GDPR

Usklađivanje s uredbom

KONTO d.o.o. Požega

Sadržaj

1. UVOD – ŠTO JE GDPR

GDPR (General Data Protection Regulation) je uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

Pojednostavljeno rečeno, GDPR je uredba koja brine o zaštiti prava pojedinaca (fizičkih osoba) na teritoriju EU. Ovo naročito dolazi do izražaja u digitalnom svijetu i na Internetu, no odnosi se i na sve ostale oblike podataka (papirnate arhive i sl).

Uredba je usvojena 27.04.2016. a njena obavezna primjena počinje 25.05.2018. Uredba je obvezujuća za sve pravne subjekte registrirane na teritoriju EU, kao i za sve oblike organizacija koje prikupljaju i obrađuju u bilo kom obliku osobne podatke građana EU (kao što su npr. međunarodne web trgovine, društvene mreže, pružatelji cloud i e-mail usluga i sl). Uredba se ne odnosi na osobne podatke koje prikuplja pojedinac za svoje osobne potrebe (npr. osobni adresar i sl).

2. ZAŠTO NAM JE GDPR BITAN

GDPR je bitan jer pojedincima (fizičkim osobama) donosi zaštitu od zloupotrebe njihovih osobnih podataka i uvodi red u području obrade osobnih podataka, dok organizacijama GDPR pomaže da obradu osobnih, ali i ostalih kategorija, podataka obavljaju na jedan sigurniji i kvalitetniji način.

GDPR u fazi uvođenja u organizaciji iziskuje određene investicije i napore, no dugoročno donosi sigurnost i poboljšanje načina rada s podacima i digitalnim sadržajima.

GDPR je jedan od najvećih koraka naprijed kad je u pitanju zaštita privatnosti u posljednjih 20-ak godina, naročito u kontekstu digitalnog društva.

3. ŠTO GDPR TRAŽI

U odnosu na dosadašnju praksu obrade osobnih podataka GDPR uvodi nekoliko novosti koje se odnose na prava ispitanika (fizičkih osoba čiji se osobni podaci prikupljaju i obrađuju), kao i novosti vezane uz obaveze organizacije koja prikuplja, čuva i obrađuje osobne podatke.

Prava ispitanika:

Osobni podaci se ne smiju prikupljati ako ispitanik nije dao privolu (pisano odobrenje da se slaže s time da se određeni osobni podaci prikupljaju, obrađuju i čuvaju u određene svrhe). Ispitaniku GDPR garantira sljedeća prava:

- pravo na povlačenje privole
- pravo na uvid u prikupljene osobne podatke
- pravo na izmjenu prikupljenih osobnih podataka
- pravo na brisanje (zaborav) prikupljenih osobnih podataka
- pravo na prijenos prikupljenih osobnih podataka

Obaveze organizacije koja prikuplja, čuva i obrađuje osobne podatke:

- obavezno upravljanje privolama
- obaveze sigurne obrade i čuvanja osobnih podataka
- obaveza obavještavanja nadzornog tijela i ispitanika u slučaju incidenata (gubitak, krađa, neovlašteni pristup podacima i sl.)
- obaveza imenovanja službenika za zaštitu osobnih podataka

U slučaju nepridržavanja odredbi uredbe predviđene su kazne koje mogu biti novčane do 20 000 000 Eura ili 4% globalnog bruto prihoda, a u nekim zemljama EU predviđene su i zatvorske kazne za odgovorne osobe unutar organizacije.

4. DEFINICIJE POJMOVA U GDPR-u

GDPR koristi nekoliko pojmova specifičnih za ovu uredbu pa ćemo te pojmove ovdje definirati.

Osobni podaci

„Osobni podaci" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili 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.

Primjeri osobnih podataka u praksi su npr. ime, matični broj, email adresa, online identifikator korisnika, postovi na društvenim medijima, fizičke, fiziološke ili genetske informacije, medicinske informacije, mjesto, bankovni detalji, ip adresa, internet kolačići i sl.

Posebne kategorije osobnih podataka

Osobni podaci koji su po svojoj naravi posebno osjetljive prirode u pogledu temeljnih prava i sloboda zaslužuju posebnu zaštitu jer bi u okviru njihove obrade moglo doći do značajnih rizika za temeljna prava i slobode. Ti bi osobni podaci trebali obuhvatiti osobne podatke koji otkrivaju rasno ili etničko podrijetlo, pri čemu upotreba termina „rasno podrijetlo" u uredbi ne podrazumijeva da Unija prihvaća teorije koje pokušavaju odrediti postojanje odvojenih ljudskih rasa. Obradu fotografija ne bi trebalo sustavno smatrati obradom posebnih kategorija osobnih podataka jer su one u biti obuhvaćene samo definicijom biometrijskih podataka pri obradi posebnim tehničkim sredstvima kojima se omogućuje jedinstvena identifikacija ili autentifikacija pojedinca. Takvi osobni podaci ne bi se smjeli obrađivati osim ako je obrada dopuštena u posebnim slučajevima navedenima u Uredbi.

