Awareness raising campaign for SMEs

OSNOVE ZAŠTITE 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.

Kada se primjenjuju propisi o zaštiti podataka i što sve obuhvaćaju?

Propisi o zaštiti podataka pokrivaju većinu situacija u kojima podatke o pojedincu („osobni podaci“ „ispitanika“) na određeni način koristi („obrađuje“) neka druga osoba ili mali ili srednji poduzetnik (voditelj obrade), osim u izričito osobnom kontekstu.

Tijela za zaštitu podataka su u svakoj državi članici odgovorna za reguliranje propisa koji pokrivaju različite načine i okolnosti u kojima se osobni podaci mogu obrađivati.

„Opća uredba o zaštiti podataka “(GDPR) je propis koji se primjenjuje na većinu vrsta obrade osobnih podataka. Primjenjuje se u cijeloj EU, zajedno s daljnjim nacionalnim pravilima utvrđenim u svakoj pojedinoj državi članici.

Međutim, GDPR se ne odnosi na obradu osobnih podataka od strane pojedinca za ‘isključivo osobne ili kućne’ aktivnosti, bez poveznice s profesionalnom ili komercijalnom djelatnosti. To je poznato i kao „izuzeće za osobno /kućanstvo / domaćinstvo“.Tobi moglo obuhvaćati aktivnosti poput dopisivanja, vođenja adresara ili određenih društvenih mreža, gdje su te aktivnosti isključivo osobne naravi. GDPR bi se i dalje primjenjivao na male i srednje poduzetnike koji obrađuju osobne podatke kako bi olakšali ove aktivnosti(poput vođenja društvenihmreža).

Ako se obrada odvija u svrhu provođenja zakona (kao što je sprječavanje ili otkrivanje kriminala), GDPR se ne primjenjuje, već Direktiva o zaštiti pojedinaca u vezi s obradomosobnih podatakaod strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka koja pokriva te situacije.

Ako ispitanik ima sumnju odnosno brigu da mali ili srednji poduzetnik nije poštivao zakon ili nije podržao njegova prava, mnogi (a) podnose zahtjev poduzetniku ili (b) podnose pritužbu tijelu za zaštitu podataka, ako mali ili srednji poduzetnik ne udovoljava zahtjevu ili svojim obvezama prema propisima o zaštiti podataka.

Što su ‘osobni podaci’ i kada se ‘obrađuju’?

Osobni podaci u osnovi znače svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”). Osobni podaci mogu obuhvaćati razne vrste podataka, kao što su ime, datum rođenja, adresa e-pošte, telefonski broj, adresa, fizičke karakteristike ili podaci o lokaciji - kad je jasno na koga se ti podaci odnose ili je moguće saznati.

Osobni podaci ne moraju biti u pisanom obliku, oni također mogu biti informacije o tome kako ispitanik izgleda ili zvuči, na primjer fotografije ili audio ili video snimke, ali propis o zaštiti podataka primjenjuje se samo tamo gdje se ti podaci obrađuju 'automatizirano' "(elektronički) ili kao dio neke druge vrste sustava pohrane.

Osobni podaci mogu biti informacije gdje je ispitanik identificiran - "Johnova omiljena boja je plava"- ili gdje ih je"moguće prepoznati"-"Omiljena boja Johnove sestre je plava"(gdje ne znate identitet njegove sestre,ali bistemogli pronaći koristeći kontekst i/ili dodatne informacije).

Čak i ako su osobni podaci djelomično anonimizirani ili 'pseudonimizirani', ali to bi se moglo poništiti i ispitanik bi se mogao identificirati pomoću dodatnih podataka, i dalje bi ih se trebalo

smatrati osobnim podacima.Međutim, ako su podaci uistinu anonimni, nepovratno i ne mogu se koristiti do identifikacije osobe, ne smatraju se osobnim podacima.

Da bi se utvrdilo je li neka osoba „prepoznatljiva“, posebno ako su podaci o toj osobi pseudonimizirani, sve metode i informacije za koje postoji vjerojatnost da će ih mali ili srednji poduzetnik (voditelj obrade podataka) ili druga osoba upotrijebiti za identifikaciju pojedinca, bilo izravno ili neizravno, moraju se uzeti u obzir.

