



17/SL

DS 248 rev.01

**Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je „verjetno, da bi [obdelava] povzročila veliko tveganje“, za namene Uredbe (EU) 2016/679**

**Sprejete 4. aprila 2017**

**Kakor so bile zadnjič revidirane in sprejete 4. oktobra 2017**

Ta delovna skupina je bila ustanovljena na podlagi člena 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Njene naloge so opisane v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES.

Naloge sekretariata opravlja Direktorat C (Temeljne pravice in državljanstvo Unije) Evropske komisije, Generalni direktorat za pravosodje, 1049 Bruselj, Belgija, pisarna št. MO-59 03/075.

Spletišče: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm).

**DELOVNA SKUPINA ZA VARSTVO POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV,**

ustanovljena na podlagi Direktive Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995,  
je –

ob upoštevanju členov 29 in 30 Direktive,

ob upoštevanju svojega poslovnika –

**SPREJELA NASLEDNJE SMERNICE:**

# Kazalo

I.	UVOD.....	4
II.	PODROČJE UPORABE SMERNIC.....	5
III.	OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV: POJASNILO GLEDE UREDBE.....	7
A.	KAJ OBRAVNAVA OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV? ENO DEJANJE OBDELAVE ALI NIZ PODOBNIH DEJANJ OBDELAVE? .....	8
B.	ZA KATERA DEJANJA OBDELAVE JE TREBA IZVESTI OCENO UČINKA V ZVEZI Z VARSTVOM PODATKOV? KADAR „JE VERJETNO, DA [BODO] POVZROČILA VELIKO TVEGANJE“, RAZEN V PRIMERIH IZJEM. ....	9
a)	<i>Kdaj je ocena učinka v zvezi z varstvom podatkov obvezna? Kadar „je verjetno, da [bo obdelava] povzročila veliko tveganje“.....</i>	9
b)	<i>Kdaj ocena učinka v zvezi z varstvom podatkov ni potrebna? Kadar ni „verjetno, da [bi obdelava] povzročila veliko tveganje“, ali kadar obstaja podobna ocena učinka v zvezi z varstvom podatkov, ali če je bila odobrena pred majem 2018, ali če obstaja pravna podlaga, ali če je na seznamu dejanj obdelave, za katere ocena učinka v zvezi z varstvom podatkov ni potrebna. ....</i>	14
C.	KAJ PA GLEDE ŽE OBSTOJEČIH DEJANJ OBDELAVE? OCENA UČINKA V ZVEZI Z VARSTVOM PODATKOV JE POTREBNA V NEKATERIH OKOLIŠČINAH. ....	15
D.	KAKO IZVESTI OCENO UČINKA V ZVEZI Z VARSTVOM PODATKOV? .....	16
a)	<i>Kdaj je treba izvesti oceno učinka v zvezi z varstvom podatkov? Pred obdelavo.....</i>	16
b)	<i>Kdo mora izvesti oceno učinka v zvezi z varstvom podatkov? Upravljaavec skupaj s pooblaščen o sebo za varstvo podatkov in obdelovalci. ....</i>	17
c)	<i>Katero metodologijo uporabiti za izvedbo ocene učinka v zvezi z varstvom podatkov? Različne metodologije, vendar skupna merila.....</i>	18
d)	<i>Ali je treba oceno učinka v zvezi z varstvom podatkov objaviti? Ne, vendar bi lahko objava povzetka spodbudila zaupanje, celotno oceno učinka v zvezi z varstvom podatkov pa je treba nadzornemu organu sporočiti v primeru predhodnega posvetovanja ali če tako zahteva organ za varstvo podatkov. ....</i>	21
E.	KDAJ SE JE TREBA POSVETOVATI Z NADZORNIM ORGANOM? KADAR JE PREOSTALO TVEGANJE VELIKO.....	21
IV.	SKLEPNE UGOTOVITVE IN PRIPOROČILA .....	22
	PRILOGA 1: PRIMERI OBSTOJEČIH OKVIROV EU GLEDE OCENE UČINKA V ZVEZI Z VARSTVOM PODATKOV ....	24
	PRILOGA 2: MERILA ZA SPREJEMLJIVOST OCENE UČINKA V ZVEZI Z VARSTVOM PODATKOV .....	26