Zabranjuje se obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

Voditelj obrade osobnih podataka

„Voditelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka.

Izvršitelj obrade osobnih podataka

„Izvršitelj obrade" znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade.

Ispitanik

Fizička osoba čiji se osobni podaci prikupljaju, čuvaju i obrađuju.

Službenik za zaštitu podataka

Službenik za zaštitu podataka (engl. Data Protection Officer = DPO) je pojedinac zaposlen ili unajmljen od strane voditelja ili izvršitelja obrade koji savjetuje sve sudionike obrade podataka o tome na koji način pravilno obrađivati osobne podatke. On ujedno prati poštuju li se u organizaciji odredbe uredbe GDPR te je kontakt prema agenciji koja na nacionalnoj razini provodi odredbe GDPR-a.

5. PRIPREMA ZA USKLAĐIVANJE S GDPR-om

5.1. KORAK 1: Analiza poslovnih procesa

Da bi mogli uspješno čuvati i štiti osobne podatke, najprije trebamo napraviti analizu procesa koji se odvijaju unutar naše organizacije kako bi utvrdili u kojim se sve procesima prikupljaju, obrađuju i čuvaju osobni podaci.

Trebalo bi se utvrditi koji se podaci prikupljaju, obrađuju i čuvaju unutar svakog procesa, zašto se to čini, te koja je zakonska ili ugovorna osnova za takvo postupanje s podacima.

Poželjno je također utvrditi može li se u pojedinim procesima reducirati rad s osobnim podacima.

5.2. KORAK 2: Analiza trenutnog stanja

Tijekom analize poslovnih procesa trebali bi odgovoriti na nekoliko pitanja:

- gdje se u našem poslovanju koriste osobni podaci i koji su to osobni podaci?
- zašto koristimo te podatke?
- kako ih štitimo i kako možemo dokazati da ih štitimo?
- na koji način arhiviramo osobne podatke i što radimo s njima kad nam više nisu potrebni?

6. PROCES USKLAĐIVANJA S UREDBOM

Uredba GDPR prilično jasno propisuje prakse kojih se organizacije trebaju pridržavati kad rade s osobnim podacima, počevši od načina prikupljanja osobnih podataka, preko obrade i čuvanja, do razmjene podataka s drugim organizacijama.

Neovisno o samoj uredbi bilo bi dobro da organizacija definira i javno objavi (npr. na vlastitim web stranicama) svoju politiku privatnosti u kojoj jednostavnim jezikom objašnjava tko prikuplja osobne podatke, način njihova prikupljanja, zašto se osobni podaci prikupljaju i obrađuju, te koliko će dugo oni biti pohranjeni i tko ih sve dobiva (ukoliko se ti podaci razmjenjuju s drugim organizacijama).

U ovom ćemo poglavlju proći kroz neke od zahtijevanih praksi uredbe.

6.1. KORAK 1: Prikupljanje osobnih podataka

GDPR dozvoljava tri osnove na temelju kojih se mogu prikupljati osobni podaci ispitanika:

1. **zakonska osnova** (npr. Zakon o radu i sl.)
2. **ugovorna obveza** između ispitanika i voditelja obrade (npr. potpisivanje ugovora o korištenju usluga)
3. **privola** koju ispitanik daje dobrovoljno voditelju obrade

U poslovnim odnosima najčešća osnova za prikupljanje osobnih podataka su zakonska osnova (npr. prilikom zapošljavanja djelatnika) i ugovorne obveze (npr. prilikom potpisivanja ugovora o izvršenju usluga). Ukoliko postoji valjanja zakonska obveza ili ugovorna obveza, tada nema veće razlike između dosadašnjeg načina prikupljanja osobnih podataka i novog načina usklađenog s GDPR-om, osim što GDPR naglašava da prikupljanje podataka treba svesti na najmanju moguću mjeru (tj. ne prikupljati osobne podatke koji nisu neophodni).

U nastavku ćemo se više pozabaviti privolama koje su novost unutar GDPR-a.

