VODIČ KROZ OPĆU UREDBU O ZAŠTITI PODATAKA

ŠTO JE OPĆA UREDBA O ZAŠTITI PODATAKA ILI GDPR?

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 - Opća uredba o zaštiti podataka - GDPR izravno će se primjenjivati u Republici Hrvatskoj od 25. svibnja 2018. godine. Ista predstavlja bitan napredak u području zaštite osobnih podataka.

Tehnološkim razvojem i novim načinima obrade osobnih podataka, postalo je nužno donošenje novog instrumenta koji će osigurati zaštitu prava i temeljnih sloboda pojedinaca u vezi s obradom njihovih osobnih podataka. Također, Općom uredbom se osigurava ujednačeno i jednoobrazno postupanje nadzornih tijela za zaštitu osobnih podataka, što će imati za posljedicu jednostavniju i jednaku zaštitu prava svih pojedinaca u Europskoj uniji.
Općom uredbom o zaštiti podataka uvode se nove i pojednostavljuju se neke već postojeće definicije, određuju biometrijski i genetski podaci, preciznije opisuju postojeći pojmovi, jačaju prava ispitanika te se smanjuju i pojednostavljuju pojedine administrativne obveze voditelja zbirke osobnih podataka, jačaju nadzorne ovlasti te mogućnost izricanja kazni od strane tijela za zaštitu osobnih podataka.
Uz navedenu Opću uredbu, sastavni dio usvojenog zakonodavnog paketa je i Direktiva o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka. Tom će se Direktivom ujednačiti zaštita osobnih podataka koje obrađuju pravosudna i policijska tijela u državama članicama Europske unije. Ista jasno definira mogućnosti obrade osobnih podataka ispitanika, uključujući njihovo iznošenje u treće zemlje, pri čemu se osiguravaju visoki standardi zaštite pojedinaca razmjerno s potrebama provedbe odgovarajućih policijskih i pravosudnih postupaka. Ovom Direktivom jasno se određuje nadzor neovisnog tijela za zaštitu osobnih podataka nad obradom istih.

Uredba određuje koja su prava pojedinaca, a u skladu s tim i koje su obveze subjekata koji obrađuju osobne podatke poput voditelja obrade odnosno izvršitelja obrade. Uredba također propisuje koje su zadaće i ovlasti Agencije, a možemo reći da su to savjetodavne, istražne i korektivne ovlasti. Kada govorimo o tvrtkama može se reći da se Uredba primjenjuje na sve tvrtke i da tu nema iznimaka, a također se primjenjuje i na pojedince koji obavljaju određenu profesionalnu aktivnost, udruge, bolnice, klubove, pa i na fizičke osobe kada obrađuju osobne podatke izvan okvira potreba kućanstva (npr. postavljanje video nadzora ispred ulaznih vrata kuće/stana). Uredba se primjenjuje na sve državne institucije koje su dužne obrađivati osobne podatke u okviru njenih odredaba, osim u slučajevima kaznenopravnih aktivnosti, poput sprečavanja kaznenih djela ili progona počinitelja istih te u područjima izvan nadležnosti prava EU-a.

AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA – NADZORNO TIJELO

U skladu s važećim zakonodavstvom Europske unije svaka država članica mora uspostaviti neovisno nadzorno tijelo zaduženo za praćenje provedbe propisa o zaštititi podataka, a istu takvu obvezu propisuje i Opća uredba o zaštiti podataka. U Republici Hrvatskoj kao nadzorno tijelo uspostavljena je Agencija za zaštitu osobnih podataka.

Među ostalim zadaćama, nadzorno tijelo

• prati i provodi primjenu Uredbe;

• promiče javnu svijest o pravilima, rizicima, zaštitnim mjerama, i pravima u vezi s obradom te njihovo razumijevanje te također promiče osviještenost voditelja obrade i izvršitelja obrade o njihovim obvezama;

• savjetuje parlament, vladu i druga tijela o zakonodavnim i administrativnim mjerama u vezi s obradom podataka;

• rješava i istražuje pritužbe te podnositelja pritužbe izvješćuje o napretku i ishodu istrage;

• surađuje s nadzornim tijelima drugih država članica EU-a s ciljem osiguranja konzistentnosti primjene i provedbe Opće uredbe o zaštiti podataka te sudjeluje u radu Europskog odbora za zaštitu podataka;

• prati bitne razvoje u onoj mjeri u kojoj utječu na zaštitu osobnih podataka, osobito razvoj informacijskih i komunikacijskih tehnologija te komercijalnih praksi.