Određene vrste osjetljivih osobnih podataka, nazvane "posebne kategorije", podliježu dodatnoj zaštiti prema GDPR-u, a njihova je obrada općenito zabranjena, osimtamogdje su zadovoljeni posebni zahtjevi (kao što je izričita privola), kao što je detaljno izloženo u članku 9. GDPR-a.
Posebne su kategorije: osobni 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.

Propis o zaštiti podataka uređuje situacije u kojima se osobni podaci ‘obrađuju’. Obrada u osnovi znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvimakao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje. Iako se, kao što je gore spomenuto, propis o zaštiti podataka ne primjenjuje tamo gdje se to radi isključivo za osobne ili kućanske djelatnosti.

Što je ‘voditelj obrade’ i koje su njegove obveze?

‘Voditelj obrade’ se odnosi na osobu, tvrtku (npr. mali ili srednji poduzetnik) ili drugo tijelo koje odlučuje kako i zašto se obrađuju osobni podaci ispitanika. Ako dvije ili više osoba ili entiteta odluče kako i zašto se osobni podaci obrađuju, oni mogu biti ‘zajedničkivoditelji’ i oboje bi dijelili odgovornost za obveze u vezi obrade podataka.

‘Izvršitelj’ se odnosi na osobu, tvrtku ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade. Oni ne odlučuju kako izašto će se obradaodvijati,već izvršavaju obradu po nalogu voditelja obrade.

Kao što je gore spomenuto, ako osoba (ali ne tvrtka ili drugo tijelo) odluči kako i zašto se osobni podaci obrađuju i/ili obrađuju te podatke, ali to čine samou osobnomsvojstvu ilisvojstvu kućanstva, neće biti predmet obveza voditelja obrade prema GDPR-u.

Mali ili srednji poduzetnici imaju niz obveza prema propisima o zaštiti podataka, a posebno se moraju pridržavati načela zaštite podataka, a koja su propisana u članku 5. GDPR-a, osiguravajući da se osobni podaci: obrađuju zakonito, pošteno i transparentno; obrađuju u posebne svrhe; ograničeni na ono što je nužno; održavaju se preciznim i ažuriranim; ne čuvaju se duže nego što je potrebno; I zaštićeni od neovlaštene ili nezakonite obrade, slučajnog gubitka, uništenja ili oštećenja. Mali ili srednji poduzetnici također moraju biti sposobni dokazati usklađenost s tim načelima, prema načelupouzdanosti.

Prema načelu transparentnosti, mali ili srednji poduzetnici (voditelji obrade) trebali bi pružiti određene podatke ispitanicima kada prikupljaju njihove osobne podatke, kao što su: identitet voditelja obrade; kontaktne podatke voditelja i (ako ga imaju) svog 'službenika za zaštitu podataka'(DPO); svrhe i „pravna osnova" za obradu; s kime će se dijeliti podaci; Koliko dugo će se podaci pohranjivati; i postojanje različitih prava ispitanika.

Što se podrazumijeva pod 'pravnom osnovom' za obradu osobnih podataka?

Prema terminologiji zaštite podataka, "pravna osnova" (koja se naziva i "zakonska osnova" ili "pravni temelj") znači pravno opravdanje za obradu osobnih podataka. Važeća pravna osnova potrebna je u svim slučajevima u kojima se osobni podaci ispitanika trebaju zakonito obrađivati u skladu sa propisom o zaštiti podataka.

Prema GDPR-u postoji šest mogućih pravnih osnova za obradu osobnih podataka, pronađenih u članku 6., i to: privola; ugovorna nužnost; poštivanje zakonske obveze; zaštita životno važnih interesa; izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade; i legitimni interesi (gdje interes nije nadjačan interesom ispitanika).

Na ovom popisu nepostojihijerarhija nitipreferirana opcija,već bi se sva obrada osobnih podataka trebala temeljiti na pravnoj osnovi koja je najprikladnija u posebnim okolnostimate obrade. Mali ili srednji poduzetnici trebaju biti svjesni da mogu postojati različite pravne osnove primjenjive na različite vrste obrade istih osobnih podataka.