## I. Uvod

Uredba (EU) 2016/679<sup>1</sup> (splošna uredba o varstvu podatkov) se bo začela uporabljati 25. maja 2018. Z njenim členom 35 in z Direktivo 2016/680<sup>2</sup> se uvaja koncept ocene učinka v zvezi z varstvom podatkov<sup>3</sup>.

Ocena učinka v zvezi z varstvom podatkov je postopek, katerega namen je opisati obdelavo, oceniti njeno potrebnost in sorazmernost ter pripomoči k obvladovanju tveganj za pravice in svoboščine posameznikov, ki izhajajo iz obdelave osebnih podatkov<sup>4</sup>, tako, da se ta ocenijo in da se določijo ukrepi za njihovo obravnavo. Ocene učinka v zvezi z varstvom podatkov so pomembna orodja za prevzemanje odgovornosti, saj so upravljavcem v pomoč ne le pri izpolnjevanju zahtev iz splošne uredbe o varstvu podatkov, ampak tudi pri dokazovanju, da so bili sprejeti ustrezni ukrepi za zagotovitev skladnosti z Uredbo (glej tudi člen 24)<sup>5</sup>. Drugače rečeno, **ocena učinka v zvezi z varstvom podatkov je postopek za vzpostavitev in dokazovanje skladnosti**.

V skladu s splošno uredbo o varstvu podatkov lahko pristojni nadzorni organ zaradi neskladnosti z zahtevami iz ocene učinka v zvezi z varstvom podatkov izreče globo. Če se ne izvede ocena učinka v zvezi z varstvom podatkov, kadar jo je v zvezi z obdelavo treba opraviti (člen 35(1), (3) in (4)), če je izvedena nepravilno (člen 35(2) in (7)–(9)) ali če se ne opravi posvetovanje s pristojnim nadzornim organom, kadar se to zahteva (člen 36(3)(e)), se lahko izreče upravna globa v višini do

---

<sup>1</sup> 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).

<sup>2</sup> Člen 27 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 določa tudi, da je ocena učinka na zasebnost potrebna tudi, „kadar je možno, da bi [obdelava lahko] povzročila veliko tveganje za pravice in svoboščine posameznikov“.

<sup>3</sup> V drugih okoliščinah se za isti koncept pogosto uporablja izraz „ocena učinka na zasebnost“.

<sup>4</sup> V splošni uredbi o varstvu podatkov koncept ocene učinka v zvezi z varstvom podatkov kot tak ni formalno opredeljen, vendar

- je minimalni obseg njene vsebine določen v členu 35(7), kot sledi:
  - o „(a) sistematičen opis predvidenih dejanj obdelave in namenov obdelave, kadar je ustrezno pa tudi zakonitih interesov, za katere si prizadeva upravljavec;
  - o (b) ocen[a] potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen;
  - o (c) ocen[a] tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, iz odstavka 1, ter
  - o (d) ukrep[i] za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostn[i] ukrep[i] ter mehanizm[i] 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“;
- njen pomen in vloga pa sta pojasnjena v uvodni izjavi (84), kot sledi: „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.“

<sup>5</sup> Glej tudi uvodno izjavo (84): „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.“

10 milijonov EUR, v primeru družbe pa do 2 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji.

## II. Področje uporabe smernic

V teh smernicah se upoštevajo:

- Izjava 14/EN (WP 218) Delovne skupine za varstvo podatkov iz člena 29<sup>6</sup>;
- Smernice 16/EN (WP 243) Delovne skupine za varstvo podatkov iz člena 29 o pooblaščenim osebam za varstvo podatkov<sup>7</sup>;
- Mnenje 13/EN (WP 203) Delovne skupine za varstvo podatkov iz člena 29 o omejitvi namena<sup>8</sup>;
- mednarodni standardi<sup>9</sup>.

