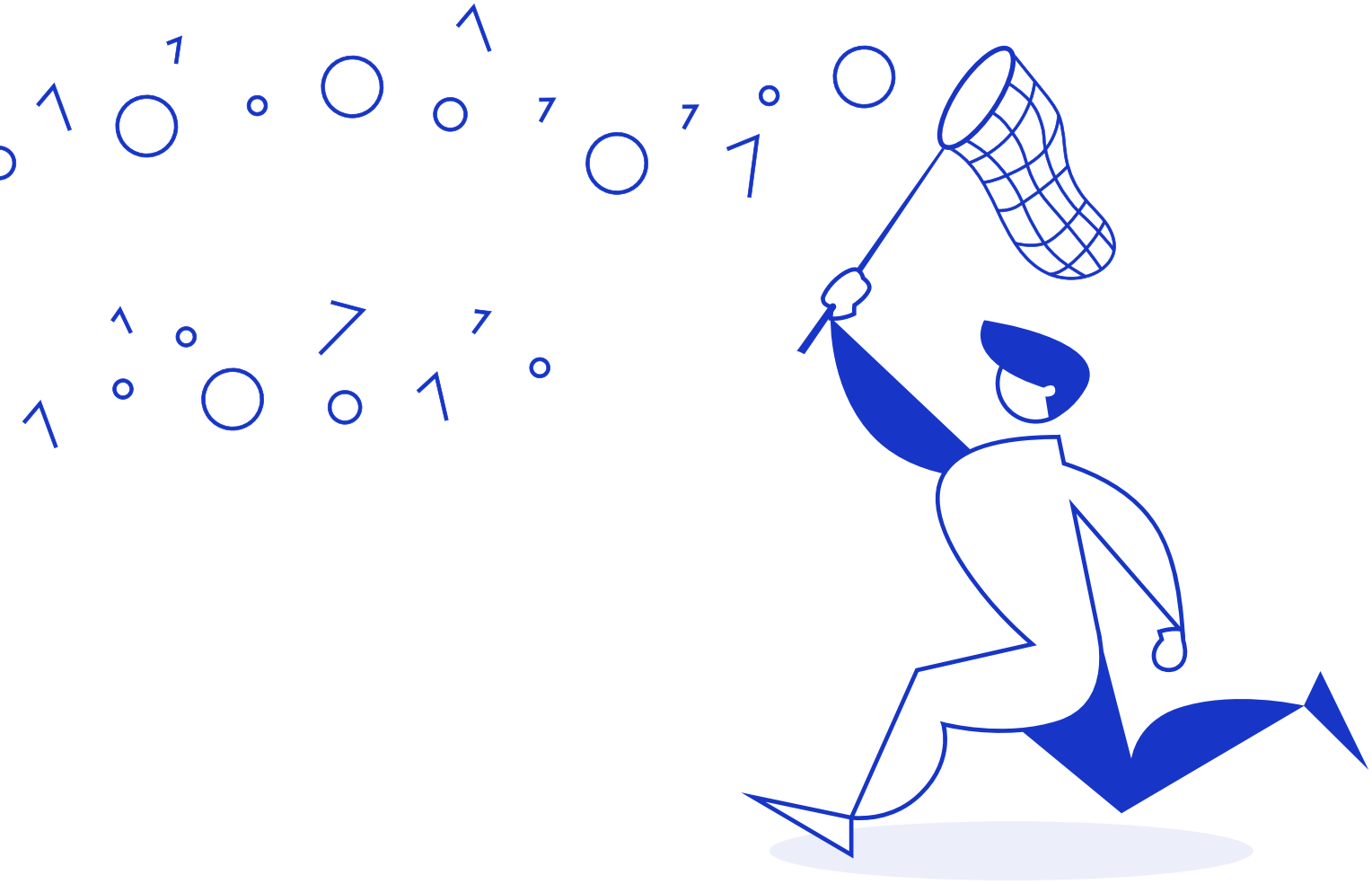
CONSENT

#kulturaprivatnosti
www.consent.hr



GDPR upitnik*
za samoprocjenu

*Upitnik je namijenjen primarno poslovnim subjektima manje do srednje veličine.

