Prvi koraki do uskladitve z GDPR

Začnite tako, da vzpostavite projekt za ustrezno uskladitev z novo zakonodajo o varstvu osebnih podatkov, pri čemer se priporoča projektni pristop.

Renata Zatler, CIPP/E, svetovalka in zunanja pooblaščena oseba za varstvo osebnih podatkov, Dataofficer

Foto: Osebni arhiv

Postavite vodjo projekta in ekipo sodelavcev, ki bodo pri projektu aktivno sodelovali. Naredite analizo stanja trenutne skladnosti z zakonodajo o varstvu osebnih podatkov in pripravite seznam organizacijskih in tehničnih ukrepov za ustrezno uskladitev z GDPR. Vodstvo naj potrdi seznam, nato takoj pristopite k izvedbi. Večino ukrepov je treba izvesti do 25. maja 2018.

Zaposleni se morajo seznaniti z notranjimi pravili, sprejetimi za ustrezno varstvo osebnih podatkov v vašem podjetju. Po uvedbi ukrepov ne pozabite na izvajanje nadzornih mehanizmov, vzdrževanje sistema, preverjanje skladnosti in stalno osveščanje zaposlenih prek notranje ali zunanje pooblaščene osebe za varstvo osebnih podatkov (DPO - Data Protection Officer). Če je glede na zahteve GDPR ne potrebujete, določite osebo, ki bo zadolžena za ustrezno vzdrževanje sistema, svetovanje in nadzor nad obdelavo. Pomembno je, da sistem varstva vzdržujete na ustrezni ravni in dejansko izvajate notranje akte in druga pravila.

Kako se odzvati na varnostni incident?

Kljub ustrezni uskladitvi vašega poslovanja z GDPR lahko pride do varnostnega incidenta. Pomembno je, da ste ga sposobni hitro zaznati in se nanj pravilno odzvati. Nadzornemu organu morate biti sposobni dokazati, poleg hitre odzivnosti, tudi ustrezno raven skrbnosti za zaščito osebnih podatkov. Če vam uspe dokazati skladnost z GDPR in da sprejeta pravila za ustrezno raven varstva osebnih podatkov izvajate tudi v praksi, se boste kljub incidentu oziroma kršitvi osebnih podatkov, v praksi uspeli izogniti visoki globi.

Ukrepi, ki jih mora sprejeti upravljavec

Od stopnje tveganja za kršitve pravic posameznikov je odvisno, kakšne tehnične in organizacijske ukrepe mora izvesti upravljavec. Med organizacijske ukrepe uvrščamo politiko varstva, ki je določena z notranjimi akti. Akti določajo pravila za varstvo, pooblastila in odgovornosti za obdelavo, ustrezen nadzor nad izvajanjem (glede na stopnjo tveganja), proces odzivanja na kršitve osebnih podatkov ter druge mehanizme, ki zagotavljajo vzdrževanje ustrezne ravni varstva.

S tehničnimi ukrepi zagotavljamo ustrezno raven varnosti osebnih podatkov. Med drugim določimo način fizičnega (na primer ustrezno zaklepanje prostorov, kjer se obdelujejo osebni podatki) in IT varovanja (informacijska varnost), način uničevanja osebnih podatkov, posredovanja osebnih podatkov, način zagotavljanja revizijske sledi in podobno.

Obseg in vrsta ukrepov sta odvisna od stopnje tveganja

Strožje ukrepe in nadzorne mehanizme je treba uvesti, ko se izvajajo večje obdelave osebnih podatkov ali avtomatizirana obdelava (vključno z oblikovanjem profilov). Najstrožje ukrepe se izvaja, ko se obdelujejo posebne vrste (občutljivih) osebnih podatkov (npr. zdravstveni podatki, podatki o spolnem življenju ali usmerjenosti posameznikov).

Najnižji nivo zahtev velja za tiste poslovne subjekte, ki obdelujejo le osebne podatke svojih zaposlenih in nimajo zahtevnejših ali obsežnejših obdelav osebnih podatkov ter jih tudi ne posredujejo v obdelavo zunanjim obdelovalcem. Nivo zahtevnosti je odvisen tudi od števila zaposlenih.

Najstrožje organizacijske in tehnične mehanizme varstva bodo morali uvesti subjekti javnega sektorja in nosilci javnih pooblastil, zdravstvene ustanove, banke in zavarovalnice, javna komunalna podjetja, večji trgovci s karticami zvestobe, spletne trgovine, IT podjetja (tako v vlogi upravljavca kot tudi v vlogi obdelovalca) in podobni subjekti, ki obdelujejo večje količine osebnih podatkov. gg

gg svetovalec

Človeški faktor predstavlja največje tveganje za zlorabe. S sistematičnim uvajanjem nadzornih mehanizmov, osveščanjem in usposabljanjem zaposlenih, lahko pomembno prispevamo k zmanjšanju tveganja.

Primeri slabe prakse ali kaj v praksi pogostokrat delamo narobe:

1. »Pravila samo na papirju«; sprejet je pravilnik, ki pa ga ne izvajamo.
2. Zaposleni ne vedo, kakšna so pravila varstva, niso osveščeni oziroma usposobljeni. Pogostokrat podpišejo izjavo, da varujejo osebne podatke v skladu z notranjim akti in zakonodajo, vendar v praksi ne vedo, kakšna so ta pravila.
3. Ne veste, kdo obdeluje osebne podatke; dostopne pravice za obdelavo osebnih podatkov niso določene.
4. Ne veste, kje vse se osebni podatki nahajajo.
5. Pravila glede določanja in spreminjanja gesel se ne izvajajo.
6. Gesla si zaposleni posojajo med seboj.
7. Protivirusna oprema se ne posodablja.
8. Osebni podatki se posredujejo v obdelavo zunanjim obdelovalcem, ki ne zagotavljajo ustrezne ravni varstva osebnih podatkov.
9. Posnetki videonadzornega sistema se hranijo predolgo, obdelujejo jih nepooblaščeni uporabniki, poslovni prostori o videonadzoru niso ustrezno označeni.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.