ABC urejanja varstva osebnih podatkov v organizaciji

1. Popis procesov obdelave

Vsaka organizacija mora najprej sploh vedeti, katere osebne podatke obdeluje, katere so osebe, ki te podatke potrebujejo za svoje delo, kaj je pravna podlaga za določeno obdelavo. Zato je treba popisati vse obdelave osebnih podatkov, kar bo nato služilo tudi za evidenco dejavnosti obdelave po GDPR[1].

Popis procesov je v velikih organizacijah v tem delu priporočljivo razširiti tudi na ostale procese dela, saj se takšen popis pogosto zanemarja, posledično pa procesi dela niso optimalni. Gre torej za poslovno odločitev, ki vodstvu lahko pomaga k optimizaciji procesov (gledano povsem poslovno, ne zgolj skozi določila GDPR).

Kako začeti?
Določite osebo, ki bo zbirala informacije in ki dobro pozna delovanje organizacije. Ta oseba naj izdela Excelovo tabelo, kamor bodo ostali vpisovali procese obdelave. Minimum, ki ga je treba vstaviti v tabelo, so:

- vrste osebnih podatkov (npr. ime, priimek, IP naslov, e-naslov, naslov ...);
- kdo jih obdeluje (navesti vse osebe, ki obdelujejo navedene osebne podatke – po delovnih mestih);
- zakaj jih obdelujejo (namen obdelave) – npr. za obračun plač, za potrebe vpisa, za potrebe izobraževanj, za potrebe pošiljanja e-novic ...
- na koga se osebni podatki nanašajo (npr. zaposleni, prejemniki e-novic, stranke, poslovni partnerji ...);
- pravna podlaga, če jo zaposleni poznajo;
- koliko časa se ti osebni podatki hranijo (5 let, do preklica, trajno ...);
- dejstvo, ali za določeno obdelavo uporabljamo zunanje partnerje (npr. računovodski servis, MailChimp, ponudnik spletnega gostovanja ...);
- dejstvo, ali mi obdelujemo osebne podatke za nekoga drugega (npr. računovodski servis za drugo organizacijo);
- komu vse osebne podatke posredujemo;
    - znotraj organizacije;
    - zunaj organizacije.
- na kakšen način varujemo osebne podatke v določenem procesu (geslo, VPN, SS.

Določena oseba naj torej izdela Excel tabelo, ki bo vsebovala zgoraj našteto in jo pošlje vsem vodjem oddelkov, direktorjem ali vodjem določenih služb oz. osebam, ki so vodje posameznega področja. Če teh ni ali je v organizaciji malo zaposlenih, naj ta oseba pač določi tisto osebo, ki najbolje pozna procese dela in bo ta popisala vse potrebno.

[1] Če že imate izdelane kataloge zbirk osebnih podatkov še po ZVOP-1, si lahko pomagate z njimi in prihranite kar nekaj časa.

Oseba, ki bo tabelo pošiljala odgovornim, naj postavi rok, do katerega morajo prejemniki te tabele vanjo vpisati zahtevane podatke in navodilo, da se ti podatki do roka pošljejo tej osebi.

2. Pregled podatkov in izdelava evidence dejavnosti obdelave (EDO)

Ko so vsi podatke iz 1. poglavja na enem mestu, mora za to določena oseba vse te podatke ustrezno urediti. To pomeni, da podvojene vnose ustrezno združi in izdela popis vseh procesov obdelave[2] oz. ustrezno poimenuje zbirke osebnih podatkov. Določene zbirke so že zakonsko določene oz. obvezne – npr. delovnopravne zbirke, ki so natančno popisane v Zakonu o evidencah na področju dela in socialne varnosti. Te je treba potem uskladiti z zakonskimi zahtevami, v EDO pa več ali manj večinoma samo *kopipejstati* ime zbirke, vrste osebnih podatkov, rok hrambe.

Od tu dalje je treba za vsako zbirko osebnih podatkov ugotoviti, katera je pravna podlaga, da te zbirke sploh smemo obdelovati. Ta postopek nam že pokaže, ali imamo za vsako zbirko osebnih podatkov ustrezno pravno podlago in, ali moramo še kaj dopolniti, spremeniti, popraviti informacije za posameznika ...

