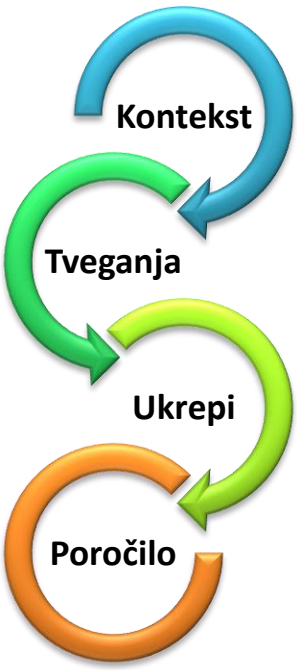
GDPR

OCENE UČINKOV NA VARSTVO PODATKOV

Smernice Informacijskega pooblaščenca



INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo opis ocen učinkov v zvezi z varstvom (osebnih) podatkov (DPIA) kot orodja za pravočasno identifikacijo in upravljanje tveganj v povezavi z osebnimi podatki. Smernice pojasnjujejo zakonske določbe in dajejo odgovore kdo, kdaj, zakaj in kako naj izvede DPIA.
Ciljne javnosti:	Upravljavci in obdelovalci podatkov iz javnega in zasebnega sektorja.
Status:	Javno
Verzija:	1.0
Datum izdaje:	23. 11. 2017
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, ocene učinkov v zvezi z varstvom (osebnih) podatkov, DPIA, načelo odgovornosti, tveganja, predhodno posvetovanje, Splošna uredba o varstvu podatkov, GDPR, pooblaščene osebe za varstvo osebnih podatkov, DPO.

KAZALO

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

Namen smernic Informacijskega pooblaščenca je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način ter s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk osebnih podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam zakonodaje o varstvu osebnih podatkov.

Pravno podlago za izdajo smernic Informacijskemu pooblaščencu daje 3(b) odstavek 58. člena Splošne Uredbe (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; GDPR), ki določa, da ima vsak nadzorni organ pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, med drugim, da na lastno pobudo ali na zahtevo izdaja mnenja za nacionalni parlament, vlado države članice ali, v skladu s pravom države članice, druge institucije in telesa, pa tudi za javnost, o vseh vprašanjih v zvezi z varstvom osebnih podatkov. Podobno določa tudi 27. člen Direktive (EU) 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 (njen prenos v slovenski pravni red naj bi poskrbel nov Zakon o varstvu osebnih podatkov).

Vse smernice, ki jih je izdal Informacijski pooblaščenec, so objavljene na spletni strani: https://www.ip-rs.si/publikacije/prirocniki-in-smernice/.

Informacijski pooblaščenec priporoča, da si ogledate tudi:

- mnenja na: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ in
- brošure na: http://www.ip-rs.si/publikacije/prirocniki/.

HITRI VODIČ

OCENA UČINKA (DPIA) JE ORODJE ZA IDENTIFIKACIJO, ANALIZO IN ZMANJŠEVANJE TVEGANJ GLEDE NEZAKONITIH RAVNANJ Z OSEBNIMI PODATKI, DO KATERIH LAHKO PRIDE PRI DOLOČENEM PROJEKTU, SISTEMU ALI UPORABI TEHNOLOGIJE.

1 PREVERIMO, ALI MORAMO IZVESTI DPIA?

GLEJ KRITERIJE NA STRANI 15
GLEJ SEZNAME V PRILOGAH 3 IN 4

2 OK, MORAMO IZVESTI DPIA… KAKO?

IZVEDBA DPIA V 4 KORAKIH

3 A IMATE ŠE KAKŠEN NASVET?

IMAMO STRAN 36

PRIMER OBLADOVANJA TVEGANJ – KORISTI DPIA:

Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
Neveljavna privolitev posameznikov ZAKONITOST, PRAVIČNOST IN PREGLEDNOST	Velika, če ne bomo previdno oblikovali obrazca za privolitev, če ne bo dokazljiva …	Velika: nezakonita obdelava, grozijo visoke kazni, izbris podatkov	Visoka	Podrobno preverimo pogoje za veljavnost privolitve in jih upoštevamo pri snovanju obrazca za privolitev

OSNOVA SO **TEMELJNA NAČELA VARSTVA OSEBNIH PODATKOV**

UVOD

Splošna 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; v nadaljevanju **GDPR**[1]), ki se začne uporabljati 25. 5. 2018, daje velik poudarek preventivnim ukrepom varstva osebnih podatkov v okviru novega temeljnega načela, **načela odgovornosti** (angl. accountability), ki poudarja in obenem zahteva preventivno in proaktivno ravnanje upravljavcev in obdelovalcev podatkov. Ocene učinkov v zvezi z varstvom podatkov (angl. Data Protection Impact Assessment; v nadaljevanju DPIA[2]), kot jih opredeljuje **35. člen GDPR**[3], predstavljajo enega ključnih konceptov v okviru načela odgovornosti.

Upravljavci, ki stremijo k odgovornemu ravnanju z osebnimi podatki posameznikov, bi morali prepoznati **DPIA kot orodje, ki je primarno v njihovem interesu**. Namenjeno je namreč **pravočasni identifikaciji tveganj** in sprejemu ustreznih ukrepov za **obvladovanje tveganj**, s čimer lahko upravljavci in obdelovalci **preprečijo, da bi prišlo do kršitve zakonodaje**. Kršitve namreč prinašajo možnost visokih kazni, obveznost poročanja o zaznanih kršitvah (v določenih primerih tudi obveščanje vseh prizadetih posameznikov), kar lahko vodi v zahtevne popravljalne ukrepe, sankcije, negativno publiciteto in izgubo zaupanja. Zaupanje v odgovorno ravnanje s podatki posameznikov bi moralo biti v informacijski družbi, kjer so osebni podatki najpomembnejša valuta, ključno. Podjetja in inštitucije, ki bodo prepoznale pomen svobodne izbire posameznika in zaupanja v odgovorno ravnanje s podatki bodo bolj uspešna od tistih, ki ne bodo izvajala ukrepov za ohranitev in dvig zaupanja. DPIA v tem kontekstu predstavljajo eno ključnih orodij, pričujoče smernice pa naj bi vam pomagale, kako DPIA izvesti zakonsko skladno in s tem učinkovito obvladovati tveganja glede osebnih podatkov.

Smernice temeljijo na **smernicah Delovne skupine iz člena 29** (Article 29 Working Party; A29 WP[4]), katere član je tudi IP, s tem da smo smernice A29WP **nadgradili s hitrim vodičem, praktičnimi prikazi in konkretnimi priporočili**, podane pa so na uporabnikom **bolj razumljiv in prijazen način**.

Sestavni del smernic so tudi **seznami vrst obdelav osebnih podatkov**, pri katerih je **DPIA obvezna** (Priloga 3) in vrst obdelav osebnih podatkov, kjer **DPIA ni obvezna (Priloga 4)**. Sezname po določbah GDPR sprejmejo nacionalni nadzorni organi po 25. 5. 2018, ko se začne uporabljati GDPR.

[1] Več o GDPR: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/#c1647.
[2] Več o zgodovinskem ozadju in značilnostih (D)PIA: http://www.rogerclarke.com/DV/PIAHist-08.html.
[3] DPIA predvideva tudi 27. člen **Direktive (EU) 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.
[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

1 O OCENAH UČINKOV V ZVEZI Z VARSTVOM PODATKOV (DPIA)

1.1 Kaj so ocene učinkov v zvezi z varstvom osebnih podatkov?

Ocene učinkov v zvezi z varstvom osebnih podatkov (DPIA) predstavljajo **orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki**, do katerih lahko pride pri določenem **projektu**, **sistemu** ali **uporabi tehnologije**. DPIA so se najprej uveljavile kot orodje pri snovalcih zakonodaje, politik in projektov v Kanadi, Avstraliji in ZDA[5], počasi pa si utirajo pot tudi v evropskem prostoru, kjer so glavni zagon dobile s sprejemom **GDPR**. DPIA so namreč po določbah GDPR **pod določenimi pogoji obvezne**.

DPIA temeljijo na sistematični in pravočasni identifikaciji tveganj za nezakonita ravnanja z osebnimi podatki, s katerimi se lahko **tveganja ustrezno upravlja -** pravočasno identificira, odpravi, zmanjša ali sprejme. Po eni strani so DPIA podobne inšpekcijskemu nadzoru zakonitosti obdelave osebnih podatkov, ki ga izvaja Informacijski pooblaščenec in kjer je poudarek na *ex-post* ugotavljanju skladnosti z zakonodajo, medtem ko je namen DPIA *ex-ante* analiza tveganj ter prilagajanje in optimizacija postopkov za doseganje skladnosti z zakonodajo.

1.2 Zakaj so DPIA koristne?

Informacijski pooblaščenec je v inšpekcijskem nadzoru pogosto odkril nepravilnosti in kršitve zakona, do katerih ne bi prišlo, če bi zavezanec (upravljavec ali pogodbeni obdelovalec osebnih podatkov), pred izvedbo določnega projekta ali uporabo določene tehnologije pravočasno izvedel DPIA in tako sam zmanjšal tveganje za nastanek nezakonitosti ali takšno tveganje v celoti izničil.

Pomen in učinkovitost DPIA narašča z velikostjo in intenzivnostjo obdelave osebnih podatkov v projektu, pri čemer lahko za »projekt« štejemo:

- spremembo zakonodaje,
- uvedbo, povezovanje ali razvoj novih informacijskih rešitev,
- konkretno uporabo določene tehnologije,
- razširitev namena obdelave že zbranih osebnih podatkov ali načina obdelave (npr. izvoz podatkov),
- drugo pomembno spremembo v poslovnem okolju s pomembnejšim vplivom na varstvo osebnih podatkov.

Marsikdaj je namreč mogoče cilje projekta doseči na način, ki ne zahteva obdelave osebnih podatkov, ali pa z manjšo količino in težo osebnih podatkov oziroma z upoštevanjem koncepta vgrajenega varstva podatkov (angl. Data Protection by Design) poskrbeti za skladnost s temeljnimi načeli in zahtevami zakona. »*Zberimo še te podatke – nam bodo že kdaj prišli prav!*«, ali pa »*Nič ne bomo brisali podatkov, kaj veš, kdaj jih bomo še potrebovali.*« in »*Tehnologija omogoča zbiranje in obdelavo teh podatkov, torej moramo to tudi izkoristiti.*«, so klasična napačna razmišljanja, ki kasneje vodijo v težave pri doseganju skladnosti z zakonodajo.

Z izvedbo DPIA lahko:

- pravočasno ugotovimo, kje bi lahko kršili zakonodajo,
- uvedemo primerne ukrepe za izogibanje in zmanjševanje tveganj,
- izkazujemo skladnost z načelom odgovornega ravnanja s podatki in
- se izognemo kršitvam zakonodaje, ki lahko vodijo v:
    - uvedbo inšpekcijskih postopkov

[5] V omenjenih državah predvsem kot presoje vplivov oz. ocene učinkov na širši koncept zasebnosti - Privacy Impact Assesments oz. PIA; v evropskem prostoru se z GDPR uveljavlja koncept »Data Protection Impact Assessment« oz. DPIA.

- izrek upravnih glob
- negativno medijsko poročanje
- izgubo dobrega imena zaupanja s strani posameznikov, deležnikov in javnosti v našo organizacijo.

In ne nazadnje – izvedbo DPIA v določnih primerih zahteva zakonodaja.