Privola

Privola je jedan od najvažnijih pojmova kad je u pitanju obrada osobnih podataka usklađena s GDPR-om.

„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.

Obavezno provjerite na koje sve načine prikupljate osobne podatke, objašnjavate li pri tom jasno čemu će ti podaci služiti i je li je prikupljanje na dobrovoljnoj bazi. Kada se prikupljaju osobni podaci od ispitanika, trebalo bi ga također obavijestiti o tome je li obvezan pružiti osobne podatke te o posljedicama ako takve podatke ne pruži. Izuzetak od ovoga su tijela javne uprave,

sudovi i slične institucije koje prikupljaju i obrađuje osobne podatke po službenoj dužnosti i u skladu sa zakonskom regulativom.

Privola bi se trebala davati jasnom potvrdnom radnjom kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave. To bi moglo obuhvaćati označivanje polja kvačicom pri posjetu internetskim stranicama, biranje tehničkih postavaka usluga informacijskog društva ili drugu izjavu ili ponašanje koje jasno pokazuje u tom kontekstu da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti stoga se ne bi smjeli smatrati privolom. Privola bi trebala obuhvatiti sve aktivnosti obrade koje se obavljaju u istu svrhu ili svrhe. Kada obrada ima višestruke svrhe, privolu bi trebalo dati za sve njih. Ako se privola ispitanika treba dati nakon zahtjeva upućenog elektroničkim putem, taj zahtjev mora biti jasan, jezgrovit i ne smije nepotrebno ometati upotrebu usluge za koju se upotrebljava.

Jedan primjer davanja privole u praksi je pretplata na primanje obavijesti (newsletter) ili sl. na web stranicama organizacije. U obrascu za prikupljanje podataka potrebno je prikupiti samo najosnovnije podatke koji su potrebni za primanje obavijesti (u ovom primjeru e-mail adresa i eventualno ime ispitanika). Da bi se predao obrazac treba označiti kvačicom polje pored kojeg piše da je ispitanik razumio da će se njegovi osobni podaci ime i e-mail adresa koristiti za slanje obavijesti i da se on s tim slaže. Kad ispitanik klikne na gumb za predaju obrasca on bi trebao dobiti e-mail poruku u kojoj se od njega traži potvrda da želi biti pretplaćen na primanje obavijesti. Na ovaj način dobivamo povratni e-mail od ispitanika koji predstavlja danu privolu i koji se može čuvati. Naravno, pretplata na primanje obavijesti se može i drugačije regulirati, ovo je samo jedan primjer mogućeg prikupljanja privola.

Voditelj obrade trebao bi moći dokazati da je ispitanik dao privolu za postupak obrade. Zaštitnim mjerama, posebno u kontekstu pisane izjave trebalo bi se osigurati da je ispitanik svjestan činjenice da daje privolu i do koje mjere se ona daje. Izjavu o privoli koju je unaprijed sastavio voditelj obrade trebalo bi ponuditi u razumljivom i lako dostupnom obliku, uz upotrebu jasnog i jednostavnog jezika te u njoj ne bi smjelo biti nepoštenih uvjeta. Da bi ispitanik mogao dati privolu informiran, trebao bi barem znati identitet voditelja obrade i svrhe obrade za koju se upotrebljavaju osobni podaci. Ne može se smatrati da je privola dana dobrovoljno ako ispitanik nema istinski slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica.

Ako ispitanik da privolu u vidu pisane izjave koja se odnosi i na druga pitanja, zahtjev za privolu mora biti predočen na način da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz uporabu jasnog i jednostavnog jezika.

Ispitanik ima pravo u svakom trenutku povući svoju privolu. Povlačenje privole ne utječe na zakonitost obrade na temelju privole prije njezina povlačenja. Prije davanja privole, ispitanika se o tome obavješćuje. Povlačenje privole mora biti jednako jednostavno kao i njezino davanje.

Upravljanje privolama

Voditelj obrade dužan je upravljati prikupljenim privolama ispitanika na takav način da je omogućen uvid u svaku privolu koju je ispitanik dao, da je moguće pratiti životni ciklus privole (njezino zaprimanje, promjene i eventualno povlačenje), kao i obrade podataka koje se vrše temeljem te privole.

Upravljanje privolama može se vršiti kroz specijalizirane softverske programe, kroz rješenja za upravljanje dokumentima unutar organizacije, ručno i sl. Sam način realizacije upravljanja nije bitan, već je bitno da se po potrebi može doći do određene privole i pratiti njen životni ciklus, od

početnog davanja kroz eventualne izmjene do povlačenja privole ako do nje dođe. Poželjno je također da rješenje za upravljanje privolama omogućuje uvid u sve privole određenog ispitanika.

