GDPR

Splošna uredba o varstvu podatkov (General Data Protection Regulation)

kratek povzetek

Mitja Lasič ©

december 2017

GDPR - Kazalo

GDPR – Uvod - Podatki so nova nafta

MLADINA

Kdor ima danes podatke in jih zna uporabiti, ne bo le obogatel, ampak bo znal izključiti naključja, napovedati prihodnost in jo z malo spretnosti tudi spremeniti. **Podatki zato niso le nova nafta, ampak tudi nov bog**. Njegovo ime je Big Data.

Finance.si

S pravilno analizo podatkov lahko ugotovimo, kaj so resnične želje in potrebe kupcev, kako povečati storilnost zaposlenih ali kdaj se bo v tovarni pokvaril stroj. **Podatki so nafta digitalne ekonomije, surovina spletnih platform, pametnih naprav in programov umetne inteligence**.

The Economist

A NEW commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in **data, the oil of the digital era**. These titans - Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft - look unstoppable. They are the five most valuable listed firms in the world. Their profits are surging: they collectively racked up over $25bn in net profit in the first quarter of 2017. Amazon captures half of all dollars spent online in America. Google and Facebook accounted for almost all the revenue growth in digital advertising in America last year.

GDPR - Spremembe v zakonodaji

GDPR (EU)

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)

Začetek veljavnosti in uporaba

- Objava v Uradnem listu EU - 4. maj 2016.
- Uredba začne veljati dvajseti dan po objavi v Uradnem listu EU – 25. maj 2016.
- Obvezen pričetek uporabe - 25. maj 2018.

Pravni pomen

- Uredba (obvezno upoštevanje) in ne več Direktiva (priporočilo).

Poglavitni cilji

- Posamezniku omogočiti večji nadzor nad njegovimi podatki.
- Poenotenje sistema varstva (osebnih) podatkov na ravni celotne EU.
- Posodobitev varstva (osebnih) podatkov glede na nove tehnologije in nova varnosna tveganja.
- Zagotoviti prost pretok osebnih podatkov v EU.

GDPR - Spremembe v zakonodaji

GDPR (EU)

Obsežna uredba

- 173 uvodnih izjav (Recitali)
- 99 členov

Pomembnejše določbe (gledano s strani upravljavcev / obdelovalcev podatkov)

- Uvodne izjave od 1 do 97, 171
- Poglavje 1 / člen 4 (Opredelitev pojmov)
- Poglavje 2 / členi 5 do 11 (Načela)
- Poglavje 3 / členi 12 do 23 (Pravice posameznika, na katerega se nanašajo podatki)
- Poglavje 4 / členi 24 do 39 (Upravljavec in Obdelovalec)

Časovni obseg

Zavedati se je treba, da uvedba GDPR ni enkratno dejanje, temveč bo treba ves čas skrbeti za skladnost z zakonodajo.

GDPR - Spremembe v zakonodaji

Direktiva (EU)

Direktiva 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.

Začetek veljavnosti in uporaba

- Objava v Uradnem listu EU - 4. maj 2016.
- Direktiva začne veljati dan po objavi v Uradnem listu EU – 5. maj 2016

GDPR - Spremembe v zakonodaji

ZVOP-2 (SLO)

Zakon o Varstvu Osebnih Podatkov 2

Začetek veljavnosti in uporaba

- V pripravi
- V uvodni obrazložitvi osnutka je zapisano, da mora biti ZVOP-2 sprejet in objavljen v Uradnem listu RS ter uveljavljen pred 25. majem 2018, v uporabi pa mora biti od 25. maja 2018.
- V končni določbi v 100. členu Osnutka ZVOP-2 je predlagano, da začne veljati naslednji dan po objavi v Uradnem listu RS, uporabljati pa se začne 25. maja 2018.

Poglavitna cilja

- Zagotovitev izvrševanja določb GDPR v pravnem redu RS.
- Zagotovitev uresničevanja osebne človekove pravice do varstva osebnih podatkov.