1.3 Kakšni so konkretni primeri koristi DPIA?

Naštejmo nekaj primerov, s katerimi se je srečal Informacijski pooblaščenec:

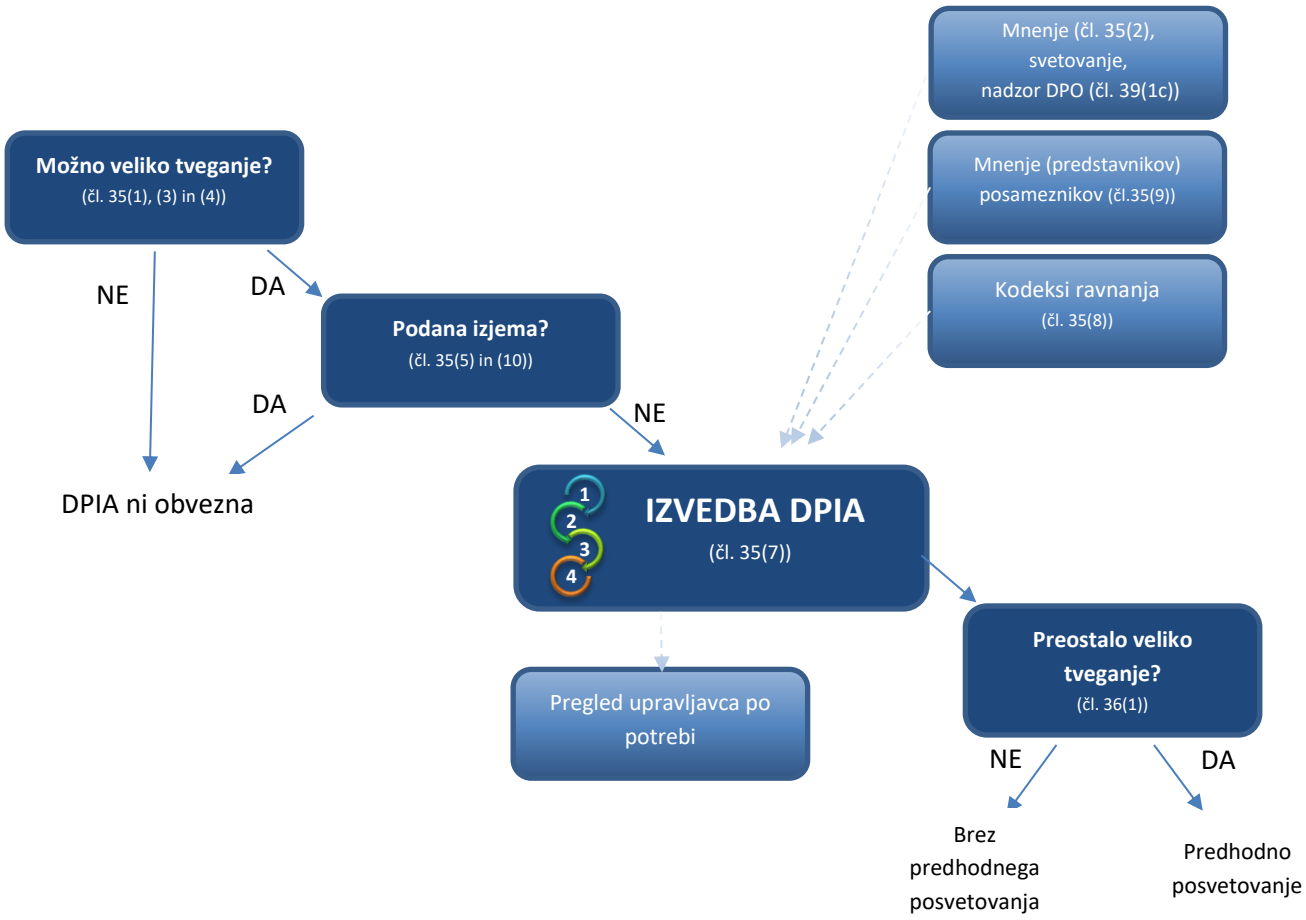
- Podjetje je pred zagonom **projekta za avtomatsko upravljanje parkirišča na podlagi bralnika registrskih tablic** opravilo DPIA po temeljnih načelih varstva osebnih podatkov, na podlagi tega minimiziralo nabor zbranih podatkov, uvedlo dodatne varnostne ukrepe in za opravljeno DPIA prejelo priznanje Informacijskega pooblaščenca Ambasador zasebnosti.
- **Sistem za elektronske vozovnice** v javnem potniškem prometu je nepotrebno beležil osebne podatke o času in kraju vstopa potnikov z mesečnimi vozovnicami, s čimer je prišlo do nesorazmerne obdelave osebnih podatkov – predhodna DPIA ni bila izvedena in potrebni so bili dragi ter zamudni popravki informacijskega sistema.
- Trgovec, ki izdaja **kartice zaupanja**, je želel začeti z zbiranjem osebnih podatkov o nakupnih navadah kupcev – po izvedeni DPIA je pravočasno ustavil načrt pisnega obveščanja kupcev o načrtovanem zbiranju teh osebnih podatkov s predvidevanjem *tihe privolitve* kupcev in je uvedel pravilno zbiranje *aktivno podanih* osebnih privolitev posameznikov ter si s tem prihranil verjetno visoko globo in zahtevo po brisanju podatkov.
- Programska oprema določenega ponudnika ne zagotavlja **sledljivosti obdelave osebnih podatkov**. Če tega nismo ugotovili pred odločitvijo za njegovo opremo, bomo morali bodisi zamenjati ponudnika programske opreme, bodisi naročiti verjetno drago nadgradnjo. Obojemu bi se lahko izognili s pravočasno izvedeno DPIA.

2 ZAKONSKA UREDITEV DPIA

Zahteve glede ocen učinkov opredeljuje **35. člen GDPR**. V primeru, ko je iz ocene učinka v zvezi z varstvom podatkov razvidno, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja, se mora upravljavec pred obdelavo posvetovati z nadzornim organom, kot to zahteva **36. člen GDPR**. Pomembna je tudi vloga **pooblaščene osebe za varstvo podatkov** (Data Protection Officer; DPO) pri izvajanju DPIA (**39. člen**).

Ozadje, pomen in dodatne informacije v zvezi z DPIA pa podajajo tudi **številne uvodne določbe GDPR**, zato v tem poglavju najdete zadevne določbe, kot se nahajajo v GDPR.

Umeščenost DPIA v GDPR prikazuje naslednja slika[6]:



2.1 Določbe GDPR

35. člen GDPR določa naslednje[7]:

1. 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, upravljavec pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov. V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.

2. Upravljavec pri izvedbi ocene učinka v zvezi z varstvom podatkov za mnenje zaprosi pooblaščeno osebo za varstvo podatkov, kjer je ta imenovana.

3. Ocena učinka v zvezi z varstvom podatkov iz odstavka 1 se zahteva zlasti v primeru:

*a) **sistematičnega in obsežnega vrednotenja osebnih vidikov** v zvezi s posamezniki, ki temelji na **avtomatizirani obdelavi**, vključno z oblikovanjem **profilov**, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;*

[6] Nadgrajeno po smernicah A29 WP.
[7] Op.: poudaril Informacijski pooblaščenec.

b) ***obsežne obdelave posebnih vrst podatkov*** *iz člena 9(1)* ***ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški*** *iz člena 10, ali*
c) ***obsežnega sistematičnega spremljanja javno dostopnega območja****.*

4. Nadzorni organ ***določi in objavi seznam vrst dejanj obdelave****, za katere* ***velja zahteva po oceni učinka****. Nadzorni organ te* ***sezname posreduje odboru iz člena 68***[8]*.*

5. Nadzorni organ lahko tudi določi in objavi ***seznam vrst dejanj obdelave****,* ***za katere ne velja*** *zahteva po oceni učinka v zvezi z varstvom podatkov. Nadzorni organ te sezname posreduje odboru.*

6. Pristojni nadzorni organ pred sprejetjem seznamov iz odstavkov 4 in 5 uporabi ***mehanizem za skladnost****, kadar taki seznami vključujejo dejavnosti obdelave, ki so povezane z nudenjem blaga ali storitev posameznikom, ali s spremljanjem njihovega ravnanja v več državah članicah ali pa lahko znatno vplivajo na prosti pretok osebnih podatkov v Uniji.*

7. ***Ocena zajema vsaj****:*
a) ***sistematičen opis predvidenih dejanj*** *obdelave in* ***namenov*** *obdelave, kadar je ustrezno pa tudi* ***zakonitih interesov****, za katere si prizadeva upravljavec;*
b) *oceno* ***potrebnosti*** *in* ***sorazmernosti*** *dejanj obdelave glede na njihov namen;*
c) ***oceno tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka 1, ter***
d) ***ukrepe za obravnavanje tveganj****, vključno z zaščitnimi ukrepi,* ***varnostne ukrepe*** *ter mehanizme za zagotavljanje varstva osebnih podatkov in za* ***dokazovanje skladnosti*** *s to uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, ter drugih oseb, ki jih to zadeva.*

8. Pri ocenjevanju učinka dejanj obdelave, ki jih izvajajo upravljavci ali obdelovalci, opravljenem zlasti za namene ocene učinka v zvezi z varstvom podatkov, se ***upošteva****, ali zadevni upravljavci ali obdelovalci spoštujejo odobrene* ***kodekse ravnanja iz člena 40****.*

9. Po potrebi upravljavec glede predvidene obdelave zaprosi za mnenje posameznikov, na katere se nanašajo osebni podatki, ali njihovih predstavnikov, brez poseganja v zaščito komercialnega ali javnega interesa ali varnost dejanj obdelave.

10. Kadar je pravna podlaga za obdelavo v skladu s točko (c) ali (e) člena 6(1) pravo Unije ali pravo države članice, ki velja za upravljavca, to pravo ureja zadevno posebno dejanje obdelave ali niz zadevnih dejanj obdelave, in je bila ocena učinka v zvezi z varstvom podatkov že izvedena v okviru splošne ocene učinkov med sprejemanjem te pravne podlage, se odstavki 1 do 7 ne uporabljajo, razen če države članice menijo, da je treba tako oceno opraviti pred dejavnostmi obdelave.

11. Upravljavec ***po potrebi opravi pregled***[9]*, da bi ocenil, ali obdelava poteka v skladu z oceno učinka v zvezi z varstvom podatkov vsaj takrat,* ***ko se spremeni tveganje****, ki ga predstavljajo dejanja obdelave.*

V tesni povezavi s členom 35 je tudi člen 36, ki opredeljuje zahteve glede predhodnega posvetovanja z nadzornim organom.

Člen 36 - Predhodno posvetovanje

1. Upravljavec se pred obdelavo posvetuje z nadzornim organom, ***kadar je iz ocene učinka*** *v zvezi z varstvom podatkov iz člena 35* ***razvidno, da bi obdelava povzročila veliko tveganje****, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.*

[8] European Data Protection Board oz. krajše "odbor" (EDPB).
[9] Angl. review.

2. Kadar nadzorni organ meni, da bi predvidena obdelava iz odstavka 1 ***kršila to uredbo****, zlasti kadar upravljavec ni ustrezno opredelil ali ublažil tveganja, nadzorni organ v roku do osmih tednov po prejemu zahteve za posvetovanje pisno svetuje upravljavcu, kadar je ustrezno, pa tudi obdelovalcu, in lahko uporabi katero koli pooblastilo iz člena 58. To obdobje se lahko ob upoštevanju kompleksnosti predvidene obdelave podaljša za nadaljnjih šest tednov. Nadzorni organ o vsakem takem podaljšanju obvesti upravljavca in, kadar je potrebno, obdelovalca v enem mesecu od prejema zahteve za posvetovanje, skupaj z razlogi za zamudo. Ta rok se lahko začasno odloži, dokler nadzorni organ ne pridobi informacij, ki jih je zahteval za namene posvetovanja.*

3. Pri posvetovanju z nadzornim organom v skladu z odstavkom 1 upravljavec ***nadzornemu organu predloži****:*

(a) kadar je ustrezno, dolžnosti upravljavca, skupnih upravljavcev in obdelovalcev, vključenih v obdelavo, zlasti pri obdelavi v povezani družbi;
(b) namene in sredstva predvidene obdelave;
(c) ukrepe in zaščitne ukrepe za zaščito pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, v skladu s to uredbo;
(d) kadar je ustrezno, kontaktne podatke pooblaščene osebe za varstvo podatkov;
(e) ***oceno učinka*** *v zvezi z varstvom podatkov iz člena 35 in*
(f) vsakršne druge informacije, ki jih zahteva nadzorni organ.

4. Države članice se med pripravo predloga zakonodajnega ukrepa, ki ga sprejme nacionalni parlament, ali regulativnega ukrepa, ki temelji na takšnem zakonodajnem ukrepu, ki se nanaša na obdelavo, posvetujejo z nadzornim organom.

5. Ne glede na odstavek 1 lahko pravo države članice od upravljavcev zahteva, naj se posvetujejo z nadzornim organom in od njega prejmejo predhodno dovoljenje v zvezi z obdelavo s strani upravljavca z namenom izvajanja naloge, ki jo upravljavec izvaja v javnem interesu, vključno z obdelavo v zvezi s socialnim varstvom in javnim zdravjem.

2.2 Pomembne uvodne določbe GDPR

Za boljše razumevanje DPIA je treba upoštevati tudi relevantne uvodne določbe GDPR, in sicer: (75), (76), (77), (84), (90), (91), (92), (93), (95). Bistvene elemente smo posebej oblikovno poudarili.