Važno je napomenuti da „privola", iako možda najpoznatija, nije jedina pravna osnova za obradu osobnih podataka - niti čak najprikladnija u mnogim slučajevima. Tamo gdje se koristi privola, postoji niz posebnih zahtjeva da bi se osigurala valjana pravna osnova za obradu; mora biti specifična, informirana i nedvosmislena i mora se slobodno odnosno dobrovoljno dati. Uvijek mora biti moguće povući privolu nakon što je dana; nakon što je povučena,osobni se podaci ne mogu dalje obrađivati na temelju privole.

Kaošto je gorespomenuto,premaGDPR-u, određene posebne kategorije osobnih podataka ne bi se trebale obrađivati, osim u ograničenim okolnostima. Za takvu obradu potrebna je pravna osnova prema članku 6. GDPR-a, kao i ispunjavanje jedne od iznimki iz članka 9. (poput izričite privole ili zaštite životno važnih interesa)koji omogućuju obradu takvih podataka.

Odgovornost je svakog malog i srednjeg poduzetnika da utvrdi na koju se pravnu osnovu oslanja za svakuvrstuobradeosobnihpodatakaukoje se uključuje. Te podatke treba pružiti ispitanicima, kao dio načela transparentnosti, a mala i srednja poduzeća uvijek trebaju biti sposobna identificirati pravnu osnovu na koju se oslanjaju u obradi ako to zatraži ispitanik ili nadležno nadzorno tijelo.

Koja prava imaju ispitanici i kako ih mogu ostvariti?

Pojedinci imaju niz specifičnih prava prema propisima o zaštiti podataka kako bi bili informirani i kontrolirali obradu svojih osobnih podataka. Ta se prava najčešće ostvaruju u skladu s GDPR-om (u člancima 12-22 i 34).

PravaispitanikapremaGDPR-u uključuju: pravo na informiranje ako, kako izašto se njihovi podaci obrađuju;parvo na pristup i dobivanje kopije njihovih podataka; pravo na ispravakili

dopunu podataka ako su netočni ili nepotpuni; pravo na brisanje podataka; parvo ograničenja načina na koji se podaci koriste; pravo na prenosivost podataka;pravo na prigovor na obradu podataka; i pravo da se na ispitanika ne odnosi odluka koja se temelji isključivona automatiziranoj obradi.

Informacije koje se daju ispitanicima prilikom ostvarivanja ovih prava moraju biti transparentne, razumljive i lako dostupne, koristeći jasan i jednostavan jezik. Informacije treba pružiti u pisanom obliku ili na drugi način,uključujući, gdje je moguće, elektroničkimputem. Na zahtjev ispitanika
podaci se mogu pružiti usmeno, pod uvjetom da je identitet ispitanika jasan ili se može dokazati.

Važno je napomenuti da ta prava nisu apsolutna i podliježu brojnim ograničenjima. Određena prava primjenjuju se na sve aktivnosti obrade, poput prava na informacije ili pristup osobnim podacima, dok se druga prava primjenjuju samo u određenim okolnostima, poput prava na
brisanje, ograničenje, prijenos i prigovor. GDPR postavlja ograničenja tih prava.

Kada se osobni podaci obrađuju za provedbu Direktive o zaštiti pojedinaca u vezi s obradom osobnih podataka od stranenadležnihtijelau svrhesprečavanja,istrage,otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka, ispitanici imaju slična prava koja podliježu nizu ograničenja. Ta prava uključuju pravo na informacije, pravo pristupa i pravo na ispravak, brisanje i ograničenje.

Da bi ostvarili bilo koje od ovih prava na zaštitu podataka, ispitanici trebaju prvo podnijeti zahtjev voditelju obrade (malom ili srednjem poduzetniku). Ako poduzetnik ne odgovori ili ne dopusti da ispitanik izvršava svojaprava, ispitanici tada mogu kontaktirati nadležno nadzorno tijelo radi
podnošenja pritužbe.

Kada je dozvoljen izravni marketing elektroničkim putem?

Izravni elektronički marketing uključuje slanje ili stvaranje neželjenih marketinških komunikacija sa primateljem, uključujući e-poštom, tekstualnomporukom, telefonomilifaksom. Te se komunikacije obično izrađuju u svrhu oglašavanja proizvoda ili usluge ili u druge promotivne svrhe. Takav elektronički izravni marketing podliježe posebnim pravilima utvrđenim u propisima o e-privatnosti.

