

10 stvari, ki jih morate vedeti o novostih na področju varstva osebnih podatkov



Zakaj se vas to tiče?

Zaradi sprejete nove Evropske Uredbe - General Data Protection Regulation ali Splošna Uredba o varstvu podatkov

Uredba dopolnjuje ureditev (nova pravila) varstva osebnih podatkov na ravni vseh članic EU

KAZNI:

- do 20 milijonov EUR oz.
- 4 % letnega prometa – KAR JE VIŠJE
- + morebitna odškodnina prizadetim posameznikom

Kdo vas nadzira in tudi kaznuje: Informacijski pooblaščenec – inšpekcijski organ.

Možnost izogniti se plačilu globe, kljub kršitvi !!

SKRAJNI ROK:

25.5.2018

nova zakonodaja velja za vsako ustanovo in podjetje, ki uporablja in kakorkoli obdeluje osebne podatke državljanov EU

Kaj prinaša nova uredba o varovanju osebnih podatkov



višje globe za kršitelje



obvezno poročanje
o vdorih v baze



poenotenje varovanja
osebnih podatkov



uveljavitev pravice
do pozabe



strožje pogoje
za obdelavo osebnih
podatkov



jasno in nedvoumno
privolitev k uporabi
osebnih podatkov



imenovanje pooblaščen
osebe za varstvo
podatkov



prenosljivost podatkov
(posameznik bo lahko
prevzel podatke in jih
prenesel h konkurenčnemu
ponudniku)



Privolitev / soglasje

- **DA – ni ustrezno**
- **IZJAVA VOLJE :**
 - Prostovoljna, izrecna, informirana, nedvoumna (zavedati se moramo, da dajemo privolitev in v kakšnem obsegu jo dajemo)
 - vsebovati mora informacijo o identiteti upravljavca in o namenu obdelave
 - Dokazovanje ustreznosti izjave je na upravljalcu
- **IZPIS OSEBNIH PODATKOV OTROK**
- Pazite na privolitev staršev ali skrbnikov, če je otrok mlajši od 15 let oz 14 let (uredba določa 13 let)
- Boste morali pridobiti soglasja ponovno?
Ni nujno – v kolikor so že obstoječa skladna z novo ureditvijo.
Zato jih je potrebno natančno pregledati.



Namen obdelave OP

- **KONKRETNO** (ni dovolj: za izboljšanje storitve)
- **DRUG NAMEN, KOT JE POSAMEZNIKU PRVOTNO PREDSTAVLJEN – LE S PRIVOLITVIJO POSAMEZNIKA**

(Pri zbiranju osebnih podatkov (registracija uporabnika, pridobitev e-naslova, telefonskega kontakta prijava na e-časopis,...) bodo morali upravljavci natančno opredeliti, za kakšen namen se osebni podatki zbirajo in kdo jih bo obdeloval. To pomeni, da dikcija »zbrane podatke bomo uporabljali v raziskovalne namene« ni več dovolj. Kako natančno definirati namen obdelave, je odvisno od konkretne situacije, predvsem pa je potrebno paziti, da je zadoščeno pravilom iz področja varstva osebnih podatkov.



IZPIS, IZBRIS, POPRAVEK in PRENOSLJIVOST osebnih podatkov na zahtevo uporabnika

- Vsak uporabnik lahko od upravljalca vselej zahteva izpis vseh svojih osebnih podatkov, ki jih ta obdeluje.
- Pravica do pozabe, a le, če to ne ogroža svobode izražanja ali možnosti raziskovanja.
- Kdaj se morajo izbrisati: ko niso več potrebni za namene za katere so bili pridobljeni, če so bili pridobljeni nezakonito, če to določa zakon ali pravnomočna sodna odločba
- Še posebej morajo biti upravljalci pozorni na strožje določbe glede izbrisa podatkov, pri čemer morajo za izvajanje in načrtovanje ukrepov iz GDPR izvesti oceno tveganja



Zdravstveni osebni podatki sodijo v posebno kategorijo podatkov za katere veljajo strožja pravila obdelave (prej t.i. občutljivi podatki)

Vaše temeljne dejavnosti zajemajo obsežno obdelavo posebnih vrst podatkov, ki so vsi občutljivi osebni podatki. V to kategorijo spadajo: politične stranke in sindikati, zasebne zdravstvene institucije ter zdravniki in zobozdravniki, s koncesijo ali brez ter drugi koncesionarji.