(75) *Tveganje za pravice in svoboščine posameznika, ki se razlikuje po **verjetnosti** in **resnosti**, je lahko **posledica obdelave OP**, ki bi lahko povzročila **fizično**, **premoženjsko** in ali **nepremoženjsko škodo**, zlasti:*

- *kadar obdelava lahko privede do **diskriminacije, kraje ali zlorabe identitete, finančne izgube**, **okrnitve ugleda**, **izgube zaupnosti osebnih podatkov**, zaščitenih s poklicno molčečnostjo, neodobrene reverzije psevdonimizacije ali katere koli druge **znatne gospodarske** ali **socialne škode**;*
- *kadar bi bile posameznikom, na katere se nanašajo osebni podatki, lahko **odvzete pravice in svoboščine** ali bi jim bilo **preprečeno izvajanje nadzora nad njihovimi osebnimi podatki**;*
- *kadar se obdelujejo osebni podatki, ki razkrivajo **rasno ali etnično poreklo**, politična mnenja, veroizpoved ali filozofsko prepričanje ali članstvo v sindikatu, ter obdelovanje genetskih podatkov ali podatkov v zvezi z zdravjem ali podatkov v zvezi s spolnim življenjem ali kazenskimi obsodbami in prekrški ali s tem povezanimi varnostnimi ukrepi;*
- *kadar se **vrednotijo osebni vidiki**, zlasti analiziranje ali predvidevanje vidikov, ki zadevajo uspešnost pri delu, ekonomski položaj, zdravje, osebni okus ali interese, zanesljivost ali vedenje, lokacijo ali gibanje, da bi se ustvarili ali uporabljali osebni profili, kadar se obdelujejo osebni podatki ranljivih posameznikov, zlasti otrok;*
- *ali kadar obdelava vključuje **veliko število osebnih podatkov** in zadeva **veliko število posameznikov**, na katere se nanašajo OP.*

(76) ***Verjetnost in resnost tveganja*** *za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, bi bilo treba **ugotavljati glede na** **vrsto, obseg, okoliščine in namene obdelave**. Tveganje bi bilo treba oceniti na podlagi **objektivne ocene**, s katero se določi, ali dejanja obdelave podatkov pomenijo **tveganje** ali **veliko tveganje**.*

(77) *Usmerjanje izvajanja ustreznih ukrepov in dokazovanja skladnosti s strani upravljavca ali obdelovalca, zlasti kar zadeva **opredelitev tveganja**, povezanega z obdelavo, njegovo **oceno v smislu izvora, narave, verjetnosti in resnosti** ter opredelitev **najboljših praks za ublažitev tveganja**, bi se **lahko zagotovilo zlasti z** **odobrenimi kodeksi ravnanja**, **odobrenimi postopki potrjevanja**, **smernicami**, ki bi jih zagotovil odbor, ali **navodili pooblaščene osebe za varstvo podatkov**. Odbor lahko izda tudi smernice za dejanja obdelave, za katere ni verjetno, da bi povzročila veliko tveganje za pravice in svoboščine posameznikov, in navede, kateri ukrepi bi v takih primerih morda zadostovali za obravnavanje takega tveganja.*

(84) *Za povečanje skladnosti s to uredbo, kadar bodo dejanja obdelave verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov, bi moral biti **upravljavec odgovoren za izvedbo ocene učinka** v zvezi z varstvom podatkov, da bi ocenili predvsem izvor, naravo, posebnost in resnost tega tveganja. Rezultat ocene bi bilo treba upoštevati pri določitvi ustreznih ukrepov, ki jih je treba sprejeti, da bi dokazali, da je obdelava osebnih podatkov v skladu s to uredbo. Kadar se na podlagi ocene učinka v zvezi z varstvom podatkov ugotovi, da dejanja obdelave predstavljajo **veliko tveganje**, ki ga **upravljavec ne more ublažiti** z ustreznimi ukrepi v smislu razpoložljive tehnologije in stroškov izvajanja, bi se bilo **treba pred obdelavo posvetovati z nadzornim organom.***

(89) *Direktiva 95/46/ES je določala splošno obveznost glede obveščanja nadzornih organov o obdelavi osebnih podatkov. Ta obveznost prinaša upravna in finančna bremena, ni pa v vseh primerih pripomogla k izboljšanju varstva osebnih podatkov. Zato bi bilo treba take nerazlikovalne splošne obveznosti obveščanja odpraviti ter nadomestiti z učinkovitimi postopki in mehanizmi, ki se namesto tega osredotočajo na tiste vrste dejanj obdelave, ki zaradi svoje narave,*

obsega, okoliščin in namenov verjetno povzročajo veliko tveganje za pravice in svoboščine posameznikov. Take vrste dejanj obdelave so lahko tiste, ki zlasti vključujejo ***uporabo novih tehnologij*** *ali ki so nove in zanje upravljavec* ***še ni izvedel ocene učinka*** *v zvezi z varstvom podatkov ali* ***postanejo potrebne zaradi časa, ki je pretekel od prvotne obdelave****.*

(90) *V takih primerih bi moral upravljavec pred obdelavo izvesti oceno učinka v zvezi z varstvom podatkov, da bi se ocenili* ***posebna verjetnost in resnost velikega tveganja****, pri čemer bi upoštevali naravo, obseg, okoliščine in namene obdelave ter izvor tveganja. Ta ocena učinka pa* ***bi morala obsegati*** *zlasti ukrepe, zaščitne ukrepe in mehanizme, ki so načrtovani za ublažitev tega tveganja, zagotavljanje varstva osebnih podatkov in dokazovanje skladnosti s to uredbo.*

(91) *To bi moralo* ***veljati zlasti za obsežna dejanja obdelave****, ki so namenjena obdelavi precejšnje količine osebnih podatkov na regionalni, nacionalni ali nadnacionalni ravni in* ***bi lahko vplivali na veliko število posameznikov****, na katere se nanašajo osebni podatki, ter za katere je* ***verjetno, da bodo povzročila veliko tveganje****, na primer zaradi njihove občutljivosti, kadar se v skladu z doseženo stopnjo tehnološkega znanja uporablja nova tehnologija v velikem obsegu, ter tudi za* ***druga dejanja obdelave, ki povzročajo veliko tveganje*** *za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zlasti kadar ta dejanja posameznikom, na katere se nanašajo osebni podatki, otežijo uresničevanje njihovih pravic.*

Oceno učinka v zvezi z varstvom podatkov bi bilo treba izvesti ***tudi, kadar se osebni podatki obdelujejo za sprejemanje odločitev v zvezi z določenimi posamezniki*** *po kakršnem koli* ***sistematičnem in obsežnem vrednotenju osebnih vidikov*** *v zvezi s posamezniki na podlagi* ***oblikovanja profilov*** *teh podatkov ali* ***po obdelavi posebnih vrst osebnih podatkov, biometričnih podatkov ali podatkov o kazenskih obsodbah in prekrških*** *ali s tem povezanih varnostnih ukrepih. Ocena učinka v zvezi z varstvom podatkov se zahteva* ***tudi za spremljanje javno dostopnih območij v velikem obsegu, zlasti z uporabo optično-elektronskih naprav****,* ***ali za katera koli druga dejanja, za katera pristojni nadzorni organ meni, da bo obdelava verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov****, na katere se nanašajo osebni podatki, zlasti ker tem posameznikom preprečujejo uresničevanje pravice ali uporabo storitve ali pogodbe ali ker se sistematično izvajajo v velikem obsegu. Obdelava osebnih podatkov se ne bi smela šteti kot obdelava v velikem obsegu, če gre za obdelavo osebnih podatkov pacientov ali strank s strani posameznega zdravnika, drugega zdravstvenega delavca ali odvetnika. V takih primerih ocena učinka v zvezi z varstvom podatkov ne bi smela biti obvezna.*

(92) *V nekaterih okoliščinah je razumno in gospodarno, da je predmet ocene učinka v zvezi z varstvom podatkov obširnejši in ne obsega samo enega projekta, na primer* ***kadar nameravajo javni organi ali telesa vzpostaviti skupno platformo za uporabo ali obdelavo*** *ali kadar namerava več upravljavcev uvesti skupno okolje za uporabo ali obdelavo v celotnem industrijskem sektorju ali njegovem delu ali za horizontalno dejavnost v široki rabi.*

(93) *V okviru sprejetja prava držav članic, na katerem temelji opravljanje nalog javnega organa ali telesa in ki ureja zadevne posebna dejanja obdelave ali nize dejanj, lahko države članice menijo, da je treba tako oceno opraviti pred dejavnostmi obdelave.*

(94) *Kadar ocena učinka v zvezi z varstvom podatkov pokaže, da bi zaradi neobstoječih zaščitnih ukrepov, varnostnih ukrepov in mehanizmov za ublažitev tveganja* ***obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov****, in* ***upravljavec meni, da tveganja ni mogoče ublažiti z razumnimi sredstvi*** *v smislu razpoložljivih tehnologij in stroškov izvajanja,* ***bi moralo biti pred začetkom dejavnosti obdelave opravljeno posvetovanje z nadzornim organom****. Za tako veliko tveganje je verjetno, da izhaja iz določenih vrst obdelave ter določenega obsega in pogostosti obdelave, kar lahko povzroči tudi škodo za pravice in svoboščine posameznika ali poseg vanje. Nadzorni organ bi se moral na zahtevo po posvetovanju odzvati v določenem obdobju. Vendar odsotnost odziva nadzornega organa v tem obdobju ne bi smela posegati v kakršno koli posredovanje tega organa v skladu z njegovimi nalogami in pooblastili iz te uredbe, vključno s pooblastilom za prepoved dejanj obdelave. Rezultat ocene učinka v zvezi z varstvom podatkov, ki se izvede v zvezi z zadevno obdelavo, se lahko kot del tega postopka posvetovanja predloži nadzornemu organu, zlasti ukrepi, ki so predvideni za ublažitev tveganja za pravice in svoboščine posameznikov.*

(95) *Obdelovalec bi moral upravljavcu po potrebi in na zahtevo pomagati pri izpolnjevanju obveznosti, ki izhajajo iz izvedbe ocene učinka v zvezi z varstvom podatkov in predhodnega posvetovanja z nadzornim organom.*

3 DPIA – KAJ, KDO, KDAJ IN ZAKAJ?

3.1 Kaj naslavlja DPIA?

DPIA se lahko nanaša in izvede za **posamezen proces obdelav** osebnih podatkov ali pa na **več procesov (podobnih) obdelav osebnih podatkov**. Določba 35(1) namreč dopušča, da je v »eni oceni lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.«, dodatno pa to možnost omenja tudi uvodna določba 92, pri čemer mora iti za podobno naravo, obseg, okoliščine in namen obdelave[10]. Takšni primeri so lahko npr.:

- uvedba videonadzora v stavbi, kjer se nahaja več podjetij,
- uvedba sistema za nakup vozovnic, ki bo v uporabi na večjem številu prodajnih mest (en upravljavec),
- obsežna nagradna igra, kjer bo podatke sodelujočih dobilo več podjetij (skupni upravljavci).

DPIA je lahko zelo **koristno orodje tudi za proizvajalce in ponudnike različnih tehnoloških rešitev**, npr. strojne ali programske opreme ter informacijskih sistemov, ki se bo uporabljala s strani upravljavcev za obdelavo osebnih podatkov. Takšni primeri so lahko:

- programska oprema za podporo vodenju šole,
- mobilna aplikacija za rezervacijo in najem vozil,
- razvoj informacijskega sistema za bolnišnice,
- pametni števci za električno energijo ali pa
- rešitev za hrambo podatkov v oblaku.

Upoštevati je treba seveda, da so lahko upravljavci teh rešitev dolžni izvesti lastne DPIA glede specifične implementacije in uporabe opreme.

3.2 Kdo mora izvesti DPIA?

Izvedba DPIA je **obveznost upravljavca.** Načeloma se lahko njeno izvedbo zaupa tudi različnim osebam znotraj ali zunaj upravljavca, a končno je za DPIA in njeno ustreznost odgovoren upravljavec.

Kdo znotraj upravljavca naj izvede DPIA? DPIA bo pogosto terjala sodelovanje različnih služb oziroma kadrov znotraj upravljavca, praviloma bo vključena pravna služba, služba za IT, pogosto pa tudi služba za trženje, služba za informacijsko varnost. Odvisno od obsega DPIA se lahko v pripravo DPIA vključijo tudi predstavniki zaposlenih in zunanji strokovnjaki. Glede na določbe člena 35(2) mora upravljavec za mnenje oziroma sodelovanje zaprositi **pooblaščeno osebo za varstvo podatkov (DPO)**, kar mora biti tudi ustrezno dokumentirano v DPIA**. Naloga DPO[11] je med drugim tudi nadzor izvajanja DPIA (člen 39(1c)).** Pomembno pa je, da **DPO ni primarno odgovoren za izvedbo DPIA**, temveč je to lastnik ali skrbnik določenega procesa obdelave osebnih podatkov, npr. vodja trženja, če gre za projekt vpeljave kluba zvestobe ali pa vodja IT, če gre za prenovo IT sistema v organizaciji, razvoj nove aplikacije za končne porabnike ipd. DPO naj vsekakor *sodeluje* pri izvedbi DPIA, ni pa izvedba njegova odgovornost.

[10] »V nekaterih okoliščinah je razumno in gospodarno, da je predmet ocene učinka v zvezi z varstvom podatkov obširnejši in ne obsega samo enega projekta, na primer kadar nameravajo javni organi ali telesa vzpostaviti skupno platformo za uporabo ali obdelavo ali kadar namerava več upravljavcev uvesti skupno okolje za uporabo ali obdelavo v celotnem industrijskem sektorju ali njegovem delu ali za horizontalno dejavnost v široki rabi.«

[11] Glej tudi po javni razpravi revidirane Smernice o pooblaščenih osebah za varstvo podatkov (WP 243, 5. 4. 2017; https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp243_rev01_enpdf.pdf)

V določnih primerih mora upravljavec **za mnenje zaprositi posameznike oziroma predstavnike posameznikov**, kot to določa člen 35(9). A29WP glede tega meni, da:

- bi bilo treba takšna mnenja iskati na različne načine, odvisno od okoliščin, in sicer so to lahko študije, posvetovanja, javne razprave, ankete in druge analize pomembnih vprašanj npr. glede namena obdelave, varovalk in podobno;
- bi morali biti v primeru neupoštevanja mnenja posameznikov oziroma predstavnikov posameznikov razlogi za nadaljevanje s projektom *dokumentirani*:
- bi moral upravljavec dokumentirati morebitne razloge, da se ni posvetoval s posamezniki oziroma predstavniki posameznikov.

