Awareness raising campaign for SMEs

KRATKI VODIČ KROZ IZVJEŠĆIVANJE O POVREDAMA OSOBNIH PODATAKA

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

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

Kratki vodič kroz izvješćivanje o povredama osobnih podataka

Ovaj je brzi vodič prvenstveno namijenjen pomaganju malim i srednjim poduzetnicima da bolje razumiju svoje obveze u vezi s zahtjevima za obavješćivanjem i komunikacijom – vezano uz obavještavanje nadležnog nadzornog tijela za zaštitu podataka, ali i komunikaciju s ispitanicima, tamo gdje je to primjenjivo.

Ključna pitanja obrađena u nastavku trebala bi dati pregled režima obavijesti o povredi osobnih podataka prema GDPR-u a kako bi pomogla malim i srednjim poduzetnicima da shvate svoje osnovne obveze prema ovom režimu.

Postoje dvije primarne obveze za male i srednje poduzetnike prema ovom režimu: (a) obavijest o bilo kojoj povredi osobnih podataka odgovarajućem nadležnom nadzornom tijelu, osim ako mogu dokazati da vjerojatno neće dovesti do rizika za ispitanike; i (b) priopćavanje te povrede ispitanicima, gdje će povreda vjerojatno rezultirati visokim rizikom za ispitanike. Od iznimne je važnosti da mali i srednji poduzetnici razumiju i ispunjavaju obje ove obveze.

Mali i srednji poduzetnici također moraju osigurati, u skladu s načelom pouzdanosti utvrđenim u članku 5. stavku 2. GDPR-a, kao i zahtjevima članka 33. stavka 5., da dokumentiraju bilo koje odnosno sve povrede osobnih podataka, uključujući činjenice koje se odnose na povrede osobnih podataka, učinke i poduzete korektivne radnje - to će im omogućiti da odgovarajućem nadležnom nadzornom tijelu dokažu usklađenost s režimom obavijesti o povredi podataka.

Preporučuje se da mali i srednji poduzetnici pročitaju detaljne smjernice o temama, uključujući definiciju povrede osobnih podataka, procjenu zahtjeva za obavješćivanjem o riziku i komunikaciji te pouzdanosti, pronađene u "Smjernicama o obavješćivanju o povredi osobnih podataka" Radne skupine za zaštitu podataka iz članka 29.[1]

Što je povreda osobnih podataka?

Povreda osobnih podataka znači povredu sigurnosti koja dovodi do slučajnog ili nezakonitog uništavanja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima[2]. Pojam "osobni podaci" znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”). Mali i srednji poduzetnici bi trebali biti svjesni da povreda osobnih podataka može obuhvatiti puno više od pukog 'gubljenja' osobnih podataka. Povrede osobnih podataka uključuju incidente koji su rezultat nezgode (poput slanja e-pošte pogrešnom primatelju), kao i namjernih radnji kao što su phishing napadi (primjerice krađa identiteta) kako bi se dobio pristup podacima kupaca).

Povreda osobnih podataka događa se u slučajevima kada se osobni podaci izgube, unište, oštete ili nezakonito otkriju. To uključuje situacije poput primjerice kada netko pristupa osobnim podacima ili ih prosljeđuje bez odgovarajućeg odobrenja ili kada se osobni podaci učine nedostupnima šifriranjem ransomware-om ili slučajnim gubitkom ili uništenjem.

Ukratko, povreda osobnih podataka sigurnosni je incident koji negativno utječe na povjerljivost, integritet ili dostupnost osobnih podataka; što znači da mali ili srednji poduzetnik nije u mogućnosti osigurati poštivanje načela koja se odnose na obradu osobnih podataka kako je

[1] Radnu skupinu iz članka 29. zamijenio je Europski odbor za zaštitu podataka (EDPB) koji je odobrio ove smjernice
[2] Vidjeti članak 4. stavak 12. GDPR-a za definiciju "povrede osobnih podataka"

navedeno u članku 5. GDPR-a. Iako su sve povrede osobnih podataka sigurnosni incidenti, nisu svi sigurnosni incidenti nužno povrede osobnih podataka.