Prema propisima o e-privatnosti, mali ili srednji poduzetnik ili osoba u čije se ime šalju izravne marketinške komunikacije moraju općenito dobiti prethodnu privolu primatelja koji se slaže s primanjem takvih komunikacija –i moraju biti u mogućnosti dokazati da se primatelj unaprijed aktivno dogovorio za primanje takvih komunikacija. Privola mora biti jasna, potvrdna radnja, slobodno data, informirana i nedvosmislena, kako zahtijevaGDPR(ova dva propisa u takvim
Slučajevima djeluju zajedno).Ako je dana privola za marketing, ona se može povući u bilo kojem trenutku.

GDPR napominje da šutnja, prethodno označene kućice ili neaktivnost uglavnom neće biti dovoljni da označe privolu. To znači da se prodavač ne može, na primjer, osloniti na primatelja koji nije odznačio unaprijed označeni okvir kao valjani oblik privole. Svaka poruka izravnog marketinga poslana e-poštom ili tekstom također treba identificirati pošiljatelja ili u čije ime se šalje i navesti valjanu adresu kako bi primatelj mogao zatražiti da slanje takvih poruka prestane.

Postoje određene iznimke kada se elektroničke komunikacije izravnog marketinga mogu slati bez prethodne privole primatelja. Na primjer, mala i srednja poduzeća mogu svojim klijentima slati elektroničke poruke izravnog marketinga bez izričite privole, ali samo ako; su prikupili podatke za kontakt tijekom prodaje proizvoda ili usluge; oni prodaju vlastiti proizvod ili uslugu; to je proizvod ili usluga sličan originalnoj prodaji; prva marketinška poruka poslana je u roku od 12 mjeseci od originalne prodaje; i, što je najvažnije, ispitanik je dobio priliku da se usprotivi primanju marketinških poruka, kako u vrijeme originalne prodaje, tako i sa svakom sljedećom marketinškom porukom.

Prema GDPR-u (članak21.), pojedinci također imaju pravo u bilo kojem trenutku prigovoriti da se njihovi osobni podaci koriste u svrhe izravnog marketinga. To uključuje ne samo elektronički izravni marketing već i poštanski i druge oblike izravnog marketinga. Ako se uloži takav prigovor, mali ili srednji poduzetnik mora prestati koristiti njihove osobne podatke za izravni marketing; to uključuje brisanje iz bilo koje marketinške baze podataka.

Koja su pravila u vezi s upotrebom kolačića na web mjestima?

Kolačići su obično male tekstualne datoteke pohranjene na uređaju, poput računala, mobilnog uređaja ili bilo kojeg drugog uređaja koji može pohraniti podatke. Uređaji koji mogu koristiti kolačiće uključuju i takozvane uređaje 'Internet stvari – IoT (Internet of things)' koji se povezuju s internetom.

Kolačići služe brojnim važnim funkcijama, uključujući pamćenje korisnika i njegove prethodne interakcije s web stranicom. Mogu se koristiti, na primjer, za praćenje predmeta u mrežnoj košarici iliza praćenjepodatakakada unositedetalje u internetski obrazac za prijavu. Kolačići za autentifikaciju također su važni za identificiranje korisnika kada se prijave na bankarske usluge i druge internetske usluge. Određeni kolačići također se koriste za brže učitavanje web stranica i za usmjeravanje podataka putem mreže.

Podaci pohranjeni u kolačićima mogu uključivati osobne podatke, poput IP adrese, korisničkog imena, jedinstvenog identifikatora ili adrese e-pošte. Ali mogu sadržavati i neosobne podatke kao što su postavke jezika ili informacije o vrsti uređaja koji osoba koristi za pregledavanje web stranice. Oglasni ID-ovi, korisnički ID-ovi i drugi ID-ovi za praćenje mogu također biti sadržani u kolačićima.