Če tega še niste storili, v tem delu prepoznajte pogodbeno obdelavo in z obdelovalcem sklenite pogodbo o obdelavi, ki mora vsebovati vse sestavine oz. klavzule iz odst. (3) člena 28 GDPR[3].

Ko je zadeva urejena, za to določena oseba izdela EDO s kategorijami, kot so te določene v členu GDPR. EDO je lahko izdelan na način, da so v njej samo zahtevane informacije, lahko pa – glede na obseg organizacije oz. kompleksnost procesov – to razširite tudi z drugimi rubrikami. Pri tem opozarjamo, da če bo teh rubrik preveč, EDO zaradi nepreglednosti hitro lahko postane neuporaben, zato bodite pazljivi z dodatnimi polji. Tisto, kar priporočamo (skorajda kot nujno), je, da za vsako zbirko osebnih podatkov (oz. proces, če bo EDO temeljil na procesih), določite odgovorno osebo, kot jo pozna še ZVOP-1 – ne glede na to, kaj bo določal ZVOP-2, je določitev odgovorne osebe zelo praktična, saj je ta oseba nekakšen skrbnik zbirke in najbolje ve, kaj se z osebnimi podatki dogaja, kako se jih varuje ... Prav zato priporočamo, da so odgovorne osebe za posamezne zbirke vodje področij (npr. kadrovski direktor je odgovorna oseba za kadrovske zbirke). V EDO pa ne priporočamo, da jih poimenujete z imeni in priimki, saj boste sicer morali ta podatek spreminjati vedno, ko se oseba na tem položaju zamenja – lahko navedete delovno mesto.

V večjih organizacijah je skoraj nujno treba izdelati tudi popis vseh oseb, ki zaradi narave svojega dela smejo obdelovati osebne podatke – poimenujmo jih »pooblaščene osebe[4]«. Tudi

---

[2] Na tem mestu opozarjamo na nekoliko drugačno logiko GDPR v primerjavi z ZVOP-1. Nekdanji katalogi zbirk osebnih podatkov so temeljili na popisu **zbirk**, medtem, ko EDO temelji na popisu **procesov**. Glede na dejstvo, da pri nas zakonodaja, ki določa obdelavo OP, še vedno temelji na zbirkah, zaenkrat še ni bilo zaznati, da bi lahko bilo karkoli narobe, če tudi EDO še vedno temelji na zbirkah.

[3] POZOR! Če boste od vašega obdelovalca prejeli pogodbo, ki jo je sam pripravil, zelo pazljivo preverite, ali ta vsebuje vse zahtevane vsebine oz. se z njo obrnite na svojega DPO.

[4] V tem kontekstu naj vas ne zavede beseda »pooblaščen« v smislu, da mora zakoniti zastopnik vsako osebo posebej pooblaščati (celo pisno) – dovolj je samo, da se oseba navede na seznam in ni treba pisati nobenih posebnih pooblastil, razen če bi to od vas zahtevala področna zakonodaja. Enako velja za določitev odgovorne osebe.

v tem primeru je bolje, da na seznam navedete delovno mesto in ne imena in priimka. Takšen zapis se lahko vstavi tudi v akt o sistemizaciji delovnih mest in torej ni treba, da je to posebna tabela / seznam – odvisno od vašega načina dela. Še eno pomembno opozorilo: pogosto se zgodi, da delavec zavrne delo, ker naj za obdelavo konkretnih osebnih podatkov ne bi bil posebej »pooblaščen«. Zakoniti zastopnik se lahko kadarkoli odloči, da bo delavec moral opravljati delo tudi na drugi zbirki osebnih podatkov in za to delavec ne potrebuje posebnega dovoljenja ali pooblastila[5]. Dovolj je ustno navodilo[6].

Ko je seznam odgovornih in pooblaščenih oseb potrjen s strani zakonitega zastopnika, je treba EDO v pregled posredovati pooblaščeni osebi za varstvo podatkov (DPO), če jo organizacija ima. Njegove predloge mora organizacija upoštevati pri dokončni verziji EDO – če se z DPO ne strinja, mora to posebej utemeljiti (pisno, po e-pošti ...).

