

Ljubljana, 10.05.2018

Priporočila ZPN v zvezi z GDPR

Sprejetje Splošne uredbe o varstvu osebnih podatkov je priložnost, da vsi skupaj uredimo svoje evidence, prečistimo in pospravimo računalnike, omare, poslovne prostore in arhive.

Z osebnimi podatki v vašem podjetju ravnajte tako, kot si želite, da bi z vašimi osebnimi podatki ravnajo drugi – skrbno in odgovorno.

Ključne novosti za **vse nas osebno in naše osebne podatke**, ki jih prinaša nova uredba so:

- Večji nadzor in učinkovito izvajanje nadzora nad osebnimi podatki
- Lažji dostop do lastnih osebnih podatkov
- Pravica do pozabe
- Pravica vedeti kako dolgo se hranijo osebni podatki
- Pravica zahtevati popravek, izbris ali vložiti pritožbo
- Pravica do prenosljivosti osebnih podatkov
- Pravica do pravnega sredstva in sankcije
- Posebno varstvo otrok

Pomembne novosti za **upravljalce in obdelovalce (pravne in fizične osebe)** med drugim pa so:

- Zbiranje osebnih podatkov na podlagi dokazljive privolitve oz. soglasja
- Možnost preklica privolitve oz. pravica do umika soglasja
- Dolžnosti upravljalcev pri prenosljivosti podatkov
- Zagotovitev informacij o obdelavi osebnih podatkov
- Obveznost uradnega obveščanja o kršitvah varstva osebnih podatkov
- Imenovanje pooblaščenih osebe za varstvo osebnih podatkov (javni sektor in nekatera podjetja
- Obveznost vodenja evidenc obdelave ne velja za podjetja, ki zaposlujejo manj kot 250 oseb, in ne obdelujejo posebnih vrst podatkov iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10. člena GDPR.
- Občutljivi osebni podatki so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ... so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.
- Učinkovite, sorazmerne in odvračilne sankcije

Kaj morate storiti glede GDPR?

1. Preverite veljavnost obstoječih privolitev in preverite način pridobivanja privolitev v bodoče

Odgovorite si na vprašanje: **ali imate pravno podlago** za obdelavo osebnih podatkov. Podlaga je lahko sam zakon, sklenitev ali izvajanje pogodbe ali pa osebna privolitev. Npr. za zbirko podatkov o naročiteljih imate pravno podlago v ZNPosr oz. v sklenitvi pogodbe o posredovanju, medtem ko je potrebno za zbirko podatkov o potencialnih strankah pridobiti osebno privolitev.

Osebnih podatkov, za katere nimate ustrezne pravne podlage, ne smete hraniti oz. obdelovati. Soglasja ali privolitve morajo biti dokazljive.

- Vzorec soglasja oz. privolitve posameznika za različne namene (fotokopiranje osebnega dokumenta, obveščanje o ponudbi)
- Vzorec soglasja oz. privolitve za nazaj za uskladitev obstoječih evidenc oz. zbirk

2. Prilagodite pogodbe s pogodbenimi obdelovalci

Preglejte kakšne **pogodbe** imate sklenjene z **zunanjiimi pogodbenimi obdelovalci** (programi za posrednike, računovodski servisi, ipd.).

Na spletni strani informacijskega pooblaščenca je pripravljen vzorec pogodbe o obdelavi osebnih podatkov <https://www.ip-rs.si/obrazci/varstvo-osebni-podatkov/>

3. Preverite in prilagodite popis zbirk osebnih podatkov – evidenc

Najprej je potrebno, da vsaka gospodarska družba pripravi **enotni popis zbirk osebnih podatkov**. V ta namen morate **predhodno popisati vse zbirke osebnih podatkov, ki jih vodite in vzdržujete**. Celovita in verodostojna ugotovitev stanja je prvi in ključni pogoj za uspešno izvedbo prilagoditve Uredbi GDPR.

Primer osebnega podatka: janez.novak@gzs.si ali pa Janez Novak, direktor, GZS, ali pa Janez Novak, tel. 01 58 98 000, ni pa osebni podatek: info@gzs.si

Zbirka osebnih podatkov je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; **strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika**.

