Awareness raising campaign for SMEs

Upitnik za samoprocjenu usklađenosti s GDPR-om

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

An Coimisiún um Chosaint Sonraí Data Protection Commission

Croatian Personal Data Protection Agency azop Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Osim općeg popisa za provjeru u nastavku, ovaj upitnik za samoprocjenu usklađenosti s GDPR-om sadrži detaljnija pitanja iz sljedećih područja:

• osobni podaci

• prava ispitanika

• točnost i pohrana

• transparentnost

• druge obveze voditelja obrade podataka

• sigurnost podataka

• povrede podataka

• međunarodni prijenosi podataka

Sljedeće informacije pomoći će organizacijama u mapiranju osobnih podataka koje trenutno obrađuju, identificiranju pravne osnove na temelju kojih su podaci prikupljeni i razdoblja pohrane za svaku kategoriju podataka. Provođenje ove vježbe pomoći će identificirati gdje su potrebne hitne korektivne radnje za postizanje usklađenosti s GDPR-om.

Kategorije osobnih podataka i ispitanika

Navedite kategorije ispitanika i osobnih podataka koji se prikupljaju i čuvaju, npr. podaci o zaposlenicima; podaci o umirovljenim zaposlenicima; podaci o kupcima (podaci o prodaji); marketinška baza podataka; snimke videonadzornog sustava.

Elementi osobnih podataka uključeni u svaku kategoriju podataka

Navedite svaku vrstu osobnih podataka uključenih u pojedinu kategoriju osobnih podataka, npr. ime, adresa, bankovni podaci, povijest kupnje, povijest pregledavanja na internetu, video i slike.

Izvor osobnog podatka

Navedite izvor(e) osobnih podataka, npr. prikupljeni izravno od pojedinaca, od trećih strana

Svrhe u koje se osobni podaci obrađuju

Unutar svake kategorije osobnih podataka navedite svrhe u koje se prikupljaju i čuvaju podaci, npr. marketing, poboljšanje usluga, istraživanje, razvoj proizvoda, integritet sustava, ljudski resursi, oglašavanje, zaštita ljudi i imovine.

Pravna osnova za svaku svrhu obrade

Za svaku svrhu u kojoj se osobni podaci obrađuju navedite pravnu osnovu na kojoj se temelji npr. privola, ugovor, pravna obveza (članak 6.).

Posebne kategorije osobnih podataka

Ako obrađujete posebne kategorije osobnih podataka, navedite pojedinosti o prirodi podataka, npr. zdravstveni, genetski, biometrijski podaci.

Pravna osnova za obradu posebnih kategorija osobnih podataka

Navedite pravnu osnovu na temelju koje se prikupljaju i čuvaju posebne kategorije osobnih podataka npr. izričita privola, pravna osnova (članak 9).

Pohrana osobnih podataka

Za svaku kategoriju osobnih podataka navedite razdoblje u kojem će se podaci čuvati npr. jedan mjesec? Jedna godina?

Kao opće pravilo, podaci se ne smiju čuvati dulje nego što je potrebno za svrhu u koju su prikupljeni. Vrlo često rok čuvanja osobnih podataka je propisan zakonskim i podzakonskim propisima, npr. osobne podatke zaposlenika iz evidencija o radnom vremenu poslodavac je dužan čuvati najmanje 6 godina od dana prestanka njegovog rada.

Potrebne radnje za usklađivanje s GDPR-om?

Identificirajte radnje koje su potrebne kako bi se osiguralo da su sve aktivnosti obrade osobnih podataka usklađene s GDPR-om, npr. ovo može uključivati brisanje podataka ako nema daljnje svrhe zadržavanja.

Obrada podataka na temelju privole (Članci 7., 8. i 9.)

Jeste li pregledali mehanizme svoje organizacije za prikupljanje privole kako biste osigurali da je ona slobodno dana, posebna, informirana i da je jasan pokazatelj da je pojedinac odlučio pristati na obradu svojih podataka putem izjave ili jasne potvrdne radnje?

○ Da ○ Ne

U slučaju da obrađujete osobne podatke na temelju privole: ako privola ne ispunjava uvjete propisane GDPR-om, jeste li ponovno tražili privolu pojedinca koja je u skladu s GDPR-om?

Da Ne

Jesu li uspostavljeni postupci kojima se dokazuje da je pojedinac pristao na obradu svojih podataka?

Da Ne

Jesu li uspostavljeni postupci koji pojedincu omogućuju povlačenje privole za obradu svojih osobnih podataka?

Da Ne

Osobni podaci djece (Članak 8.)

Ako se djetetu pružaju internetske usluge, postoje li postupci za provjeru dobi i dobivanje privole roditelja/nositelja roditeljske odgovornosti, ako je potrebno?