Politika zaštite osobnih podataka

Organizacija može donijeti i politiku zaštite osobnih podataka (naziva se još i politika privatnosti ili pravila o privatnosti) koja može biti objavljena i kao javni dokument (npr. na Internet stranicama organizacije), a koja pokazuje na koji način se organizacija odnosi prema osobnim podacima koje prikuplja. Ovakav dokument naglašava transparentnost obrade osobnih podataka u organizaciji čime se jača povjerenje partnera i korisnika.

Što moramo činiti?

Trebamo oformiti jasne i razumljive privole pisane jednostavnim jezikom za svaku situaciju kada prikupljamo osobne podatke. Također trebamo uspostaviti sustav upravljanja privolama.

Korisno je i poželjno također oformiti Politiku zaštite osobnih podataka i objaviti ju javno na Internet stranicama ili nekom drugom mediju.

6.2. KORAK 2: Čuvanje osobnih podataka

Kad su na temelju dane privole prikupljeni osobni podaci ispitanika, oni se moraju čuvati na takav način da su zaštićeni od gubitka i neovlaštenog pristupa, a da se istovremeno ispitanicima mogu omogućiti prava koja im GDPR garantira.

Tehničke mjere zaštite čuvanih osobnih podataka

Uredba zahtjeva poduzimanje određenih tehničkih mjera po izboru voditelja obrade, a u skladu s utvrđenim rizicima, kojima se nastoji osigurati dostupnost, integritet i povjerljivost osobnih podataka.

Dostupnost podrazumijeva da su podaci uvijek dostupni i zaštićeni od gubitka i nemogućnosti pristupa. U praksi se to postiže upotrebom sigurnosnih kopija (backup) podataka pri čemu same sigurnosne kopije trebaju biti verificirane i zaštićene od neovlaštenog pristupa.

Integritet podrazumijeva da se podaci ne mogu neovlašteno mijenjati. U praksi se to postiže definiranjem prava pristupa podacima čime se drastično smanjuje mogućnost manipulacije

podacima. Pravo pristupa, uvida i mijenjanja podataka omogućuje se samo osobama i funkcijama čiji opis posla to zahtijeva i u mjeri koja je neophodna za obavljanje zadataka.

Povjerljivost podrazumijeva da se osobnim podacima ne može neovlašteno pristupiti tj. da je njihov sadržaj zaštićen/skriven. Tehničke mjere kojima se ovo postiže mogu biti enkripcija (šifriranje) podataka a uz to se mogu koristiti i metode anonimizacije i pseudomizacije podataka tj. namjerna promjena dijela podataka kako se ne bi mogao utvrditi stvarni identitet osobe na koju se odnose određeni podaci. Primjer primjene ovih mjera u praksi je šifriranje pohrane (diska, memorije) prijenosnih računala i mobilnih uređaja.

Upotrebom ovakvih i sl. tehničkih i organizacijskih mjera znatno se smanjuje mogućnost gubitka i neovlaštenog pristupa podacima.

Pouzdani proizvođači softvera svoj softver grade na principima povjerljivosti, integriteta i dostupnosti kako bi time osigurali besprijekorno funkcioniranje sustava i zaštitu podataka korisnika. Jedan od načina kako se dokazuje usklađenost s ovim zahtjevima je ISO27001 certifikat informacijske sigurnosti kojim se dokazuje da nositelj certifikata poštuje najviše standarde u zaštiti podataka. Tvrtka KONTO d.o.o. je jedan od nositelja ISO27001 certifikata za informacijsku sigurnost u RH.

Osim što trebaju brinuti o sigurnosti i dostupnosti podataka, organizacije trebaju ispitanicima omogućiti i određena prava:

Pravo na uvid u prikupljene osobne podatke

Ispitanik ima pravo 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 sljedećim informacijama:

(a) svrsi obrade;

(b) kategorijama osobnih podataka o kojima je riječ;

(c) primateljima ili kategorijama primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama;

(d) ako je to moguće, predviđenom razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterijima korištenima za utvrđivanje tog razdoblja;

Pravo na ispravak

Ispitanik bi trebao imati pravo na ispravak osobnih podataka koji se na njega odnose te „pravo na zaborav” ako zadržavanje takvih podataka više nije neophodno.