Pojasnilo v zvezi s pripombami na osnutek ZVOP-2

1.12.2017 - Peter Pavlin, Ministrstvo za pravosodje

GDPR - Spremembe v zakonodaji

ZIV (SLO)

Zakon o Informacijski Varnosti – v pripravi

- Člen 4 (5) - Informacijska varnost pomeni zaščito, varovanje in obrambo omrežij in informacijskih sistemov ter informacij pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti;
- Člen 4 (35) - Varnost omrežij in informacijskih sistemov pomeni zmožnost omrežij in informacijskih sistemov, da na določeni ravni zaupanja preprečijo vse dogodke, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali pripadajočih storitev, ki jih navedena omrežja in informacijski sistemi zagotavljajo ali so prek njih dostopne.

Začetek veljavnosti in uporaba

- V pripravi
- Petnajsti dan po objavi v Uradnem listu RS.

Poglavitna cilja

- V pravni red RS se prenaša vsebine Direktive 2016 / 1148 / ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.
- Zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov v RS.

GDPR - Spremembe v zakonodaji

Uredba o zasebnosti in elektronskih komunikacijah (EU)

Predlagana je nova uredba o spoštovanju zasebnega življenja in varstvu osebnih podatkov v elektronskih komunikacijah (Uredba Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (Uredba o zasebnosti in elektronskih komunikacijah)), ki naj bi tudi razveljavila Direktivo 2002/58/ES (Direktiva 2002/58/ES evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah).

Začetek veljavnosti in uporaba

- Morala bi biti sprejeti do maja 2018.

Poglavitni cilji

- Izboljšanje usklajevanja med državami EU.
- Ekstrateritorialni učinek, ki omogoča centralno "kaznovanje".
- Strožja pravila o "piškotih".
- Izrecno razlikovanje med vsebino komunikaciji in komunikacijo metapodatkov.
- Definicija telefonskih klicov za neposredno trženje kot opt-in (potreben aktiven ukrep uporabnika, da se naroči npr. na seznam glasila). Državam članicam EU je sicer dovoljeno, da uredijo zakonodajo tako, da omogoča opt-out osnovo (uporabnik se veliko bolj preprosto prijavi, zato mu je treba omogočiti, da brez težav odstopi).

GDPR – Izrazi in pojmi

Upravljavec podatkov

ZVOP-1: Upravljavec osebnih podatkov (OP) je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave OP oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

Obdelovalec podatkov

ZVOP-1: Obdelovalec OP je v fizična ali pravna oseba, ki obdeluje OP v imenu in na račun upravljavca OP.

Obdelovalec OP je lahko tudi zunanji izvajalec.

Posebne vrste OP (prej: Občutljivi OP)

Za te podatke **ZVOP-2** prepoveduje obdelavo tistih osebnih podatkov, ki razkrivajo

- rasno ali etično pripadnost,
- politično mnenje,
- versko ali filozofsko prepričanje,
- članstvo v sindikatu,
- spolno usmerjenost.

Zakon pa dovoljuje nekaj izjem, kdaj te podatke lahko obdelujete:

- če dobite izrecno osebno privolitev posameznika,
- če je posameznik te podatke sam javno objavil brez očitnega ali izrecnega namena, da omeji namen njihove uporabe,
- . . .

GDPR – Izrazi in pojmi

Evidence obdelav OP (prej: Katalogi zbirk OP)

Obvezno vodenje evidenc

Evidence obdelav morajo voditi:

- velika podjetja (250 zaposlenih ali več),
- upravljavci, ki podatke obdelujejo redno,
- upravljavci, pri katerih je verjetno, da obdelava, ki jo izvajajo, pomeni tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki,
- upravljavci, ki pri obdelavi ravnajo z občutljivimi podatki ali kazenskimi evidencami.

Obvezna vsebina evidenc

Evidenca mora vsebovati:

- ime in kontaktne podatke podjetja,
- razloge (namen) za obdelavo podatkov,
- opis kategorij OP in posameznikov, na katere se nanašajo OP,
- kategorije organizacij, ki prejemajo podatke,
- podatke o prenosu podatkov v drugo državo ali organizacijo,
- rok za odstranitev podatkov (če je mogoče),
- opis varnostnih ukrepov, ki se uporabljajo pri obdelavi (če je mogoče).

GDPR – Izrazi in pojmi

Profiliranje

Profiliranje je spremljanje vedenja posameznika.

GDPR in **ZVOP-2**: Profiliranje je vsaka oblika avtomatizirane obdelave OP, ki vključuje uporabo OP za ocenjevanje nekaterih osebnih vidikov v zvezi s konkretnim posameznikom, zlasti za analizo ali predvidevanje:

- uspešnosti pri delu,
- ekonomskega položaja,
- zdravja,
- osebnega okusa,
- interesov,
- zanesljivosti,
- vedenja,
- lokacije ali gibanja.