So pri vas občutljivi osebni podatki res varno shranjeni? Ali ste preverili, če so občutljivi podatkih vaših pacientov ustrezno zavarovani? Ali izvajate redne letne preglede ustreznosti zaščite in izvajate organizacijske in tehnične ukrepe za ustrezno varovanje? Primer Belgija (julij, 2017): Neznani heker je uspel ukrasti nekatere podatke o pacientih preko flamske spletne strani »Digitale Wachtkamer«, spletnega mesta, ki omogoča bolnikom ureditev sestankov s svojimi zdravniki. Heker je dostopal do e-poštne naslovov, telefonskih števil in gesel bolnikov in posledično tudi do občutljivih zdravstvenih podatkov. Ta vrsta osebnih "zdravstvenih" podatkov je dejansko posebna kategorija podatkov, ki se po naravi šteje za posebno "občutljivo" in bi morala imeti koristi od dodatne zaščite pred nezakonitim dostopom in razkritjem.

Uporabljajte dodatne zaščitne ukrepe !! za podatke o zdravju, rasi, spolni usmerjenosti, veroizpovedi in političnih prepričanjih.

A5. Pooblaščenec za varstvo osebnih podatkov (DPO) – SKRBI ZA MIRNEJŠI SPANEC UPRAVLJALCA

Javni sektor

- celoten javni sektor, denimo šole, vrtce, muzeje, knjižnice, javne agencije, zdravstvene domove, bolnišnice.
- zasebni sektor, ki osebne podatke obdeluje za javni sektor).

Zasebni sektor

- podjetja, ki redno, sistematično in obsežno spremljajo osebne podatke posameznikov - banke, zavarovalnice, trgovci s klubi zvestobe, spletne trgovine, kadrovske agencije
- vsi, ki tržijo, oblikujejo storitve, glede na preference in zmožnosti posameznika, vsi, ki se kakorkoli ukvarjajo z obdelavo velikih količin podatkov za namen napovedovanja trendov ali identifikacije potreb posamezne skupine
- Vsi, ki zajemajo obsežno obdelavo posebnih vrst osebnih podatkov

ZUNANJI ALI NOTRANJI?

Notranji – večja podjetja

- sistemiziranje delovnega mesta
- podvojitve funkcije – paziti na neodvisnost in konflikt interesov

Zunanji – manjša podjetja

- ustrezna raven neodvisnosti bi bila še najbolj zagotovljena z imenovanjem zunanjega DPO
- bo imenovan kot oseba za varstvo osebnih podatkov in bo v vseh zadevah ravnal na podoben način, kot bi ravnal notranji DPO

OCENA UČINKA ZA VARSTVO PODATKOV

Ocene učinkov bodo potrebne v primerih, kjer so tveganja za varstvo osebnih podatkov velika. Taki primeri so npr.:

- vzpostavitev novega kluba zvestobe,
- aplikacija za zajem in zbiranje zdravstvenih podatkov,
- vse oblike obdelave podatkov o zdravju,
- programska rešitev za vodenje ocen otrok v šolah,
- državni projekti e-uprave in centralni gradniki,
- videonadzor javnih površin,...



IP še vedno opaža določene kršitve. Med njimi so:

- pošiljanje zdravstvenih podatkov po nezavarovanih povezavah,
- posojanje avtentikacijskih sredstev za dostop do podatkov,
- vpogledi v zdravstvene podatke brez utemeljenega razloga.

Zaradi načela sledljivosti, opozarjamo na obstoj utemeljenega razloga za vsakokratni vpogled v bazo osebnih podatkov!

POVZETEK

- Apokalipsa? Ni potrebno.
- Zavedanje o pomembnosti varovanja OP
- Ves čas vedeti kaj se z osebnimi podatki dogaja – zajemanje, obdelava, posredovanje, hranjenje, brisanje,
- DPO – izobražuje, svetuje, komunicira z Informacijskim pooblaščencom
- Veljavna soglasja za obdelavo OP (strožja pravila) ter nameni obdelave (za kakšen namen zbiramo podatke, od tega je odvisna tudi hramba, uporaba za drug namen)
- Ocena učinka dejanj obdelave na varnost OP
- Obveznost poročanja o kršitvah varstva OP – 72 ur
- IZBIRA PRAVEGA PONUDNIKA ZA POMOČ PRI DOSEGANJU ZGORNJIH ZAHTEV