Ko je EDO ustvarjen in pregledan tudi s strani DPO, se seznam odgovornih in pooblaščenih oseb pošlje v IT oddelek, kjer na podlagi teh podatkov izdelajo seznam dostopnih pravic v IKT okolju, lahko pa uporabijo kar neposredno podatke iz EDO.

EDO ni treba javno objavljati, mora pa biti vedno dostopen DPO in nadzornemu organu.

POMEMBNO
Ko ste EDO potrdili, ne pozabite, da jo je treba ažurirati, če organizacija uvede nove postopke obdelave osebnih podatkov, če se spremenijo delovna mesta in v drugih primerih, ko določene spremembe oz. novosti vplivajo na podatke v EDO.

3. Varnost obdelave[7] in izdelava Pravilnika o zavarovanju

Ko je EDO izdelan, je potrebno opraviti najpomembnejši korak v organizaciji, in sicer določitev stopnje varnosti obdelave osebnih podatkov. Pri tem je treba misliti na 4 področja:

- **fizično** varovanje (alarm gibanja, protipožarni alarm, samodejne gasilne naprave v strežniških sobah, varnostnik, alarm za vodo, zaklepanje pisarn ...);
- **IT** zavarovanje (požarni zidovi, revizijska sled in njena avtentičnost, struktura gesel, posodabljanje programske opreme, testna okolja ...);
- **striktno izvrševanje pogodbe o obdelavi** osebnih podatkov (točna določitev pogojev zavarovanja v teh pogodbah, nadzor nad prenosom osebnih podatkov k obdelovalcu in nadzor nad njim ...);
- **izobraževanje** zaposlenih.

[5] V tem delu gre za klasično klavzulo pogodbe o zaposlitvi »... in druge naloge po odredbi delodajalca ...«.
[6] Pri tem je pomebno samo to, da zakoniti zastopnik zagotovi, da se ne izgubi sledljivost obdelave osebnih podatkov (več spodaj pri varnosti obdelave).
[7] ZVOP-1 je uporabljal termin »zavarovanje«, GDPR pa je ta termin zamenjala z »varnost obdelave« - samo poimenovanje ni toliko pomembno, kot je pomembno, da je zavarovanje oz. varnost obdelave ustrezna.

Ker je to področje izjemno obsežno, ne navajamo konkretnih primerov za pravilnost zavarovanja, pač pa samo povezavo na vprašalnik Informacijskega pooblaščenca, kjer boste lahko prebrali, na kaj vse morate biti pozorni: klikni tukaj za vprašalnik[8].

ZELO POMEMBNO!!!
Vsa 4 navedena področja so enako pomebna in eden brez drugega ne morejo obstajati. To poudarjamo predvsem zaradi dejstva, da organizacije izjemno pogosto pozabljajo na izobraževanje za zaposlene – moramo se zavedati, da največ vdorov v sisteme nastane zaradi nepoučenih zaposlenih (klasičen primer: zaposleni prejme t. i. *phishing* e-pošto, klikne na povezavo v njej, s tem pa sproži postopek kriptiranja vseh podatkov v sistemu, napadalec pa zahteva odkupnino za kriptirni ključ – to je t. i. *ransomeware*). Zavedajmo se, da na koncu vedno človek klikne tipko *Enter* ali klikne z miško.

Kako visoko stopnjo varnosti obdelave bomo vpeljali, ni pogojeno s tem, koliko finančnih in kadrovskih virov imamo na razpolago, pač pa predvsem z dvema kriterijama[9]:

1. količina osebnih podatkov, ki ji obdelujemo;
2. občutljivost osebnih podatkov, ki jih obdelujemo (posebne vrste osebnih podatkov[10]).

