Awareness raising campaign for SMEs

Smjernice za poduzetnike koji angažiraju pružatelje usluga u Cloudu

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.

An Coimisiún um Chosaint Sonraí Data Protection Commission

Croatian Personal Data Protection Agency azop Agencija za zaštitu osobnih podataka

VUB VRIJE UNIVERSITEIT BRUSSEL

Sadržaj

Jedna od glavnih obveza prema Općoj uredbi o zaštiti podataka (GDPR) za organizacije koje obrađuju osobne podatke („voditelji obrade”) je da to moraju učiniti na način koji osigurava odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštenih ili nezakonitih obrada (uključujući krađu, uništavanje ili oštećenje, ili otkrivanje) korištenjem "odgovarajućih tehničkih ili organizacijskih mjera". To se ponekad naziva načelom 'cjelovitosti i povjerljivosti' ili 'načelo sigurnosti'.

Ova je obveza vrlo važna, te bi voditelji obrade trebali biti svjesni njene važnosti, a posebice oni koji koriste ili pohranjuju osjetljive osobne podatke. Ima li organizacija odgovarajuće tehničke i organizacijske mjere kako bi osigurala sigurnost osobnih podataka koje obrađuje jedno je od prvih pitanja koje se postavlja u slučaju povrede osobnih podataka. Voditelji obrade također mogu konzultirati smjernice za voditelje obrade o sigurnosti podataka kada procjenjuju odgovarajuće sigurnosne mjere koje trebaju provesti.

Sve je veći broj usluga koje nude 'pohranu u oblaku/Cloudu', dopuštajući da se dokumenti, fotografije, videozapisi i druge datoteke učitaju i pohrane na udaljeni poslužitelj, da se omogući dijeljenje ili udaljeni pristup ili da se ponašaju kao sigurnosna kopija. Korištenje bilo koje usluge u Cloudu kao dio poslovanja važno je područje u kojem organizacije moraju osigurati odgovarajuću sigurnost osobnih podataka koje obrađuju.

Rizik za sigurnost osobnih podataka može nastati kada voditelj obrade podataka prepusti kontrolu nad podacima pružatelju usluga u Cloudu, kada nema dovoljno dostupnih informacija o uslugama obrade u Cloudu i njihovim zaštitnim mjerama ili kada pružatelj usluge ne može na odgovarajući način podržati obveze voditelja obrade ili prava ispitanika.

Voditelj obrade mora zadržati kontrolu nad osobnim podacima koje prikuplja kada podugovara obradu s pružateljem usluga u Cloudu. Ključni element kontrole je osigurati sigurnost podataka. Voditelji obrade (i klijenti i pružatelji usluga u Cloudu) također moraju biti transparentni u pogledu obrade osobnih podataka. Za kontrolu i sigurnost važno je mjesto gdje se pohranjuju podaci.

Što je računalstvo u Cloudu?

Ljudi često misle na različite stvari kada govore o obradi podataka 'u oblaku'. Za organizaciju koja obrađuje osobne podatke, to obično uključuje korištenje vanjskog pružatelja usluga u Cloudu koji obavlja dio ili cijelu obradu ili pohranu na poslužiteljima i/ili u podatkovnom centru pod kontrolom tog pružatelja. U mnogim slučajevima vanjski pružatelji usluga djelovat će kao 'izvršitelji obrade' podataka, koji također imaju niz odgovornosti prema GDPR-u, iako manje od onih koje se odnose na voditelje obrade. Izvršitelj obrade je svaka osoba ili organizacija koja obrađuje osobne podatke u ime i prema uputama voditelja obrade.

Organizacijama su općenito dostupna tri različita modela usluga za računalstvo u Cloudu. U svom najnaprednijem obliku, pružatelj usluga u Cloudu brine se o svim aspektima obrade podataka u ime klijenta, osim o sirovim podacima koje unose pojedinačni korisnici. Organizacija Clouda tako osigurava:

- fizičku infrastrukturu u podatkovnom centru;
- operativni sustav za pokretanje potrebnog softvera; i
- softver potreban za obradu samih podataka.

Klijent (voditelj obrade) također može odabrati koristiti samo dio usluge dostupne od pružatelja usluga – na primjer, samo poslužiteljski prostor (ponekad se naziva 'Infrastruktura kao usluga' ili 'IaaS') ili poslužiteljski prostor plus softverski alati (ponekad se nazivaju 'Platforma kao usluga' ili 'PaaS').