Kada mali ili srednji poduzetnik mora obavijestiti nadležno nadzorno tijelo o povredi

Mali ili srednji poduzetnik je dužan obavijestiti nadležno nadzorno tijelo o svakoj povredi osobnih podataka koja se dogodila, osim ako je u stanju dokazati da povreda osobnih podataka 'vjerojatno neće rezultirati rizikom za prava i slobode fizičkih osoba'[3]. To znači da je zadana pozicija za male i srednje poduzetnike da se o svim povredama podataka mora obavijestiti nadležno nadzorno tijelo, osim onima za koje je poduzetnik procijenio da povreda podatakane
predstavlja rizik za ispitanike, a poduzetnik može pokazati kako je došlo do tog zaključka. U svakom slučaju, za sve povrede - čak i one koje nisu prijavljene nadzornom tijelu na temelju toga što je procijenjeno da vjerojatno neće rezultirati rizikom – mali i srednji poduzetnici moraju zabilježiti barem osnovne detalje povrede, procjenu, učinke i korake poduzete kao odgovor, kako zahtijeva članak 33. stavak 5. GDPR-a.

Kada mali ili srednji poduzetnik sazna za povredu osobnih podataka koja može rezultirati rizikom za prava i slobode ispitanika, mora obavijestiti nadležno nadzorno tijelo „bez nepotrebnog odgađanja”; gdje je to izvedivo, najkasnije u roku od 72 sata od kada je poduzetnik postao svjestan povrede. Treba smatrati da je poduzetnik "postao svjestan" kada ima razumnu razinu sigurnosti da se dogodio sigurnosni incident i da je ugrozio osobne podatke.

Kako bi ispunili svoje obveze prema članku 5. stavku 2. odnosno načelu pouzdanosti, kao i zahtjev za bilježenjem relevantnih podataka prema članku 33. stavku 5., mali i srednji poduzetnici trebali bi moći pokazati nadležnom nadzornom tijelu kada su i kako postala svjesna povrede osobnih podataka. Preporučuje se da poduzetnik, kao dio svojih internih postupaka vezanih uz povrede, uspostavi sustav za bilježenje kako i kada postaju svjesni povrede osobnih podataka i kako procjenjuju potencijalni rizik koji povreda predstavlja.

Ako mali ili srednji poduzetnik ne prijavi nadležnom nadzornom tijelu u roku od 72 sata, mora navesti razlog za odgodu, zajedno sa kasnim obavješćivanjem nadzornog tijela, i možda krši svoju obvezu da obavještava bez nepotrebnog odgađanja - osim ako navedeni razlog nije dovoljan kako bi opravdao kašnjenje. Ako nadzornom tijelu nije moguće pružiti sve relevantne informacije u roku od 72 sata, treba podnijeti početnu obavijest, a zatim se informacije mogu pružati u fazama, pod uvjetom da je to učinjeno bez nepotrebnog odgađanja i pod uvjetom da mali ili srednji poduzetnik može obrazložiti kašnjenje u skladu s člankom 33. stavkom 1.

Slično tome, prema članku 33. stavku 2. GDPR-a, izvršitelj obrade, koji obrađuje osobne podatke na temelju uputa malog ili srednjeg poduzetnika, mora bez nepotrebnog odgađanja obavijestiti poduzetnika o svakoj povredi osobnih podataka nakon što sazna za nju. To je od ključne važnosti za omogućavanje malim i srednjim poduzetnicima da ispune svoje obveze prijavljivanja. Zahtjevi za prijavljivanje povreda trebali bi također biti detaljno navedeni u ugovoru između poduzetnika i izvršitelja, kako se zahtijeva prema članku 28. GDPR-a.

[3] Vidjeti uvodnu izjavu 85. i članak 33. stavak 1. GDPR-a

Što bi trebala sadržavati obavijest nadležnom nadzornom tijelu?

Obavijest o povredi osobnih podataka od strane malog ili srednjeg poduzetnika nadležnom nadzornom tijelu mora sadržavati najmanje sljedeće:[4]

a) opisati prirodu povrede osobnih podataka, uključujući, gdje je to moguće, kategorije i približni broj ispitanika kojih se povreda tiče te kategorije i približni broj evidencija osobnih podataka;

b) priopćiti ime i kontaktne podatke službenika za zaštitu podataka (DPO) ili druge kontaktne točke gdje se mogu dobiti dodatne informacije;

c) opisati vjerojatne posljedice povrede osobnih podataka; i

d) opisati mjere poduzete ili predložene za poduzimanje od strane malog ili srednjeg poduzetnika radi rješavanja povrede osobnih podataka, uključujući, prema potrebi, mjere za ublažavanje mogućih štetnih učinaka.

Da bi se nadležnom nadzornom tijelu pomoglo u procjeni sukladnosti sa zahtjevom da se obavijesti "bez nepotrebnog odgađanja", kao i načelom pouzdanosti, preporučuje se da mali i srednji poduzetnici u početnu obavijest uključe informacije o tome kako i kada su postali svjesni povrede osobnih podataka, zajedno s objašnjenjem za svako kašnjenje, ako je primjenjivo.