Podjetje, ki profilira, obvezno potrebuje:

- pooblaščeno osebo za varstvo osebnih podatkov (DPO – Data Protection Officer),
- oceno učinkov na varstvo osebnih podatkov (DPIA - Data Protection Impact Assessment).

Privolitev v profiliranje

Profiliranje ne sme biti izvajano brez privolitve oziroma soglasja posameznika, ki ga profiliramo.

GDPR – Izrazi in pojmi

Ocena učinka na varstvo podatkov (DPIA – Data Protection Impact Assessment)

Ni obvezna za vsako obdelavo OP.

GDPR: DPIA je obvezna, kadar je možno, da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave, povzročila veliko tveganje za pravice in svoboščine posameznikov.

Primeri, ko je DPIA obvezna:

- sistematično in obsežno vrednotenje osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno s profiliranjem, in je podlaga za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;
- obsežna obdelava posebnih vrst podatkov (dozdajšnji občutljivi OP);
- obsežno sistematično spremljanje javno dostopnega območja, denimo videonadzor.

Kaj mora DPIA vsebovati:

- sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno, pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
- oceno potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
- oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- ukrepe za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti z uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo OP, ter drugih oseb, ki jih to zadeva.

GDPR – Izrazi in pojmi

Opt-in / Opt-out

"**Opt-in**" je postopek, pri katerem je potreben aktiven ukrep uporabnika, da pride ta uporabnik v neko bazo podatkov (da se npr. naroči na nek seznam za prejemanje obvestil).

"**Opt-out**" je postopek, po katerem lahko uporabnik veliko bolj preprosto (morda celo nevede) pride v neko bazo podatkov. Zato mu je treba omogočiti, da lahko iz te baze podatkov brez težav izstopi.

Običajno se princip opt-in uporablja v skladu s pravili evropske in kanadske zaščite podatkov, medtem ko se princip opt-out uporablja v delovanju ameriškega neposrednega trženja.

Anonimizacija OP

Anonimizacija pomeni odstranitev neposrednih identifikacijskih podatkov (npr. ime, matična številka, davčna številka, naslov, telefon, spletni identifikatorji, IP naslov, ID piškotkov, RFID oznake itd.) z namenom nepreklicne preprečitve identifikacije.

Upravljalci morajo pri anonimizaciji upoštevati vsa sredstva, ki bi lahko prišla v poštev pri poskusu povrnitve identifikacije.

Anonimizirani podatki se lahko uporabljajo za nadaljnjo obdelavo. Ker so anonimizirani, ne spadajo več pod zakonodajo o varstvu OP, vendar so posamezniki, na katere se nanašajo ti podatki, še vedno upravičeni do zaščite.

Glavni anonimizacijski tehniki sta randomizacija in generalizacija.

Psevdonimizacija OP

Psevdonimizacija pomeni nadomeščanje identifikacijskih podatkov s psevdonimi (npr. ponarejeno ime ali številka). Največkrat se uporablja poseben psevdonimizacijski algoritemski ključ, kar načelom omogoča tudi izvajanje obratnega procesa in povrnitev originalnih identifikacijskih podatkov.

GDPR – Zbiranje osebnih podatkov (OP)

Kdaj lahko zbiramo OP

ZVOP-2: Podatki se obdelujejo zakonito, če so določene zakonske podlage za njihovo obdelavo. Določeni morajo biti:

- namen obdelave,
- vrste OP, ki naj bi jih obdelovali,
- rok hrambe teh podatkov.

Namen obdelave OP

Jasna opredelitev

Iz namena mora jasno izhajati, za kaj konkretno se bodo podatki uporabljali.

Sprememba namena

Obdelava OP za drug namen je dovoljena le:

- če dobite privolitev posameznika, na katerega se nanašajo OP;
- če obdelavo za drug namen določajo zakon, pravni akti, odločitev EU (ki se uporablja neposredno);
- če to morate storiti, ker te podatke potrebujete za namene preprečevanja, preiskovanja, odkrivanja, pregona kaznivih dejanj;
- če morate podatke za drug namen od prvotnega obdelati, ker je to potrebno za uveljavljanje, izvajanje ali obrambo civilnopravnih zahtevkov, če ne prevladujejo interesi posameznika, na katerega se nanašajo osebni podatki.

