

# Ali ste poslovne procese že uskladili z zahtevami GDPR? Zagotavljanje skladnosti z GDPR

..PROCESNI PRISTOP PREDSTAVLJA UČINKOVITO METODOLOŠKO PODLAGO ZA ZAGOTAVLJANJE SKLADNOSTI DELOVANJA PODJETJA Z ZAHTEVAMI GDPR. POLEG SISTEMATIČNEGA PRISTOPA V FAZI UVAJANJA SPREMENB, OMOGOČA TUDI IZVAJANJE REDNIH LETNIH PREGLEDOV, KI JIH GDPR NA VEČ MESTIH ZAHTEVA..

## GDPR DA! AMPAK KAKO?

Nobenega dvoma ni, da bo prilagoditev zahtevam Splošne uredbe o varstvu osebnih podatkov povzročila spremembe v poslovnih procesih podjetij, ki pri svojem poslovanju uporabljajo in obdelujejo osebne podatke. Novosti, ki jih GDPR uvaja na področju obdelovanja osebnih podatkov bodo zahtevale prilagoditev poslovnih procesov podjetij tako iz tehničnega kot iz procesnega vidika. V preteklih mesecih je bilo veliko govora o vsebini uredbe, malo pa o načinu in izvedbi prilagoditev poslovnih procesov v podjetju v skladu z zahtevami GDPR.

## FAZE PRILAGAJANJA POSLOVNEGA PROCESA

V nadaljevanju je predstavljano prilagajanje poslovnih procesov podjetja zahtevam GDPR skozi tri faze. Prvo fazo predstavlja analiza dejavnikov tveganj in identifikacija »kritičnih« poslovnih procesov iz vidika izpolnjevanja zahtev GDPR. Druga faza temelji na pripravi podrobne in poglobljene analize izbranih »kritičnih« poslovnih procesov z vidika izpolnjevanja zahtev GDPR. V tretji fazi pa se identificirajo in implementirajo ukrepi, ki ugotovljena neskladja med trenutnim potekom poslovnih procesov v podjetju in zahtevami GDPR sanirajo.

## PRVA FAZA - IDENTIFIKACIJA

### »KRITIČNIH« PROCESOV

V prvi fazi prilagoditve poslovnih procesov je opravljen podroben pregled ključnih poslovnih procesov v podjetju s katerim se ugotovi ali se v okviru poslovnih procesov podjetja obdelujejo oziroma upravljajo osebni podatki ali zbirke osebnih podatkov in ali se obdelava in upravljanje podatkov izvaja v okviru podjetja, tretje osebe ali povezane družbe. Pri tem je potrebno ugotoviti tudi, ali v podjetju obstajajo zavezujoča poslovna pravila oziroma dogovorjeni postopki, ki jim je upravljalca ali obdelovalec osebnih podatkov dolžan slediti, ter lokacijo in namen obdelovanja osebnih podatkov. Ključni namen prve faze je, da se identificirajo tisti poslovni procesi, ki so z vidika zahtev GDPR najbolj tvegani in posledično »kritični«, ter zahtevajo poglobljeno obravnavo v naslednjih fazah.



## DRUGA FAZA – POGLOBLJENA ANALIZA STANJA

Po ugotovitvi ključnih poslovnih procesov v podjetju z vidika izpolnjevanja zahtev GDPR se pristopi k izdelavi poglobljene analize izbranih poslovnih procesov, s katero se preveri, ali so pri obdelovanju osebnih podatkov upoštevana vsa načela v zvezi z obdelavo osebnih podatkov, ki jih GDPR določa. Nadaljnje je potrebno ugotoviti in določiti kategorije osebnih podatkov, ki so predmet zbiranja in obdelovanja, saj je od kategorije osebnega podatka odvisen njegov način obdelave. V drugi fazi je tudi potrebno natančno pregledati ustreznost soglasij, na podlagi katerih so osebni podatki posredovani, postopkov in možnih načinov privolitve v zvezi z njihovim zbiranjem, možnosti načina dostopa do obdelovanih osebnih podatkov, ter ugotoviti ustreznost postopkov pridobivanja, varovanja, posredovanja, hranjenja in brisanja osebnih podatkov.

Druga faza je namenjena tudi poglobljenemu tehničnemu delu pregleda skladnosti poslovnih procesov z GDPR. Tehnični pregled se običajno opravlja v skladu z metodološkimi smernicami mednarodnega standarda ISO 27001 in zajema pregled dostopov do sistema, kjer se osebni podatki obdelujejo in shranjujejo, ugotovitev ustreznosti fizičnega in tehničnega varovanja prostorov ter varovanja pred negativnimi vplivi okolja, ustreznost varovanja osebnih podatkov (npr. proti zlonamerni kodi), ustreznosti ravnanja z nosilci podatkov in ravnanja z občutljivimi osebnimi podatki, ter obstoj ustreznih varnostnih kopij podatkov. Ključni cilj druge faze prilagoditve poslovnih procesov v podjetju je ugotovitev tveganj in dejanskega razkoraka z zahtevami GDPR, kar omogoča identifikacijo potrebnih organizacijskih in tehničnih ukrepov za zagotovitev skladnosti izvajanja poslovnih procesov v podjetju zahtevam GDPR.

## TRETTJA FAZA - IMPLEMENTACIJA

V tretji fazi se, na podlagi ugotovitev iz predhodnih faz, pripravi in implementira ustrezne ukrepe, ki zagotavljajo prilagoditev poslovnih procesov. V tretji fazi je ravno tako kot vsebinski pomemben tudi finančni vidik načrtovanja sprememb, saj je odprava neskladij največkrat povezana z organizacijskimi in tehničnimi rešitvami, ki zahtevajo mobilizacijo dodatnih finančnih in kadrovskih resursov.

## ZAKAJ PROCESNI PRISTOP?

GDPR podjetja in organizacije postavlja pred veliko odgovornost, saj znaša zagrožena kazen za kršitve določb uredbe do 4 % letnega prometa, ki ga zavezanec dosega. Pri presoji skladnosti in določanju morebitnih kazni s strani nadzornih organov pa je pomembno predvsem dokazovanje podjetja, da je z ustrežno skrbnostjo pristopilo k sprejemu tehničnih, organizacijskih in pravnih ukrepov za varnost osebnih podatkov, ter da z rednimi pregledi skrbi, da se poslovni procesi izvajajo v skladu s sprejetimi zavezami in postavljenimi zahtevami GDPR. Procesni pristop in izdelane procesne metodologije (npr. ISO 27001) gotovo predstavljajo učinkovit način za doseganje zelenih učinkov v zvezi z izpolnjevanjem zahtev GDPR. Ne odlašajte in prilagodite poslovni proces uredbi GDPR še pred začetkom njene veljavnosti.

(P. R.)



# Eudace

**EUDACE, d. o. o.**

Litostrojska cesta 44e

1000 Ljubljana

M: +386 (0) 31 337 392

T: +386 (0) 599 42 160

E: igor@eudace.eu

W: www.eudace.eu