Nadzorno tijelo prilikom obavljanja zadaća ima sljedeće ovlasti

• izdati upozorenja i službene opomene voditelju obrade ili izvršitelju obrade;

• naložiti voditelju obrade ili izvršitelju obrade da poštuje zahtjeve ispitanika za ostvarivanje njegovih prava i da postupke obrade uskladi s odredbama Opće uredbe o zaštiti podataka;

• privremeno ili konačno ograničavati te zabraniti obradu podataka, pa i iznošenje podataka u treće zemlje;

• u skladu s nacionalnim pravom, izreći upravnu novčanu kaznu

ŠTO JE SVE OSOBNI PODATAK U SMISLU OPĆE UREDBE?

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi. Pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, 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, jako je širok spektar što su osobni podaci, no jednostavnije rečeno to su: ime i prezime, identifikacijski broj, slika, glas, adresa, broj telefona, IP adresa, povijest bolesti, popis najdraže literature ili pjesama, ako takvi podaci mogu dovesti do izravnog ili neizravnog identificiranja pojedinca. Ističemo da i prije prikupljanja osobnih podataka subjekt koji ih prikuplja ima obvezu pružanja informacija u koju svrhu se podaci prikupljaju, na temelju koje pravne osnove, komu se podaci otkrivaju te o pravu pojedinca da svojim podacima pristupi, da zahtijeva njihov ispravak ili eventualno brisanje.

POJEDINI POJMOVI IZ OPĆE UREDBE? (4)

"pseudonimizacija" znači obrada 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 utvrdit

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

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

"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

ŠTO JE OBRADA OSOBNIH PODATAKA?

Obrada obuhvaća radnje poput prikupljanja, bilježenja, čuvanja, uvida, otkrivanja, prenošenja ili uništavanja. Tako primjerice možemo navesti da će Opća uredba o zaštiti podataka obuhvatiti obradu podataka zaposlenika, potrošača i klijenata, građana od strane državne administracije, pacijenata, učenika, studenata, članova udruga, korisnika društvenih mreža i svaku drugu obradu osobnih podataka koja nije u okviru gore navedenih iznimki. Također, novim ili jačim pravilima bit će obuhvaćene one djelatnosti koje se bave obradom osobnih podataka visokog rizika za koje će biti potrebno provesti procjenu učinka. To su obrade koje se odnose na sustavnu i opsežnu procjenu osobnih aspekata pojedinaca automatiziranim putem, opsežnu obradu posebnih kategorija podataka ili podataka o kaznenim osudama ili kažnjivim djelima te sustavno praćenje javno dostupnog područja u velikoj mjeri.

KOJA SU NAČELA OBRADE? (5)

• zakonitost, poštenost i transparentnost obrade: to znači da obrada treba biti u skladu s određenim pravnim temeljem, a načelima poštene i transparentne obrade zahtijeva se da je pojedinac informiran o postupku obrade i njegovim svrhama, te voditelj obrade je obvezan ispitaniku pružiti sve dodatne informacije neophodne za osiguravanje poštene i transparentne obrade uzimajući u obzir posebne okolnosti i kontekst obrade osobnih podataka, a osim toga ispitanik bi trebao biti informiran o postupku izrade profila i posljedicama takve izrade profila;
• ograničavanje svrhe: to znači da podaci trebaju biti prikupljeni u posebne, izričite i zakonite

svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama; ali je moguća daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe;
• smanjenje količine podataka: to znači da podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju;
• točnost: to znači da podaci moraju biti točni i prema potrebi ažurni; mora se 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;
• ograničenje pohrane: to znači da podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju; na dulja razdoblja čuvanja su moguća samo ako će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe uz provedbu primjerenih mjera zaštite propisanih Uredbom;
• cjelovitost i povjerljivost: to znači da podaci moraju biti obrađivani na način kojim se osigurava odgovarajuća razina sigurnosti, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja;
• pouzdanost: to znači da je voditelj obrade odgovoran za poštivanje načela i da je teret dokaza na njemu.

PRAVNI TEMELJ OBRADE? (6)

Za zakonitu obradu osobnih podataka potrebno je ispuniti barem jedno od narednih pravnih temelja:

(a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha - privola je dobrovoljno, posebno, informirano i nedvosmisleno izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose, Uredbom se među ostalim utvrđuje da uvjet dobrovoljnosti nije ispunjen ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica (npr. privola se daje radi uvrštenja potrošača u neki program vjernosti, dok je u velikoj većini radnopravnih odnosa nemoguće koristiti privolu kao pravnih temelj za obradu podataka radnika);