Kdo so lahko relevantni predstavniki posameznikov? Gre lahko npr. za združenje potrošnikov, civilne iniciative, strokovna združenja, zbornice in forume (npr. s področja informacijskih tehnologij, komunikacij in varnosti, trženja, medicine …). Takšni predstavniki lahko pravočasno opozorijo na morebitne težave z vidika informacijske varnosti, pravic posameznikov, lahko predlagajo primerne varovalke za minimizacijo obdelave podatkov in na splošno pripomorejo k pravočasni identifikaciji tveganj in njihovem upravljanju.

Dobra praksa	Primer
Upoštevanje in vključitev relevantnih poslovnih enot oziroma sektorjev v pripravo DPIA.	Pri izvedbi DPIA za vzpostavitev kluba zvestobe je smiselno vključiti sektor za IT in/ali informacijsko varnost, saj bodo pomembni IT vidiki in informacijska varnost.
Vključitev primernih strokovnjakov oz. pridobitev strokovnih mnenj (pravnikov, tehnikov, varnostnih strokovnjakov), kjer je to primerno.	Pred razvojem aplikacije za oddaljeno hrambo zdravstvenih podatkov izvedemo posvetovanja s strokovnjaki na področju medicine.
Vključitev DPO v pripravo DPIA.	DPO lahko: • predlaga, kdaj je treba izvesti DPIA, • pomaga pri izbiri in uporabi DPIA metodologije, • pomaga pri oceni tveganj, • pomaga pri ozaveščanju sodelujočih pri DPIA glede načel, definicij, pravil in dolžnosti glede varstva osebnih podatkov.

3.3 Kdaj je DPIA obvezna?

DPIA ni obvezna splošno za vse upravljavce in za vse obdelave osebnih podatkov, temveč takrat, ko je možno (obstaja verjetnost), da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave **povzročila <u>veliko tveganje</u> za pravice in svoboščine posameznikov**. GDPR taksativno določa nekaj primerov, kjer bi obdelava »povzročila veliko tveganje za pravice in svoboščine posameznikov«, in sicer npr. v naslednjih primerih:

a) ***sistematičnega in obsežnega vrednotenja osebnih vidikov*** *v zvezi s posamezniki, ki temelji na* ***avtomatizirani obdelavi****, vključno z oblikovanjem* ***profilov****, in je osnova za odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo;*
b) ***obsežne obdelave posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški****, ali*
c) ***obsežnega sistematičnega spremljanja javno dostopnega območja****.*

Posebej relevantne so pri uvajanju novih tehnologij[12]. Opozoriti je treba, da **ne gre za končen seznam**, saj lahko velika tveganja povzročijo tudi druge vrste obdelave. Smernice A29WP zato podajajo nekaj kriterijev, ki naj bi bolj ilustrativno pokazali, kdaj gre za visoka tveganja. **Konkreten seznam obdelav, kdaj je DPIA obvezna (35(4)) in kdaj ni obvezna (35(5)) sprejme posamezen nadzorni organ (glej Prilogi 3 in 4) in jih posreduje EDPB. Spodaj navedeni kriteriji in primeri so ilustrativne narave.**

Smernice A29WP podajajo naslednje **kriterije**, ki naj bi se upoštevali pri odločitvi, **ali je DPIA obvezna ali ne**:

Kriterij	Primeri
Evalvacija in razvrščanje posameznikov, vključno s profiliranjem in napovedovanjem[13]	- odločanje o ustreznosti komitenta glede pridobitve kredita na podlagi podatkov v SISBONU in drugih podatkov - genetsko testiranje in ugotavljanje verjetnosti za nastanek določene bolezni - beleženje podatkov o vožnjah in ustvarjanje profilov voznikov za popust pri zavarovanju
Avtomatizirano odločanje s pravnimi ali podobnimi pomembnimi učinki	- avtomatizirano odločanje o pridobitvi/zavrnitvi: stanovanjskega ali drugega kredita, denarne socialne omoči, štipendije, usposobljenosti za delo, zdravstvenega zavarovanja …
Sistematični nadzor[14]	- Beleženje registrskih tablic mimo vozečih vozil - Preverjanje uporabnikov bencinskega servisa s seznamom ubežnikov brez plačila - Videonadzor prireditve na javnem prostoru iz brezpilotnika - Videonadzor javnih površin
Posebne vrste osebnih podatkov[15] in drugi podatki bolj občutljive narave[16]	- Zdravstveni podatki o pacientih v bolnišnici - Kazenske in prekrškovne evidence - Podatki o lokaciji, elektronski komunikaciji posameznika, spletne varnostne kopije podatkov posameznika[17], pametne naprave, ki beležijo aktivnosti posameznika - Podatki o varovankah v varnih hišah, o pripadnikih določene vere, članih drugih društev, ki zbirajo posebne vrste podatkov
Množičnost obdelave osebnih podatkov, podkriteriji: - **število (ali delež) zadevnih posameznikov,** - **obseg podatkov,** - **trajanje ali stalnost obdelave,** - **geografski obseg obdelave.**	- Klubi zvestobe pri trgovcih - Podatki o uporabi elektronskih komunikacij pri operaterjih - Podatki o zavarovancih in škodnih primerih pri zavarovalnicah

[12] Glej uvodni določbi 89 in 91.
[13] Glej uvodni določbi 71 in 91.
[14] Zlasti primeri, kjer se posameznik ne more izogniti obdelavi njegovih podatkov ali se obdelave sploh ne zaveda.
[15] Kot jih definira 9. člen GDPR.
[16] Smernice A29WP poudarjajo, da lahko »občutljivost podatkov« izvira iz razloga, ker so povezani z zasebnim življenjem (npr. zasebne komunikacije), ker imajo vpliv na temeljene človekove pravice (npr. na pravico do nediskriminaicje, prostorske zasebnosti ipd.) ali ker imajo lahko resne posledice za posameznika v primeru zlorab (npr. kraja finančnih podatkov).
[17] Čeprav gre lahko za t.i. izjemo domače, osebne rabe, ima uporaba takšnih podatkov s strani ponudnika za druge namene (npr. prodaja podatkov tretjim osebam)ali pa kršitev varnosti (izguba podatkov, javna objava podatkov) za posameznika lahko zelo resne posledic.

	- Registri na državni ravni - Podatki o komitentih in njihovi uporabi bančnih storitev v bankah in hranilnicah
Primerjanje in kombiniranje različnih zbirk podatkov (npr. pridobljenih skozi različne aktivnosti upravljavca) in analitika na osnovi masovnih podatkov	- Primerjanje podatkov o zavarovancih in podatkov o škodnih primerih pri zavarovalnici z namenom ugotavljanje deležev, trendov, vzročno-posledičnih povezav ipd. - Primerjanje podatkov o absentizmu in podatkov o spolu, starosti in izobrazbi zaposlenih - Primerjanje nakupovalnih navad in podatkov o gibanju kupcev
Obdelava podatkov ranljivih (skupin) posameznikov[18], kjer obstaja občutno nesorazmerje moči med upravljavcem in posameznikom.	- Obdelava osebnih podatkov zaposlenih, otrok, psihičnih bolnikov, prosilcev za azil, migrantov, starejših, pacientov …
Inovativna uporaba obstoječih in novih tehnologij, katerih osebne in družbene posledice niso nujno dobro raziskane in poznane	- Biometrijska prepoznava prstnih odtisov, obraza - Testiranje genetskih vzorcev - Določene naprave in senzorji v okviru interneta stvari (npr. »pametne igrače«)
Obdelava, ki omejuje pravice posameznika[19] ali obdelava podatkov, katere cilje je omogočiti ali preprečiti posamezniku dostop do storitev ali pogodbe	- Obdelava podatkov o uporabi avtocestnega omrežja z elektronskim cestninjenjem - Predhodno preverjanje kreditne sposobnosti komitenta

A29WP meni, da **več kot je kriterijev izpolnjenih, večja je verjetnost, da bo DPIA obvezna. Zlasti če sta izpolnjena dva ali več kriterijev**. Če je izpolnjen samo en kriterij, potem DPIA mogoče ne bo potrebna, a je treba upoštevati, da se kriteriji pogosto prepletajo. V določenih primerih pa bo DPIA obvezna, tudi če je relevanten samo en kriterij. Upoštevati je namreč treba vse pomembne okoliščine in imeti celovit pregled - včasih bo imel en vidik zelo visoko težo. Po drugi strani – če upravljavec meni, da obdelava sicer izpolnjuje kriterije, a po njegovem prepričanju ne terja izvedbe DPIA, mora za to navesti in dokumentirati svoje argumente, ki ji lahko preveri nadzorni organ.

A29WP in IP podajamo nekaj dodatnih primerov:

Primer	Možni relevantni kriteriji	DPIA obvezna?
Bolnišnica v okviru bolnišničnega informacijskega sistema obdeluje podatke o genetskih in zdravstvenih podatkih pacientov.	- Posebne vrste podatkov - Podatki o ranljivih vrstah posameznikov	Da
Uporaba videonadzornih kamer za nadzor obnašanja voznikov na avtocestah. Upravljavec predvideva namestitev inteligentne video analitike z možnostjo prepoznave registrskih tablic.	- Sistematični nadzor - Inovativna uporaba obstoječih in novih tehnologij, katerih osebne in družbene posledice niso nujno dobro raziskane in poznane	Da
Zbiranje podatkov z družabnih omrežij z namenom ustvarjanja profilov.	- Evalvacija in razvrščanje posameznikov - Množičnost obdelave osebnih podatkov	Da

[18] Glej uvodno določbo 75.
[19] 22. člen in 91. uvodna določba.

Arhivska hramba psevdonimiziranih podatkov iz klinične raziskave	-	Posebne vrste podatkov - Podatki o ranljivih vrstah posameznikov - Obdelava, ki omejuje pravice posameznika	Da
Obdelava zdravstvenih podatkov pri posameznem zdravniku ali odvetniku[20]	-	Posebne vrste podatkov - Podatki o ranljivih vrstah posameznikov	Ne
Pošiljanje dnevnih novičk po e-pošti s strani spletnega časopisa	-	Množičnost obdelave osebnih podatkov	Ne
Uvrstitev tekačev v tekaškem društvu v različne hitrostne skupine na podlagi podatkov o dosežkih na posameznih razdaljah[21]	-	Evalvacija in razvrščanje posameznikov, toda nesistematično in neintenzivno	Ne

Smernice A29WP navajajo, da lahko v določenih primerih pride do situacije, ki je blizu zgoraj navedenim kriterijem, a upravljavec meni, da pogoji za obvezno izvedbo DPIA niso podani. V takšnih primerih se priporoča, da upravljavec dokumentira razloge, zaradi katerih se je odločil ne izvesti DPIA in zabeleži morebitno mnenje DPO[22] glede tega.

V določenih primerih DPIA **ni obvezna,** in sicer:

- ko obdelava verjetno ne bo **povzročila velikega tveganja za pravice in svoboščine posameznikov (člen 35(1));**
- ko so narava, obseg, okoliščin in nameni obdelave **zelo podobni obdelavi, za katero je DPIA že bila izvedena (člen 35(1[23]));**
- ko je **pravna podlaga za obdelavo pravo Unije ali pravo države članice**, ki velja za upravljavca, to pravo ureja zadevno posebno dejanje obdelave ali niz zadevnih dejanj obdelave, in je bila ocena učinka v zvezi z varstvom podatkov že izvedena v okviru splošne ocene učinkov med sprejemanjem te pravne podlage, razen če država članica meni, da je treba tako oceno opraviti pred dejavnostmi obdelave (člen 35(10));
- ko gre za takšno obdelavo, ki je na seznamu vrst obdelav, za katere **nadzorni organ meni, da DPIA ni potrebna** (člen 35(5). Takšen seznam lahko taksativno našteva vrste obdelave ali pa podaja usmeritve in kriterije v obliki priporočil, smernic in podobno.
- Ko je bila **obdelava osebnih podatkov v okviru izdane odločbe že predhodno preverjena s strani nadzornega organa[24]** pred 25. 5. 2018 in se specifične okoliščine niso spremenile (glej tudi odgovor na naslednje vprašanje).

Ne pozabite – izvedba DPIA je primarno v interesu upravljavca!

[20] Glej uvodno določbo 91.
[21] Primer iz smernic A29WP se nanaša na spletno stran, ki prodaja avtomobile starodobnike in v omejenem obsegu profilira glede na prej ogledane ali kupljene starodobnike v okviru iste spletne strani.
[22] Če ga mora imenovati po GDPR.
[23] »V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.«
[24] Npr. v postopkih, kjer je bila potrebna pridobitev predhodnega dovoljenja (odločbe) IP, kot na področju biometrijskih ukrepov ali povezovanja zbirk v javnem sektorju.