Kolačići mogu biti kolačići prve ili treće strane. Općenito, kolačić koji je postavila vaša web lokacija, tj. domena domaćina, kolačić je prve strane. Kolačić treće strane je onaj koji postavlja druga domena od one koju korisnikposjećuje, tj. Domena koja nije onakojumogu vidjeti u svojoj adresnoj traci. Takvi se kolačići mogu povezati s oglašavanjem ili dodacima za društvene medije

koje omogućuje voditelj web stranice, na primjer u obliku gumba "sviđamise" ili alata za dijeljenje.

Kolačići također mogu imati datum isteka. Na primjer, kolačići sesije, koji su dizajnirani da funkcioniraju samo tijekom trajanja sesije preglednika ili nešto dulje, vjerojatno će imati vrlo kratak životni vijek ili datum isteka i bit će postavljeni da isteču nakon što odsluže svoju ograničenu svrhu. Datum isteka kolačića trebao bi biti proporcionalan njegovoj namjeni. Stoga kolačićsesije koji se koristi za funkciju popuput pamćenja podataka u košarici ili korisnikovih podataka o putovanju za jedno putovanje ne bi trebao imati neodređeni datum isteka i trebao bi biti postavljen da istječe nakon što je odslužio svoju funkciju ili ubrzo nakon toga .

Propisi o e-privatnosti zahtijevaju da pribavite privolu za dobivanje bilo kakvog pristupa informacijama pohranjenim u terminalnoj opremi pretplatnika ili korisnika ili za pohranu bilo kakvih podataka na uređaju te osobe. To znači da morate dobiti privolu za pohranu ili postavljanje kolačića, bez obzira sadrže li kolačići ili druge tehnologije praćenja koje upotrebljavate osobne podatke.

Kao voditelj obrade potencijalno upotrebljavate kolačiće u analitičke svrhe ili u svrhu marketinga, ciljanja ili profiliranja i možete ih dodijeliti određenim kategorijama kada pružate informacije korisnicima na vašoj web stranici. Međutim, bez obzira na to kako ste ih odlučili kategorizirati, kolačići koji ne udovoljavaju jednom od dva specifična slučaja korištenja u propisima o e-privatnosti i zbog kojih su izuzeti od potrebe za dobivanjem privole ne smiju se postavljati niti primjenjivati na korisnikovom uređaju prije nego što nabavite njihovu privolu. Ta su dva izuzeća poznata kao **a)** izuzeće od komunikacija i b) strogo neophodno izuzeće.

a) Izuzeće od komunikacija. To se odnosi na kolačiće čija je jedina svrha obavljanje prijenosa komunikacije putem mreže, na primjer identificiranje krajnjih točaka komunikacije. To se također može odnositi na kolačiće koji se koriste za omogućavanje razmjene stavki podataka prema željenom redoslijedu, tj. Numeriranjem podatkovnih paketa. Također se odnosi na kolačiće koji se koriste za otkrivanje pogrešaka u prijenosu ili gubitka podataka.

b) strogo neophodno izuzeće: Kolačić koji je izuzeti prema ovom kriteriju mora istovremeno proći dva testa: Izuzeće se odnosi na „usluge informacijskog društva“ (ISS) - tj. usluga koja se pruža putem Interneta, poput web stranice ili aplikacije. Uz to, korisnik je izričito zatražio tu uslugu, a upotreba kolačića mora biti ograničena na ono što je nužno potrebno za pružanje te usluge. Kolačići povezani soglašavanjem nisu nužni i na njih se mora pristati.

Odredba 5 (3) Propisa o e-privatnosti zahtijeva da korisnik mora dobiti " jasne i sveobuhvatne informacije" o upotrebi kolačića u skladu sa propisima o zaštiti podataka. Iako " jasan i sveobuhvatan " nije definiran u Uredbama, potreban standard mora biti u skladu sa zakonodavstvom o zaštiti podataka, tj. GDPR-om. U praksi, ako vaša obrada uključuje osobne podatke, morat ćete udovoljiti zahtjevima transparentnosti prema člancima 12-14 Opće uredbe o zaštiti podataka. To znači da ponekad može doći do dupliciranja podataka navedenih u pravilima o kolačićima i pravilima o privatnosti. I dalje je dobra praksa zadržati oba, kako bi se olakšali različiti slojevi podataka koji mogu biti potrebni u skladu s Uredbom o e-privatnosti i GDPR-om.