz Opće uredbe, među ostalim u pogledu sigurnosti obrade. Poštivanje odobrenog kodeksa ponašanja, ili mehanizma certificiranja odobrenog od strane izvršitelja obrade može se upotrijebiti kao element u dokazivanju poštivanja obveza voditelja obrade.

Provođenje obrade od strane izvršitelja obrade trebalo bi biti uređeno ugovorom, ili drugim pravnim aktom u skladu s pravom EU, ili pravom države članice koji izvršitelja obrade obvezuje prema voditelju obrade. Sadržaj ugovora određen je u čl. 28. Opće uredbe. Voditelj obrade osobnih podataka i izvršitelj obrade mogu izabrati sklapanje pojedinačnog ugovora, ili standardne ugovorne klauzule koje je izravno donijela Europska komisija (u nastavku teksta: EK), ili ih je donijelo nadzorno tijelo sukladno mehanizmu konzistentnosti, a potom donijela EK.

ističemo...

Ugovor između voditelja obrade osobnih podataka i izvršitelja obrade mora biti sklopljen u pisanom obliku (uključujući i elektronski oblik).

Nakon što završi obradu u ime voditelja obrade, izvršitelj obrade trebao bi, prema izboru voditelja obrade, vratiti, ili izbrisati osobne podatke osim ako postoji obveza pohrane osobnih podataka sukladno pravu EU, ili pravu države članice kojeg primjenjuje izvršitelj obrade.

4. Odgovornost voditelja obrade osobnih podataka za štetu

ističemo...

Voditelj obrade osobnih podataka, kao i izvršitelj obrade, mora nadoknaditi svaku materijalnu i nematerijalnu štetu koju osoba može pretrpjeti zbog obrade osobnih podataka kojom se postupa protivno odredbama Opće uredbe.

Svaki voditelj obrade osobnih podataka koji je uključen u obradu odgovoran je za štetu prouzročenu obradom kojom se krši Opća uredba[34]. Voditelj obrade izuzet je od odgovornosti za naknadu štete prouzročenu obradom osobnih podataka ako dokaže da nije ni na koji način odgovoran za događaj koji je prouzročio štetu.

U slučaju da je u istu obradu uključeno više od jednog voditelja obrade, ili su u istu obradu uključeni i voditelj obrade i izvršitelj obrade i ako su, sukladno navedenim odredbama čl. 82. st. 2. i 3. Opće uredbe, odgovorni za bilo kakvu štetu prouzročenu obradom, svaki voditelj obrade, ili izvršitelj obrade smatra se odgovornim za cjelokupnu štetu kako bi se osigurala učinkovita naknada ispitaniku[35]. Znači, u ovakvim situacijama radi se o solidarnoj odgovornosti za štetu ispitaniku. To znači kako voditelj obrade osobnih podataka, ili izvršitelj obrade, koji je sukladno navedenoj odredbi čl. 82. st. 4. Opće uredbe platio punu odštetu za pretrpljenu štetu, ima pravo zatražiti od drugih voditelja obrade, ili izvršitelja obrade koji su uključeni u istu obradu dio odštete koji odgovara njihovu udjelu u odgovornosti za štetu sukladno uvjetima iz čl. 82. st. 2. Opće uredbe.

Sudski postupak za ostvarivanje prava na naknadu štete vodi se pred sudovima koji su nadležni prema pravu države članice iz čl. 79. st. 2. Opće uredbe, odnosno pred sudovima države članice u kojoj voditelj obrade, ili izvršitelj obrade ima poslovni nastan. Osim toga, takvi se postupci mogu voditi pred sudovima države članice u kojoj ispitanik ima uobičajeno boravište.

5. Upravne novčane kazne i novčane kazne za prekršaj

Općom uredbom, ali i Konačnim prijedlogom Zakona o provedbi Opće uredbe o zaštiti osobnih podataka (u nastavku teksta: Konačni prijedlog Zakona)[36] koji je usvojen na sjednici Vlade RH, predviđene su upravne novčane kazne i novčane kazne za prekršaj za voditelje obrade osobnih podataka koji postupaju protivno odredbama Opće uredbe i Konačnog prijedloga Zakona. Konačni prijedlog Zakona sadrži uglavnom procesne odredbe o izricanju upravnih novčanih kazni, odredbe o zastari i odredbe o iznosima upravnih novčanih kazni za postupanje suprotno njegovim odredbama o video nadzoru. U nastavku dajemo prikaz odredbi Opće uredbe i Konačnog prijedloga Zakona koje se odnose na iznose upravnih novčanih kazni.

