Awareness raising campaign for SMEs

MJERE ZAŠTITE OSOBNIH PODATAKA

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

Awareness raising campaign for SMEs

Croatian Personal Data Protection Agency
azop
Agencija za zaštitu osobnih podataka

An Coimisiún um Chosaint Sonraí
Data Protection Commission

VUB VRIJE UNIVERSITEIT BRUSSEL

KAKO ADEKVATNO ZAŠTITITI OSOBNE PODATKE

Jedna od glavnih obveza svakog voditelja i izvršitelja obrade prema GDPR-u je osigurati odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštenih ili nezakonitih obrada osobnih podataka.

Kako bi zaštitili osobne podatke s kojima raspolažete (zaposlenika, klijenata, korisnika usluga...) dužni ste provoditi odgovarajuće **tehničke i organizacijske mjere.** Na ovaj način svest ćete mogućnost nezakonite obrade osobnih podataka i povreda osobnih podataka na minimum.

Opća uredba o zaštiti podataka ne definira koje konkretno tehničke i organizacijske mjere je potrebno poduzeti, a iste ovise o poslovnim procesima, postupcima obrade koje organizacija provodi, kategoriji osobnih podataka koje prikuplja i rizičnosti obrade. Što su osobni podaci osjetljiviji, to im treba osigurati veću razinu zaštite.

Sve organizacije (mikro, mala, srednja, velika poduzeća, tijela javne vlasti i svi ostali voditelji i izvršitelji obrade) trebaju biti svjesne važnosti ove obveze, a posebice organizacije koje prikupljaju i pohranjuju posebne kategorije osobnih podataka.

U slučaju povrede osobnih podataka i prilikom nadzornih postupanja, jedno od prvih pitanja koje će postaviti nadzorno tijelo za zaštitu podataka (Agencija za zaštitu osobnih podataka) upravo je koje su mjere poduzete kako bi se osigurala sigurnost osobnih podataka.

RAZMISLITE koje osobne podatke obrađujete. Jesu li to podaci vaših zaposlenika, klijenata, partnera?
Kako ih čuvate? Jeste li ih adekvatno zaštitili od krađe, uništenja, otkrivanja trećim osobama?

TEHNIČKE MJERE ZAŠTITE OSOBNIH PODATAKA

Tehničke mjere odnose se na zaštitne mjere koje se postavljaju na fizička mjesta te IT sustave ili proizvode.
Neka od njih su:

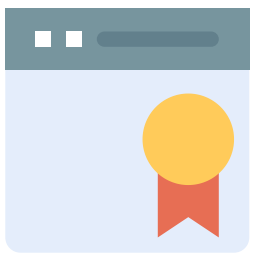
- **pseudonimizacija** obrada osobnih podataka na način da se osobni podaci ne mogu pripisati određenom pojedincu bez dodatnih informacija

- **enkripcija** je proces kodiranja informacija pohranjenih na uređaju i može dodati korisni sloj sigurnosti. Smatra se bitnom sigurnosnom mjerom kada se osobni podaci pohranjuju na prijenosnom uređaju ili prenose putem javne mreže

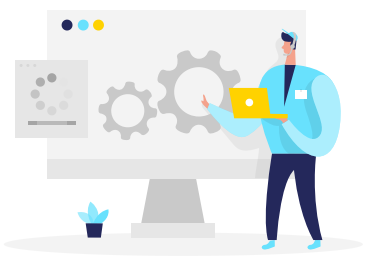
- korištenje **korisničkih imena i snažnih lozinki** za pristup računalima i računalnoj opremi. Preporuka za snažnu lozinku je: 16 ili više znakova (velika i mala slova, brojeve, simbole i interpunkciju).

- **postavljanje adekvatnih programa** na računala koji sprječavaju neovlaštene pristupe

- redovito **izrađivanje sigurnosnih kopija podataka.** Učestalost i priroda sigurnosnog kopiranja ovisi„ između ostalih čimbenika, o vrsti organizacije i prirodi podataka koji se obrađuju.



- korištenje **provjerenih/certificiranih uređaja, programa i tehničke opreme**



- redovita **nadogradnja operativnih sustava** računala, mobilnih uređaja i računalnih programa.

- Papirnata dokumentacija koja sadrži osobne podatke trebala bi se nalaziti u **zaključanim ormarićima i prostorijama, sefovima ili bi trebala biti zaštićena protuprovalnim sustavom.**

ORGANIZACIJSKE MJERE ZAŠTITE OSOBNIH PODATAKA

Organizacijske mjere zaštite odnose se na dokumentirano uređenje unutar društva/organizacije/obrta na način da se internim aktima uredi područje zaštite osobnih podataka koje obrađujete, odnosno da se, primjerice, vodi evidencija pristupa osobnim podacima (tzv. logovi) i odredi kojim osobnim podacima zaposlenici imaju pristup prilikom obavljanja svojih poslova.

Neki od takvih internih akata su:

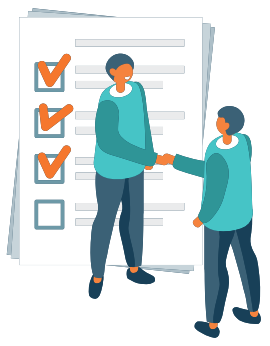
- **Pravilnik o informacijskoj sigurnosti** kojim se, između ostalog, propisuju tehničke mjere zaštite koje se primjenjuju za zaštitu podataka od neovlaštenog pristupa u poslovnom subjektu.

- **Pravilnici kojima se uređuje obrada osobnih podataka:** propisuju tko obrađuje osobne podatke, u koju svrhu, koji je pravni temelj obrade, koji je opseg osobnih podataka u obradi, tko ima pravo pristupa i obrade osobnih podataka, koliko dugo se podaci čuvaju, koje su tehničke mjere zaštite provedene za taj sustav pohrane (bazu podataka) itd.

- **U ugovornim klauzulama unutar ugovora o radu** mogu biti definirani sustavi pohrane koje će zaposlenik obrađivati i koja prava će imati za obradu tih sustava pohrane (baza podataka).

- **Izjavom o povjerljivosti** zaposlenik poslovnog subjekta ili vanjski suradnik daje pisanu izjavu da će osobne podatke obrađivati u skladu sa zakonskim odredbama o zaštiti osobnih podataka, kao i da će nad istima provoditi odgovarajuće mjere zaštite te da ih neće zlorabiti i davati neovlaštenim trećim stranama.

- **Ugovor o obradi osobnih podataka između voditelja i izvršitelja obrade**



NE ZABORAVITE: EDUKACIJA JE VAŽNA!

Ljudski faktor je najbitniji u postupku provođenja informacijske sigurnosti i zaštite podataka. Ako svi zaposlenici nemaju razvijenu svijest o važnosti informacijske sigurnosti i o zaštiti podataka, poduzete tehničke i organizacijske mjere neće biti od prevelike koristi.

Do najvećeg broja povreda osobnih podataka dolazi iz ljudske nepažnje, nemara ili neznanja. Upravo iz tog razloga važno je sve zaposlenike educirati o računalnim virusima i prijevarama (ransomware, phishing, socijalni inženjering itd.), potencijalnim rizicima od krađe, zlouporabe i gubitka osobnih podataka, pomoću kojih zaštitnih mjera se osobni podaci mogu zaštititi, kao i o posljedicama krađe, zlouporabe i gubitka osobnih podataka. Zato informirajte sebe i svoje zaposlenike!

SCAN ME

Skenirajte i pronađite još mnoštvo edukativnih materijala!

https://arc-rec-project.eu/

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