GDPR – Zbiranje osebnih podatkov (OP)

Privolitev za zbiranje OP

Zbiranje osebnih podatkov je možno na podlagi privolitve oziroma soglasja (**opt-in**).

ZVOP-2: privolitev je "prostovoljna, izrecna, informirana in nedvoumna izjava volje posameznika, na katerega se nanašajo OP".

Urad informacijske pooblaščenke: Če oseba zgolj odkljuka "da", to ni zadostna privolitev.

Da je privolitev skladna z GDPR:

- Mora biti izjava jasna in razumljiva, dana z nedvoumnim pritrdilnim dejanjem, ki vsebuje predvsem informacijo o identiteti upravljavca in namenu obdelave posameznih OP.
- Iz nje mora jasno in nedvoumno izhajati, da se posameznik, na katerega se nanašajo OP, zaveda dejstva, da daje privolitev in v kakšnem obsegu jo daje.

Ob tem je pomembno vedeti: molk ni privolitev.

Ponovno pridobivanje privolitev

Če dosedanje privolitve niso skladne z GDPR oziroma ZVOP-2, jih je treba pridobiti še enkrat.

Preklic dane privolitve

GDPR: Privolitev mora biti enako enostavno preklicati kot dati.

GDPR – Zbiranje osebnih podatkov (OP)

Hramba OP

Rok hrambe OP

- mora biti določen,
- mora biti omejen na najkrajše možno obdobje.

Če ni mogoče določiti roka hrambe osebnih podatkov (npr. ni bil predpisan v zakonu, ni zapisan v pogodbi …), je rok hrambe v osnutku ZVOP-2 za zdaj določen na pet let.

Obvezno brisanje OP

ZVOP-2: OP je treba obvezno brisati:

- ko OP niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani,
- če so bili OP obdelani nezakonito,
- če je izbris OP potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi.

Pravica do izpisa OP

Vsak uporabnik lahko od podjetja kadarkoli zahteva izpis vseh OP, ki jih o njem hrani to podjetje.

Pri tem je treba izpisati tudi podatke, ki jih o tej osebi zbirajo, hranijo ali obdelujejo zunanji partnerji.

Pravica do popravkov OP

Če so podatki nepravilni, posameznik vedno lahko zahteva popravek, ki ga upravljavec podatkov mora izvesti.

GDPR – Zbiranje osebnih podatkov (OP)

Pravica do izbrisa OP (Pravica do pozabe)

Če posameznik ne bo več želel, da se njegovi OP obdelujejo, lahko zahteva, da se njegovi podatki zbrišejo.

Upravljavec mora podatke zbrisati, če ni zakonitih razlogov za njihovo nadaljnjo hrambo.

Pravica do prenosljivosti OP

Upravljavec je dolžan posamezniku zagotoviti v strukturirani, splošno uporabljani in strojno berljivi obliki vse OP, ki so povezani s konkretnim posameznikom in jih je ta posameznik posredoval upravljavcu.

Otroški OP

GDPR uvaja starostne omejitve. Privolitev samega otroka je zakonita, če je ta starejši od 16 let. V nasprotnem primeru je treba pridobiti privolitev od staršev ali zakonitih skrbnikov.

GDPR dopušča, da države članice EU same določijo nižjo starost, vendar mejna starost ne sme biti nižja od 13 let.

V osnutku ZVOP-2 piše, da je možno tudi, da bo mejna starost v Sloveniji 14 ali 15 let.

GDPR – Zbiranje osebnih podatkov (OP)

Pravica do pravnega sredstva in sankcije

Posameznik ima pri nadzornem organu pravico vložiti pritožbo v zvezi z obravnavanjem njegovih OP.

Posameznik ima pravico do pravnih sredstev zoper odločitev nadzornega organa ali v primeru neukrepanja nadzornega organa.

Posameznik ima pravico do odškodnine in odgovornosti.

Pravica do osebnega posredovanja

Posameznik ne sme biti podvržen obravnavi in odločitvi, ki izhaja le iz avtomatiziranih načinov profiliranja, analize in predvidevanj (npr. ocena osebnih lastnosti, zdravja, navad itd.). Še zlasti, kadar ima taka obravnava ali odločitev pravni učinek v zvezi z njim ali na podoben način nanj znatno vpliva

Nevarnost avtomatiziranega profiliranja: Ujetost v informacijski mehurček.