(b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora (npr. obrada podataka tražitelja posla radi pozivanja na testiranje, obrada podataka osiguranika radi izvršenja ugovora o osiguranju ili obrada podataka radnika na poslovima održavanja instalacija radi slanja na teren);

(c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade (npr. slanje podataka o radnicima HZZO-u ili HZMO-u ili slanje podataka stranaka od strane javnog bilježnika Poreznoj upravi sukladno posebnim propisima);

(d) obrada je nužna kako bi se zaštitili ključni interesi ispitanika ili druge fizičke osobe (npr. otkrivanje od strane nadležnih tijela podataka jednog roditelja drugomu radi uzdržavanja djeteta);

(e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade (npr. zbog službene ovlasti Državnog zavoda za statistiku pojedini voditelji obrade su dužni tom zavodu dostavljati određene osobne podatke);

(f) 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, s time da se ova točka ne odnosi na obradu koju provode tijela javne vlasti pri izvršavanju svojih zadaća (npr. legitimni interes vlasnika nekretnine da postavi sustav video nazora da bi spriječio realan rizik po njegovoj imovini).

UTJECAJ OPĆE UREDBE NA GRAĐANE/ISPITANIKE? (Poglavlje 3)
Opća Uredba o zaštiti podataka pojašnjava i uvodi određena nova prava za ispitanike te osigurava, osim u iznimnim situacijama, jednaku razinu zaštite svakom pojedincu iz Europske unije, bez obzira na državu članicu nadležnu za postupanje u konkretnom slučaju.
Voditelj obrade dužan je poduzeti odgovarajuće mjere kako bi se ispitaniku pružile sve informacije o aspektima obrade osobnih podataka te o pravima ispitanika na pristup svojim podacima, brisanje podataka, ograničenje obrade, prenosivost podataka, upućivanje prigovora te u vezi s automatiziranim pojedinačnim donošenjem odluka (što uključuje profiliranje).

Navedene informacije trebaju se pružiti u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu. Također, ako ispitanik uputi određeni zahtjev voditelju obrade za ostvarivanje svojih prava iz Opće uredbe o zaštiti podataka, a voditelj obrade ne postupi po tom zahtjevu, tada voditelj obrade bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvješćuje ispitanika o razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženja pravnog lijeka.

POJEDINA PRAVA GRAĐANA/ISPITANIKA:
• **transparentnost** (12 - 14): pružanje informacija prilikom prikupljanja osobnih podatak kada voditelj obrade mora među ostalim informacijama obavijestiti ispitanika i o svojem identitetu i kontakt podacima, svrhama obrade i pravnoj osnovi za obradu podataka, primateljima, iznošenju u treće zemlje, razdoblju pohrane, mogućnosti povlačenja privole, itd.;
• **pristup podacima** (15): dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacije, među ostalim, o obrađenim osobnim podacima, o svrsi obrade, roku pohrane, iznošenju u treće

zemlje itd.;

• **pravo na ispravak** (16): ispitanik ima pravo zahtijevati ispravak netočnih osobnih podataka koji se na njega odnose, a uzimajući u obzir svrhe obrade, ispitanik ima pravo dopuniti nepotpune osobne podatke, među ostalim i davanjem dodatne izjave;

• **brisanje („pravo na zaborav“)** (17): ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako, među ostalim, osobni podaci više nisu nužni u odnosu na svrhu obrade, ispitanik je povukao privolu za obradu, osobni podaci su nezakonito obrađeni itd., ovo pravo ima ograničenja pa tako na primjer političar ne može zatražiti brisanje informacija o sebi koje su dane u okviru svojega političkog djelovanja;

• pravo na ograničenje obrade (18): u pojedinim situacijama (na primjer kada je točnost podataka osporavana ili kada pravo na brisanju ispitanik želi da voditelj obrade zadrži njegove podatke) ispitanik ima pravo zahtijevati da se obrada ograniči uz iznimku pohrane i nekih drugih vrsta obrade;

• **pravo na prenosivost** (20): ispitanik ima pravo zaprimiti svoje osobne podatke, a koje je prethodno pružio voditelju obrade, u strukturiranom obliku te u uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi, ako se obrada provodi automatiziranim putem i temelji na privoli ili ugovoru;

• **pravo na prigovor** (21): ispitanik ima pravo uložiti prigovor na obradu osobnih podataka ako se ista temelji na zadaće od javnog interesa, na izvršavanje službenih ovlasti voditelja obrade ili na legitimne interesa voditelja obrade (uključujući i profiliranje), tada voditelj obrade ne smoje 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 usprotiviti se donošenju automatiziranih pojedinačnih odluka (profiliranje)** (22): ispitanik ima pravo da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući izradu profila, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega 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 koji se propisuju odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika ili temeljena na izričitoj privoli ispitanika.