Ali je DPIA obvezna za obdelave, ki so se pričele izvajati pred uporabo GDPR?

Zahteve GDPR glede izvedbe DPIA stopijo v uporabo s 25. 5. 2018, A29WP in IP pa priporočata, da se DPIA začnejo izvajati že prej. Če se je obdelava podatkov pričela pred 25. 5. 2018, pa je po tem datumu prišlo do pomembnih sprememb v tveganjih, naravi, obsegu, kontekstu ali namenih, je DPIA treba izvesti. Večji nabor zbranih podatkov, dodatni nameni obdelave in druge okoliščin imajo namreč lahko pomembne vpliv na ustrezno pravno podlago, sorazmernost, varnost podatkov in druge pomembne vidike, zato je DPIA treba izvesti. Takšni so lahko naslednji **primeri**:

- Podjetje ima že vrsto let klub zvestobe, za uvedbo katerega je sicer izvedlo predhodno oceno učinkov, po 25. 5. 2018 pa bi ga rado nadgradilo z uvedbo profiliranja najbolj zvestih strank in izvajanjem posamezniku prilagojenega oglaševanja (**novi nameni, nove funkcionalnosti, profiliranje**).
- Podjetje želi nadgraditi svoj obstoječi videonadzorni sistem z zmožnostjo video analitike za prepoznavo čakalnih vrst in detekcije pozabljenih predmetov (**novi nameni, nove funkcionalnosti, večji obseg zbranih podatkov**).
- Državni organ se odloči za zamenjavo IT platforme, ki nudi dokumentni sistem in možnost elektronske komunikacije med zaposlenimi (**nov pogodbeni obdelovalec, iznos podatkov v tretje države, novi vidiki informacijske varnosti**).

Kdaj izvesti DPIA – pred obdelavo, vmes ali potem?

DPIA je treba vedno izvesti **pred obdelavo osebnih podatkov**, kot to določa 35. člen GDPR in uvodni določbi 90 in 93 in skladno s konceptoma vgrajenega in privzetega varstva podatkov. Kot smo že omenili, gre za orodje za upravljanje tveganj in v podporo odločanju *preden pride do tveganj* in naknadna DPIA ne bi imela toliko pozitivnih učinkov. DPIA bo pogosto treba razumeti kot proces, zlasti v primerih, ko se lahko okoliščine delovanja dinamično spreminjajo.

Osveževanje DPIA v rednih intervalih, npr. **vsaj na 3 leta**, je dobra praksa, saj se v vmesnem času ob hitrih tehnoloških in družbenih spremembah, lahko pomembno spremenijo okoliščine obdelave osebnih podatkov; navedeno velja tudi za obdelave, ki so se pričele pred 25. 5. 2018. Odgovorni upravljavci bodo verjetno zaradi zasledovanja lastnih interesov po skladnosti poslovanja skozi bolj ali manj formalne postopke DPIA ponovno ovrednotili tveganja in ukrepe za zagotavljanje skladnosti z zakonodajo. Smernice A29WP poudarjajo, da je osveževanje DPIA ključno za ohranjanje skladnosti[25].

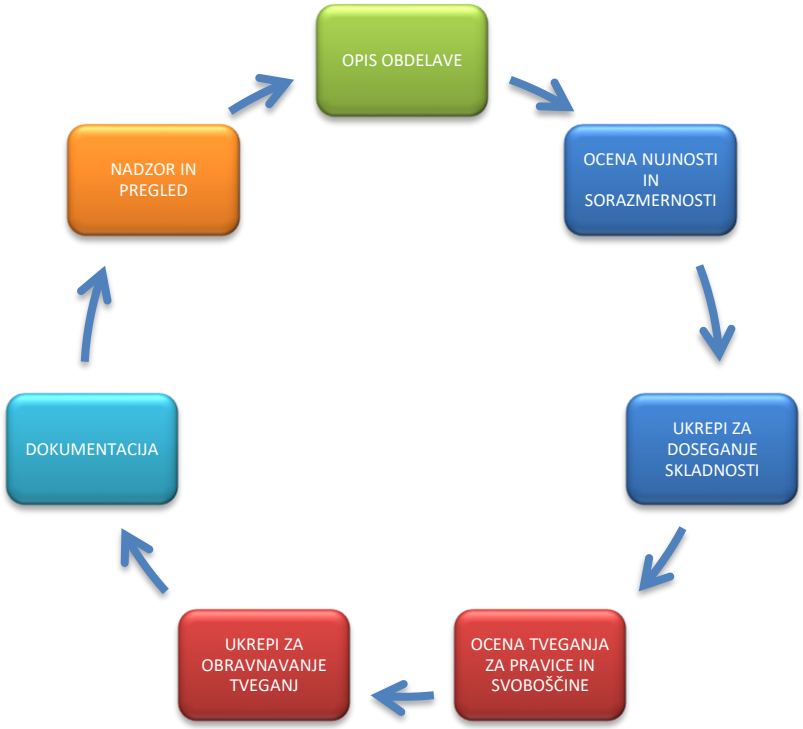
4 KAKO IZVESTI DPIA?

GDPR določa minimalni **nabor obveznih sestavin DPIA** (člen 35(7) in uvodni določbi 84 in 90), in sicer naj **DPIA vsebuje**:

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

[25] Smernice A29WP navajajo, da se lahko tveganja tudi znižajo (npr. s prenehanjem avtomatiziranega odločanja)

Na spodnji sliki je prikazan generični proces izvedbe DPIA[26].



Opozoriti velja, da gre za iterativni proces - posamezne faze bo verjetno treba izvesti večkrat, preden se lahko DPIA dokonča. IP priporoča, da uporabite vsaj 4-fazni postopek, kot ga opisujemo v nadaljevanju.

4.1 Metodologija izvedbe DPIA

Najprej je treba priti do ocene, **ali je DPIA obvezna ali ne**.

Za **kriterije**, ki naj bi se upoštevali pri odločitvi, **ali je DPIA obvezna ali ne,** glej **poglavje 3.3. ter Prilogi 3 in 4.** Če ugotovimo, da bi obdelava, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave **povzročila veliko tveganje za pravice in svoboščine posameznikov**, potem moramo nadaljevati in izvesti DPIA.

S pomočjo kriterijev in seznamov s strani nadzornih organov smo torej prišli do ugotovitve, da moramo izvesti DPIA. Kako jo izvedemo?

[26] Vir: Smernice A29WP.

Obstajajo različne metodologije za izvedbo DPIA – nekaj metodoloških okvirov predstavljamo v prilogi. Glede na to, da je DPIA v izhodišču orodje za upravljanje s tveganji (na sicer specifičnem področju varstva osebnih podatkov), je moč iskati vzporednice in smernice v uveljavljenih **standardih za upravljanje s tveganji**, kot je standard ISO/IEC 31000[27], saj gre za[28]:

- **Ugotovitev konteksta** (»ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov«).
- **Oceno tveganj** (»oceniti posebno verjetnost in resnost velikega tveganja«).
- **Obvladovanje tveganj** (»ukrepe, zaščitne ukrepe in mehanizme, ki so načrtovani za ublažitev tega tveganja, zagotavljanje varstva osebnih podatkov in dokazovanje skladnosti s to uredbo.«).

DPIA in standard varovanja informacij ISO/IEC 27001

*Analize tveganj v DPIA imajo načeloma širši obseg kot analiza tveganj po standardu varovanja informacij ISO/IEC 27001. Velja upoštevati, da je v izhodišču ocene tveganj po DPIA **posameznik in njegove pravice**, medtem ko je pri ocenah tveganj na drugih področjih, kot je informacijska varnost, izhodišče **organizacija.** DPIA namreč temeljijo na temeljnih načelih varstva osebnih podatkov, od katerih je zavarovanje osebnih podatkov, ki je sorodno cilju varovanja informacij po ISO/IEC 27001, samo eno od temeljnih gradnikov varstva osebnih podatkov. DPIA namreč obravnava, ali se obdeluje prekomerno število podatkov, za kakšne namene se podatki obdelujejo, ali obstaja pravna podlaga za obdelavo osebnih podatkov, ali so podatki ustrezno zavarovani itd. Segment zavarovanja osebnih podatkov (angl. data security) pa je tisto stično področje med DPIA in ISO/IEC 27001 in tu standard ISO/IEC 27001 s fazami, kot so analiza tveganja in načrt obravnave tveganja, odlično sovpada z zahtevo GDPR glede zagotavljanja celovitosti, zaupnosti in razpoložljivosti osebnih podatkov.*

GDPR **ne predpisuje uporabe določene metodologije** za DPIA in upravljavcem pušča določeno mero **fleksibilnosti** glede izbire in uporabe metodologije. Ena najpomembnejših zahtev glede DPIA pa je, da to ni promocijski material, ki našteva cilje in prednosti določenega projekta, storitve ali procesa, temveč da gre primarno za oceno in upravljanje s tveganji. DPIA, ki se večinoma ukvarjajo s prednostmi nekega projekta, npr. zakaj bi bilo dobro videonadzorni sistem nadgraditi z bralniki registrskih tablic, kaj bomo s tem dosegli in podobno, ne opravljajo svoje naloge. Poudarek je na pravem razmisleku o

DPIA, ki se večinoma ukvarja s prednostmi nekega projekta in premalo pozornosti posveča tveganjem, jih podcenjuje ali zapostavlja, ni ustrezna! *Če sami ne boste pravočasno identificirali tveganj, bodo tveganja namesto vas odkrili **mediji, nadzorni organi, posamezniki**.*

[27] Več o standardu: https://www.iso.org/iso-31000-risk-management.html.
[28] Uvodna določba 90.

tveganjih, o negativnih plateh, o možnih kršitvah in zlorabah, s ciljem, da se jim izognemo, in ne zgolj na prednostih nekega projekta.

Primeri **metodoloških pristopov** k DPIA so predstavljeni v **Prilogi 1**. Nadzorni organi spodbujamo in priporočamo nastanek **sektorsko-specifičnih metodologij** za izvedbo DPIA, saj so kot takšne lahko bolje prilagojene specifikam posameznega sektorja. Tveganja, ukrepi, tehnologija in druge okoliščine so namreč lahko zelo različne v sektorju pametnih števcev, pri uporabi brezpilotnikov ali pri uvajanju novih policijskih pooblastil. Pri nas tako že imamo nekaj specifičnih okvirjev za DPIA oziroma za presoje vplivov na zasebnost, in sicer so bile s strani IP (pred sprejemom Splošne uredbe o varstvu podatkov) že izdane smernice za:

- **Presoje vplivov na zasebnost pri projektih eUprave** (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf),
- **Smernice o presoji vplivov na zasebnost pri uvajanju novih policijskih pooblastil** (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf) in
- **Obrazec ocene učinkov v zvezi z varstvom osebnih podatkov pri brezpilotnih letalnikih** (https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Obrazec_ocene_ucinkov_v_zvezi_z__varstvom_osebnih_podatkov.doc).

Upravljavci lahko, kot rečeno, **sami izberejo metodologijo za izvedbo DPIA**. Ne glede na izbrano metodologijo pa mora DPIA ustrezati zahtevam, kot jih določa GDPR. A29WP je zato razvila **kriterije**, ki se lahko uporabijo za oceno, ali je DPIA bila ustrezno izvedena – **kriterije ustreznosti DPIA** najdete v **Prilogi 2**.

Priporočamo, da izvedba DPIA poteka v **4 fazah**:

4.1.1 Opredelitev konteksta

V prvi fazi opredelimo kontekst obdelave, »**osebno izkaznico projekta**«, v katerem navedemo oz. opišemo:

- nabor podatkov,
- namene obdelave,
- podatkovne tokove,
- način(e) pridobivanja podatkov,
- način in sredstva obdelave podatkov (uporabljeno opremo, omrežja, človeške vire …),
- udeležene subjekte (pravne osebe: upravljavce in obdelovalce ter uporabnike),
- roke hrambe.

Iz opis projekta mora biti razvidno, kateri podatki bodo obdelovani, kako se bodo zbirali, izmenjevali in kdo bo imel v teh procesih kakšne vloge. Pomembno je opisati tudi morebitne posebne okoliščine, npr. visoko občutljivost podatkov (npr. podatki o zdravstvenem stanju), nizko transparentnost obdelave (posamezniki ne bodo razumeli obdelave oz. se ne bodo zavedali, da poteka), posebna varnostna tveganja (npr. posebna privlačnost za hekerske napade). **Namen opredelitve konteksta ni navajanja prednosti projekta in podrobno opisovanje, kaj želimo doseči s projektom!** Ne pozabite, da je namen DPIA predvsem obvladovanje tveganj in ne promocija.

4.1.2 Analiza tveganj

Ko smo projekt okvirno opisali, sledi identifikacija možnih tveganj, pri čemer smo pozorni na raven tveganja. Več poudarka moramo posvetiti tveganjem, katerih dejanska uresničitev je bolj verjetna in ima težje posledice, zato moramo oceniti raven tveganja.

Raven tveganja predstavlja vsoto ali zmnožek:

a) **verjetnosti**, da se bo tveganje uresničilo, in
b) **resnosti** oziroma teže posledic, ki jih bo imela uresničitev tveganja.

