Awareness raising campaign for SMEs

Kratki vodič za načela zaštite podataka

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.

Kratki vodič za načela zaštite podataka

Načela - široka pravila o ponašanju ili željenim ishodima - važan su dio propisa o zaštiti podataka i zapravo su srž Opće uredbe o zaštiti podataka (GDPR). Iako se razna načela mogu naći u GDPR-u, članak 5. GDPR-a posebno utvrđuje sedam ključnih načela povezanih s obradom osobnih podataka, s kojima mali i srednji poduzetnici (poduzetnik je voditelj obrade jer odlučuje kako i zašto se podaci obrađuju) moraju biti upoznati i pridržavati ih se prilikom prikupljanja i obrade osobnih podataka:

- Zakonitost, poštenost i transparentnost;
- Ograničavanje svrhe;
- Smanjenje količine podataka;
- Točnost;
- Ograničenje pohrane;
- Cjelovitost i povjerljivost; i
- Pouzdanost.

Ta su načela navedena na samom početku GDPR-a i informiraju i prožimaju sve ostale odredbe navedenog propisa. Treba ih razumjeti kao temeljna sveobuhvatna načela kojima je cilj osigurati poštivanje duha propisa o zaštiti podataka i zaštite prava pojedinaca („ispitanika“).

U uvodnim izjavama GDPR-a napominje se da mnoga od ovih načela nisu posve nova i da su načela navedena u prethodnoj Direktivi o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (95/46 / EZ) u velikoj mjeri prenesena ili nadograđena. Postoje i druga srodna pravila i elementi gore navedenih načela koji se spominju tijekom cijele Opće uredbe, poput načela proporcionalnosti i nužnosti, te načela tehničke i integrirane zaštite podataka. Detaljnije o tim elementima možete pronaći u nastavku.

Usklađenost s načelima zaštite podataka prvi je i možda najvažniji korak koji mali i srednji poduzetnici mogu poduzeti kako bi osigurali da udovoljavaju zahtjevima GDPR-a i propisa o zaštiti podataka općenito; međutim, mali i srednji poduzetnici također bi se trebali savjetovati s odredbama GDPR-a koje detaljno razrađuju kako ta načela utječu na određene obveze.

Mali i srednji poduzetnici bi trebali primijetiti da se vrlo slična načela zaštite podataka primjenjuju u slučajevima kada se osobni podaci obrađuju u ‘svrhe provođenja zakona’ prema Direktivi o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka.

Zakonitost, poštenost i transparentnost

Osobni podaci moraju se obrađivati zakonito, pošteno i na transparentan način u odnosu na ispitanika.

Zakonitost znači da svaka obrada osobnih podataka koju provodi mali ili srednji poduzetnik mora imati pravnu osnovu prema GDPR-u, te biti u skladu sa zahtjevima GDPR-a (vidjeti posebno Članci 6., 7., 8. i 9. GDPR-a), i da ne uključuje bilo kakvu nezakonitu obradu ili upotrebu osobnih podataka.

Poštenost je također relativno široko načelo koje zahtijeva da svaka obrada osobnih podataka mora biti poštena prema pojedincu čiji su osobni podaci u pitanju i izbjegavati neprimjerenu štetu, neočekivano i obmanjujuće.

Transparentnost je posebno važno načelo zaštite podataka u GDPR-u, s različitim srodnim pravima i obvezama kojima se nastoji osigurati da obrada osobnih podataka bude jasna i transparentna za pojedince i voditelje obrade. Mali i srednji poduzetnici moraju pojedincima pružiti informacije u vezi s obradom njihovih osobnih podataka u formatu koji je sažet, lako dostupan, lako razumljiv i na jasnom i jednostavnom jeziku. To bi trebalo učiniti prije prikupljanja osobnih podataka i naknadno kad god se naprave promjene u postupku obrade.

Posebna pravila u vezi s obvezama transparentnosti nalaze se u člancima 12., 13. i 14. GDPR-a, uključujući detalje o određenim vrstama informacija koje se moraju pružiti ispitanicima i načinu na koji se moraju pružiti. Kako bi bili transparentni, mali i srednji poduzetnici moraju osigurati da način prenošenja informacija odgovara njihovoj platformi i ciljanoj publici. Načela poštene i transparentne obrade zahtijevaju da se pojedinac obavijesti o postojanju postupka obrade i njegovim svrhama.

Ograničavanje svrhe

Osobni podaci moraju se prikupljati u posebne, izričite i zakonite svrhe, koje su utvrđene u vrijeme prikupljanja osobnih podataka, i ne smiju se dalje obrađivati na način koji je nespojiv s tim svrhama. Međutim, mala i srednja poduzeća mogu poduzeti daljnju obradu u svrhe arhiviranja u javni interes, znanstvene ili povijesne istraživačke svrhe ili statističke svrhe, jer se ne smatraju nekompatibilnima s početnim svrhama, ako postoje dovoljne zaštitne mjere.