Dopustnost avtomatiziranega odločanja ali profiliranja

Avtomatizirano odločanje ali profiliranje je dopustno, če je odločitev:

- nujna za sklenitev ali izvajanje pogodbe med posameznikom in upravljavcem,
- dovoljena v pravu EU ali pravu države članice,
- utemeljena z izrecno privolitvijo posameznika.

GDPR – Pooblaščena oseba za varstvo OP (DPO – Data Protection Officer)

Funkcija DPO

GDPR (poglavje 4 , od 37. člena dalje) in **ZVOP-2**.

Predpisana sta imenovanje in področje delovanja.

DPO je pooblaščena oseba za varstvo OP. Ta obdelovalcu ali upravljavcu OP neodvisno pomaga pri zagotavljanju skladnosti obdelave OP z GDPR in ZVOP-2.

Obvezna uvedba DPO

DPO obvezen za:

- upravljavce in obdelovalce osebnih podatkov v javnem sektorju (tudi tisti v zasebnem sektorju, ki osebne podatke obdelujejo za javni 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)

DPO lahko uvedejo tudi podjetja, ki ga po zakonu ne potrebujejo.

GDPR – Pooblaščena oseba za varstvo OP (DPO – Data Protection Officer)

Pogoji za imenovanje DPO

Poglavitna pogoja

- Biti mora strokovnjak za varstvo OP.
- Ne sme obstajati konflikt interesov - biti mora zagotovljena neodvisnost. Mnenje **WP29** (guidelines on the DPO requirement in the GDPR):
  - ne sme biti zaposlen v kadrovski službi,
  - ne sme biti vodja IT oddelka,
  - ne sme biti vodja marketinga,
  - ne sme biti vodja prodaje,
  - ne sme biti direktor.

Redna zaposlitev DPO

DPO je lahko tudi zunanji izvajalec.

ZVOP-2: članice povezane družbe ali članice zveze društev lahko imenujejo skupnega DPO.

GDPR – Pooblaščena oseba za varstvo OP (DPO – Data Protection Officer)

Položaj DPO

- **ustrezno in pravočasno vključen** v vse zadeve v zvezi z varstvom OP,
- **ima sredstva, dostop do OP in dejanj obdelave, ter ohranjanje znanja**,
- pri opravljanju teh nalog **ne prejema nobenih navodil**,
- **ne sme biti razrešen ali kaznovan** zaradi opravljanja svojih nalog,
- **poroča neposredno najvišji upravni ravni** upravljavca ali obdelovalca,
- pri opravljanju svojih nalog **zavezan varovati skrivnost ali zaupnost**,
- **lahko opravlja druge naloge in dolžnosti** (če ni **nasprotja interesov**).

Naloge DPO

- **obveščanje** upravljavca in zaposlenih ter **svetovanje** o njihovih obveznostih po uredbi in predpisih o VOP,
- **spremljanje skladnosti** z uredbo, drugimi predpisi VOP, politikami upravljavca ali obdelovalca,
- **svetovanje** glede ocene učinka v zvezi z varstvom OP in spremljanje izvajanja,
- **sodelovanje** z nadzornim organom.

GDPR – Varnost podatkov

Pristopi k obvladovanju varnosti podatkov

- Standard **ISO 27001** - eden od temeljnih pristopov upravljanja tveganj pri upravljanju varovanja informacij.
- Vpeljava in obvladovanje celostnega nabora tehnoloških informacijskih rešitev na področjih:
  - zaščita komunikacijskih omrežij,
  - upravljanje uporabniških identitet (dostopov in pooblastil),
  - zaščita pred zlonamernimi kodami,
  - spremljanje dejavnosti (revizijske sledi),
  - zaznavanje varnostnih incidentov,
  - maskiranje (psevdonimizacija / anonimizacija) in šifriranje podatkov.

Upravljanje identitet

Pri obvladovanju varnosti OP (in tudi vseh ostalih podatkov) potrebujemo tudi obvladovanje življenjskega cikla identitet.