Daljnja razlika koja se često pravi je između „privatnog Clouda" – gdje pružatelj usluge dodjeljuje resurse određenom klijentu – i „javnog Clouda" – gdje klijent može raditi u okruženju s više zakupaca koje uključuje dijeljene sustave i infrastrukturu. Mogu postojati i 'hibridne' verzije gore navedenog u kojima postoji mješavina obrade i dijeljenja podataka između vlastite infrastrukture voditelja obrade i infrastrukture pružatelja usluge.

Pružatelji usluga u Cloudu općenito pružaju usluge obrade voditeljima obrade, ali također mogu pružati usluge podobrade drugim pružateljima. Međutim, u nekim slučajevima pružatelji usluga u Cloudu također su voditelji obrade ili "zajednički voditelji obrade". U takvim slučajevima podliježu jačim obvezama prema GDPR-u nego kada djeluju kao izvršitelji obrade. Ove smjernice prvenstveno se odnose na pružatelje usluga u Cloudu koji djeluju kao izvršitelji obrade i voditelje obrade koji surađuju s njima.

Koja su sigurnosna razmatranja vezana uz računalstvo u Cloudu?

☑ Članak 28. stavak 1. GDPR-a zahtijeva da ako se obrada provodi u ime voditelja obrade, voditelj obrade koristi se jedino izvršiteljima obrade koji u dovoljnoj mjeri jamče provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu sa zahtjevima iz ove Uredbe i da se njome osigurava zaštita prava ispitanika. Nadalje, članak 32. GDPR-a zahtijeva da voditelj obrade i izvršitelj obrade provedu odgovarajuće tehničke i organizacijske mjere kako bi se osigurala razina sigurnosti primjerena riziku. Odobreni kodeks ponašanja (članak 40. GDPR-a) ili odobreni mehanizam certificiranja (članak 42. GDPR-a) može se koristiti kao dopuna usklađenosti s člankom 32. GDPR-a. Voditelj obrade stoga mora biti uvjeren da će osobni podaci biti sigurni ako se predaju pružatelju usluga u Cloudu.

☑ Sigurnost u ovom kontekstu ima dva glavna aspekta:

☑ Prvo, voditelj obrade mora biti uvjeren da će izvršitelj obrade (pružatelj Clouda) obrađivati podatke samo u skladu s uputama voditelja obrade. To je izravno povezano s potrebom za ugovorom između voditelja obrade i pružatelja usluga u Cloudu.

☑ Drugo, voditelj obrade mora biti uvjeren da je pružatelj usluga u Cloudu uzeo u obzir rizike koji se pojavljuju od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji se prenose, pohranjuju ili na drugi način obrađuju.

☑ Voditelj obrade, prije nego što razmisli o povjeravanju osobnih podataka pružatelju usluga u Cloudu, mora biti uvjeren da su sigurnosni standardi pružatelja usluga u Cloudu dostatni i prikladni za obradu osobnih podataka koju će poduzeti u ime voditelja obrade. Pružatelj usluga u Cloudu trebao bi biti u poziciji dati jamstva o ključnim pitanjima kao što su:

- ☑ Pseudonimizacija i enkripcija osobnih podataka ako je potrebno.
- ☑ Izolacija ili odvajanje osobnih podataka koje daje voditelj obrade od podataka drugih kupaca pružatelja usluga u Cloudu.
- ☑ Sposobnost osiguravanja trajne povjerljivosti, integriteta, dostupnosti i otpornosti procesa i usluga. To obuhvaća organizacijska i tehnička sredstva, od zahtjeva za povjerljivost osoblja do ispunjavanja sigurnosnih zahtjeva iz članka 32. GDPR-a.
- ☑ Mogućnost pravovremenog vraćanja dostupnosti i pristupa osobnim podacima u slučaju fizičkog ili tehničkog incidenta.
- ☑ Proces redovitog testiranja, procjene i ocjenjivanja učinkovitosti tehničkih i organizacijskih mjera za osiguranje sigurnosti obrade.
- ☑ Postupci u slučaju povrede podataka. To će značiti da postoji plan odgovora na incidente i da je sklopljen obvezujući sporazum o obavijesti o povredi između voditelja obrade i izvršitelja obrade, kako se ispitanici ne bi nepotrebno izložili riziku.
- ☑ Sredstva za brisanje ili vraćanje svih osobnih podataka voditelju obrade nakon raskida ugovora.