01 Uvod

Opća uredba o zaštiti podataka 2016/679 EU propisuje mjere, obaveze, uloge, prava, svrhe, rokove čuvanja te preporuke zaštite osobnih i pseudo podataka. U praksi se uvriježio naziv GDPR – skraćenica od engleskog naziva General Data Protection Regulation, a primjenjuje se od 25.05.2018.

Osim izbjegavanja visokih novčanih kazni propisanih za sve poslovne subjekte koji je ozbiljnije krše, potpuna prilagodba poslovanja Uredbi donosi i niz drugih važnih benefita:

01 **Briga o zaštiti osobnih podataka povećava povjerenje klijenata i zaposlenika te reputaciju poslovnog subjekta.**

02 **Smanjuje rizik povrede (incidenta) osobnih podataka te omogućava učinkovito reagiranje ako se povreda ipak dogodi.**

03 **Postavljanje privatnosti na visoku razinu pruža kompetitivnu razliku u odnosu na konkurenciju.**

Koristeći naš besplatni upitnik za samoprocjenu, samostalno možete provjeriti najvažnije korake u procesu prilagodbe poslovanja.

Svaki poslovni sektor ima svoje posebnosti, a svaki zasebni poslovni subjekt određene specifičnosti funkcioniranja, no ako je odgovor na sva pitanja u našem upitniku pozitivan – izrazito je vjerojatno da je vaš osnovni proces prilagodbe na zahtjeve GDPR-a uspješno odrađen.

Treba razumjeti i da usklađenost nije jednokratna stvar: poslovni procesi, zaposlenici i okolnosti se mijenjaju – zaštita osobnih podataka segment je koji kontinuirano treba prilagođavati te unaprjeđivati. Ako ste odradili prilagodbu na Uredbu, no trebate "osvježenje" o aktualnim smjernicama, preporukama te praksi nadzornih tijela i sudova, slobodno nas kontaktirajte.

Ako su pak odgovori na neka pitanja u upitniku negativni, a mogu se odnositi na vaše poslovanje, nedostaju vam još određeni koraci kako biste završili temeljni proces usklađivanja s Uredbom. Ako smatrate da te korake niste sposobni provesti samostalno – javite nam se da to učinimo zajedno.

02 Zašto Consent?

01 Vodili smo kompletne projekte GDPR prilagodbe brojnih poslovnih subjekata iz čitavog spektra različitih sektora u Hrvatskoj, a naši educirani stručnjaci te profesionalni stručni suradnici detaljno su upoznati sa svakim korakom opsežnog procesa.

02 Obavljamo funkciju vanjskog službenika za zaštitu podataka za niz organizacija, u sklopu čega sudjelujemo u izgradnji, implementaciji te upravljanju njihovim programom privatnosti s mjerljivim ciljevima i strateškim planom za njegovo ostvarenje.

03 Završili smo European Data Protection te Privacy Program Management treninge IAPP-a, najveće međunarodne organizacije za profesionalce u sferi privatnosti, kao i T4Data trening AZOP-a za službenike za zaštitu podataka javnopravnih tijela.

Usluge koje nudimo:

Puna prilagodba poslovanja na GDPR

Analiza trenutnog stanja zaštite osobnih podataka

Izrada procjene učinka na zaštitu osobnih podataka

Obavljanje funkcije vanjskog službenika za zaštitu podataka

Upravljanje privolama

Regulacija odnosa/ugovora s trećim stranama

Predavanja i edukacije vezane uz zaštitu osobnih podataka i privatnost

"Privacy by design" savjetovanje za nove tehnologije i usluge

03 | Upitnik

01 **Znamo li primjenjuje li se GDPR na nas u teritorijalnom smislu?**

Uredba se primjenjuje ako imate poslovni nastan u Europskoj uniji ili na bilo koji način obrađujete osobne podatke stanovnika Europske Unije - čak i ako je vaš poslovni nastan van EU.

Primjerice: ako imate stanovnike EU na mailing listi ili su vam s tog područja kupci, zaposlenici, ugovorni partneri, pružatelji usluga – GDPR se primjenjuje. Također, ako možete identificirati pojedince iz EU, npr. pomoću kolačića na web stranici, spadate u opseg primjene Uredbe.