Daljnja obrada prikladna je samo ako nova svrha obrade nije nespojiva s izvornom svrhom. Hoće li bilo koja naknadna obrada biti kompatibilna s izvornom svrhom, ovisit će o bilo kojoj vezi s izvornom svrhom, kontekstom u kojem su prikupljeni osobni podaci, priroda osobnih podataka, moguće posljedice namjeravane daljnje obrade za pojedince, i postojanje odgovarajućih zaštitnih mjera.

Svrha ovog načela je osigurati da mali i srednji poduzetnici od samog početka budu jasni i otvoreni o predloženoj obradi osobnih podataka te osigurati da su svrhe u skladu s razumnim očekivanjima pojedinaca. Pažljivo razmatranje i robusno poštivanje ovog načela također pomaže malim i srednjim poduzetnicima u načelima smanjenja količine podataka i pouzdanosti.

Smanjenje količine podataka

Ovo načelo zahtijeva da mali i srednji poduzetnici prikupljaju i obrađuju samo osobne podatke koji su primjereni, relevantni i ograničeni na ono što je nužno za svrhe u koje se obrađuju. To u osnovi znači da bi poduzetnici trebali prikupiti minimalnu količinu podataka koja im je potrebna za njihov planirani postupak obrade; nikada ne bi smjeli prikupljati nepotrebne osobne podatke. Ovo načelo nadopunjuje, posebno, načelo ograničavanja svrhe, ali također podržava poštivanje niza načela zaštite podataka.

Primjena smanjenja količine podataka podržava tehničku i integriranu zaštitu podataka, ograničava količinu osobnih podataka koji bi se mogli izgubiti ili ukrasti u slučaju povrede

osobnih podataka, pomažući u osiguravanju cjelovitosti i povjerljivosti osobnih podataka, a to olakšava poduzetnicima kako bi osigurali da su osobni podaci koje posjeduju točni i ažurirani, podržavajući poštivanje načela točnosti.

GDPR ne definira koja je količina osobnih podataka 'primjerena, relevantna i ograničena'. To će mali i srednji poduzetnici morati procijeniti ovisno o okolnostima njihovih namjeravanih obrada. Poduzetnici bi također trebali povremeno pregledavati količinu i prirodu osobnih podataka koje obrađuju, osiguravajući da ostanu primjereni, relevantni i potrebni, uključujući brisanjem podataka koji više ne ispunjavaju ove kriterije.

Točnost

Ovo načelo zahtijeva da mali i srednji poduzetnici osiguraju da su osobni podaci točni i da se, po potrebi, ažuriraju. Poduzetnici bi trebali poduzeti sve razumne korake kako bi osiguralo da se osobni podaci koji nisu točni brišu ili ispravljaju bez odgađanja, uzimajući u obzir svrhe u koje se obrađuju.

To je izravni zahtjev da svi osobni podaci koje poduzetnik prikuplja, pohranjuje ili na neki drugi način obrađuje moraju biti točni i ažurirani. Moraju se poduzeti svi razumni koraci kako bi se sve netočnosti odmah ispravile, uključujući razmatranje je li potrebno povremeno ažurirati bilo kakve osobne podatke koje poduzetnik posjeduje. Mali i srednji poduzetnici koji prikupljaju osobne podatke trebali bi imati jasne postupke za ispravljanje ili brisanje bilo kakvih netočnih osobnih podataka kao dio svojih aktivnosti upravljanja podacima.

Općenito, razumni koraci koje mali i srednji poduzetnici trebaju poduzeti kako bi se osigurala točnost osobnih podataka ovisit će o okolnostima, a posebno o prirodi osobnih podataka i obrade. Oni također moraju imati na umu svoje obveze u vezi s pravom ispitanika na ispravak - ispraviti ili popuniti netočne osobne podatke ako su nepotpuni.

Ograničenje pohrane

Mali i srednji poduzetnici moraju posjedovati osobne podatke u obliku koji dopušta identifikaciju pojedinaca najdulje onoliko koliko je potrebno za svrhe u koje se osobni podaci obrađuju. Osobni podaci mogu se čuvati dulje vrijeme onda kada će se osobni podaci obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s GDPR-om, i dok postoje odgovarajuće tehničke i organizacijske mjere radi zaštite prava i sloboda pojedinca.