Bolj kot je verjetno, da se tveganje udejanji, in težje kot so posledice, če se to res zgodi, višja bo raven tveganja, ki ga moramo obravnavati. Vsem tveganjem se bomo težko izognili, a če njihovo raven znižamo na raven sprejemljivega, smo storili veliko. Nekatera tveganja so nizke ravni, ker:

- je zelo majhna verjetnost, da se bodo uresničila,
- tudi če se uresničijo, ne bodo imela težkih posledic.

Kombinacija verjetnosti uresničitve in teže posledic nam da odgovor, ali moramo tveganje obravnavati.

Primeri:

Tveganje	Verjetnost	Resnost	Raven tveganja
Poplava, ki lahko uniči sistemsko sobo, kjer imamo vse podatke **CELOVITOST IN ZAUPNOST (INFORMACIJSKA VARNOST)**	Majhna, ker nismo na poplavnem območju, v bližini sistemske sobe ni vodovodnih cevi	Velika, izguba vseh podatkov, ker nimamo varnostnih kopij na drugi lokaciji	**Visoka**
Zbrani podatki ne bodo točni **TOČNOST**	Majhna, ker zbiramo samo e-naslov, ki ga posameznik sam vpiše	Majhna, ker uporabljamo potrditveni e-mail, da se prepreči nezaželene vpise	**Nizka**
Privolitev posameznikov ni veljavna **ZAKONITOST, PRAVIČNOST IN PREGLEDNOST**	Velika, če ne bomo previdno oblikovali obrazca za privolitev, če ne bo dokazljiva …	Velika, vse nadaljnje obdelave podatkov so lahko nezakonite, grozijo visoke kazni, potencialno izbris nezakonito zbranih podatkov	**Visoka**

Za ocene tveganj obstajajo številne metodologije in tudi prilagojena programska orodja (vsaj za področje informacijske varnosti). Izbira metodologije in orodij je prepuščena upravljavcu.

Ocena tveganja se izvede po temeljnih načelih varstva osebnih podatkov. Ključni deli ocene tveganj naj bi sledili (vsem) temeljnim načelom varstva osebnih podatkov, kot jih določa 5. člen GDPR:

Ne gre torej samo za vprašanja varnosti – kako zaščititi podatke pred izgubo in nepooblaščenim dostopom, temveč obdelamo tudi tveganja, ki izhajajo iz drugih načel. Nič nam ne pomaga, če smo podatke odlično zašifrirali, če pa sploh nimamo pravne podlage, da smo jih zbrali. Tveganja poskusimo razvrstiti glede na temeljna načela. Z drugimi besedami – temeljna načela lahko uporabimo kot kazalo oz. poglavja, v katere razvrstimo ugotovljena tveganja.

Zakonitost, poštenost in preglednost

Načelo zakonitosti pomeni, da mora za obdelavo osebnih podatkov obstajati **pravna podlaga**. Možne pravne podlage, najpogostejši sta podlaga v zakonu in privolitev, opredeljuje 6. člen[29] GDPR:

a) **privolitev** posameznika;
b) **potrebnost za izvajanje pogodbe, katere pogodbena stranka je posameznik**;
c) obdelava je **potrebna za izpolnitev zakonske obveznosti**, ki velja za upravljavca;
d) obdelava je potrebna **za zaščito življenjskih interesov posameznika**;
e) obdelava je **potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti**;
f) obdelava je **potrebna zaradi prevladujočih zakonitih interesov** upravljavca ali tretje oseba, **razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika**.

[29] Upoštevati je treba tudi preostale določbe 6. člena GDPR, ki omejujejo uporabo določenih podlag oz. omogočajo državi članic, da v svoji zakonodaji določena področja posebej uredi. Prav tako je treba upoštevati specifične določbe glede **posebnih vrst osebnih podatkov** (člen 9).

Z oceno učinka preverimo vprašanja, kot so npr.:

- Katera je ustrezna pravna podlaga v našem primeru?
- Kakšno obliko privolitve bomo izbrali (pisno, elektronsko, ustno …)?
- Ali bomo lahko dokazali privolitev?
- Ali je bila privolitev podana aktivno in ali je bila informirana?
- Ali lahko uporabimo pravno podlago prevladujočih interesov?
- Ali potrebujemo izrecno privolitev (npr. ker želimo izvajati profiliranje)?
- Na ta način ocenimo tveganja, kot so:
    - Nimamo dokazov o zbranih privolitvah.
    - Privolitev je nična, ker ni informirana.
    - Zanašali smo se na napačno pravno podlago.

Tveganja pri načelu zakonitosti so izjemno pomembna, saj si ne želimo privoščiti, da imamo osebne podatke zbrane nezakonito! Posebej preverite člene 6, 7 in 9 ter uvodne določbe: 32, 33, 42, 43 in 171.

Poštenost in preglednost

Poštenost se nanaša na to, da mora obdelava osebnih podatkov potekati na pošten način do posameznika, kar pomeni, da posameznik ne sme biti zaveden, da se mora zavedati, v kaj se spušča, da se njegove privolitve ne pogojuje ali izsiljuje. Preglednost pa v povezavi s poštenostjo pomeni, da je posameznik jasno in pravočasno informiran o tem, kateri njegovi osebni podatki se bodo obdelovali, za katere namene in kdo (vse) jih bo obdeloval, komu in pod kakšnimi pogoji bodo posredovani, kakšni so roki hrambe. Poleg tega bi moral biti posameznik obveščen o obstoju oblikovanja profilov in njegovih posledicah. Prav tako ga je treba obvestiti tudi o tem, ali je dolžan predložiti osebne podatke, in o posledicah, kadar takih podatkov ne predloži, ter o pravicah, ki jih ima v zvezi s svojimi podatki. V javnem sektorju naj bi ti načeli zagotovili z upoštevanjem načela zakonitosti (določenost v zakonu), v zasebnem sektorju pa je bistvena ustrezna informiranost posameznika, da lahko na podlagi zadostnih informacij poda svojo privolitev kot prostovoljno izjavo volje v obdelavo določenih osebnih podatkov za določene namene. **Posebej preverite zahteve iz poglavja III GDPR.**

Brez poštenosti in preglednosti ne moremo govoriti o zakonitosti – brez ustrezne informiranosti je privolitev posameznika lahko nična, obdelava osebnih podatkov pa posledično nezakonita!

Z oceno učinka se izognemo tveganjem, npr. da bo privolitev posameznika:

- neveljavna, ker ni bil ustrezno seznanjen, kdo in zakaj bo uporabljal njegove podatke,
- pod vprašajem, ker je bila pogojevana ali ker je bil posameznik prisiljen v podajo osebnih podatkov.

Posebno pozornost moramo nameniti **izvrševanju pravic posameznika** (glej predvsem člene GDPR od 15 do 22), saj tudi v zvezi s tem obstajajo določena tveganja (npr. da nimamo ustreznih procesov in ne moremo pravočasno ali pravilno odgovoriti na zahtevek posameznika).

Omejitev namena

Osebni podatki se lahko uporabljajo samo za namene, za katere so bili zbrani. Takšno določbo vsebuje že Ustava RS, z oceno učinka pa poskušamo ugotoviti npr.:

- Za katere vse namene bi želeli uporabljati osebne podatke?
- Kako bomo zastavljene namene opredelili in predstavili posamezniku?
- V povezavi z načelom najmanjšega obsega podatkov – kateri je tisti minimalni nabor podatkov, s katerim lahko dosežemo zadane cilje in minimalni nabor oseb, ki se morajo seznaniti z osebnimi podatki?

Pravočasen in temeljit razmislek o namenih in potencialnih namenih uporabe osebnih podatkov je pomemben, saj bomo za namene, ki jih nismo predvideli na začetku, potrebovali novo privolitev, ker je neizogibno povezano z dodatnimi stroški in časom.

DPIA mora analizirati tudi **tveganja za zlorabe načela namenskosti**, ko že uporabljamo osebne podatke, zato premislimo:

- Ali bomo znali ugotoviti, ali naši zaposleni uporabljajo osebne podatke **za zakonite namene** ali pa za **svoje zasebne namene** (radovednost, delanje uslug prijateljem, celo prodaja osebnih podatkov za postranski zaslužek)?
- Ali bi z **združevanjem zbirk** podatkov, ki se vodijo za različne namene, lahko **prišlo do novih namenov** obdelave podatkov, ki jih prvotno nismo načrtovali in za katere nimamo pravne podlage?

Posebna tveganja zlasti pri velikih, centraliziranih zbirkah podatkov predstavlja t.i. pojav spremembe namembnosti, ang. »**function creep**«, ko se podatki primarno zberejo za ene namene, nato pa se s časom pojavijo dodatne ideje, za kaj vse bi se lahko še uporabili ti podatki. Pomislite na primeru obstoja centralizirane zbirke podatkov o uporabi avtocest – prvotni namen bi bil plačevanje cestnine po prevoženem kilometru. Koga vse bi še zanimali ti podatki? **Omenjeno tveganje je še posebej pomembno pri pripravi predlogov predpisov.**

Najmanjši obseg podatkov

Najmanjši obseg podatkov oziroma minimizacija, kot strogo upoštevanje načela sorazmernosti pomeni, da je dopustno zbrati in obdelovati le **najmanjši obseg osebnih podatkov**, ki je **potreben za dosego namena obdelave** osebnih podatkov. Sorazmernost lahko pomeni predvsem to, da **če osebni podatki niso potrebni za dosego cilja, jih ni primerno zbirati**. Polega samega obsega podatkov se sorazmernost nanaša tudi na **uporabo manj občutljivih podatkov** od tistih, katerih narava oziroma zloraba ima večjo težo (**psevdonimi** so boljši kot navadni podatki, govoreče šifre so slabše od naključnih nizov ipd.) in na to, da se dajo podatki na voljo **samo tistim osebam, ki jih dejansko potrebujejo (angl. »need to know«).**

Nekaj zelo očitnih primerov nesorazmernosti:

- aplikacija, ki pametni telefon pretvori v svetilko, zahteva pa dostop do naših sms sporočil in stikov;
- hramba podatkov o času in lokaciji vstopa potnika na mestni avtobus, če ta uporablja mesečno, pavšalno vozovnico;
- zahtevanje več enoličnih identifikatorjev hkrati (npr. EMŠO in DAVČNE številke), ko za to ni utemeljenih argumentov;
- hramba podatkov brez utemeljenega namena, »na zalogo, za vsak slučaj«;
- zbiranje podatkov od vseh vnaprej, čeprav bi zadostovali podatki samo od določenih oseb v določenih primerih.

GDPR izrecno zahteva upoštevanje sorazmernosti tudi skozi zahtevo po **upoštevanju načela vgrajenega in privzetega varstva osebnih podatkov** (člen 25). Poenostavljeno gre za to, da se privzeto obdelajo samo tisti osebni podatki, ki so potrebni za vsak poseben namen obdelave, pri tem pa se minimizira:

1. **količina** zbranih osebnih podatkov,
2. **obseg** obdelave,
3. **obdobje hrambe**,
4. **dostopnost** podatkov.

Točnost

Načelo točnosti (in ažurnosti) narekuje, da morajo biti podatki, ki se obdelujejo, točni in ažurni. Točnost pomeni, da podatki niso napačni ali nepopolni, ažurnost pa pomeni, da se uporablja zadnji, ažuren podatek. Osebni podatki so lahko točni, niso pa ažurni, kar pomeni, da se uporablja podatek, ki je bil sicer točen in veljaven v določenem obdobju ali trenutku, vendar pa obstaja novejši, bolj ažuren podatek. Pogosto slišani argument »saj nimam kaj skrivati« hitro zvodeni, če ni spoštovano načelo točnosti in ažurnosti in so o posamezniku v določeni evidenci nahajajo napačni, nepopolni ali neažurni podatki. **Težave z netočnostjo** imajo lahko **tako za posameznika kot za upravljavca zelo hude posledice**, pomislite npr.:

- da vam je zaradi podobnosti z imenom iskane osebe zavrnjena viza za potovanje,
- da zaradi pomote v EMŠO ne dobite socialne podpore,
- da se v zdravstveni dokumentaciji nahaja napačen podatek o krvni skupini ali alergijah,
- da upravljavec vaše občutljive podatke pošlje na napačen naslov.

V okviru DPIA je treba preveriti:

- ali obstaja **verjetnost, da zbrani podatki ne bodo točni in ažurni**,
- če ta verjetnost obstaja, **kako bomo preverili** točnost in ažurnost podatkov,
- ali smo pripravljeni na upoštevanje pravice posameznika do **omejitve obdelave osebnih podatkov**, ko se pojavi dvom v točnost in ažurnost podatkov (glej **18. člen GDPR**).

Omejitev shranjevanja - rok hrambe

Rok hrambe je v tesni povezavi z načelom **sorazmernosti in določa, da se osebni podatki lahko shranjujejo le toliko** časa, dokler je to **potrebno za dosego namena**, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Eden od bistvenih elementov DPIA je tudi preučitev in določitev ustreznega roka hrambe osebnih podatkov, pri čemer je ta rok lahko že določen v zakonodaji, bistveno pa je, da rok hrambe ni odprt, temveč mora biti opredeljen.