POSTOJE LI KRITERIJI ZA OGRANIČENJE PRAVA GRAĐANA/ISPITANIKA? (23)

Zaštita osobnih podataka nije apsolutno pravo već pravo koje se treba balansirati s drugim pravima. Stoga, Opća uredba o zaštiti podataka pruža mehanizam za uvažavanje i balansiranje između prava na zaštitu podataka i drugih prava.

Na taj način, na temelju prava EU-a ili nacionalnog prava voditelj ili izvršitelj obrade mogu ograničiti opseg prava ispitanika ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda

te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu značajnih vrijednosti poput nacionalne sigurnosti, obrane, javne sigurnosti, drugih važnih ciljeva od općeg javnog interesa EU-a ili države članice, zaštite neovisnosti pravosuđa itd.

Svaka takva zakonodavna mjera sadrži posebne odredbe o svrhama obrade ili kategorijama obrade, kategorijama osobnih podataka, opsegu uvedenih ograničenja, zaštitnim mjerama za sprečavanje zlouporabe i drugim aspektima kako bi se zaštitila prava pojedinaca.

KOJE SU OBVEZE VODITELJA I IZVRŠITELJA OBRADE?

Obveze voditelja (24)

• Voditelj obrade mora, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade te njezinu rizičnost, poduzeti odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s Općom uredbom o zaštiti podataka.

Tehnička i integrirana zaštita podataka (Data protection by design and by default) (25)

• Također, uzimajući u obzir okolnosti konkretne situacije, voditelj obrade mora u vrijeme određivanja sredstava obrade i u vrijeme same obrade provoditi odgovarajuće tehničke i organizacijske mjere, poput pseudonimizacije, za omogućavanje učinkovite primjene načela zaštite podataka.

• Voditelj obrade je ujedno dužan provoditi odgovarajuće tehničke i organizacijske mjere kojima se osigurava da integriranim načinom budu obrađeni samo osobni podaci koji su nužni za svaku posebnu svrhu obrade.

Izvršitelj obrade (28)

• Ako voditelj obrade angažira izvršitelja obrade, tada izvršitelj obrade provodi obradu u ime voditelja obrade. Pri tomu, voditelj obrade može angažirati jedino izvršitelje obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu s Općom uredbom o zaštiti podataka. Izvršitelj obrade ne smije angažirati drugog izvršitelja obrade bez prethodnog posebnog ili općeg pisanog odobrenja voditelja obrade.

• Obrada koju provodi izvršitelj obrade uređuje se pravnim aktom, kojim se izvršitelja obrade obvezuje prema voditelju obrade, te se u njemu moraju navesti predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade. Tim se pravnim aktom osobito određuje da izvršitelj obrade mora među ostalim postupati prema uputama voditelja obrade, da fizičke osobe koje obrađuju osobne podatke su dužne čuvati povjerljivost istih, da će postupiti u skladu s odredbama Opće uredbe o zaštiti podataka koje se odnose na sigurnost obrade, itd.

Evidencije o aktivnostima obrade (30)

• Prema trenutno važećem hrvatskom zakonodavstvu, osim u iznimnim slučajevima, voditelj obrade je dužan Agenciji za zaštitu osobnih podataka dostaviti evidenciju o zbirkama osobnih podataka. Navedena obveza je administrativni teret koji nestaje stupanjem na snagu Opće

uredbe o zaštiti podataka.

• Opća uredba o zaštiti podataka propisuje obvezu voditelja obrade koji (1) zapošljava više od 250 radnika ili (2) voditelja obrade čija obrada predstavlja vjerojatan rizik za prava i slobode ispitanika (ali samo u slučaju ako obrada nije povremena) te (3) voditelja obrade koji obrađuje posebne kategorije osobnih podataka ili podataka o kaznenim djelima ili osudama, da vodi i da nadzornom tijelu na zahtjev preda evidenciju o aktivnostima obrade koja sadržava sve bitne elemente obrade, poput identiteta voditelja s kontakt podacima, svrhu obrade, opis ispitanika i osobnih podataka, primatelje podataka, prijenose podataka u treće zemlje, predviđene rokove čuvanja podataka, itd.