02 **Znamo li obrađujemo li uopće podatke na koje se GDPR odnosi?**

Ako obrađujete podatke kojima možete pojedince identificirati u cijelosti ili djelomično, putem automatiziranih sredstava ili ručno kao dio arhivskog sustava, tada se GDPR primjenjuje. Osobnim podacima u smislu GDPR-a smatraju se i, primjerice, kolačići na webu te IP adrese. U praksi, šansa da u sklopu poslovanja uopće ne obrađujete osobne podatke u smislu Uredbe je praktički minimalna.

03 **Jesmo li identificirali koje točno osobne podatke obrađujemo, u koje svrhe to činimo, kome ih šaljemo i koliko ih zadržavamo?**

Pripremite popis podataka o vrstama podataka koje obrađujete, svrhama zbog kojih to činite, trećim stranama kojima prosljeđujete podatke te vremenskom periodu tijekom kojeg ih čuvate - ovaj popis treba biti dinamičan dokument koji se kontinuirano ažurira u svrhu vođenja evidencije.

04 **Razumijemo li koje su pravne osnove za svaku obradu koju smo prepoznali?**

Obrada osobnih podataka je zakonita isključivo ako imate valjanu pravnu osnovu za obradu. Postoji šest pravnih osnova, a niti jedna nije važnija od ostalih - osnova koja je najprigodnija za određenu obradu ovisi o vašoj svrsi obrade te odnosu s ispitanikom:

- **A** Ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha;
- **B** Obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
- **C** Obrada je nužna radi poštovanja pravnih obveza voditelja obrade;
- **D** Obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe;
- **E** Obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
- **F** Obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane;

05 Jesmo li ustanovili obrađujemo li posebne kategorije podataka i imamo li valjanu pravnu osnovu za to?

Prema Uredbi, posebne kategorije podataka su: podaci 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.

Uredba načelno zabranjuje obradu ovih kategorija podataka, osim ako ne ispunjavate jedan od uvjeta iz članka 9. stavka 2. Važno je ustanoviti imamo li doista valjanu pravnu osnovu za obradu takvih podataka, tu činjenicu dokumentirati te na primjeren način obavijestiti ispitanike o obradi posebnih kategorija podataka.

06 Jesmo li identificirali sve prijenose podataka trećim stranama i države u kojima se te treće strane nalaze?

Ispitanici imaju pravo znati kome prosljeđujete njihove osobne podatke, a GDPR postavlja stroga pravila o transferima trećim stranama izvan Europskog Gospodarskog Prostora (članci 44. do 50.)

Prije prijenosa podataka u takvoj situaciji, potrebno je razmisliti je li moguće ostvariti zamišljene ciljeve bez da se doista pošalju osobni podaci (primjerice, anonimizirani podaci ne smatraju se osobnima).

07 Ako trebamo prenijeti podatke u zemlju van Europskog Gospodarskog prostora, znamo li jesu li poduzete potrebne mjere da bi se takav transfer smatrao zakonitim?

Ako ipak trebate slati osobne podatke u državu van Europskog Gospodarskog Prostora, važno je provjeriti je li riječ o državi za koju postoji odluka o primjerenosti zaštite koju donosi Europska Komisija – takav prijenos ne zahtjeva posebno odobrenje.

Ako nije donesena takva odluka, trećoj zemlji ili međunarodnoj organizaciji osobni podaci mogu se prenijeti samo ako je voditelj obrade ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere iz članka 46. (obvezujuća korporativna pravila, standardne klauzule o zaštiti podataka, odobreni kodeks ponašanja...) te pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi. U tom slučaju, potrebno je adekvatno dokumentirati detalje o zaštitnoj mjeri koja je korištena.

08 Imamo li napisanu obavijest o privatnosti za ispitanike sukladnu Uredbi?

Postoji mogućnost da čak i kada imate napisanu te objavljenu obavijest o privatnosti, ona ne odgovara svim zahtjevima Uredbe – članak 13. i 14. detaljno preciziraju kompletan niz elemenata koje takva vrsta obavijesti mora sadržavati.

Uz to, Uredba naglašava da takva obavijest uvijek treba biti napisana u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika - osobito za svaku informaciju koja je posebno namijenjena djetetu. Obavijest treba biti dostupna ispitanicima u svakoj situaciji kada prikupljate osobne podatke.