Pravo na zaborav

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 je ispunjen jedan od sljedećih uvjeta:

(a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;

(b) ispitanik povuče privolu na kojoj se obrada temelji i ako ne postoji druga pravna osnova za obradu;

(c) ispitanik uloži prigovor na obradu te ne postoje jači legitimni razlozi za obradu

(d) osobni podaci obrađeni su nezakonito;

Ovo je pravo osobito bitno ako je ispitanik dao svoju privolu dok je bio dijete i nije bio u potpunosti svjestan rizika obrade, a kasnije želi ukloniti takve osobne podatke, osobito na internetu. Ispitanik bi trebao biti u mogućnosti ostvariti to pravo neovisno o činjenici da više nije dijete.

Pravo na prenosivost osobnih podataka

Ispitanik ima pravo zatražiti od organizacije osobne podatke koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, 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:

(a) obrada se temelji na privoli ili na ugovoru

(b) obrada se provodi automatiziranim putem.

Prilikom ostvarivanja svojih prava na prenosivost podataka ispitanik ima pravo na izravni prijenos od jednog voditelja obrade drugome ako je to tehnički izvedivo.

To u praksi znači da ispitanik može zatražiti da jedna organizacija prenese sve podatke koje ima o njemu drugoj organizaciji, npr. kod promjene davatelja usluge ili sl. pri čemu organizacija koja treba prenijeti podatke to treba uraditi bez nepotrebnog odugovlačenja. Time se sprečava praksa da ispitanik treba iste podatke višestruko davati u različitim organizacijama.

Pravo na prigovor

Ispitanik ima pravo na temelju svoje posebne situacije u svakom trenutku uložiti prigovor na obradu osobnih podataka koji se odnose na njega, uključujući izradu profila koja se temelji na tim odredbama. Voditelj obrade više ne smije obrađivati osobne podatke osim ako voditelj

obrade dokaže da postoje uvjerljivi legitimni razlozi za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Ako se osobni podaci obrađuju za potrebe izravnog marketinga, ispitanik u svakom trenutku ima pravo uložiti prigovor na obradu osobnih podataka koji se odnose na njega za potrebe takvog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom.

Što moramo činiti?

Trebamo osigurati povjerljivost, integritet i dostupnost čuvanih osobnih podataka, a ispitanicima moramo osigurati gore nabrojana prava koja proizlaze iz uredbe.

6.3. KORAK 3: Obrada i prijenos osobnih podataka

Bez obzira koju vrstu obrade osobnih podataka radimo, uredba traži da se ta obrada radi zakonito, pošteno i na transparentan način. Drugim riječima, ispitanici trebaju znati u koju svrhu se obrađuju osobni podaci i smiju se obrađivati samo u tu navedenu svrhu za koju je dana privola. Sve ostalo je protuzakonito.

Količinu prikupljenih podataka i opseg obrade potrebno je svesti na minimum i pri tome primijeniti tehničke mjere zaštite koje smo prikazali u prethodnoj točki. Po završetku obrade ukoliko ne postoji druga zakonska obaveza, osobne podatke treba obrisati na siguran način.

Evidencija obrade

Članak 30. uredbe također traži da se kod organizacija s više od 250 zaposlenika, ili u slučaju kad se obrađuju posebne kategorije osobnih podataka, vodi evidencija aktivnosti obrade u kojoj se navode:

(a) ime i kontaktne podatke voditelja obrade i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka;

(b) svrhe obrade;

(c) opis kategorija ispitanika i kategorija osobnih podataka;

(d) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije;

(e) ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije, te dokumentaciju o odgovarajućim zaštitnim mjerama;

(f) ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka;

(g) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera

Ova obaveza odnosi se i na organizacije s manje od 250 zaposlenika ako će obrada koju provode vjerojatno prouzročiti visok rizik za prava i slobode ispitanika, ako obrada nije povremena ili obrada uključuje posebne kategorije podataka ili je riječ o osobnim podacima u vezi s kaznenim osudama i kažnjivim djelima.

Sigurnost obrade

Članak 32. propisuje da voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

(a) pseudonimizaciju i enkripciju osobnih podataka;

(b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;

(c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;

(d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

U praksi to znači da je uz enkripciju podataka potrebno raditi i sigurnosne kopije (backup) podataka koje treba testirati kako bi u slučaju gubitka podataka iz sigurnosnih kopija sa sigurnošću mogli obnoviti podatke.

Također je potrebno redovito raditi sigurnosna testiranja sustava kako bi se utvrdile eventualne ranjivosti samog sustava u kojem se obrađuju podaci.