V vsakem trenutku je treba vedeti, kdo ima pooblastila za dostop do določenih podatkov, sistemov in do kdaj so ta pooblastila veljavna. To velja za zaposlene in tudi za zunanje uporabnike (poslovne partnerje, končne stranke itd.), ki uporabljajo različne spletne in mobilne aplikacije. Organizacija mora ob tem imeti vzpostavljene tudi postopke za ustrezno potrjevanje in periodično pregledovanje dodeljenih pooblastil.

Sistemi za upravljanje identitet in nadzor privilegiranih pooblastil so med glavnimi tehnologijami za zagotavljanje zakonske skladnosti pri zaščiti OP.

GDPR – Varnost podatkov

Varnost obdelave OP

Upravljavec in obdelovalec OP sta dolžna zagotavljati ustrezno raven varnosti OP glede na tveganje. Varnost zagotavljata z izvajanjem ustreznih tehničnih in organizacijskih ukrepov, kot npr.:

- maskiranjem in šifriranjem OP;
- s stalnim zagotavljanjem zaupnosti, celovitosti, dostopnosti in odpornosti sistemov za obdelavo;
- z zagotavljanjem zmožnosti pravočasne povrnitve razpoložljivosti in dostopa do Op v primeru fizičnega ali tehničnega incidenta;
- z rednim izvajanjem postopka testiranja, ocenjevanja in vrednotenja teh ukrepov.

Pri določanju ustrezne ravni varnosti se upoštevajo zlasti tveganja:

- nenamerno ali nezakonito uničenje OP;
- izguba OP;
- nepooblaščeno dostopanje do OP;
- nepooblaščeno spreminjanje OP,
- nepooblaščeno razkritje OP.

Upravljavec in obdelovalec morata zagotavljati, da katera koli fizična oseba, ki ukrepa pod vodstvom upravljavca ali obdelovalca in ima dostop do OP, teh OP ne sme obdelovati brez navodil upravljavca, razen če to od nje zahteva pravo EU ali pravo države članice.

Upravljavec in obdelovalec morata zagotavljati, da se privzeto obdelajo samo OP, ki so potrebni za vsak poseben namen obdelave. To velja za:

- količino zbranih OP (načelo najmanjšega obsega podatkov),
- obseg njihove obdelave,
- obdobje njihove hrambe,
- njihovo dostopnost.

GDPR – Poročanje o kršitvah

Obvezno poročanje

Obdelovalec mora po seznanitvi s kršitvijo varstva OP o tem brez nepotrebnega odlašanja uradno obvesti upravljavca.

Upravljavec mora o kršitvi brez nepotrebnega odlašanja, najpozneje pa v 72 urah uradno obvestiti nadzorni organ (v Sloveniji bo to Informacijski pooblaščenec), razen če ni verjetno, da bi bile s kršitvijo varstva OP ogrožene pravice in svoboščine posameznikov.

Uradno obvestilo mora vsebovati vsaj:

- opis vrste kršitve varstva OP (kategorije, približno število zadevnih posameznikov, na katere se nanašajo OP, ter vrste in približno število zadevnih evidenc OP);
- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva OP;
- opis ukrepov, ki jih upravljavec sprejme oziroma predlaga za obravnavanje kršitve varstva OP;
- opis ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Kadar ni mogoče zagotoviti vseh informacij istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.

Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

Upravljavec dokumentira vsako kršitev varstva OP, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. Ta dokumentacija nadzornemu organu omogoči, da preveri skladnost z zakonsko podlago.

GDPR – Poročanje o kršitvah

Obveščanje posameznikov

Če je verjetno, da kršitev varstva OP povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo OP, da je prišlo do kršitve varstva OP.

V sporočilu posamezniku, na katerega se nanašajo OP, mora biti v jasnem in preprostem jeziku opisana vrsta kršitve varstva OP ter informacije in ukrepi, ki so bili (ali bodo) uradno posredovani nadzornemu organu.

Sporočilo posamezniku, na katerega se nanašajo OP, ni potrebno, kadar:

- je upravljavec izvedel ustrezne tehnične in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za OP, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih;
- je upravljavec sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo OP, ne bo več dogajalo;
- bi to zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo OP, enako učinkovito obveščeni.

Če upravljavec posameznika, na katerega se nanašajo OP, še ni obvestil o kršitvi varstva OP, lahko nadzorni organ to od njega zahteva po preučitvi verjetnosti, da bi kršitev varstva OP povzročila veliko tveganje, ali pa lahko odloči, da je izpolnjen kateri koli od pogojev, zaradi katerega posameznika ni treba obvestiti.