5.1. Iznosi upravnih novčanih kazni iz Opće uredbe

U slučaju da voditelj obrade, ili izvršitelj obrade za istu, ili povezane obrade namjerno, ili iz nepažnje prekrše nekoliko odredbi Opće uredbe ukupan iznos novčane kazne ne smije biti veći od administrativnog iznosa utvrđenog za najteže kršenje odredbi Opće uredbe.

ističemo...

Za postupanje voditelja i izvršitelja obrade protivno čl. 8., 11., 25.-39. te 42. i 43. Opće uredbe, sukladno čl. 83. st. 2. Opće uredbe, mogu se izreći upravne novčane kazne u iznosu do 10.000.000,00 EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće[37].

Za kršenja sljedećih odredbi mogu se voditeljima obrade osobnih podataka izreći upravne novčane kazne u iznosu do 20.000.000,00 EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće:

- osnovnih načela za obradu, što uključuje uvjete privole sukladno čl. 5.-6., 7. i 9. Opće uredbe;
- prava ispitanika sukladno čl. 12.-22. Opće uredbe.

5.2. Iznosi upravnih novčanih kazni iz Konačnog prijedloga Zakona

Odredbom čl. 51. Konačnog prijedloga Zakona predviđeno je kako će se upravnom novčanom kaznom u iznosu do 50.000,00 kuna, kazniti:

- voditelj obrade i izvršitelj obrade koji ne označe objekt, prostorije, dijelove prostorije te vanjsku površinu objekta, na način propisan čl. 27. Konačnog prijedloga zakona (radi se o označavanju objekta u kojem se provodi video nadzor);
- voditelj obrade i izvršitelj obrade koji ne uspostave automatizirani sustav zapisa za evidentiranje pristupa snimkama video nadzora, sukladno čl. 28. st. 4. Konačnog prijedloga Zakona;

34 Čl. 82. st. 2. Opće uredbe.
35 Čl. 82. st. 4. Opće uredbe.
36 www.vlada.hr
37 Čl. 83. st. 4. Opće uredbe.

- osobe iz čl. 28. st. 1. Konačnog prijedloga Zakona koje snimke iz sustava video nadzora koriste suprotno čl. 28. st. 2. Konačnog prijedloga Zakona.

6. Zaključak

Voditelji obrade osobnih podataka imaju cijeli niz obveza koje proizlaze iz odredbi Opće uredbe. Dio tih obveza svakako se odnosi i na obvezu izrade pisanih akata, uključujući i elektronski oblik. Nomotehnički voditelji obrade osobnih podataka to mogu rješiti objedinjavanjem nekih pisanih akata u jedinstveni interni akt o zaštiti osobnih podataka.

Međutim, neki pisani akti morat će po prirodi stvari egzistirati zasebno. Moramo spomenuti i usvajanje Konačnog prijedloga Zakona na sjednici VRH i njegovo upućivanje na usvajanje u Hrvatski sabor. Pri tome treba istaknuti kako veći dio primjedbi na njegov tekst istaknut u javnoj raspravi nije usvojen.

Literatura:

1) 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/EZ (SL L 119, 4.5.2016);
2) Prijedlog Zakona o provedbi Opće uredbe o zaštiti osobnih podataka s Konačnim prijedlogom Zakona - www.vlada.hr
3) Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (I. dio)", RiPup br. 3/18, str. 158.
4) Prelević, B., stručni članak „Primjena novih pravila o zaštiti osobnih podataka od 25.5.2018. (II. dio) – prava ispitanika", RiPup br. 4/18, str. 150.

Ne zaboravite:

- **Voditelj obrade osobnih podataka je fizička, ili pravna osoba, tijelo javne vlasti, agencija, ili drugo tijelo koje samo, ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.**
- **Svaki voditelj obrade osobnih podataka koji ima poslovni nastan u EU, kao i voditelj obrade osobnih podataka sa poslovnim nastanom izvan EU koji obrađuje osobne podatke ispitanika u EU mora u takvoj obradi primjenjivati Opću uredbu.**
- **Voditelj obrade osobnih podataka mora izraditi niz akata u pisanom obliku, uključujući i elektronički oblik, kojima dokumentira usklađenost svojih politika zaštite osobnih podataka sa Općom uredbom.**
- **Voditelj obrade osobnih podataka mora u slučaju povrede osobnih podataka, bez nepotrebnog odgađanja te ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi, izvjestiti nadzorno tijelo.**
- **Voditelj obrade osobnih podataka mora nadoknaditi svaku materijalnu i nematerijalnu štetu koju osoba može pretrpjeti zbog obrade osobnih podataka kojom se postupa protivno odredbama Opće uredbe.**
- **Općom uredbom i Konačnim prijedlogom Zakona predviđen je iznimno visok raspon novčanih kazni za postupanje voditelja obrade osobnih podataka suprotno njihovim odredbama.**

Bilješke