KONTO d.o.o. u svom se radu pridržava najviših sigurnosnih standarda upravljanja podacima (ISO27001) i redovito provjerava svoje sustave i proizvode kako bi svojim korisnicima osigurao najviši stupanj sigurnosti programskih rješenja koja nudimo. To uključuje i mehanizme izrade sigurnosnih kopija podataka unutar programskih rješenja koja nudimo.

Što moramo činiti?

Moramo voditi evidenciju obrade i podatke obrađivati i prenositi na siguran način, te imati dokumentaciju koja to dokazuje.

6.4. KORAK 4: Određivanje službenika za zaštitu podataka

Organizacije koje su tijelo javne vlasti ili druge javne ustanove, kao i organizacije koje obrađuju posebne kategorije osobnih podataka, trebaju odrediti službenika za zaštitu podataka. I kod ostalih tipova organizacija je poželjno da imaju službenika za zaštitu podataka, čak i kada to nisu obavezne.

Službenik za zaštitu podataka može biti zaposlenik organizacije, ili može tu ulogu obavljati temeljem ugovora. Također je moguće da više organizacija koristi istog službenika za zaštitu podataka pod uvjetom da je on po potrebi raspoloživ svakoj od tih organizacija.

Službenik za zaštitu podataka obavlja sljedeće zadaće:

(a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka;

(b) praćenje poštovanja Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

(c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja;

(d) suradnja s nadzornim tijelom;

(e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade.

Službenik za zaštitu podataka pri obavljanju svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade.

Što moramo činiti?

Poželjno je, a kod nekih organizacija i obavezno, imenovanje službenika za zaštitu podataka koji će u svom radu imati potrebne kompetencije i samostalnost, te odgovarati upravi organizacije a po potrebi biti veza između organizacije i nadzornog tijela.

6.5. KORAK 5: Analiza preostalih rizika

Kad je u pitanju sigurnost podataka, ne postoji sustav prikupljanja, obrade i čuvanja podataka koji je potpuno siguran i imun na mogućnost gubitka ili neovlaštenog pristupa podacima.

Zbog toga je potrebno napraviti analizu rizika od neovlaštenog pristupa, izmjene ili gubitka osobnih podataka. Svrha ove analize je utvrditi koji sustavi za obradu podataka i samim time koji podaci su najugroženiji kako bi se zatim poduzele određene organizacijske i tehničke mjere za smanjenje tih rizika.

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.

Analiza se provodi na taj način da se pobroje resursi za prikupljanje, obradu i čuvanje podataka, za svaki resurs se popišu potencijalne ranjivosti/prijetnje te se za svaku ranjivost/prijetnju ocjenjuje vjerojatnost ostvarenja i moguće posljedice. Na taj način se računa faktor rizika. Rizici se dijele u visoke, srednje i niske ovisno o iznosu faktora rizika.

Ovom analizom postaje nam jasno na koje resurse i podatke trebamo primijeniti dodatne mjere zaštite kako bi smanjili rizik od neovlaštenog pristupa, izmjene ili gubitka osobnih podataka.

Analiza rizika može se obavljati ručno, pomoću Excel tablica, a postoje i specijalizirani softveri koji se bave procjenom rizika.

Broj rizika	Strukturna analiza	Rizik		Odgovorna osoba	Ranjivosti	Vjerojatnost	Posljedice		Opcije za obradu rizika moguće akcije
		Vrsta resursa	Naziv resursa			Indeks vjerojatnosti	Indeks štete	Faktor rizika (vjerojatnost * posljedice)	A. Ovladavanje rizikom primjenom odabrane sigurnosne mjere B. Smanjiti rizik promjenom (restruktuiranjem) poslovne aktivnosti C. Prihvaćanje rizika D. Prenošenje (transferiranje) rizika)

Primjer analize rizika pomoću Excel tablice

Jedan od najboljih načina postizanja veće sigurnosti informacijskih sustava je implementacija standarda ISO27001. Čak ako i ne želimo obaviti certificiranje naše organizacije po tom standardu, možemo primijeniti metodologije analize rizika i mjere zaštite koje propisuje standard.

Ukoliko analizom utvrdimo postojanje visokog rizika za prava i slobode pojedinaca, a voditelj obrade smatra da se taj rizik ne može umanjiti razumnim mjerama u pogledu dostupne tehnologije i troškova provedbe, prije početka obrade trebalo bi se 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.

Što moramo činiti?

Moramo provesti analizu rizika te poduzeti mjere koje će smanjiti utvrđene visoke rizike. Sve to treba biti dokumentirano.