Klijent se mora nastojati uvjeriti u gore navedene stvari, kako prije zadržavanja određenog pružatelja usluga u Cloudu, tako i tijekom bilo kojeg sklopljenog ugovornog aranžmana. To bi se obično postiglo detaljnom tehničkom analizom koja uključuje upitnik za reviziju informacijske sigurnosti pružatelja usluga u Cloudu i/ili bilo kojeg odobrenog kodeksa ponašanja ili certifikacijskog mehanizma koji pruža pružatelj Clouda kao jamstvo. U nekim slučajevima može se zahtijevati i inspekciju prostorija na licu mjesta, način na koji je organizacija implementirala svoju sigurnosnu politiku ili reviziju određenih aktivnosti obrade osobnih podataka ili korištenja tehnologije.

Koji su zahtjevi transparentnosti?

Da bi voditelj obrade razumio kako pružatelj usluga u Cloudu može pružati svoje aktivnosti obrade na način koji je usklađen s GDPR-om, potrebna je visoka razina transparentnosti. To znači da pružatelj usluga u Cloudu mora biti u mogućnosti organizirati svoje aktivnosti obrade na zadovoljstvo svojih kupaca. Voditelji obrade također bi trebali pružati transparentne informacije ispitanicima da se obrada njihovih osobnih podataka provodi uz korištenje usluga obrade u Cloudu. Transparentnost je stoga važan element u donošenju odluka pojedinaca kada koriste usluge voditelja obrade.

Kao što je gore navedeno, u nekim slučajevima upitnik za reviziju može biti dovoljan za ispunjavanje obveza pružatelja usluga u Cloudu prema članku 28. stavku 3. točki h GDPR-a, dopuštajući voditeljima obrade obavljanje revizije njihovih aktivnosti. Ključni dio ove revizije usredotočit će se na sigurnosne aranžmane. Imajte na umu da, budući da pružatelji usluga u

Cloudu obično pružaju usluge višestrukim voditeljima obrade i imaju obveze sigurnosti i povjerljivosti sa svakim, opseg i pojedinosti onoga što je dostupno u toj reviziji mogu biti ograničeni.

Članak 30. stavak 2. GDPR-a o vođenju evidencije također se primjenjuje u slučaju pružatelja usluga u Cloudu. Kao dio zahtjeva za pouzdanosti sukladno GDPR-u, to znači da izvršitelj obrade treba dokumentirati i biti u mogućnosti staviti na raspolaganje voditelju obrade osnovne navedene podatke.

U skladu s člankom 28. stavkom 2. i 28. stavkom 4. GDPR-a, pružatelji usluga u Cloudu, kao izvršitelji obrade, također moraju pružiti svojim voditeljima obrade informacije o svim podizvršiteljima koje angažiraju za pružanje svojih usluga. To znači da voditelj obrade može pregledati ovaj aranžman prema ugovornim uvjetima te dopušta voditelju obrade da prigovori podobradi ako je potrebno.

Članak 28. stavak 5. GDPR-a navodi da pružatelj usluga u Cloudu kao izvršitelj obrade može također koristiti odobrene kodekse ponašanja ili odobrene mehanizme certificiranja kako bi se dokazala usklađenost elemenata njihove obrade. Važno je da priroda, opseg i kontekst takvih kodova ili certifikata budu jasni voditeljima kako bi mogli na odgovarajući način razumjeti u kojoj se mjeri to primjenjuje na obradu njihovih osobnih podataka i je li prikladno za postupke obrade koji su ugovoreni.

Značenje lokacije podataka?