Z oceno učinka želimo ugotoviti:

- kakšen je ustrezen rok hrambe glede na namene obdelave oziroma
- identificirati (in upoštevati) roke hrambe, ki jih določa zakonodaja.

Če roka ni mogoče natančno določiti, je lahko rok vezan tudi na podajo preklica s strani posameznika.

Pomembno je tudi, da pri določitvi roka hrambe podatkov izhajamo praviloma iz lastnih namenov in ne iz namenov drugih! Podatkov nismo dolžni hraniti za namene inšpekcijskih služb, policije in drugih organov – hrambo podatkov za te namene mora določati oziroma lahko določa le zakonodaja.

Premislite s pomočjo teh primerov, **kakšen se *vam* zdi ustrezen rok hrambe podatkov**:

Ste storitveno podjetje, vaši prostori so v več nadstropjih poslovne stavbe, zaposleni uporabljajo magnetne kartice za priklic dvigal, podatki o tem se beležijo za namen preiskave vlomov in kraj.	**Rok hrambe?** Verjetno bi zadostoval kratek, mogoče enotedenski rok hrambe.
Z isto kartico zaposleni tudi evidentirajo delovni čas.	**Rok hrambe?** Evidenca o izrabi delovnega časa se začne za posameznega delavca voditi z dnem, ko sklene pogodbo o zaposlitvi, preneha pa z dnem, ko mu preneha pogodba o zaposlitvi[30].
Zunanji obiskovalci se ob vstopu v poslovno stavbo registrirajo pri receptorju.	**Rok hrambe?** Rok hrambe je v tem primeru določen z zakonom.

[30] Zakon o evidencah na področju dela in socialne varnosti.

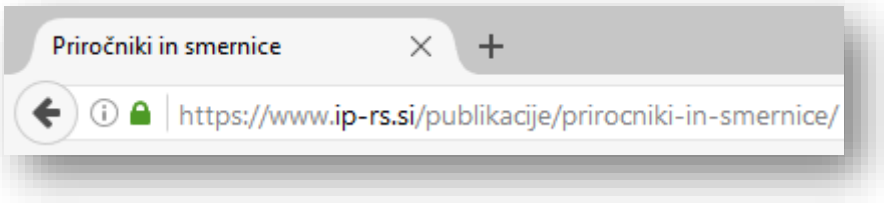
Celovitost in zaupnost (informacijska varnost)

Varstvo podatkov temelji tudi na ustreznih tehničnih in organizacijskih ukrepih, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov. Z drugimi besedami – podatke imamo lahko izjemno dobro zavarovane, kljub temu pa lahko pride do njihove zlorabe, zlasti ob neupoštevanju ostalih načel (npr. obdelava podatkov brez prave podlage, uporabe za namene, ki so različni od namena zbiranja podatkov, predolga hramba podatkov ipd.). **Načeli celovitosti in zaupnosti sta z načelom razpoložljivosti temeljna stebra informacijske varnosti.**

Z izvedeno oceno učinkov želimo:

- ugotoviti, kateri so primerni varnosti ukrepi glede na okoliščine, obseg in namene obdelave;
- premisliti, katere tehnične in katere organizacijske ukrepe moramo postaviti;
- zagotoviti, da bodo varnostni ukrepi ustrezno opredeljeni v politikah in izvajani v praksi;
- preprečiti izgubo, javno objavo, nepooblaščen dostop in druge neželene dogodke.

Glej tudi **Smernice o zavarovanju osebnih podatkov** s primeri dobrih in slabih praks, kontrolnim seznamom za manjše upravljavce, vprašalnikom, ki se uporablja v inšpekcijskih postopkih, ter napotki na standarde, smernice in dobre prakse:



Načelo odgovornosti

Načelo odgovornosti[31] predstavlja novo načelo v evropskem konceptu varstva osebnih podatkov, pomeni pa, da je upravljavec **odgovoren za skladnost** z ostalimi, zgoraj naštetimi načeli, in je to **skladnost tudi zmožen dokazati**. Načelo odgovornosti torej od upravljavcev zahteva določeno raven **proaktivnosti**, pripravljenosti in skrbnosti. Med temeljne mehanizme za zagotavljanje tega načela sodijo naslednje zahteve, ki jih pred upravljavce in obdelovalce postavlja GDPR:

- vgrajeno in privzeto varstvo podatkov (člen 25),
- zahteve glede uporabe obdelovalcev (člen 28),
- evidenca dejavnosti obdelave oz. »katalogi« (člen 30),
- varnostni ukrepi (člen 32),
- obveščanje o varnostnih incidentih (člena 33 in 34),
- ocene učinkov v zvezi z varstvom podatkov in predhodno posvetovanje (člena 35 in 36),
- pooblaščene osebe za varstvo podatkov (členi 37, 38 in 39).

Vsi navedeni mehanizmi so preventivnega značaja, z izvedeno oceno učinka pa preprečimo, da bi spregledali katere od naštetih obveznosti.

Načelo odgovornosti v praksi?

»Vemo, kdo in zakaj obdeluje podatke, držimo se temeljnih načel, imamo predpisana pravila, skrbimo za varnost podatkov in ustreznost pogodb, imamo urejene evidence in izvajamo ostale potrebne ukrepe. Pripravljeni smo na morebitni inšpekcijski pregled.«

[31] O načelu odgovornosti (oz. načelu zanesljivega izvajanja, angl. accountability) si lahko več preberete v mnenju Delovne skupine za varstvo podatkov iz člena 29, ki je dostopno na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_sl.pdf

4.1.3 Ukrepi za obvladovanje tveganj

Namen ukrepov za obvladovanje tveganj je samoumeven – kaj je treba storiti, da se identificiranim tveganjem izognemo ali jih vsaj znižamo na sprejemljivo raven. Vsem tveganjem se bomo težko izognili, a če njihovo raven znižamo na raven sprejemljivega, smo storili dovolj.

Kakšni so možni ukrepi za obvladovanje tveganj glede varstva osebnih podatkov?

Tudi ukrepe lahko razdelimo glede na **temeljna načela varstva osebnih podatkov** – poglejmo si na že predstavljenih **primerih**:

Tveganje	Verjetnost	Resnost	Raven tveganja[32]	Ukrep
Poplava, ki lahko uniči sistemsko sobo, kjer imamo vse podatke **CELOVITOST IN ZAUPNOST (INFORMACIJSKA VARNOST)**	Majhna, ker nismo na poplavnem območju, v bližini sistemske sobe ni vodovodnih cevi	Velika, izguba vseh podatkov, ker nimamo varnostnih kopij na drugi lokaciji	**Visoka**	Uvedemo oddaljeno shranjevanje varnostnih kopij …
Zbrani podatki ne bodo točni **TOČNOST**	Majhna, ker zbiramo samo e-naslov, ki ga posameznik sam vpiše	Majhna, ker uporabljamo potrditveni e-mail, da se prepreči nezaželene vpise	**Nizka**	Dodatni ukrepi niso potrebni
Privolitev posameznikov ni veljavna **ZAKONITOST, PRAVIČNOST IN PREGLEDNOST**	Velika, če ne bomo previdno oblikovali obrazca za privolitev, če ne bo dokazljiva …	Velika, vse nadaljnje obdelave podatkov so lahko nezakonite, grozijo visoke kazni, potencialno izbris nezakonito zbranih podatkov	**Visoka**	Podrobno preverimo pogoje za veljavnosti privolitve in jih upoštevamo pri snovanju obrazca za privolitev …
Podatki v bazi bodo zelo »zanimivi« za zaposlene, ki bodo do podatkov dostopali neupravičeno **OMEJITEV NAMENA**	Velika, če gre za občutljive podatke, podatke znanih oseb, podatke, ki jih je možno prodati	Velika, v primeru razkritja podatkov veljavnosti nam grozijo kazni, tožbe …	**Visoka**	Uvede se stroga sledljivost dostopov, izobraževanje zaposlenih, posebna opozorila na zaslonu pred vsakim dostopom …
Roka hrambe predala e-pošte zaposlenih nismo opredelili, po odhodu zaposlenega se lahko pojavi zahteva po dostopu do predala **OMEJITEV SHRANJEVANJA**	Srednja, dostop do predala bodo morda potrebovali drugi zaposleni ali pa nekdanji zaposleni, e-pošta pogosto nadomešča dokumentne sisteme	Srednja, postopanje bo lahko pravno sporno, ker nismo vnaprej postavili pravil in preverili zakonodaje ter smernic in priporočil	**Srednja**	V internem aktu predpišemo postopek ravnanja s predali e-pošte po odhodu zaposlenega, preverimo določbe zakonodaje, opredelimo roke hrambe …

[32] Zapisana raven tveganja ne pomeni, da je tovrstno tveganje vedno takšne stopnje.

Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep
Zbiramo osebne podatke, ki niso potrebni **NAJMANJŠI OBSEG PODATKOV**	Visoka, če prej ne preverimo, katere podatke bomo zbirali in ali so res potrebni ali če podatke zbiramo na zalogo, od vseh vnaprej	Srednja, če ne bomo zbirali občutljivih podatkov in ne bo šlo za veliko količino podatkov	**Visoka**	Ob oblikovanju obrazca za zajem podatkov za vsak podatek posebej preverimo, ali je nujen in ali bi lahko zbrali manj občutljiv podatek, ali zadostuje psevdonim …
S ponudnikom gostovanja nimamo sklenjene pogodbe o pogodbeni obdelavi, zaradi česar smo lahko v kršitvi 28. člena GDPR **NAČELO ODGOVORNOSTI**	Nizka, če imamo vpeljan sistem nadzora nad obdelovalci, vzdržujemo celovite evidence dejavnosti obdelave, DPO …	Srednja, če naša spletna stran nima velike količine osebnih podatkov in smo najeli zaupanja vrednega izvajalca	**Srednja**	Pred vsakim sklepanjem pogodb z zunanjimi izvajalci preverimo, ali bodo prišli v stik z osebnimi podatki iz naših zbirk …

Posebno pozornost moramo nameniti **preostalim tveganjem** – če so ta visoka, potem moramo opraviti **predhodno posvetovanje z nadzornim organom** (**36. člen GDPR**).

Kdaj je treba opraviti predhodno posvetovanje z nadzornim organom?

Smernice A29WP navajajo primer varnostnih tveganj glede hrambe osebnih podatkov na prenosnikih, kjer z varnostnimi ukrepi učinkovito zmanjšamo tveganja na sprejemljive ravni (npr. šifriranje celotnega diska, ustrezno upravljanje šifrirnih ključev in dostopnih pravic, izvajanje varnostnih kopij …). Če so tveganja zmanjšana na sprejemljive ravni, ni potrebno predhodno posvetovanje.

Med primere **nesprejemljivih visokih preostalih tveganj** sodijo situacije, kjer:

- lahko posamezniki utrpijo **pomembne, celo trajne posledice zaradi zlorabe osebnih podatkov** (npr. razkritje naslova varne hiše, javna objava podatka o bolezni ali spolni nagnjenosti, razkritje podatkov o zaščitenih pričah ipd.);
- je **zelo verjetno, da se bodo tveganja tudi uresničila zaradi predvidenih načinov obsežnega zbiranja in izmenjave podatkov** (npr. večja verjetnost za napake in pomote).

V takšnih in podobnih primerih se mora upravljavec skladno z določbami 36. člena GDPR posvetovati z nadzornim organom.

Velja poudariti, da uporaba metod za psevdonimizacijo in šifriranje podatkov sama po sebi še ne pomeni, da so ti ukrepi zadostni in primerni. Obe metodi sta v GDPR navedeni primeroma, imata svoje prednosti in slabosti, nista pa vsemogočni.

Upravljavec se mora posvetovati z nadzornim organom tudi takrat, ko (člen 36(5)):

- to od njega zahteva zakonodaja,
- potrebuje predhodno dovoljenje nadzornega organa.

Kadar nadzorni organ meni, da bi predvidena obdelava kršila to uredbo, zlasti kadar upravljavec ni ustrezno opredelil ali ublažil tveganja, **nadzorni organ v roku do osmih tednov** (dodatnih 6 tednov v kompleksnih primerih) **po prejemu zahteve za posvetovanje pisno svetuje upravljavcu**, kadar je ustrezno, pa tudi obdelovalcu, in lahko uporabi katero koli pooblastilo iz člena 58 (**npr. izrek opozorila**).

4.1.4 DPIA poročilo

Če smo korektno izvedli prve tri faze izvedbe DPIA:

1. opisali smo naš projekt;
2. ocenili smo tveganja;
3. opredelili smo ukrepe za obvladovanje tveganj …

so ob tem nastali določeni zapisi, ki jih sistematično uredimo v poročilo. Iz poročila mora biti razvidno, da smo **izvedli omenjene faze** in da smo **upoštevali vse kriterije**, ki se zahtevajo, da je DPIA ustrezna - glej **Prilogo 2** glede kriterijev ustreznosti uporabljene metodologije. Priporočljivo je, da ima poročilo DPIA **povzetek in/ali zaključke**, na voljo mora biti nadzornemu organu na njegovo zahtevo. Poročilo DPIA izkazuje, da smo DPIA izvedli celovito in kakovostno in s tem ravnali skladno z zahtevami GDPR.