Da Ne

Obrada osobnih podataka na temelju legitimnog interesa

Ako je legitimni interes pravna osnova na temelju koje se obrađuju osobni podaci, je li provedena odgovarajuća analiza kako bi se osiguralo da je korištenje ove pravne osnove primjereno? Ta analiza mora pokazati da 1) postoji valjani legitimni interes, 2) da je obrada podataka striktno nužna za ostvarivanje legitimnog interesa, 3) da obrada ne šteti pravima pojedinca.

Da Ne

Prava ispitanika

Pristup osobnim podacima (Članak 15.)

Postoji li dokumentirana politika/procedura vezano uz zahtjeve ispitanika za pristupom podacima?

Da Ne

Je li vaša organizacija u stanju odgovoriti na zahtjev u roku od mjesec dana?

Da Ne

Prenosivost podataka

Jesu li uspostavljene procedure kojima se pojedincima dostavljaju njihovi osobni podaci u strukturiranom, uobičajeno korištenom i strojno čitljivom formatu?

Da Ne

Brisanje I ispravak (Članci 16. i 17.)

Postoje li kontrole i postupci koji omogućuju brisanje ili ispravljanje osobnih podataka (gdje je primjenjivo)?

Da Ne

Pravo na ograničenje obrade (Članak 18.)

Postoje li kontrole i postupci za zaustavljanje obrade osobnih podataka ako je pojedinac iz valjanih razloga zatražio ograničenje obrade?

Da Ne

Pravo na prigovor (Članak 21.)

Jesu li pojedinci upoznati o svom pravu na prigovor na određene vrste obrade kao što je izravni marketing ili kada su pravne osnove obrade legitimni interesi ili je obrada nužna za izvršavanje zadaće u javnom interesu?

Da Ne

Postoje li kontrole i postupci za zaustavljanje obrade osobnih podataka ako je pojedinac uložio prigovor na obradu?

Da Ne

Automatizirano pojedinačno donošenje odluka, uključujući izradu profila (Članak 22.)

Ako se automatizirano donošenje odluka, koje ima pravni ili značajan sličan utjecaj na pojedinca, temelji na privoli, je li prikupljena izričita privola?

Da Ne

Kada se donese automatizirana odluka koja je nužna za sklapanje ili izvršenje ugovora ili na temelju izričite privole pojedinca, jesu li uspostavljeni postupci za olakšavanje prava pojedinca na ljudsku intervenciju i osporavanje odluke?

Da Ne

Ograničenje prava ispitanika (Članak 23.)

Jesu li dokumentirane okolnosti u kojima se prava pojedinca na zaštitu podataka mogu zakonski ograničiti?

Da Ne

Točnost i pohrana

Ograničavanje svrhe

Koriste li se osobni podaci samo u svrhe za koje su izvorno prikupljeni?

Da Ne

Smanjenje količine podataka

Jesu li prikupljeni osobni podaci ograničeni na ono što je nužno za svrhe u koje se obrađuju?

Da Ne

Točnost

Jesu li uspostavljeni postupci koji osiguravaju da su osobni podaci ažurni i točni i ako je potreban ispravak, provode li se potrebne promjene bez odgađanja?

Da Ne

Pohrana

Da li se primjenjuju politike i postupci pohrane kako bi se osiguralo da se podaci ne čuvaju duže nego što je potrebno za svrhe u koje su prikupljeni?

Da Ne

Ostale pravne obveze vezane uz pohranu podataka

Podliježe li vaše poslovanje drugim pravilima koja zahtijevaju minimalno razdoblje čuvanja (npr. medicinska dokumentacija/porezna evidencija)?

Da Ne

Imate li uspostavljene postupke kako biste osigurali da se podaci sigurno unište, u skladu s vašim politikama o pohrani?

Da Ne

Umnožavanje evidencija

Jesu li uspostavljene procedure koje osiguravaju da nema nepotrebnog ili nereguliranog umnožavanja evidencija?

Da Ne

Zahtjevi vezani uz transparentnost

Transparentnost prema klijentima i zaposlenicima (Članci 12., 13. i 14.)

Jesu li klijenti/zaposlenici u potpunosti informirani o tome kako koristite njihove podatke u sažetom, transparentnom, razumljivom i lako dostupnom obliku koristeći jasan i jednostavan jezik?

Da Ne

Ako se osobni podaci prikupljaju izravno od pojedinaca, postoje li postupci za pružanje informacija navedenih u članku 13. GDPR-a?

Da Ne

Ako se osobni podaci ne prikupljaju od ispitanika već od treće strane postoje li postupci za pružanje informacija navedenih u članku 14. GDPR-a?