Potem, ko ste popisali vse zbirke osebnih podatkov je priporočljivo narediti skrben pregled, ali vse te zbirke podatkov resnično potrebujete, ali jih lahko **združite** in tako **optimizirate** svoje poslovanje. Za vsako zbirko osebnih podatkov si morate odgovoriti najmanj na naslednja vprašanja: za kaj jih potrebujemo, kaj z njimi počnemo, kako dostopamo do teh podatkov, kdo in kako dostopa do teh podatkov, ...

- Vzorec Smernic z osnovnimi napotki glede oblikovanja evidenc

- [Vzorec Kataloga zbirke osebnih podatkov](#)

Preglejte vaše postopke za zagotavljanje pravic posameznika, preglejte in prilagodite vaše varnostne politike in njihovo izvajanje ter določite, kdo bo poročal v primeru varnostnega incidenta

Ko imate že pripravljene in urejene zbirke podatkov (Zbirka zaposlenih delavcev, zbirka o pogodbenem delu, zbirka naročiteljev, zbirka o opravljenih poslih, zbirka o potencialnih strankah, zbirka izdanih obračunov in računov, zbirka o podatkih za neposredno trženje) **preverite še varovanje in varnost**. Kako so varovani prostori, v katerih se nahajajo nosilci osebnih podatkov, strojna in programska oprema, kje se hranijo ključi varovanih prostorov, kje se hranijo občutljivi osebni podatki. V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje. Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje. Dokumentacija in nosilci podatkov se hranijo v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izven delovnega časa izklopljeni ali kako drugače fizično ali programsko zaklenjeni.

Razmislite o načinih **hranjenja dokumentacija**. Večino vaše dokumentacije je potrebno hraniti 10 let. Dokumentacijo in zbirke podatkov lahko hranite v fizični ali v elektronski obliki, vendar je v obeh primerih potrebno poskrbeti za varnost in preprečevanje nepooblaščenih dostopov.

- [Vzorec Pravilnika o zavarovanju osebnih podatkov](#)

Pripravite se na izvajanje načela odgovornosti

Obveznost imenovanja pooblaščenih oseb ni vezana na število zaposlenih v podjetju, temveč GDPR določa posebne **kriterije**. **Imenovanje pooblaščenca za varstvo osebnih podatkov** za nepremičninsko posredniške družbe ni obvezno (obvezno je ko obdelavo opravlja javni organ, ko temeljne dejavnosti upravljavca ali obdelovalca zajemajo dejanja obdelave, pri katerih je treba posameznike, na katere se nanašajo osebni podatki, redno in sistematično obsežno spremljati, ali ko temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov⁷ ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški).

Če ne zmorete sami, poiščite zunanje strokovnjake, a ne nasedajte vsaki ponudbi in strašenjem z visokimi kaznimi. Informacijski pooblaščenec priporoča »**zdravo pamet**«.

Ne glede na vse navedeno pa morate razumeti, da sama varnost podatkov še ne pomeni varstva osebnih podatkov. Po novem ima posameznik pravico zahtevati od vas informacije o njegovih osebnih podatkih, npr. katere osebne podatke o njem hranite in obdelujete, pa tudi pravico zahtevati, da jih izbrišete oz. uničite (pravica do pozabe).

Skratka, z osebnimi podatki je potrebno rokovati zelo skrbno, za njihovo obdelavo potrebujemo soglasje, zagotoviti moramo, da so na varnem in zavarovani pred nepooblaščenimi dostopi.

Naj na koncu še enkrat poudarimo, da so vzorci obrazcev in dokumentov informativne narave. Pri pripravi lastnih gradiv morate upoštevati specifičnost posameznih vrst osebnih podatkov (občutljivi/navadni), sredstva in načine obdelave ter druge okoliščine vašega primera. Zgolj vnos podatkov o vašem podjetju oziroma organu ne bo zadostil potrebam GDPR. GZS-ZPN ne prevzema nikakršne odgovornosti odgovornost za popolnost obrazcev, točnost informacij in zakonitost obdelave osebnih podatkov s strani upravljavcev, ki so zbrani na podlagi predmetnega obrazca.

Upamo, da vam bodo priloženi napotki v pomoč. Za dodatna pojasnila smo vam tudi na voljo ali po tel. 01 58 98 240 ali e-pošti zpn@gzs.si.

Boštjan Udovič
Direktor ZPN