GDPR – Nadzor nad skladnostjo z GDPR in ZVOP2

Nadzorni organ

Nadzorni organ bo informacijski pooblaščenec.

ZVOP-2: informacijski pooblaščenec bo:

- izvajal inšpekcijski nadzor nad vsebino OP v skladu z določbami zakona,
- izvajal nadzor nad zakonitostjo obdelave OP v skladu z določbami zakona,
- imel možnost odločati o postopkih za prekrške za kršitve zakona.

GDPR – Kazni

Odmera kazni

GDR določa zelo visoke najvišje kazni:

- do 20 milijonov €,
- do 4 % letnega prometa,

odvisno od tega, kateri znesek je višji.

Tudi ZVOP-2 (osnutek) upošteva že v GDPR predpisane kazni.

Pravosodno ministrstvo:

GDPR je zdaj zavezujoče pravo EU za Slovenijo,

- take kazni niso v interesu slovenskega gospodarstva niti niso sorazmerne,
- morda še popravki v ZVOP-2, »tako da bi morda olajšali odločanje informacijskega pooblaščenca v smer, da pri kaznih ne bi šlo primarno za globe«.

GDPR – Kazni

Pri kaznovanju se bo upoštevalo 11 kriterijev

1. **narava, teža in trajanje kršitve**, pri čemer se upoštevajo narava, obseg ali namen zadevne obdelave ter število posameznikov, na katere se nanašajo osebni podatki in ki jih je kršitev prizadela, in raven škode, ki so jo utrpeli;
2. ali je kršitev **namerna** ali posledica **malomarnosti**;
3. vsi **ukrepi, ki jih je sprejel upravljavec ali obdelovalec**, da bi ublažil škodo, ki so jo utrpeli posamezniki;
4. **stopnja odgovornosti upravljavca ali obdelovalca**, pri čemer se upoštevajo tehnični in organizacijski ukrepi;
5. vse zadevne **predhodne kršitve** upravljavca ali obdelovalca;
6. **stopnja sodelovanja z nadzornim organom** pri odpravljanju kršitve in blažitvi morebitnih škodljivih učinkov kršitve;
7. **vrste osebnih podatkov**, ki jih zadeva kršitev,
8. **kako je nadzorni organ izvedel za kršitev**, zlasti če in v kakšnem obsegu ga je upravljavec ali obdelovalec uradno obvestil o kršitvi;
9. če so bili **ukrepi že prej odrejeni zoper zadevnega upravljavca ali obdelovalca** v zvezi z enako vsebino, skladnost s temi ukrepi;
10. **upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov potrjevanja**, in
11. morebitni **drugi oteževalni ali olajševalni dejavniki** v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve.

GDPR – Kazni

Videonadzor in biometrija

ZVOP-2 se dotika tudi nekaterih področij, ki jih v GDPR ni, npr:

- videonadzor,
- biometrija,

zato so globe za te prekrške določene ločeno.

Kazen med 4 in 12 tisoč €:

- Nepravilne označbe o izvajanju videonadzora
  - če ni vidno, pisno ali grafično jasno, da gre za videonadzor,
  - če ni podan naziv tistega, ki izvaja videonadzor,
  - če ni podana tel. št. za pridobitev informacije, kje in koliko časa se shranjujejo posnetki.
- Izvajanje videonadzora v podjetju (dovoljeno je le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi, premoženja ali tajnih podatkov, poslovnih skrivnosti).