Sigurnost obrade (32)

• Uzimajući u obzir okolnosti konkretnog slučaja, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi: (1) pseudonimizaciju i enkripciju osobnih podataka, (2) osiguravanje trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade, (3) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta te (4) redovno testiranje tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Izvješćivanje o povredi osobnih podataka (data breach) (33 i 34)

• Ako je vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode ispitanika, voditelj obrade mora izvijestiti bez odgađanja nadzorno tijelo o povredi osobnih podataka (najkasnije u roku od 72 sata od saznanja o povredi). Navedeno izvješćivanje treba sadržati opis povrede uz informacije o ispitanicima i osobnim podacima, opis vjerojatnih posljedica povrede, opis mjera koje su poduzete ili predložene za rješavanje povrede te kontakt točku voditelja.

• Također, u ako je vjerojatno da će povreda prouzročiti visok rizik za prava i slobode ispitanika, voditelj obrade je dužan informirati ispitanike o povredi osobnih podataka koristeći se jasnim i jednostavnim jezikom. Iznimno, neće biti potrebno ako je voditelj obrade primijenio zaštitne mjere (npr. enkripciju) kojima je spriječio korištenje povrijeđenih osobnih podataka, poduzeo naknadne mjere zaštite zbog kojih nije vjerojatan visok rizik ili ako je kontaktiranje svakog ispitanika predstavljalo nerazmjeran napor, pri čemu je onda nužno ispitanike obavijestiti sredstvima javnog priopćavanja ili na drugi djelotvoran način.

Procjena učinka (Data protection impact assessment) i prethodno savjetovanje (35 i 36)

• Opća uredba o zaštiti podataka polazi od rizičnosti i na temelju iste propisuje različite obveze za voditelja i izvršitelja obrade. Tako da ako je vjerojatno da će neka vrsta obrade prouzročiti visok rizik za prava i slobode ispitanika, tada je voditelj obrade dužan provesti procjenu učinka. Provođenje procjene učinka je nužno ako se sustavno i opsežno procjenjuju osobni aspekti pojedinaca temeljem automatizirane obrade (profiliranje), ako se opsežno obrađuju posebne kategorije osobnih podataka ili podaci kaznenim djelima ili osudama (tu ne spada obrada doznaka o bolovanju od strane poslodavaca ili rad liječnika ili odvjetnika pojedinaca) te ako se

sustavno prati javno dostupno područje u velikoj mjeri (npr. video nadzor ulica).
• Procjena učinka treba sadržavati opis postupaka obrade i njezine svrhe, procjenu nužnosti i proporcionalnosti, procjenu rizičnosti te opis mjera kojima se umanjuje rizičnost obrade.
• Ako se procjenom učinka na zaštitu podataka pokazalo da bi, u slučaju da voditelj obrade ne donese mjere za ublažavanje rizika, obrada dovela do visokog rizika, tada je voditelj obrade dužan kontaktirati nadzorno tijelo i dostaviti mu među ostalima informacije o svrsi i sredstvima obrade, zaštitnim mjerama, provedenoj procjeni učinka itd.

Službenik za zaštitu osobnih podataka (37)

• Za razliku od trenutno važećeg hrvatskog zakonodavstva, Opća uredba o zaštiti podataka ima pristup kojim se želi poboljšati efektivnost zaštite podataka na način da se posebno nadziru rizične obrade. Važna karika u tom segmentu je službenik za zaštitu osobnih podataka koji će voditelj obrade i izvršitelj obrade morati imenovati kada (1) obradu provodi tijelo javne vlasti ili javno tijelo, (2) osnovna djelatnost se sastoji od postupaka obrade koji iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri te (3) osnovna djelatnost sastoji se od opsežne obrade posebnih kategorija osobnih podataka ili podataka o kažnjivim djelima.
• Grupa poduzetnika može imenovati zajedničkog službenika pod uvjetom da je lako dostupan iz svakog poslovnog nastana, a to uključuje i službenika za zaštitu podataka iz druge države članice EU-a uz posebne uvjete kao što su poznavanje jezika ispitanika. Imenovanje mora biti temeljeno na stručnim kvalifikacijama, osobito stručnog znanja o pravu i praksi iz područja zaštite osobnih podataka te sposobnostima izvršavanja zadaća.
• Službenik ne mora biti zaposlenik voditelja ili izvršitelja obrade, dovoljno je da bude angažiran na temelju ugovora o djelu. Službenik za zaštitu podataka ne smije biti u sukobu interesa (npr. biti zadužen za nadzor IT sustava i s druge strane biti službenik za zaštitu podataka)
• Službenik za zaštitu podataka među ostalim mora informirati i savjetovati voditelja ili izvršitelja obrade o obvezama iz područja zaštite podataka, pratiti poštivanje propisa o zaštiti podataka, sudjelovati u procjeni učinka i prethodnom savjetovanju te surađivati s nadzornim tijelom.