09 Jesmo li i na svoju web stranicu dodali obavijest o privatnosti sukladnu Uredbi?

Ako na web stranici još nemate link na obavijest o privatnosti, dodajte ga na način da je vidljiv na svakoj podstranici vašeg weba (primjerice, u podnožju web stranice). Ako link već postoji, potrebno je osigurati da je obavijest u njemu sukladna svim zahtjevima Uredbe - te je redovito ažurirati.

10 Imamo li uspostavljenu proceduru za bilježenje i čuvanje dobivenih privola?

Uredba inzistira na tome da privolu treba moći dokazati. Bilježi li vaš e-mail marketing sistem dobivene privole? Imate li uspostavljenu proceduru arhiviranja privola dobivenih u papirnatom obliku?

Consent usluga — Upravljanje privolama

11 Imamo li uspostavljenu proceduru za povlačenje privola?

Privolu treba biti moguće povući na jednostavan način, a ispitanik mora biti obaviješten o svim metodama kojima je to moguće učiniti.

12 Je li naša privola za marketing putem e-maila dobivena sukladno Uredbi?

Za slanje marketinških obavijesti putem maila, nerijetko ćete trebati dobiti valjanu privolu ispitanika. Uredba zahtjeva da privola bude: tražena odvojeno od drugih pitanja, dobrovoljna, dana jasnom potvrdnom radnjom, nedvosmislena, transparentna, dokumentirana, jednostavna za povući te bez disbalansa u odnosu.

Consent blog — Kada vam je doista potrebna privola?

13 Ako imamo kolačiće (cookies) na web stranici, postoji li za njih uspostavljen proces privole sukladan Uredbi?

Ako vaša web stranica koristi cookieje (a broj stranica koji ih uopće ne koriste je doista veoma malen), posjetitelj mora biti obaviješten o njima te dati privolu za njihovo korištenje. Ono što je ovdje važno jest da cookieji ne smiju biti pokrenuti prije nego posjetitelj da privolu – stavka kod koje izrazito velik broj webova još uvijek griješi te na taj način krši Uredbu, ali i Zakon o elektroničkim komunikacijama.

Za kolačiće koji su neophodni za funkcioniranje stranice, privola nije potrebna, no posjetitelji svejedno trebaju biti informirani o njima.

14 Ako računamo na privolu za nuđenje usluga informacijskog društva djetetu, imamo li sisteme za upravljanje tom privolom?

Kada nudite usluge informacijskog društva izravno djetetu, a za tu obradu tražite privolu - obrada osobnih podataka djeteta zakonita je samo ako dijete ima najmanje 16 godina. Ako je dijete ispod dobne granice od 16 godina, privolu treba dati nositelj roditeljske odgovornosti nad djetetom.

Navedeno znači i da trebate uložiti razuman napor kako biste ustanovili je li osoba koja daje privolu doista dovoljno stara da to učini, kao i je li osoba koja daje privolu za dijete zaista nositelj roditeljske odgovornosti.

15 Ako računamo na legitimni interes kao pravnu osnovu za obradu, jesmo li proveli Procjenu legitimnog interesa?

Legitimni interes je najfleksibilnija pravna osnova obrade, no ne možemo uvijek biti sigurni da će biti i najprigodnija. Takva će vjerojatno biti u situacijama kada koristimo podatke na način koji bi građani razumno mogli očekivati, a koji ima minimalan učinak na njihovu privatnost.

Kako bismo mogli dokazati poštovanje načela pouzdanosti, odnosno usklađenost s Uredbom, u praksi se provodi test pod nazivom Procjena legitimnog interesa. Riječ je o testu koji potiče voditelje obrade da si postave prava pitanja o konkretnoj obradi te objektivno promisle koja su razumna očekivanja pojedinaca, kao i kakav je utjecaj obrade na njih. Na taj način, Procjena leg. interesa uvelike pomaže osigurati da je obrada zakonita.

Procjena se sastoji od tri dijela:

A Test svrhe (prepoznavanje legitimnog interesa)

B Test nužnosti (je li obrada nužna za ostvarenje svrhe)

C Test ravnoteže (u odnosu na interese ispitanika)

16 **Jesmo li proveli analizu zaštite osobnih podataka naših trenutnih i potencijalnih izvršitelja obrade?**

Članak 28. Uredbe postavlja obvezu voditeljima obrade da obradu podataka svojih ispitanika povjeravaju samo subjektima koji mogu pokazati da su i oni usklađeni s GDPR-om. U skladu s tom obvezom, trebali biste od svih trenutnih i budućih izvršitelja obrade (primjerice pružateljima softvera, računovodstvenih usluga, servisa u oblaku itd.) zatražiti dokaze tehničkih i organizacijskih mjera koje su poduzeli da na adekvatan način zaštite osobne podatke koje obrađuju – i poslovati isključivo s onima koji su usklađeni s Uredbom.