GDPR – Ključne točke GDPR pripravljenosti

1. preveriti **veljavnost obstoječih privolitev** (privolitev jasna in razumljiva izjava, dana z nedvoumnim pritrdilnim dejanjem in dokazljiva) (člena 6 in 7, uvodne določbe: 32, 42, 43, 171)
2. preveriti **način pridobivanja privolitve v bodoče** (obveščenost posameznika, komu, zakaj in katere podatke, kakšne pravice ima) (členi 12, 13, 14)
3. prilagoditev **pogodbe s pogodbenimi obdelovalci** (obvezne ustrezne klavzule v pogodbah) (člen 28)
4. preveriti in prilagoditi kataloge – **evidence dejavnosti obdelave** (kje in kateri podatki) (člen 30)
5. pregledati postopke za **zagotavljanje pravic posameznika** (zahteva za seznanitev, ugovor, omejitev, izbris, prenosljivost, dajanje ugovora) (členi 12 - 22)
6. pripraviti se na **izvajanje načela odgovornosti** (ne čakati na inšpekcijo)
    a. preveriti, ali bo treba **izvajati ocene učinka** (člen 35)
    b. preveriti, ali bo treba **imenovati DPO** (37)
    c. razmisliti, kako upoštevati načelo **vgrajenega in privzetega varstva podatkov** (minimizacija zbranih podatkov, obsega obdelave, obdobja hranitve, števila obdelovalcev) (člen 25)
7. pregledati in prilagoditi **varnostno politiko in njeno izvajanje** (člen 24)
8. pripraviti **postopek poročanja in upravljanja kršitev varnosti** (kdo, kdaj in kako poroča v 72-ih urah) (člen 33)
9. oceniti interes glede **certificiranja varovanja OP** (certificiranje prostovoljno in plačljivo) (člen 42)
10. preveriti potrebo za **zunanjo pomoč** (zunanji strokovnjaki)

GDPR – Pomembnejše dejavnosti pred uvedbo

Popis vseh zbirk OP

Potrebno je narediti revizijo stanja.

Od leta 2004 je v veljavi ZVOP-1. Podjetja so takrat pregledala svoje zbirke in jih prijavila v register informacijskega pooblaščenca. Na to obveznost so marsikje sčasoma pozabili in podatkov niso posodabljali. Vmes so nastale nove zbirke, novi programi (CMS - Content Management System) in danes mnogo podjetij nima pregleda nad svojimi zbirkami na enem mestu. Veliko jih tudi nima pregleda nad vrstami sistemov hrambe baz (deljeni podatki – recimo: nekaj avtomatiziranih v sofisticiranih informatiziranih zbirkah, nekaj v Excelovih tabelah, nekaj podatkov še papirno vodenih itd.).

Pregled pravnih podlag

Na kakšni pravni podlagi so v konkretno zbirko OP vnešeni konkretni OP?

Razlikovanje pravne podlage:

- zakon ali pogodba - pričakuje se najmanj težav,
- privolitev uporabnika - pričakuje se več težav,
- legitimni interes upravljavca - pričakuje se več težav.

GDPR – Pomembnejše dejavnosti pred uvedbo

Analiza stanja

Na podlagi popisa zbirk OP in pregleda pravnih podlag ter ustrezne metodologije mora upravljavec oziroma (če so nekateri deli obdelave podatkov oddani v zunanje izvajanje) tudi obdelovalec izdelati analizo razkoraka med dejanskim in želenim stanjem varstva OP.

Analiza mora dati jasen in natančen odgovor na vprašanje, katere

- organizacijske,
- kadrovske,
- tehnološke

ukrepe bo treba izvesti, da bo obdelava podatkov skladna z GDPR in drugimi relevantnimi predpisi.

Ukrepi morajo biti:

- ustrezno notranje pravno določeni,
- dokumentirani,
- integrirani v poslovne procese, v okviru katerih se OP obdelujejo.

Z ukrepi je treba seznani zaposlene, ki se morajo zavedati svojih odgovornosti za varstvo podatkov. Še zlasti DPO.

Rešitve in oprema morajo biti vseskozi na ravni, ki omogoča zakonsko skladno obdelavo podatkov.

Ukrepe varstva OP lahko podjetje uvede in vzdržuje

- s svojimi zaposlenimi, ali
- z zunanjo strokovno pomočjo, ki mora biti skladna s predpisanimi zahtevami in ustrezno pogodbeno urejena.

GDPR – Trenutni notranji akti IJS o varovanju podatkov

- Pravilnik o zavarovanju osebnih podatkov na IJS (30. 9. 2006)
- Pravilnik o varovanju tajnih podatkov na Institutu "Jožef Stefan" (18. 8. 2014)
- Sklep o poslovni skrivnosti Instituta "Jožef Stefan" (14. 6. 2013)
  - Resolution of the Business Secrecy of the JSI
- Pravilnik o ukrepih za varovanje dostojanstva zaposlenih na Institutu "Jožef Stefan" (7. 3. 2014)
- Navodila direktorja za zagotavljanje integritete in preprečevanje korupcije (24. 4. 2014)
- Načrt inegritete (maj 2014)