Kodeksi ponašanja (40 i 41)

• Udruženja i druga tijela koja predstavljaju kategorije voditelja obrade ili izvršitelja obrade mogu izraditi kodekse ponašanja radi preciziranja primjene Opće uredbe o zaštiti podataka, uzimajući u obzir posebna obilježja različitih sektora obrade i posebne potrebe mikro, malih i srednjih poduzeća. U tom smislu kodeksima ponašanja može se precizirati primjena Opće uredbe o zaštiti podataka po pitanju poštenosti i transparentnosti obrade, legitimnih interesa voditelj obrade u posebnim kontekstima, prikupljanja osobnih podataka, pseudonimizacije osobnih podataka, informiranja javnosti i ispitanika, ostvarivanja prava ispitanika itd.
• Ako su zadovoljeni posebni uvjeti kodeksi ponašanja mogu se koristiti i kao instrument za iznošenje osobnih podataka u treće zemlje.
• Postupak odobravanja kodeksa ponašanja provodi se pred nadzornim tijelom.
• Postupanje prema kodeksu ponašanja podliježe posebnom nadzoru za što može biti

akreditirano posebno tijelo s odgovarajućim kvalifikacijama sukladno odredbama Opće uredbe o zaštiti podataka.

Certificiranje (42 i 43)

• Za razliku od kodeksa ponašanja koja se odnose na određenu kategoriju voditelja obrade ili izvršitelja obrade, certificiranje se odnosi na pojedinog voditelja ili izvršitelja.

• Svrha certificiranja je dokazivanje da su postupci obrade koje provode voditelj obrade i izvršitelj obrade u skladu s Općom uredbom o zaštiti podataka.

• Ako su zadovoljeni posebni uvjeti kodeksi ponašanja mogu se koristiti i kao instrument za iznošenje osobnih podataka u treće zemlje.

• Radi certificiranja voditelj obrade ili izvršitelj obrade kontaktiraju certifikacijska tijela koja su ujedno akreditirana od strane nadležne institucije (nadzorno tijelo i/ili akreditacijsko tijelo ovisno o propisima države članice EU-a).

• Certifikacijska tijela mogu dobiti akreditaciju ako su, među ostalim, nadzornom tijelu zadovoljavajuće dokazala svoju neovisnost i stručnost u predmetu certificiranja, ako su se obvezala poštovati kriterije nadzornog tijela, ako su uspostavila postupke izdavanja, preispitivanja i povlačenja certifikata itd.

O PRIJENOSU OSOBNIH PODATAKA U TREĆE ZEMLJE!

Osobni podaci mogu se prenositi iz Europske unije u treću državu jedino u skladu s odredbama Opće uredbe o zaštiti podataka.

Osobni podaci mogu se prenositi u treće zemlje za koje je izdana odluka o primjerenosti (prijenosi na temelju odluke o primjerenosti). Odluku o primjerenosti izdaje Europska komisija nakon savjetovanja s državama članicama EU-a, a temelji se na ocjeni vladavine prava, poštivanju ljudskih prava, relevantnom zakonodavstvu, postojanju neovisnog nadzornog tijela te međunarodnim obvezama treće države. Europska komisija sastavlja i javno objavljuje popis trećih koje pružaju primjerenu razinu zaštite osobnih podataka i u koje se osobni podaci mogu iznositi bez daljnjih ograničenja.

U određenim slučajevima postoji potreba iznošenja osobnih podataka u treće države koje ne pružaju primjerenu razinu zaštite, tada je potrebno dodatnim zaštitnim mjerama osigurati visoku razinu zaštite osobnih podataka. Instrumenti na temelju kojih je moguće iznositi osobne podatke u takve treće zemlje taksativno su navedeni u Općoj uredbi o zaštiti podataka, a ti instrumenti su pravno obvezujući instrumenti između javnih tijela, obvezujuća korporativna pravila, standardne ugovorne klauzule, kodeksi ponašanja, odobreni mehanizam certificiranja, ugovorne klauzule te odredbe iz administrativnih dogovora. Opća uredba o zaštiti podataka detaljno propisuje visoke standarde koje moraju zadovoljiti ovakvi instrumenti kako bi se osigurala jednakovrijedna zaštita osobnih podataka i u trećim državama.

Iznimno, u posebnim situacijama i ako prijenosi podataka nisu redovitog tipa, moguće je prenositi osobne podatke u treće države uz privolu ispitanika ako je bio prethodno obaviješten o rizicima

prijenosa, ako je prijenos nužan za sklapanje ili izvršenje ugovora sklopljenog s ispitanikom ili u njegovom interesu, ako je prijenos nužan iz važnih razloga javnog interesa ili za pravne zahtjeve, ako je nužan za zaštitu ključnih interesa ispitanika a on ne može dati svoju privolu, te ako se prijenos obavlja iz registra javnih tijela sukladno posebnim propisima.