Stoga bi mali i srednji poduzetnici trebali općenito brisati osobne podatke čim prestanu biti potrebni za svrhe za koje su izvorno prikupljeni. U tu svrhu, GDPR preporučuje da poduzetnik utvrdi vremenske rokove za brisanje ili za povremeni pregled. U skladu s načelom transparentnosti, mala i srednja poduzeća također bi trebala osigurati da pojedinci budu svjesni razdoblja pohrane ili kriterija korištenih za njihovo izračunavanje. Mali i srednji poduzetnici, čak i za osobne podatke koje pohranjuju izvan mreže (offline) ili u ručnom obliku u sustavu arhiviranja ako su digitalne verzije ili kopije izbrisane, i dalje moraju imati obrazloženja za zadržavanje ovih osobnih podataka u izvanmrežnom obliku i odgovarati na zahtjeve ispitanika.

Ovisno o okolnostima, možda će biti prikladno da mali i srednji poduzetnici anonimiziraju podatke kada više nije potrebno da se pojedinac može identificirati. Podaci su uistinu anonimni i stoga više nisu ‘osobni’ podaci, samo ako se pojedinac više ne može identificirati; međutim, ako bi se podaci i dalje mogli pripisivati pojedincu korištenjem dodatnih podataka, bili bi samo 'pseudonimizirani' i stoga se i dalje smatraju osobnim podacima. Ako postupak koji se primjenjuje na navodno anonimiziranje osobnih podataka nije trajan i može se poništiti, tada podaci nisu anonimizirani.

Cjelovitost i povjerljivost

Mali i srednji poduzetnici moraju obrađivati osobne podatke samo na način koji osigurava odgovarajuću razinu cjelovitosti i povjerljivosti osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade i od slučajnog gubitka, uništenja ili oštećenja. Da bi postigli taj cilj, moraju koristiti odgovarajuće tehničke ili organizacijske mjere.

Drugim riječima, mali i srednji poduzetnici moraju osigurati da njihove sigurnosne mjere na odgovarajući način štite od slučajne ili namjerne štete, gubitka ili širenja osobnih podataka koje obrađuju. Ove sigurnosne mjere trebale bi obuhvaćati ne samo kibernetičku sigurnost već i fizičke i organizacijske mjere sigurnosti. Poduzetnici također moraju rutinski provjeravati jesu li njihove sigurnosne mjere suvremene i učinkovite.

GDPR ne navodi izričito sigurnosne mjere koje bi mali i srednji poduzetnici trebali provoditi, jer se najbolja tehnološka i organizacijska praksa neprestano razvija. Poduzetnici bi trebali razmotriti niz mogućnosti za određivanje najprikladnijih mjera u datim okolnostima, jer ne postoji pristup "jednog rješenja za sve" sigurnosti podataka. Relevantna razmatranja prilikom procjene odgovarajućih mjera uključuju, ali nisu ograničena na: načelo smanjenja količine podataka; načela tehničke i integrirane zaštite podataka; transparentnost s obzirom na funkcije i obradu osobnih podataka, omogućujući pojedincu nadzor obrade podataka; te pseudonimizacija i / ili enkripcija osobnih podataka.

Pouzdanost

Načelo pouzdanosti novo je načelo propisa o zaštiti podataka, koje posebno utvrđuje da su mali i srednji poduzetnici odgovorni za ostala načela zaštite podataka i moraju biti u mogućnosti to dokazati. To znači da moraju osigurati da se pridržavaju načela, ali također moraju imati odgovarajuće procese i evidencije kako bi dokazali usklađenost.

Usklađenost s ostalim načelima zaštite podataka sama će pomoći u pouzdanosti, kao što je pristup tehničke i integrirane zaštite podataka, provedba odgovarajućih tehničkih i organizacijskih mjera, sažeti dostupni podaci o transparentnosti i jasne politike zadržavanja podataka. Ostale mjere za dokazivanje poštivanja načela zaštite podataka uključuju usvajanje internih politika, poštivanje kodeksa ponašanja ili postupaka certificiranja, bilježenje i, ako je potrebno, prijavljivanje povreda osobnih podataka te provedbu odgovarajućih politika i obavijesti o privatnosti.

Imenovanje službenika za zaštitu podataka (DPO), gdje je nužno, i osiguravanje da su pravilno uključeni u sva pitanja koja se odnose na zaštitu podataka, vođenje evidencije o aktivnostima obrade, sastavljanje jasnih ugovora s izvršiteljima obrade koji djeluju u ime malih i srednjih

poduzetnika i provođenje procjene učinka (DPIA), gdje je to prikladno, samo su neki od alata koji mogu pomoći malim i srednjim poduzetnicima u poštivanju načela pouzdanosti. Obveze po načelu pouzdanosti su u neprestano u tijeku i razvijaju se, a mala i srednja poduzeća trebala bi kontinuirano pregledavati i ažurirati svoje mjere za osiguravanje pouzdanosti.