17 **Imamo li potpisane ugovore/sporazume o obradi podataka s izvršiteljima sukladne Uredbi?**

Uredba inzistira i na pisanom sporazumu s izvršiteljima obrade te u članku 28., stavku 3. detaljno navodi minimalne elemente koje takav sporazum treba sadržavati.

Taj ugovor je ključan kako bi obje strane jasno razumjele koja su njihova prava, obveze i odgovornosti u tom odnosu. Važan je i zbog usklađenosti sa zakonskim propisima, ali i za zaštitu prava ispitanika te pomaže demonstrirati brigu o zaštiti osobnih podataka klijentima te nadzornom tijelu.

Consent usluga – Uređivanje odnosa i ugovora s trećim stranama

18 **Imamo li uspostavljenu proceduru za zahtjeve za ostvarenje prava ispitanika?**

Uredba ispitanicima jamči ostvarenje sljedećih prava: Pravo na pristup podacima, Pravo na ispravak, Pravo na brisanje, Pravo na ograničenje obrade, Pravo na prenosivost podataka, Pravo na prigovor, Pravo usprotiviti se donošenju automatiziranih pojedinačnih odluka (profiliranje). Potrebno je dobro razumjeti preduvjete u kojima ispitanik ima mogućnost ostvarenja određenog prava te uspostaviti procedure kako bismo to ostvarenje omogućili na što jednostavniji način. Za dokazivanje usklađenosti, takve procedure bi trebalo i dokumentirati.

U slučaju primanja zahtjeva za ostvarenje bilo kojeg od navedenih prava, ispitaniku je potrebno odgovoriti u roku od mjesec dana te mu ne možete naplatiti ostvarenje njegovog prava - osim ako su zahtjevi ispitanika očito neutemeljeni ili pretjerani, što biste morali moći dokazati.

19 Znamo li trebamo li imenovati Službenika za zaštitu podataka?

Uredba u članku 37. jasno naznačava u kojim slučajevima je imenovanje Službenika za zaštitu podataka obvezno. Čak i kada nije obvezno, imenovanje stručnog i pouzdanog Službenika je poželjno i donosi niz važnih prednosti za poslovni subjekt. Kvalitetan službenik za zaštitu podataka sposoban je demonstrirati usklađenost poslovnog subjekta s važećim zakonodavstvom vezanim uz zaštitu osobnih podataka, smanjiti rizike, graditi povjerenje i pouzdanost branda te povećati kompetitivne i reputacijske prednosti poslovnog subjekta.

Ako je Službenik za zaštitu podatak imenovan, važno je ispitanicima putem svake obavijesti o obradi osobnih podataka pružiti njegove/njene kontakt podatke.

Consent usluga — Obavljanje funkcije vanjskog službenika za zaštitu podataka

20 Ako za neku obradu podataka nastupamo kao zajednički voditelji obrade, jesmo li definirali pojedinačne uloge i odnose te ih jasno iskomunicirali prema ispitanicima?

Ako dvoje ili više voditelja obrade zajednički odrede svrhe i načine obrade, oni su zajednički voditelji obrade. Zajednički voditelji trebaju sporazumom odrediti svoje međusobne uloge i odnose vezane uz zaštitu osobnih podataka te ih putem obavijesti o zaštiti podataka dati do znanja i svojim ispitanicima. Posebno je važno istaknuti tko je kontaktna točka za ostvarenje prava ispitanika.

21 Znamo li trebamo li provesti Procjenu učinka na zaštitu osobnih podataka?

Procjena učinka na zaštitu podataka je proces koji pomaže da identificirate i minimizirate rizike zaštite osobnih podataka određenog projekta. Poslovni subjekt je obvezan provesti procjenu za bilo koju obradu koja bi mogla rezultirati visokim rizikom za pojedinca, što Uredba detaljizira u članku 35., a smatra se dobrom praksom napraviti je i za svaki veći projekt koji uključuje obradu osobnih podataka.