Konkretna določitev, kaj vse je treba postoriti, torej temelji na oceni, ki upošteva oba navedena kriterija. Gre za zelo pomembno odločitev, ki s seboj lahko prinese visoke finančne in kadrovske posledice, zato je izjemno priporočljivo, da se izvede analiza tveganj, v kateri morajo sodelovati vsi odločevalci, v prvi vrsti pa IT služba in DPO. Za nazoren prikaz, vzemimo obveznost vpeljave t. i. SIEM orodij, ki v strojni obliki skrbijo za avtentičnost revizijske sledi:

frizerka s petimi strankami <-----> Klinični center Ljubljana

Frizerka (1.) ne zbira veliko osebnih podatkov in (2.) ne obdeluje občutljivih osebnih podatkov, zato SIEM orodja ne potrebuje. Medtem, ko na drugi strani UKC obdeluje (1.) ogromne količine osebnih podatkov in so ti (2.) večinoma občutljivi osebni podatki (posebne vrste) → posledično mora UKC imeti zagotovljene najvišje varnostne zahteve, vključno s SIEM orodji. Ne glede na ugotovljeno, pa morata oba upravljavca še vedno zagotavljati ustrezno varovane prostore, imeti ustrezna gesla ...

Določitev stopnje varnosti tako absolutno ni enostavna. Pri tem vam lahko vsaj za IKT okolja pomagajo vaši IT sodelavci, ki so po navadi vešči izdelave analize tveganj. Pri novih procesih pa je tako ali tako treba izdelati oceno učinka v zvezi z varstvom podatkov, pri čemer se lahko za pomoč obrnete na vašega DPO.

Analiza tveganja bo tako pokazala nivo varnosti, ki jo je potrebno zagotoviti, pri čemer je možno samo dvoje:

- ali se takšno zavarovanje zagotovi;
- ali pa se obdelava osebnih podatkov preneha izvajati.

---

[8] Vprašalnik je izdelan po ISO27001/2, kar vam lahko služi tudi za podrobno urejanja varstva podatkov – ne samo osebnih, tudi drugih vrst.
[9] Teh je sicer več, navedena pa sta najpomembnejša.
[10] ZVOP-1 je posebne vrste osebnih podatkov imenoval občutljivi osebni podatki: npr. zdravstveno stanje, članstvo v sindikatu, veroizpoved ...

Na tem mestu je treba predvsem apelirati na vodstvo organizacije, da kakršnakoli obdelava osebnih podatkov s seboj prinese tudi določene stroške – in v to kislo jabolko je treba slej ko prej ugrizniti – bolje prej, saj se v primeru, da pride do vdora v katerikoli sistem, ali pa obisk Informacijskega pooblaščenca, ne bo končalo dobro (pa so enormne globe po GDPR po navadi še najmanjši »udarec« za organizacijo).

Posebej opozarjam tudi na dejstvo, da se (predvsem v javnem sektorju) zaposljuje osebe, ki nimajo izkušenj na področju kibernetske varnosti in (v primerih DPO) varstva osebnih podatkov. Gre za zelo nevarno početje, saj lahko napačna odločitev IT ali DPO osebja pripelje do nepopravljivih posledic za varnost obdelave. Verjamem, da plačni sistem v javnem sektorju ne omogoča zaposlovanja dobrih strokovnjakov, vendar vseeno močno apeliram na delodajalca, da skušajo na trgu dobiti najboljše, kar se v okviru zmožnosti da dobiti. Saj veste, kako se delijo organizacije v IT žargonu:

So organizacije, ki so že doživele vdor v sistem in so organizacije, ki ga še bodo.

Če na vdor ne boste pripravljeni oz. ga ne boste preprečili, lahko nastanejo nepopravljive posledice – eden od zadnjih primerov: 2.000.000 EUR škode zaradi izpada prihodkov in 300.000 EUR za odpravljanje posledic. In pri tem še nismo pri izgubi ugleda in globi Informacijskega pooblaščenca (4 % letnega prometa na globalni ravni).

Rezultate analize tveganja je treba prenesti tudi v Pravilnik o zavarovanju osebnih podatkov. Ne glede na to, kaj bo določal ZVOP-2, je zelo priporočljivo, da ga izdela vsaka vsaj malo večja organizacija. Če boste uporabili vzorec, mora besedilo, preden ga zakoniti zastopnik podpiše, vsebovati dejansko stanje varnosti obdelave v vaši organizaciji (v njem torej ne sme biti zapisano nekaj, česar v praksi pri vas ni). Po drugi strani pa je pri pripravi pravilnika treba upoštevati minimalne standarde zavarovanja, ki jih organizacija mora upoštevati (rezultati analize tveganj). Pravilnik naj bo – kolikor se le da, konkreten in jedrnat. Naj služi kot zelo konkretna navodila za zavarovanje osebnih podatkov, pri čemer se vzdržite tudi *kopipejstanja* materialnopravnih določb GDPR oz. zakona (v njem torej ne pisati definicij, kaj je osebni podatek, katere zbirke obdeluje organizacija, roki hrambe ...). Priporočamo tudi, da nespoštovanje pravilnika vežete na delovnopravne sankcije.

