VARNOSTI INCIDENTI IN OBVEŠČANJE V SKLADU S 33. ČLENOM GDPR

Uradno obvestilo nadzornemu organu (IP) o kršitvi varstva osebnih podatkov v roku 72 ur

V zadnjem času smo zaznali več kršitev varstva osebnih podatkov (varnostnih incidentov), ki od nas (DPO) zahtevajo pravočasno in ustrezno ravnanje v skladu s 33. in 34. členom GDPR. V nekaterih primerih smo bili obveščeni prepozno, zato vas s tem obvestilom pozivamo, da nas o morebitnem tovrstnem dogodku obvestite takoj, ko jih zaznate in sicer na tel. št ali e-naslov pooblaščene osebe za varstvo osebnih podatkov (renata.zatler@dataofficer.si, 041 325-479 ali jerneja.merva@dataofficer.si , tel. št. 041 921-762 in dodatno tudi v vednost na info@dataofficer.si).

V nadaljevanju je naša naloga, da ocenimo težo kršitve oz. stopnjo verjetnosti, da so s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Prijavo nadzornemu organu (IP) je treba izvesti v roku 72 ur. Po potrebi se izvede tudi obveščanje posameznikov.

Primeri, ki so se že zgodili:

- zaposlena, zadolžena za kadrovske zadeve pri subjektu je prejela elektronsko sporočilo s prošnjo neznane osebe, da naj ji posreduje e-mail naslov zaposlenega, s katerim je bila v preteklosti v dobrih odnosih (povedala je ime in priimek ter rojstni datum te osebe), saj bi želela zaposlenemu ob njegovem rojstnem dnevu posredovati voščilnico. Zaposlena, zadolžena za kadrovske zadeve je osebi podatke posredovala. V tem primeru je prišlo do **nepooblaščenega razkritja** (osebnih podatkov tretji osebi), ki je povpraševala po e-naslovu osebe, kateri naj bi posredovala čestitko.
- zaposleni je pomotoma na spletni strani subjekta objavil osebne podatke njihovih strank (naslovi in priimki). Prišlo je do **nepooblaščenega razkritja** osebnih podatkov.
- v enem od subjektov je prišlo do vdora v informacijski sistem z namestitvijo zlonamerne programske opreme v informacijski sistem, ki je subjektu onemogočil dostop do datotek ter aplikacij znotraj informacijskega sistema. Več dni podatki niso bili dostopni, subjekt je za dostop do podatkov moral posredovati visoko plačilo. Zaradi **izgube nadzora nad osebnimi podatki** s strani subjekta so bili ogroženi osebni podatki subjekta.
- najnovejši primer na mednarodni ravni (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/heathrow-airport-limited-fined-120-000-for-serious-failings-in-its-data-protection-practices/): delavec na londonskem letališču Heathrow je izgubil USB, ki ni bil šifriran ali zaščiten z geslom in je vseboval veliko količino osebnih podatkov in videoposnetkov. Najditelj si je ogledal vsebino in USB poslal časopisu, ki je kopiral podatke in nato USB vrnil letališču. Letališče je dobilo zelo visoko globo, ker **ni zagotovilo ustreznega varstva osebnih podatkov**. Po preiskavi so uvedli več zaščitnih ukrepov. Zaskrbljujoče pa je dejstvo, da se je pri preiskavi izkazalo, da je le 2% zaposlenih na letališču ustrezno usposobljenih za varstvo osebnih podatkov.

POMEMBNO: Sproti (takoj, ko zaznate) nas obvestite o kršitvi varstva osebnih podatkov!

Več o kršitvah in obveznostih v GDPR

Kršitev varstva osebnih podatkov pomeni **kršitev varnosti, ki vodi do nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja oziroma dostopa do osebnih podatkov**. Kršitev je lahko storjena

nehote ali namenoma (načrtovano). Kršitev je treba sporočiti nadzornemu organu v roku 72 ur. Komunikacija med upravljavcem (subjekt) in nadzornim organom (IP) poteka preko pooblaščene osebe za varstvo osebnih podatkov (DPO).

Ne glede na to ali se izvede prijava kršitve nadzornemu organu (odvisno od ocene DPO) ali ne, se mora voditi ustrezna evidenca. Vsak dogodek mora biti ustrezno dokumentiran, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njenimi učinki in **popravnimi ukrepi**. Ta dokumentacija mora biti vedno na voljo IP. Celotno evidenco z vso potrebno dokumentacijo vodi pooblaščena oseba za varstvo OP (DPO).

Primeri dogodkov o katerih nas obveščajte:

- razkritje ali posredovanje osebnih podatkov nepooblaščenim osebam (vključno z objavo na spletnih straneh, posredovanje osebnih podatkov nepravemu naslovniku),
- nepooblaščen dostop do baze podatkov,
- nepooblaščen dostop (VDOR) do prostorov, sistema, strežnika, kopij podatkov…
- vdor na spletno stran,
- nepooblaščeno uničenje osebnih podatkov,
- nepooblaščeno spreminjanje osebnih podatkov (brez dovoljenja),
- izguba, kraja ali zloraba stacionarnih, prenosnih računalnikov in drugih prenosnih medijev s podatki v elektronski obliki,
- izguba podatkov v papirnati obliki in nepooblaščen dostop do baze podatkov o posameznikih,
- zloraba in manipulacija varnostnega sistema,
- izguba dostopa do osebnih podatkov – npr. nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov (»izsiljevalski virus«),
- ogrožena gesla…

Za morebitna pojasnila smo vam na voljo.

Lep pozdrav,
Mag. Renata Zatler, CIPP/E in Jerneja Merva, CIPP/E

Dataofficer d.o.o.
Ljubljanska cesta 68
1230 Domžale
E-pošta: info@dataofficer.si, www.dataofficer.si
Tel: +386 41 921 762 in +386 41 325 479
www.dataofficer.si