Consent usluga — Izrada Procjene učinka na zaštitu podataka

22 **Jesmo li uspostavili internu politiku perioda zadržavanja podataka koja uključuje metode sigurnog uklanjanja podataka?**

Važno je precizno definirati period zadržavanja svake pojedine vrste osobnog podatka, pritom se pridržavajući načela ograničenja pohrane: osobni podaci moraju biti čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju.

U trenutku kada se podaci više ne trebaju čuvati, trebamo ih na siguran način potpuno ukloniti kako im netko ne bi mogao ponovno pristupiti. Kod podataka zabilježenih na papirima to je prilično jednostavno - najčešća metoda podrazumijeva korištenje shreddera, dok se za digitalno zabilježene podatke često koristi poseban softver, kao i doslovno uništavanje diskova u trenutku kada ih više nećemo koristiti.

23 **Jesmo li proveli analizu rizika i sigurnosti podataka te poduzeli odgovarajuće tehničke i organizacijske mjere zaštite sukladne analizi?**

Osobni podaci moraju biti obrađivani na način kojim se osigurava odgovarajuća sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja - primjenom odgovarajućih tehničkih i organizacijskih mjera.

U tom pogledu potrebno je napraviti analizu rizika obrade osobnih podataka u vašem poslovanju te razraditi interne protokole, kao i same fizičke te tehničke mjere zaštite. Prilikom odlučivanja o mjerama, potrebno je uzeti u obzir trenutno stanje dostupne tehnologije, kao i troškove implementacije – trebaju biti proporcionalni okolnostima te visini rizika obrade. Sve poduzete mjere, kao i analize, potrebno je dokumentirati na adekvatan način.

Consent usluga — “Privacy by design” savjetovanje za nove tehnologije i usluge

24 **Ako imamo Pravilnik o informacijskoj sigurnosti - jesmo li u njega ubacili i detalje o zaštiti osobnih podataka?**

Velik broj poslovnih subjekata ima usvojenu neku vrstu internog pravilnika ili politike koja se tiče zaštite računalnog informacijskog sustava. Takav interni dokument trebalo bi osvježiti na način da uključuje i primjerene tehničke te organizacijske mjere zaštite podataka koje smo usvojili.

25 **Imamo li uspostavljen protokol za obavijesti u slučaju povrede osobnih podataka?**

Važno je razumijeti što sve spada u okvir povrede osobnih podataka prema Uredbi: prema definiciji, riječ je o kršenju 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.

Ako se povreda dogodi, potrebno je prepoznati koliko je rizik za prava i slobode pojedinaca visok te je li potrebno obavijestiti nadzorno tijelo i povrijeđene ispitanike. Nadzorno tijelo u pripadajućim situacijama treba obavijestiti najkasnije 72 sata nakon saznanja o toj povredi - članak 33. Uredbe propisuje osnovni sadržaj koji takva obavijest treba sadržavati.

Voditelj obrade mora dokumentirati sve povrede osobnih podataka koje su mu se dogodile – kako one zbog kojih je morao obavijestiti nadzorno tijelo i/ili ispitanike, tako i one kod kojih rizik za prava i slobode pojedinaca nije postojao. Takva evidencija treba sadržavati sve činjenice vezane uz povredu, njezine posljedice i mjere poduzete za popravljanje štete.

26 **Ako imamo zaposlenike, jesmo li identificirali pravne osnove za obradu njihovih podataka te ih pravilno obavijestili o svim obradama?**

Kod ovog koraka jako velik broj poslodavaca griješi: privola je pravna osnova koja najrjeđe može biti korištena za obradu podataka zaposlenika. Primjerice, za podatke potrebne za isplatu plaće pravna osnova obrade je ispunjenje ugovorne obveze, kada obrađujete podatke za mirovinsko osiguranje – riječ je o vašoj zakonskoj obvezi itd. Kao i vaši klijenti/korisnici, i zaposlenici imaju pravo biti transparentno obaviješteni o svim obradama njihovih osobnih podataka koje provodite.