7. UPRAVLJANJE INCIDENTIMA

Ukoliko dođe do incidenta, čim voditelj obrade primijeti da je došlo do povrede osobnih podataka, trebao bi o tome izvijestiti nadležno nadzorno tijelo bez nepotrebnog odgađanja i to, ako je izvedivo, najkasnije 72 sata nakon saznanja o toj povredi osobnih podataka, osim ako voditelj obrade može dokazati, u skladu s načelom odgovornosti, da povreda osobnih podataka vjerojatno neće prouzročiti rizik za prava i slobode pojedinaca. Ako se takvo obavješćivanje ne može postići u roku od 72 sata, obavijest bi trebala biti popraćena razlozima kašnjenja, a informacije se mogu pružiti u fazama bez nepotrebnog daljnjeg odgađanja.

U slučaju povrede osobnih podataka koje će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade bez nepotrebnog odgađanja obavješćuje ispitanika o povredi osobnih podataka.

Da bi to bilo moguće potrebno je razviti sustav nadgledanja obrade, bilježiti svaku aktivnost nad osobnim podacima (tko pristupa osobnim podacima, na koji način, kada i odakle, te koju vrstu aktivnosti obavlja nad podacima), te razviti sustav upozoravanja na eventualne nepravilnosti.

Ukoliko primijetimo da je došlo do povrede osobnih podataka, bitno je utvrditi može li se na temelju osobnih podataka koji su ugroženi utvrditi identitet ispitanika. Ukoliko je to moguće tada je prema zahtjevu uredbe potrebno obavijestiti ispitanike o incidentu, kao i o mjerama koje su poduzete nakon incidenta kako bi se smanjila eventualna šteta.

Ukoliko dođe do incidenta važno je sačuvati što je moguće više dokaza o tome kako je došlo do incidenta kako bi se lakše utvrdila potencijalna šteta, ali i kako bi naučili kako se u budućnosti bolje zaštiti od sličnih incidenata.

KONTO d.o.o. pomaže svojim korisnicima na način da su KONTO programskim rješenjima uvedena prava pristupa čime je ograničen pristup određenim kategorijama podataka i određenim funkcionalnostima aplikacija. Također se bilježe određene aktivnosti nad podacima čime je olakšano utvrđivanje odgovornosti u slučaju eventualnog incidenta nad osobnim podacima. Uz to je tehnički omogućena redovita sigurnosna zaštita podataka pa se u slučaju gubitka može vratiti barem dio podataka. Na taj način smo poduzeli određene preventivne mjere kako bi se spriječili incidenti, kao i mjere za lakši oporavak i utvrđivanje odgovornosti u slučaju da do incidenta dođe.

Što moramo činiti?

Trebamo uspostaviti sustav upravljanja incidentima, imati dokumentirani proces i procedure odgovora na incidente ukoliko do njih dođe.

8. DOKAZIVANJE USKLAĐENOSTI - AUDIT

Voditelj obrade ili izvršitelj obrade trebao bi voditi evidenciju o aktivnostima obrade pod svojom odgovornošću radi dokazivanja sukladnosti s Uredbom.

Nadzorno tijelo može izvršiti audit (provjeru) usklađenosti organizacije s Uredbom pa je bitno biti unaprijed pripremljen za takve postupke. Najbolji način pripreme za audit je samoprovjera tj. interni audit kojeg organizacija sama provodi kako bi utvrdila je li i u kojoj je mjeri usklađena s Uredbom.

Interni audit se može provoditi periodički, poželjno je najmanje jednom godišnje, a poželjno je da ga vrše djelatnici ili vanjski suradnici koji ne rade direktno na pozicijama koje se provjeravaju kako bi se osigurala transparentnost i nepristranost audita.

Napominjemo da interni audit nije zahtjev same Uredbe, već jedna mjera provjere usklađenosti koju organizacija može sama provesti.

Prilikom internog audita provjerava se između ostalog:

- poduzimaju li se odgovarajuće tehničke i organizacijske mjere radi osiguravanja poštovanja uvjeta Uredbe.
- jesu li uvedene interne politike i provedene 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.
- je li omogućeno ispitaniku da prati obradu podataka,
- je li omogućeno voditelju obrade da stvara i poboljšava sigurnosne značajke.
- uzima li se u obzir pravo na zaštitu podataka prilikom razvijanja i osmišljavanja takvih proizvoda, usluga i aplikacija
- uzimaju li se načela tehničke i integrirane zaštite podataka u obzir u kontekstu javnih natječaja.
- I dr.

Bitno je napomenuti da za sve ove točke treba postojati pisani trag. Dokumentacija je najvažnija u auditu, usmeni dogovori i općeprihvaćena praksa nisu dovoljni.