Osobni podaci koji se čuvaju unutar Europskog gospodarskog prostora (EGP) imaju koristi od zajedničkog standarda zaštite utvrđenog na razini EU-a. Kada se podaci prenose izvan EGP-a, moraju se poduzeti posebne mjere kako bi se osiguralo da i dalje uživaju odgovarajuću zaštitu. Raspon opcija naveden je u smjernicama o međunarodnim transferima. U praksi, kada pružatelj usluga u Cloudu obrađuje osobne podatke izvan EGP-a, mora se osloniti na jedan od sljedećih mehanizama:

• Prijenos podataka odvija se na temelju odluke o primjerenosti, kako je navedeno u članku 45. GDPR-a

• Prijenos podataka podliježe odgovarajućim zaštitnim mjerama (kao što su modeli odobreni u EU-u) kako je navedeno u članku 46. GDPR-a

• Prijenos podataka podliježe obvezujućim korporativnim pravilima u skladu s člankom 47. GDPR-a

Kada se koriste 'modeli ugovora' ili 'obvezujuća korporativna pravila', važno je da se zaštita koju pružaju ti mehanizmi također proširuje na sve podizvršitelje koje angažira pružatelj usluga u Cloudu.

Kakav ugovor zahtijeva korištenje usluge u Cloudu?

Članak 28. stavak 3. GDPR-a zahtijeva da se obrada od strane izvršitelja obrade regulira ugovorom. Nadalje, kao što je gore navedeno, izvršitelj obrade ne smije angažirati drugog izvršitelja bez ovlaštenja voditelja obrade. To znači da voditelj obrade koji angažira pružatelja Clouda kao izvršitelja zadržava kontrolu nad osobnim podacima koje on obrađuje, da postoje dogovorena i jasna ograničenja za tu obradu te da je izvršitelj jasan u svojim obvezama prema voditelju obrade.

Ugovor bi trebao uključivati ključne točke navedene u nastavku:

- Da će pružatelj usluga u Cloudu – i svi podizvršitelji koje koristi pružatelj – obrađivati podatke samo prema uputama voditelja obrade.

- Detaljno jamstvo pružatelja usluga u Cloudu o sigurnosnim mjerama i načinu na koji će zahtjevi iz članka 32. GDPR-a biti ispunjeni.

- Nabrajanje podizvršitelja koje je angažirao izvršitelj i pojedinosti o tome kako se ažuriranja o navedenom komuniciraju s voditeljem obrade.

- Informacije potrebne za dokazivanje usklađenosti pružatelja usluga u Cloudu s člankom 28. GDPR-a i kako će izvršitelj doprinijeti reviziji ili inspekcijama voditelja obrade podataka.

- Mjere koje se osiguravaju kako bi se jamčila sigurnost osobnih podataka koji se obrađuju izvan Europskog gospodarskog prostora.

- Odgovornost podijeljena između voditelja obrade i izvršitelja u slučaju povrede GDPR-a ili povrede osobnih podataka i način na koji se o takvim događajima obavještava voditelj obrade.

- Kako izvršitelj ispunjava svoje obveze u svrhu ispunjenja prava ispitanika.

- Predmet, opseg, priroda, kontekst, svrha i trajanje obrade te način na koji se postupa s vrstama i kategorijama osobnih podataka na početku, prijenosu, rutinskoj obradi i „kraju životnog vijeka” – uključujući vraćanje ili brisanje.

Daljnje smjernice

Europska agencija za sigurnost mreža i informacija (ENISA) pružila je korisne smjernice, napisane iz europske perspektive, o temama uključujući 'Prema sigurnoj konvergenciji Clouda i IoT-a', 'Tehničke smjernice za provedbu minimalnih sigurnosnih mjera za pružatelje digitalnih usluga', i 'Vodič za sigurnost u Cloudu za mala i srednja poduzeća'.

Europski nadzornik za zaštitu podataka (EDPS), koji je odgovoran za zaštitu podataka u institucijama EU-a, objavio je 'Smjernice o korištenju usluga računalstva u Cloudu od strane europskih institucija i tijela' koje (iako se temelje na nešto drugačijem skupu propisa) mogu biti od praktične koristi za organizacije koje žele bolje razumjeti sigurnost u oblaku.

Podsjećamo organizacije da prema GDPR-u moraju prijaviti povredu osobnih podataka nadležnom nadzornom tijelu ako povreda predstavlja rizik za pogođene pojedince. Organizacije to moraju učiniti u roku od 72 sata od saznanja o povredi. Ako je vjerojatnost da će povreda rezultirati visokim rizikom za pogođene pojedince, organizacije također moraju obavijestiti te pojedince bez nepotrebnog odgađanja.