3.1 Izdelava IKT varnostne politike

Na podlagi analize tveganj in določil v Pravilniku o zavarovanju osebnih podatkov, priporočamo, da večje organizacije izdelajo tudi varnostno politiko v IKT sistemih, ki so lahko nekoliko podrobnejša in namenjena v prvi vrsti varnosti v IKT okoljih (jih torej ne rabijo poznati vsi zaposleni) – ta politika naj vsebuje načine neprekinjenega poslovanja, konkretizacijo varnostnih kopij, navodila za obravnavo incidentov ...

4. Izdelava ustreznih informacij za posameznike

Ta del začnite delati čim prej, saj je treba posameznike, na katere se osebni podatki nanašajo, seznaniti z informacijami o obdelavi osebnih podatkov, kot te zahtevata člena 13 oz. 14 GDPR.

Pri tem je pomembno, da upoštevate naslednje napotke:

- posameznika je treba o informacijah obvestiti, preden ta posreduje svoje osebne podatke oz. preden jih organizacija prejme;
- obveščanje je obvezno na vseh fizičnih ali IT točkah, kjer se osebni podatki posameznika razkrijejo oz. posredujejo organizaciji (prijava na e-novice na spletni strani, sklenitev pogodbe o zaposlitvi, prijava na nagradno igro ...);
- pri pisanju informacij bodite pazljivi na to, za katero pravno podlago gre pri obdelavi in posledično tej pravni podlagi prilagodite pravice posameznika – kdaj se uporablja katera od pravic, je določeno v členih 15 – 21 GDPR (primer: če gre za izvajanje pogodbe, posameznik nima pravice do izbrisa osebnih podatkov);
- primarno morajo biti informacije podane v isti obliki, kot je oblika, preko katere posameznik posreduje osebne podatke (npr. če gre za prijavo na e-novice na spletni strani, morajte informacije biti na tej strani);
- primarno morajo biti vse informacije na isti (pod-)strani ali na istem dokumentu (lahko so informacije tudi priložene k izvirnemu dokumentu – bistveno je, da so skupaj), kot je oblika, preko katere se osebni podatki pridobivajo – na spletni strani je dovoljeno, da so (glede na prakso Informacijskega pooblaščenca) največ 1 klik stran (*one click away*).

5. Posebna področja

Ne pozabite, da so določena področja posebej urejena – bodisi s področno zakonodajo bodisi z ZVOP-1/2. Zato morate pri teh področjih upoštevati specialna določila – npr. videonadzor, biometrija, neposredno trženje (še posebej tudi ZEKom-1 v primeru e-trženja), obdelava zbirk v javnem sektorju, povezovanje zbirk ...

6. »Ponovi vajo«

Ko enkrat izvedete vse doslej opisane postopke, morate vedno znova preverjati, ali vse skupaj še vedno drži, torej:

- ali smo začeli obdelovati nove osebne podatke za nov namen –> treba je izdelati DPIA, po potrebi dopolniti pravilnik, dodatno izobraziti zaposlene ...
- preverba tehnološkega razvoja → ali je treba vpeljati dodatne varovalke, posodobiti sisteme, nadgraditi gesla ... → dopolniti pravila zavarovanja ...
- ali se je spremenila zakonodaja → dopolniti EDO, pravilnik, dodatna izobraževanja ...

Skladnost torej ni enkratna zadeva, pač pa je konstantna in vsaka organizacija mora slediti tako zakonodaji, tehnološkemu napredku, kakor tudi dejanskemu stanju v organizaciji.

Pripravil: Klemen Kraigher Mišič, DPO Univerze v Ljubljani