9. KAKO VAM KONTO POMAŽE U PRIMJENI GDPR-a

KONTO d.o.o, kao jedna od vodećih domaćih IT tvrtki specijaliziranih za razvoj računovodstvenog softvera, polaže veliku pažnju u sigurnost programskih rješenja koje razvija, kao i podataka koje ti programi obrađuju.

U skladu s tim u našim programima vodimo brigu o najvišoj razini sigurnosti i zaštite podataka, od postupaka autentikacije i autorizacije za korištenje programa, preko dodjeljivanja prava korištenja unutar naših programskih rješenja i praćenja određenih aktivnosti nad podacima, do postupaka omogućavanja izrade sigurnosne kopije podataka.

KONTO d.o.o. je među 50 prvih uspješno certificiranih organizacija prema normi ISO27001 za sigurnost informacija u Hrvatskoj što pokazuje našu posvećenost sigurnosti i zaštiti naših korisnika. Usklađivanje poslovanja sa standardom ISO27001 je ujedno jedna od najboljih priprema za implementaciju i provođenje zahtjeva uredbe GDPR.

Osim što je svoje poslovanje i svoja programska rješenja uskladio s Uredbom GDPR, KONTO d.o.o. može pomoći i svojim korisnicima u njihovom lakšem usklađivanju s Uredbom na nekoliko načina:

- kroz ugradnju principa privatnosti u dizajn na način da se korisničkom imenu dodjeljuju prava pristupa na module, izbornike unutar pojedinih modula, funkcionalnosti u modulu te sve više i prava pristupa na određene radnje unutar svake pojedinačne evidencije podataka (svaki šifarnik, unos i izvješće);
- KONTO programska rješenja podatke čuvaju u sigurnim bazama podataka;
- kroz praćenje zapisa aktivnosti unutar KONTO programskih rješenja, olakšano je utvrđivanje odgovornosti u slučaju pojave incidenta;
- u slučaju gubitka podataka moguć je oporavaka iz sigurnosne kopije podataka koju je korisnik radio;
- može Vam preporučiti vrhunske konzultante s kojima mi surađujemo specijalizirane u područjima informacijske sigurnosti i usklađivanja s regulativama.

Naši korisnici su se kroz godine uvjerili da KONTO uvijek daje više jer osim kvalitetnih i sigurnih programskih rješenja, našim korisnicima nudimo i podršku u radu kako bi im maksimalno olakšali svakodnevni posao.

10. DODATNE INFORMACIJE

Za dodatne informacije o uredbi GDPR molimo posjetite službene stranice uredbe na Internet adresi www.eugdpr.org kao i stranice Agencije za zaštitu osobnih podataka www.azop.hr

11. POPIS LITERATURE

- 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 (Opća uredba o zaštiti podataka), Službeni list Europske unije L 119, 4. svibnja 2016.

  http://data.europa.eu/eli/reg/2016/679/oj

- Velika škola GDPR-a ICTbusiness portala

KONTO d.o.o. Požega

ISO 9001 za kvalitetu

ISO 27001 za sigurnost informacija

Tvrtka Konto d.o.o. posluje na hrvatskom tržištu od 1993. godine. Primarno se bavi projektiranjem, razvojem i održavanjem informacijskih sustava. Nudimo kompletna softverska rješenja za upravljanje poslovanjem, kao i aplikacije za pojedinačne poslovne procese koje prilagođavamo potrebama i zahtjevima naših korisnika. Aplikacije su međusobno povezane i modularne, te se na taj način optimalno prilagođavaju korisniku u njegovom radu.

Danas tvrtka zapošljava preko 20 visokokvalificiranih stručnjaka.

Baza od preko 400 korisnika Konto aplikacija sastoji se od profitnih poduzeća, obrtnika, neprofitnih organizacija te proračunskih korisnika.

Sjedište u Požegi
Zrinska 48, 34000 Požega
Telefon: 034.313.900; 034.313.901

www.konto.hr

Ured u Varaždinu
S. S. Kranjčevića 7, 42000 Varaždin
Telefon: 042.300.900; 042.300.901

info@konto.hr

Ova uputa, kao i rad programa koji je opisan, rađeni su u dobroj vjeri sa ciljem olakšanja rada korisnika programa. Bez obzira na sve navedeno u uputi, potrebno je da sve tvrdnje iz upute i rezultate obrada provjerite jesu li su točni i u skladu sa zakonskim propisima te ih ne primjenjujte ako nisu.