U KOJE SVRHE KOMPANIJE NAJČEŠĆE KORISTE OSOBNE PODATKE? (44 - 49)
Tvrtke koriste osobne podatke kako bi maksimizirale svoj profit, jer je to i glavni cilj svih gospodarskih subjekata. U prvom redu možemo reći da je tu logična potreba vezana uz isporuku određene robe/usluge da se raspolaže kontaktom kupca, kao što je e-mail, telefon ili adresa. Ovdje je također potreba tvrtki da kontinuirano nude svoje proizvode postojećim, ali i novim potencijalnim kupcima pa obrađuju osobne podatke u marketinške svrhe, a u tom slučaju pojedinci uvijek mogu zahtijevati od tvrtke prestanak takve obrade osobnih podataka. Nadalje, ponekad tvrtke obrađuju osobne podatke na način da prikupljanjem više podataka prate ponašanje i kupovne navike pojedinaca i tako prilagode svoje poslovne aktivnosti potrebama tržišta. Pored navedenog tvrtke obrađuju osobne podatke svojih zaposlenika, što je uređeno i propisima o radu kao posebnim propisima, ali i dobavljača ako su oni fizičke osobe.

KAKO ĆE SE SANKCIONIRATI POVREDE OPĆE UREDBE O ZAŠTITI PODATAKA? (83)
Opća uredba o zaštiti podataka razlikuje se od trenutno važećeg hrvatskog zakonodavstva i po priželjkivanoj efektivnosti sankcioniranja povreda. Prema odredbama Opće uredbe o zaštiti podataka svaka povreda će se sankcionirati novčanim upravnim kaznama koje će se izricati uz ili umjesto drugih sankcija poput upozorenja, opomena, zabrana, ograničenja, itd. Iznimno, ako je riječ o manjoj povredi fizičke osobe i ako bi upravna novčana kazna bila nerazmjerna, ista se neće izricati nego će se izreći upozorenje.
Najprije će se utvrditi postoji li kršenje, a zatim će se odabrati sankcija uključujući novčane upravne kazne.

Postoje dva seta kršenja , za neka kršenja (obveze voditelja i izvršitelja obrade te certifikacijskog tijela i tijela za praćenje kodeksa ponašanja) propisana je maksimalna kazna u iznosu od 10 milijuna eura ili 2% godišnjeg prometa na svjetskoj razini, a za druga kršenja (načela obrade, prava ispitanika, prijenosi u treće države, obveze u skladu s nacionalnim pravom, nepoštovanja naredbe ili pravo pristupa nadzornog tijela) propisana je maksimalna kazna do 20 milijuna eura ili 4% godišnjeg prometa na svjetskoj razini, ovisno o tomu što je veće.

Prilikom izricanja novčanih upravnih kazni vodit će se računa da je takva sankcija učinkovita, razmjerna i odvraćajuća, a za određivanje iznosa konkretne novčane upravne kazne morat će se uzeti u obzir jedanaest kriterija poput prirode, težine i trajanje kršenja, vrstu krivnje, mjere ublažavanja štete, prijašnja kršenja, tehničke i organizacijske mjere primijenjene u obradi podataka, itd.

NACIONALNO ZAKONODAVSTVO

Što se tiče nacionalnog zakonodavstva o zaštiti osobnih podataka, obveza je Hrvatske i svake druge države članice da zakonom uredi sljedeća pitanja:

• osnivanje nadzornog tijela; (u Republici Hrvatskoj je to AZOP-osnovan 2004.godine)
• kvalifikacije i uvjete prihvatljivosti potrebne za imenovanje čelnika nadzornog tijela;
• pravila i postupke za imenovanje čelnika nadzornog tijela;
• trajanje mandata čelnika nadzornog tijela ne kraćeg od četiri godine (osim za prvo imenovanje nakon 24. svibnja 2016.);
• postoji li mogućnost reizbora i, ako da, na koliko mandata;
• uvjete kojima se uređuju obveze čelnika nadzornog tijela i osoblja istoga, zabrane djelovanja, poslova i pogodnosti koji nisu u skladu u tijeku i nakon mandata te pravila kojima se uređuje prestanak radnog odnosa.