V skladu s pristopom na podlagi tveganj, ki je določen v splošni uredbi o varstvu podatkov, izvedba ocene učinka v zvezi z varstvom podatkov ni obvezna za vsako dejanje obdelave. Zahteva se le, kadar „je možno, da bi [obdelava lahko] povzročila veliko tveganje za pravice in svoboščine posameznikov“ (člen 35(1)). Prvi cilj teh smernic je pojasniti okoliščine, v katerih je ocena učinka v zvezi z varstvom podatkov obvezna (člen 35(3)), in določiti merila za sezname, ki jih morajo pripraviti organi za varstvo podatkov na podlagi člena 35(4), ter tako zagotoviti dosledno razlago.

Evropski odbor za varstvo podatkov bo lahko na podlagi člena 70(1)(e) izdal smernice, priporočila in dobre prakse, da se spodbudi dosledna uporaba splošne uredbe o varstvu podatkov. Namen tega dokumenta je predvideti tako prihodnje delo Evropskega odbora za varstvo podatkov in v ta namen pojasniti ustrezne določbe splošne uredbe o varstvu podatkov ter tako upravljavcem pomagati, da bodo delovali skladno s pravom, hkrati pa upravljavcem, ki morajo izvesti oceno učinka v zvezi z varstvom podatkov, zagotoviti večjo pravno varnost.

Namen teh smernic je tudi spodbujanje razvoja:

- skupnega seznama Evropske unije, na katerega se uvrstijo dejanja obdelave, za katera je ocena učinka v zvezi z varstvom podatkov obvezna (člen 35(4)),
- skupnega seznama EU, na katerega se uvrstijo dejanja obdelave, za katera ocena učinka v zvezi z varstvom podatkov ni potrebna (člen 35(5)),

---

<sup>6</sup> Izjava 14/EN (WP 218) Delovne skupine za varstvo podatkov iz člena 29 o vlogi pristopa na podlagi tveganj v pravnih okvirih varstva podatkov, sprejeta 30. maja 2014.

[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218\\_en.pdf?wb48617274=72C54532](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532).

<sup>7</sup> Smernice 16/EN (WP 243) Delovne skupine za varstvo podatkov iz člena 29 o pooblaščenim osebam za varstvo podatkov, sprejete 13. decembra 2016.

[http://ec.europa.eu/information\\_society/newsroom/image/document/2016-51/wp243\\_en\\_40855.pdf?wb48617274=CD63BD9A](http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A).

<sup>8</sup> Mnenje 3/2013 (13/EN, WP 203) Delovne skupine za varstvo podatkov iz člena 29, sprejeto 2. aprila 2013.

[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf?wb48617274=39E0E409](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409).

<sup>9</sup> Na primer ISO 31000:2009 *Risk management – Principles and guidelines* (Obvladovanje tveganj: načela in smernice), Mednarodna organizacija za standardizacijo (ISO); ISO/IEC 29134 (projekt), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (Informacijska tehnologija – varnostne tehnike – ocena učinka na zasebnost – smernice), Mednarodna organizacija za standardizacijo (ISO).

- skupnih meril za metodologijo izvedbe ocene učinka v zvezi z varstvom podatkov (člen 35(5)),
- skupnih meril za določanje, kdaj se je treba posvetovati z nadzornim organom (člen 36(1)),
- priporočil, po možnosti na podlagi izkušenj držav članic EU.

### III. Ocena učinka v zvezi z varstvom podatkov: pojasnilo glede Uredbe

V skladu s splošno uredbo o varstvu podatkov morajo upravljavci izvesti ustrezne ukrepe, da zagotovijo in lahko dokažejo skladnost z navedeno uredbo, pri čemer morajo med drugim upoštevati „tveganj[a] za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti“ (člen 24(1)). Obveznost upravljavcev, da v nekaterih okoliščinah opravijo oceno učinka v zvezi z varstvom podatkov, bi bilo treba razumeti glede na njihovo splošno obveznost ustreznega obvladovanja tveganj<sup>10</sup>, ki izhajajo iz obdelave osebnih podatkov.