Kao što je gore spomenuto, ako nije moguće istovremeno pružiti sve tražene informacije, informacije se mogu davati u fazama, sve dok se to radi bez nepotrebnog daljnjeg odgađanja.[5]

Kada mali ili srednji poduzetnik mora prijaviti povredu osobnih podataka

Mali i srednji poduzetnici također su dužni priopćiti ispitaniku povredu osobnih podataka „bez nepotrebnog odgađanja“, pri čemu će ta povreda osobnih podataka „vjerojatno rezultirati velikim rizikom za prava i slobode fizičke osobe“.[6]

Ova je obveza dodatna i odvojena od obveze obavještavanja nadležnog nadzornog tijela o povredama osobnih podataka i postavlja viši prag prije nego što se primijeni obveza obavještavanja ispitanika. Namjera ovog zahtjeva je osigurati da ispitanici mogu poduzeti potrebne mjere predostrožnosti tamo gdje su se dogodili incidenti koji će vjerojatno za njih rezultirati visokim rizikom.

Takve komunikacije s ispitanicima trebaju se izvršiti bez odgađanja, prema potrebi, u uskoj suradnji s nadležnim nadzornim tijelom. U slučajevima kada postoji potreba za ublažavanjem neposrednog rizika za ispitanike bit će potrebna brza komunikacija s njima.

Postoje, međutim, okolnosti u kojima se od malih i srednjih poduzetnika možda neće tražiti da prenose informacije koje se odnose na povredu podataka ispitanicima, čak i kad bi povreda mogla rezultirati visokim rizikom za prava i slobode fizičke osobe. Ove okolnosti postoje kada je ispunjen bilo koji od sljedećih uvjeta:[7]

[4] Vidjeti članak 33. stavak 3. GDPR-a
[5] Vidjeti članak 33. stavak 4. GDPR-a
[6] Vidjeti uvodnu izjavu 86 i članak 34. Stavak 1. GDPR-a
[7] Vidjeti članak 34. stavak 3. GDPR-a

a) Mali ili srednji poduzetnik je primijenio odgovarajuće tehničke i organizacijske mjere zaštite, a te su mjere primijenjene na osobne podatke na koje utječe povreda osobnih podataka, posebno mjere zbog kojih osobni podaci postaju nerazumljivi bilo kojoj osobi koja nije
ovlaštena pristupiti im, poput enkripcije;

b) Mali ili srednji poduzetnik je poduzeo naknadne mjere kojima se osigurava da se više vjerojatno neće ostvariti visoki rizik za prava i slobode ispitanika;

ili

c) Gdje bi bio potreban nesrazmjeran napor. U takvom slučaju, međutim, mali i srednji poduzetnici i dalje moraju putem javne komunikacije ili slične mjere osigurati da su ispitanici informirani na jednako učinkovit način.

Što treba sadržavati komunikacija s ispitanikom?

Komunikacija povrede osobnih podataka pogođenom ispitaniku (-icima) podataka treba opisati prirodu povrede osobnih podataka, kao i preporuke dotičnom ispitaniku za ublažavanje
potencijalnih štetnih učinaka povrede.

Ova komunikacija ispitaniku trebala bi jasnim i jednostavnim jezikom opisati prirodu povrede osobnih podataka i trebala bi sadržavati najmanje sljedeće podatke (kako zahtijeva članak 34. stavak 2. GDPR-a):

- ime i kontakt službenika za zaštitu podataka ili druge kontakt točke gdje se mogu dobiti dodatne informacije;
- opis vjerojatnih posljedica povrede osobnih podataka; i
- opis mjera poduzetih ili predloženih za poduzimanje od strane malih i srednjih poduzetnika radi rješavanja povrede osobnih podataka, uključujući, prema potrebi, mjere za ublažavanje mogućih štetnih učinaka.

Mogu li mali i srednji poduzetnici obavijestiti ispitanike o povredi čak i ako rizik nije procijenjen kao visok?

Iako mali i srednji poduzetnici nisu obvezni prijaviti povredu osobnih podataka pogođenim ispitanicima za koje nije vjerojatno da će rezultirati visokim rizikom za njih, poduzetnici ipak mogu slobodno priopćiti povredu osobnih podataka tamo gdje je to još uvijek u njihovom
interesu ili gdje je prikladno to učiniti u svakom slučaju, u kontekstu te određene povrede.