Ali je treba DPIA javno objaviti?

GDPR ne zahteva objave DPIA, gre za odločitev zavezanca. Upravljavci bi **lahko objavili povzetek, dela ali zaključke DPIA** z namenom večje **preglednosti** in doseganja večjega **zaupanja** v svoje postopke obdelave podatkov in upoštevanje načela odgovornosti. Smernice A29WP posebej priporočajo **objavo DPIA, ko gre za obdelavo s strani javnih organov**. Ni treba objaviti celotne DPIA, temveč pomembne dele, izpustijo pa se lahko deli, katerih razkritje bi lahko povzročilo varnostna tveganja (npr. analiza varnostnih tveganj in konkretne navedbe sprejetih ukrepov) ali razkrijte poslovnih skrivnosti – v takšnem primeru se lahko objavi povzete informacije. V primeru priprave predpisov, ki se pomembno dotikajo vprašanj varstva osebnih podatkov, bi morale biti DPIA sestavni del zakonodajnega gradiva in tudi predmet javne obravnave. Po potrebi bodo za tovrstne namene razvite specifične DPIA metodologije.

5 PRIPOROČILA

Če ne boste uporabili druge specifične metodologije vam priporočamo, da DPIA izvedete **po korakih**, kot smo jih opisali in da si kot opomnik glede celovitosti pomagate s točkami iz **Priloge 2**.

Zakaj pa nimate kakšnega konkretnega primera (»vzorca«) v celoti izdelane DPIA?

DPIA v slovenskem prostoru še niso uveljavljeno orodje za varstvo osebnih podatkov, zato ne bi želeli, da se posamezen primer izvedene DPIA dojame kot edini ustrezen primeren in da služi kot vzorec ostalim. Tudi metodologije in priročniki ostalih nadzornih organov praviloma ne podajajo konkretnih primerov izvedenih DPIA. Upoštevati je namreč treba, da se DPIA nanašajo na zelo različne situacije in kontekste in so temu primerno tudi različno obsežne in kompleksne. Pri manjših projektih lahko DPIA kvalitetno opravimo na nekaj straneh, bolj obsežni projekti pa lahko pomenijo tudi 50 in več strani dokumentacije. Če boste ustrezno sledili napotkom in priporočilom v teh smernicah, potem bi vaša DPIA morala biti dovolj kakovostna.

Na podlagi naših dosedanjih izkušenj z DPIA podajamo nekaj priporočil iz dobrih in slabih praks, ki smo jih srečali.

1. **Bodite konkretni**. »*Obdelava podatkov lahko pomeni poseg v zasebnost posameznika*, *zato mora biti skladna z zakonodajo*.« Splošne dikcije, kot je ta, niso potrebne. Raje natančno opišite tveganje, ocenite njegovo verjetnost in resnost in konkretno opredelite ukrep(e), s katerim boste to tveganje obvladovali.
2. **Bodite celoviti**. Pomislite na vsa tveganja, ki pretijo osebnim podatkom. Upoštevajte vsa temeljna načela. Ne pozabite, da **varstvo** osebnih podatkov ni samo njihova **varnost** – prva tako so pomembne pravne podlage, spoštovanje načela namenskosti in rokov hrambe ter drugih načel. Iz vsakega načela lahko izvirajo tveganja.
3. **DPIA delate zase.** Kot smo že večkrat poudarili – kakovostno opravljena DPIA vam lahko privarčuje stroške popravljalnih ukrepov, sankcij, izgube zaupanja. Odgovornim upravljavcem tega ni treba razlagati.
4. **Ocenite, koliko vas lahko stane, če *ne* izdelate DPIA.** Kakšne so možne kazni, če nimate ustreznih privolitev, če ste pozabili na kakšen varnostni ukrep in ste izgubili podatke, vam bodo stranke še zaupale?
5. **Pripravljate spremembo zakona ali drugega predpisa? Izvedite DPIA.** S tem boste lahko predstavili konkretne argumente, zakaj je določena zakonska sprememba potrebna, kako ste upoštevali varstvo osebnih podatkov in s katerimi varovalkami obvladujete tveganja, ki jih boste potrebovali v argumentaciji sorazmernosti in primernosti. Prav tako se boste izognili težavam pri izvedbi, zaradi nerealne ocene obsega dela in tudi stroškov določenega zakonodajnega ukrepa.
6. **DPIA ni reklamni material za projekt.** DPIA, ki v pretežnem delu opisuje cilje in prednosti nekega projekta, predpisa ipd. ni prava DPIA. Pretežni del DPIA se mora nanašati na oceno tveganj in možnih ukrepov.
7. **Pošteno ocenite tveganja.** Nič ne pomaga, če vsa tveganja ocenite z nizkimi stopnjami, če so v resnici visoka. Če sami ne boste pravočasno identificirali tveganj, jih bodo drugi – posamezniki, novinarji, inšpektorji, javnost, delničarji.
8. **Vključite deležnike.** Posodabljate obrazce za privolitev? V okviru DPIA vam lahko pomembno pomagajo strokovnjaki na področju uporabniške izkušnje, združenja potrošnikov in IT strokovnjaki.
9. **Vloga DPO.** DPO **svetuje** pri izdelavi DPIA, **ni pa DPO odgovoren ali zadolžen zanjo**. DPIA morajo izvesti »lastniki procesov oz. sredstev« – če npr. delate DPIA za zamenjavo dokumentnega IT sistema, potem je za izvedbo DPIA odgovorno vodstvo, direktor IT ali vodja sekretariata, ne pa DPO.
10. **Revidirajte DPIA.** Želite povečati obseg podatkov? So se pojavili dodatni nameni uporabe podatkov? Razmišljate o zamenjavi ponudnika IT sistema? Takšne spremembe okoliščin lahko bistveno vplivajo na tveganja, zato je smiselno DPIA, ki je bila izvedena pred spremembami, revidirati.

ZAKLJUČEK

Ocene učinkov predstavljajo enega temeljnih mehanizmov GDPR v smeri bolj odgovornega ravnanja z osebnimi podatki. Načelo odgovornosti namreč v GDPR dopolnjuje temeljna načela varstva osebnih podatkov, njegov smisel pa je v preventivnem delovanju in izogibanju nastanku kršitev. Kršitve na področju varstva osebnih podatkov imajo namreč lahko zelo težke, velikokrat celo nepopravljive posledice tako za posameznike kot za organizacijo, ki je uporabljala njegove osebne podatke. Upravljavci in obdelovalci osebnih podatkov lahko v primeru kršitev zakonodaje računajo na negativno medijsko poročanje, drage in zamudne popravljale ukrepe, višje sankcije in izgubo zaupanja svojih strank. Tega si nobena odgovorna organizacije ne želi in ocene učinkov so namenjene ravno izogibanju neželenim posledicam. Korektna izvedba ocene učinka, v kateri se osredotočimo na identifikacijo in obvladovanje tveganj je torej primarno v interesu upravljavcev in obdelovalcev osebnih podatkov.

Prednosti pravočasnih in celovitih izvedb ocen učinka so nekateri že dobro spoznali, žal pa so včasih napačno razumljene skoraj kot promocijski material, v katerem opišemo želene cilje in navajamo prednosti določenega projekta, aplikacije, sistema ali celo predpisa. V smernicah smo se trudili sicer relativno kompleksno ureditev ocen učinkov v GDPR prikazati na vsem razumljiv in uporaben način, saj menimo, da preveč kompleksne metodologije in suhoparne smernice, ki ne dajejo poudarka praktični uporabnosti, ne dosežejo svojega cilja.

PRILOGA 1 - Primeri obstoječih metodologij za izvedbo (D)PIA

Slovenija

- **Presoje vplivov na zasebnost pri projektih eUprave (Informacijski pooblaščenec, 2010)**: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf
- **Smernice o presoji vplivov na zasebnost pri uvajanju novih policijskih pooblastil (Informacijski pooblaščenec, 2014):** https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf
- **Obrazec ocene učinkov v zvezi z varstvom osebnih podatkov pri brezpilotnih letalnikih (Informacijski pooblaščenec, 2016):** https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/Obrazec_ocene_ucinkov_v_zvezi_z__varstvom_osebnih_podatkov.doc

Nemčija

- **Standard Data Protection Model, V.1.0 – Trial version, 2016:** https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf

Španija

- **Guía para una Evaluación de Impacto en la Protección de Datos Personales - EIPD (Agencia española de protección de datos (AGPD), 2014):** https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf

Francija

- **Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL, 2015):** https://www.cnil.fr/fr/node/15798

Združeno kraljestvo

- **Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO, 2014):** https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Primeri EU sektorskih DPIA okvirjev

- **RFID aplikacije:** Privacy and Data Protection Impact Assessment Framework for RFID Applications. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp180_annex_en.pdf
- **Napredno merjenje:** Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Kanada

- **Privacy Impact Assessments (Treasury Board of Canada Secretariat (TBS), 2010)** http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

Nova Zelandija

- **Privacy Impact Assessment Handbook (Office of the Privacy Commissioner, 2015**
  https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/

Mednarodni standardi

- **ISO/IEC 291343:**
  https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:en

PRILOGA 2 - Kriteriji za oceno ustreznosti DPIA

Kriteriji za oceno ustreznosti DPIA - **katere elemente mora vsebovati DPIA** - podajajo **smernice A29 WP:**

- ☐ **Podan je sistematičen opis obdelave (člen 35(7a)):**
  - ☐ Upoštevani so narava, obseg, okoliščine in nameni obdelave (uvodna določba 90);
  - ☐ Opredeljen je nabor podatkov, upravljavci in uporabniki ter roki hrambe;
  - ☐ Podan je opis podatkovnih tokov in udeleženih subjektov;
  - ☐ Podan je opis sredstev obdelave (strojne in programske opreme, omrežij, človeških virov in uporabljenih komunikacijskih sredstev);
  - ☐ Upoštevana je skladnost z odobrenimi kodeksi ravnanja (člen 35(8)).
- ☐ **Podana je ocena nujnosti in sorazmernosti (člen 35(7b)):**
  - ☐ Opredeljeni so ukrepi za zagotavljanje skladnosti, ki vključujejo:
    - ☐ **ukrepe, ki prispevajo k upoštevanju nujnosti in sorazmernosti, in spoštovanju temeljnih načel:**
      - ☐ določeni, izrecni in zakoniti namen(i) (člen 5(1b));
      - ☐ zakonitost obdelave (člen 6);
      - ☐ obdelava je ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki (člen 5(1c));
      - ☐ upoštevani je omejitev shranjevanja – roki hrambe (člen 5(1e));
    - ☐ **ukrepe, ki prispevajo k varstvu pravic posameznika:**
      - ☐ informiranje posameznika o obdelavi podatkov (členi 12, 13 in 14);
      - ☐ pravica do seznanitve in prenosljivosti podatkov (člena 15 in 20);
      - ☐ pravica do popravka in izbrisa podatkov (člena 16, 17 in 19);
      - ☐ pravica do ugovora in omejitve obdelave (členi 18, 19 in 21);
      - ☐ odnosi s (pogodbenimi) obdelovalci (člen 28);
      - ☐ varovalke glede prenosa podatkov v tretje države (Poglavje V.);
      - ☐ predhodno posvetovanje (člen 36).
- ☐ **Obvladovana so tveganja za pravice in svoboščine posameznika:**
  - ☐ Podana je ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84), pri čemer so tveganja ocenjena z vidika posameznika, tako da:
    - ☐ so upoštevani viri tveganj (uvodna določba 90);
    - ☐ so upoštevani možni učinki na pravice posameznika v primeru nezakonitega dostopa, spremembe ali izgube podatkov;
    - ☐ sta ocenjeni verjetnost in resnost tveganj (uvodna določba 90).
  - ☐ Opredeljeni so ukrepi za obvladovanje tveganj (člen35(7d) in uvodna določba 90).
- ☐ **Vključene so zainteresirane strani:**
  - ☐ Pridobljeno je mnenje DPO (člen 35(2));
  - ☐ Pridobljena so mnenja posameznikov oziroma predstavnikov posameznikov, kjer je to primerno (člen 35(9)).

PRILOGA 3 - SEZNAM VRST DEJANJ OBDELAVE, ZA KATERE VELJA ZAHTEVA PO OCENI UČINKA

Nadzorni organ določi in objavi seznam vrst dejanj obdelave, za katere **velja zahteva** po oceni učinka v zvezi z varstvom podatkov (35(4) člen GDPR).

Seznam bo objavljen, ko se začne uporabljati GDPR (po 25. 5. 2018).

PRILOGA 4 - SEZNAM VRST DEJANJ OBDELAVE, ZA KATERE NE VELJA ZAHTEVA PO OCENI UČINKA

Nadzorni organ lahko tudi določi in objavi seznam vrst dejanj obdelave, za katere **ne velja zahteva** po oceni učinka v zvezi z varstvom podatkov (35(5) člen GDPR).

Seznam bo objavljen, ko se začne uporabljati GDPR (po 25. 5. 2018).