„Tveganje“ je scenarij, ki opisuje dogodek in njegove posledice ter je ocenjen glede na resnost in verjetnost. „Obvladovanje tveganj“ pa je mogoče opredeliti kot usklajene dejavnosti za usmerjanje organizacije in nadzor nad njo v zvezi s tveganjem.

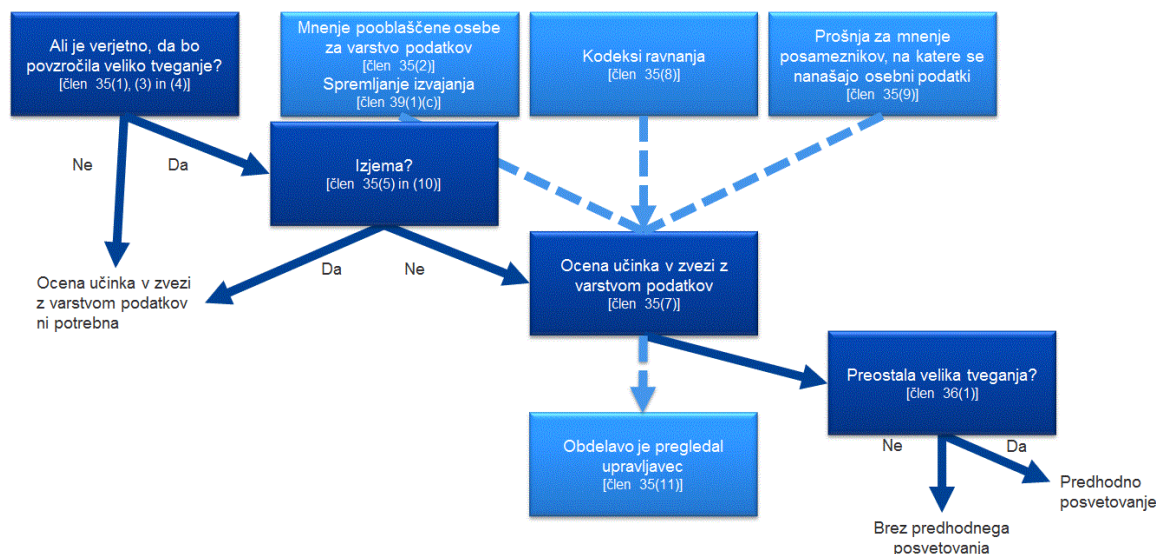
V členu 35 je navedeno verjetno veliko tveganje „za pravice in svoboščine posameznikov“. Kot je navedeno v izjavi Delovne skupine za varstvo podatkov iz člena 29 o vlogi pristopa na podlagi tveganj v pravnih okvirih varstva podatkov, se navedba „pravic in svoboščin“ posameznikov, na katere se nanašajo osebni podatki, nanaša predvsem na pravice do varstva podatkov in zasebnosti, lahko pa zajema tudi druge temeljne pravice, kot so svoboda govora, svoboda misli, svoboda gibanja, prepoved diskriminacije, pravica do svobode, vesti in vere.

V skladu s pristopom na podlagi tveganj, ki je določen v splošni uredbi o varstvu podatkov, izvedba ocene učinka v zvezi z varstvom podatkov ni obvezna za vsako dejanje obdelave. Potrebna je le, kadar „je možno, da bi lahko vrsta obdelave [...] povzročila veliko tveganje za pravice in svoboščine posameznikov“ (člen 35(1)). Zgolj dejstvo, da pogoji, ki bi sprožili obveznost izvedbe ocene učinka v zvezi z varstvom podatkov, niso izpolnjeni, še ne zmanjša splošne obveznosti upravljavca, da izvede ukrepe za ustrezno obvladovanje tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki. V praksi to pomeni, da morajo upravljavci stalno ocenjevati tveganja, ki izhajajo iz njihovih dejavnosti obdelave, da opredelijo, kdaj „je možno, da bi lahko vrsta obdelave [...] povzročila veliko tveganje za pravice in svoboščine posameznikov“.