UTJECAJ OPĆE UREDBE NA NADZORNA TIJELA

S obzirom na to da se odredbe Uredbe izravno primjenjuju, nije dopušteno u nacionalno zakonodavstvo prepisati ili parafrazirati odredbe Uredbe. Iako je zadaća Republike Hrvatske da svojim Zakonom o zaštiti osobnih podataka propiše gore navedena pitanja, države članice također imaju određeni manevarski prostor kod uređivanja pojedinih drugih pitanja poput viših standarda zaštite u odnosu na genetske, biometrijske i zdravstvene podatke ili kod privole djeteta u odnosu na usluge informacijskog društva.

U odnosu na zadaće, Uredba propisuje da nadzorno tijelo (57)**:**

• prati i provodi primjenu Uredbe;
• promiče javnu svijest o pravilima, rizicima, zaštitnim mjerama, i pravima u vezi s obradom te njihovo razumijevanje te također promiče osviještenost voditelja obrade i izvršitelja obrade o njihovim obvezama;
• u skladu s pravom države članice, savjetuje parlament, vladu i druga tijela o zakonodavnim i administrativnim mjerama u vezi s obradom podataka;
• na zahtjev pruža informacije bilo kojem ispitaniku u vezi s ostvarivanjem njihovih prava iz Uredbe, a prema potrebi, u tu svrhu surađuje s nadzornim tijelima u drugim državama članicama;
• rješava i istražuje pritužbe te podnositelja pritužbe izvješćuje o napretku i ishodu istrage;
• surađuje s nadzornim tijelima drugih država članica s ciljem osiguranja konzistentnosti primjene i provedbe Uredbe;
• prati bitne razvoje u onoj mjeri u kojoj utječu na zaštitu osobnih podataka, osobito razvoj informacijskih i komunikacijskih tehnologija te komercijalnih praksi;
• utvrđuje i vodi popis u vezi s uvjetima za procjenu učinka na zaštitu podataka te daje savjete u postupku prethodnog savjetovanja;
• sudjeluje u radu Europskog odbora za zaštitu podataka;
• vodi internu evidenciju o kršenjima Uredbe i poduzetim korektivnim mjerama.

U odnosu na prisilne mjere, Agencija će među ostalim prema Uredbi imati sljedeće ovlasti (58):

• izdati upozorenja i službene opomene voditelju obrade ili izvršitelju obrade;

• naložiti voditelju obrade ili izvršitelju obrade da poštuje zahtjeve ispitanika za ostvarivanje njegovih prava i da postupke obrade uskladi s odredbama ove Uredbe;

• privremeno ili konačno ograničavati te zabraniti obradu podataka;

• narediti suspenziju protoka podataka primatelju u trećoj zemlji ili međunarodnoj organizaciji;

• izreći upravnu novčanu kaznu (upravne novčane kazne u iznosu su do 20 000 000 EUR, ili u slučaju poduzetnika do 4%ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće)

Također, Republika Hrvatska kao i ostale zemlje članice Europske unije, a posebno tijela nadležna za nadzor nad obradom osobnih podataka u okviru nove Opće uredbe o zaštiti podataka čija puna primjena započinje 25. svibnja 2018. godine, dobivaju nove ovlasti i veće odgovornosti. Iz tog razloga, sve države članice imaju obveze (52).

• osigurati da svako nadzorno tijelo ima ljudske, tehničke i financijske resurse, prostorije i infrastrukturu potrebne za djelotvorno obavljanje svojih zadaća i izvršavanje svojih ovlasti, uključujući one koje treba izvršavati u kontekstu uzajamne pomoći, suradnje i sudjelovanja u Odboru.

• osigurati da svako nadzorno tijelo odabire i ima vlastito osoblje kojim isključivo rukovodi član ili članovi predmetnog nadzornog tijela.

• osigurati da svako nadzorno tijelo podliježe financijskoj kontroli koja ne utječe na njegovu neovisnost i da ima zasebne, javne, godišnje proračune koji mogu biti dio cjelokupnog državnog ili nacionalnog proračuna

EUROPSKI ODBOR ZA ZAŠTITU PODATAKA (68 - 70)

Europski odbor za zaštitu podataka je novo tijelo Europske unije koji se sastoji čelnika nadzornih tijela svake države članice i Europskog nadzornika za zaštitu podataka. Zadaća Europskog odbora za zaštitu podataka je osiguravanje dosljedne primjene Opće uredbe o zaštiti podataka u cijeloj Europskoj uniji, što uključuje rješavanje povodom sporova između nadzornih tijela različitih država članica EU-a te izdavanje preporuka, smjernica i primjera najbolje prakse u vezi s područjem primjene Opće uredbe o zaštiti podataka. Pojedine odluke Europskog odbora za zaštitu podataka mogu biti pravno obvezujuće.

Preuzeto s: http://azop.hr/info-servis/detaljnije/vodic-kroz-opcu-uredbu-o-zastiti-podataka