Da Ne

Kod interakcije s pojedincima, kao što je pružanje usluge, prodaja robe ili videonadzor, postoje li postupci za proaktivno informiranje pojedinaca o njihovim pravima iz GDPR-a?

Da Ne

Jesu li informacije o tome kako organizacija omogućava pojedincima ostvarivanje njihovih prava iz GDPR-a objavljene u lako dostupnom i čitljivom formatu?

Da Ne

Ostale obveze voditelja obrade

Ugovori s dobavljačima (Članci 27. do 29.)

Jesu li sklopljeni ugovori s dobavljačima i ostalim trećim stranama koje obrađuju osobne podatke u vaše ime koji uključuju sve odgovarajuće zahtjeve vezano za zaštitu podataka?

Da Ne

Službenik za zaštitu podataka (Članci 37. do 39.)

Trebate li imenovati službenika za zaštitu podataka prema članku 37. GDPR-a?

Da Ne

Ako smatrate da nije potrebno imenovati službenika za zaštitu podataka, jeste li dokumentirali razloge zašto to smatrate?

Da Ne

Jesu li javno objavljeni kontakt podaci službenika za zaštitu podataka kako bi zaposlenici i klijenti bili u mogućnosti stupiti u kontakt s njim? (napomena: dužni ste AZOP-u dostaviti izvješće/odluku o imenovanju službenika https://azop.hr/imenovanje-sluzbenika-za-zastitu-podataka/) ?

Da Ne

Procjena učinka na zaštitu podataka (Članak 35.)

Ako se vaša obrada podataka smatra visokorizičnom, imate li postupak za utvrđivanje potrebe i provođenje procjene učinka na zaštitu podataka? Jesu li ti postupci dokumentirani?

Da Ne

Sigurnost podataka

Odgovarajuće tehničke i organizacijske mjere (Članak 32.)

Jeste li procijenili rizike povezane s obradom osobnih podataka i poduzeli mjere za njihovo ublažavanje?

Da Ne

Postoji li dokumentirani sigurnosni program koji specificira tehničke, administrativne i fizičke mjere zaštite za osobne podatke?

Da Ne

Postoji li dokumentirani proces za rješavanje sigurnosnih pritužbi i problema?

Da Ne

Postoji li određena osoba koja je odgovorna za sprječavanje i istraživanje povreda osobnih podataka?

Da Ne

Koriste li se industrijske standardne tehnologije enkripcije za prijenos, pohranjivanje i primanje osjetljivih osobnih podataka?

Da Ne

Jesu li osobni podaci sustavno uništavani, brisani ili anonimizirani kada više ne postoji zakonska obveza za njihovo čuvanje?

Da Ne

Može li pristup osobnim podacima biti pravovremeno uspostavljen u slučaju fizičkog ili tehničkog incidenta?

Da Ne

Povreda osobnih podataka

Izvješćivanje o povredi osobnih podataka (Članci 33. i 34.)

Ima li organizacija uspostavljen plan odgovora na incidente u vezi s privatnošću i sigurnošću?

Da Ne

Revidiraju li se planovi i procedure redovito?

Da Ne

Postoje li postupci za obavještavanje tijela za zaštitu podataka o povredi podataka?

Da Ne

Postoje li postupci za obavještavanje ispitanika o povredi podataka (gdje je primjenjivo)?

Da Ne

Jesu li sve povrede podataka u potpunosti dokumentirane?

Da Ne

Postoje li postupci suradnje između voditelja obrade podataka, izvršitelja obrade, dobavljača, i drugih partnera za postupanje u vezi povreda podataka?

Da Ne

Međunarodni prijenosi osobnih podataka (izvan EGP) – ako je primjenjivo

Prijenosi osobnih podataka trećim zemljama ili međunarodnim organizacijama (Članci 44. do 50.)

Prenose li se osobni podaci izvan EGP-a, npr. u SAD ili druge zemlje?

○ Da ○ Ne

Uključuje li to posebne kategorije osobnih podataka?

○ Da ○ Ne

Koja je svrha prijenosa?

Kome je prijenos namijenjen?

Jesu li navedeni svi prijenosi - uključujući odgovore na prethodna pitanja (npr. priroda podataka, svrha obrade, iz koje se zemlje izvoze i koja zemlja prima podatke i tko je primatelj prijenosa?)

○ Da ○ Ne

Pravna osnova međunarodnih prijenosa podataka

Postoji li pravna osnova za prijenos, npr. odluka Komisije o primjerenosti; standardne ugovorne klauzule?

○ Da ○ Ne

Transparentnost

Jesu li ispitanici u potpunosti informirani o svim namjeravanim međunarodnim prijenosima njihovih osobnih podataka?

○ Da ○ Ne