27 **Ako imamo zaposlenike, jesmo li usvojili internu politiku/pravilnik privatnosti?**

Uredba traži da možete dokazati usklađenost s njenim načelima – interna politika ili pravilnik može pomoći jasnom definiranju procesa vezanih uz zaštitu podataka u vašem poslovnom subjektu. Takav dokument obično sadrži program privatnosti s mjerljivim ciljevima, planom za njihovo ostvarenje te definirane uloge i odgovornosti u procesu. Može biti riječ o zasebnom dokumentu, ali i ne mora, no važno je da bude biti iskomuniciran sa svim zaposlenicima te redovito ažuriran.

28 **Ako imamo zaposlenike, jesmo li za njih organizirali edukaciju o zaštiti osobnih podataka?**

Zaposlenici trebaju znati kako pravilno prikupljati i obrađivati podatke, prikupljati i arhivirati privole, koliko dugo čuvati podatke, koje tehničke i organizacijske mjere zaštite su dužni primjenjivati, što učiniti u slučaju povrede osobnih podataka, kao i kako reagirati u slučaju zahtjeva za ostvarenje prava ispitanika.

Kvalitetna praksa poslovnih subjekata koji brinu o privatnosti je u redovitim intervalima organizirati interne edukacije i treninge namijenjene osvježavanju znanja te kontinuiranom podizanju svijesti radnika o zaštiti osobnih podataka.

Consent usluga — Predavanja i edukacije vezane uz zaštitu osobnih podataka

29 **Ako koristimo sustav video nadzora, jesmo li provjerili snimamo li površine u skladu s propisanim svrhama te na primjeren način obavijestili ispitanike o snimanju?**

Obrada osobnih podataka putem videonadzora smije se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine. Isto tako, kad je riječ o perimetru snimanja kamera, on smije obuhvaćati samo površine čiji nadzor je nužan za postizanje te svrhe – nije dopušteno snimanje onih površina čiji nadzor nije opravdan zbog zaštite osoba i imovine vašeg subjekta.

Jako je važno primjeren obavijestiti osobe da ulaze u objekt/prostoriju koja je pod videonadzorom – i to najkasnije prilikom ulaska u perimetar snimanja. Takva obavijest treba sadržavati sve relevantne informacije iz članka 13. Uredbe, a hrvatski Zakon o provedbi Uredbe posebno ističe jednostavnu i lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije:

A Da je prostor pod videonadzorom
B Podatke o voditelju obrade
C Podatke za kontakt putem kojih ispitanik može ostvariti svoja prava.

Consent blog — Što treba napraviti da video nadzor bude prilagođen GDPR-u

30 **Ako koristimo sustav videonadzora, imamo li interno propisano duljinu zadržavanja snimki, osobe koje im imaju pristup te mjere zaštite?**

Internim dokumentom potrebno je definirati odgovornu osobu (ili radno mjesto) koja ima pravo pristupa snimkama, kao i navesti mjere kojima je sustav videonadzora zaštićen od pristupa neovlaštenih osoba.

Potrebno je uspostaviti i automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora koji će sadržavati vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem videonadzora.

Snimke dobivene putem videonadzora mogu se čuvati najviše šest mjeseci.

04 | Zaključak

Tijekom posljednjih nekoliko godina, zaštita osobnih podataka evoluirala je od segmenta koji poslovni subjekti smatraju samo simpatičnim dodatkom - do poslovnog imperativa te ključne investicije svake uprave koja razmišlja o budućnosti tvrtke.

Građani danas postavljaju sve više pitanja o tome kako se koriste njihovi podaci, a na privatnost gledaju kao važan dio branda neke tvrtke. Consumer privacy survey iz 2019. potvrđuje da su ljudi postali svjesni svojih prava na privatnost te se proaktivno odlučuju na interakciju s onim organizacijama za koje vjeruju da će biti odgovorne s njihovim podatcima.

Organizacije zato trebaju razmišljati o vrijednosti privatnosti u širem smislu, a ne isključivo u smjeru usklađivanja s propisima i izbjegavanju rizika.

Pravi je trenutak da poslovni prioritet pretvorite i u prednost nad konkurencijom: usvojite transparentnost i odgovornost u upravljanju osobnim podacima kao standard poslovanja te se fokusirajte na izgradnju digitalnog povjerenja sa svojim kupcima.

Ako trebate pomoć u bilo kojem koraku tog procesa, tu smo za vas.

CONSENT

EMAIL
kontakt@consent.hr

GSM
+385 91 798 4225

WEB
www.consent.hr