---

<sup>10</sup> Poudariti je treba, da je treba za obvladovanje tveganj za pravice in svoboščine posameznikov ta tveganja opredeliti, analizirati, oceniti, ovrednotiti, obravnavati (na primer zmanjšati ...) in redno pregledovati. Upravljalci se odgovornosti ne morejo izogniti tako, da tveganja vključijo v zavarovalne police.

Naslednja slika prikazuje osnovna načela, ki se nanašajo na oceno učinka v zvezi z varstvom podatkov v splošni uredbi o varstvu podatkov:



A. Kaj obravnava ocena učinka v zvezi z varstvom podatkov? Eno dejanje obdelave ali niz podobnih dejanj obdelave?

**Ocena učinka v zvezi z varstvom podatkov se lahko nanaša na eno dejanje obdelave.** V členu 35(1) pa je navedeno, da je „v eni oceni [...] lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja“. V uvodni izjavi (92) je navedeno tudi: „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.“

**Uporabiti je mogoče eno oceno učinka v zvezi z varstvom podatkov za oceno več dejanj obdelave, ki so podobna** glede na naravo, obseg, okoliščine, namen in tveganja. Cilj ocen učinka v zvezi z varstvom podatkov je sistematično proučevanje novih situacij, ki bi lahko povzročile velika tveganja za pravice in svoboščine posameznikov, zato ocene učinka v zvezi z varstvom podatkov ni treba izvesti v primerih, ki so bili že proučeni (tj. dejanja obdelave, ki so izvedena v posebnih okoliščinah in za poseben namen). Primer tega je, kadar se istovrstni podatki zbirajo za iste namene z uporabo podobne tehnologije. Skupina občinskih organov, od katerih vsak vzpostavlja podoben sistem televizije zaprtega kroga CCTV, bi lahko na primer izvedla eno oceno učinka v zvezi z varstvom podatkov, ki zajema obdelavo s strani teh ločenih upravljavcev, ali pa bi lahko železniški operater (en upravljavec) v eni oceni učinka v zvezi z varstvom podatkov zajel videonadzor na vseh svojih železniških postajah. To se lahko nanaša tudi na podobna dejanja obdelave, ki jih izvajajo različni upravljavci podatkov. V takih primerih bi morala biti referenčna ocena učinka v zvezi z varstvom podatkov v souporabi ali javno dostopna, ukrepe, opisane v oceni učinka v zvezi z varstvom podatkov, je treba izvesti in treba je utemeljiti, zakaj je bila izvedena ena ocena učinka v zvezi z varstvom podatkov.

Kadar dejanje obdelave zajema skupne upravljavce, morajo natančno opredeliti svoje obveznosti. V njihovi oceni učinka v zvezi z varstvom podatkov bi morale biti določeno, katera stranka je odgovorna



za različne ukrepe za obravnavo tveganj ter varstvo pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki. Vsak upravljavec podatkov bi moral izraziti svoje potrebe in navesti uporabne informacije, ne da bi pri tem ogrozil ohranitev skrivnosti (na primer varstvo poslovnih skrivnosti, intelektualne lastnine, zaupnih poslovnih informacij) ali razkril ranljivost.

**Ocena učinka v zvezi z varstvom podatkov se lahko uporabi tudi za oceno učinka tehnološkega proizvoda** na varstvo podatkov, na primer dela strojne ali programske opreme, kadar je verjetno, da ga bodo različni upravljavci podatkov uporabljali za izvajanje različnih dejanj obdelave. Upravljavec podatkov, ki proizvod uporabi, mora seveda izvesti tudi lastno oceno učinka v zvezi z varstvom podatkov glede posebnega izvajanja, vendar je pri tem mogoče uporabiti podatke iz ocene učinka v zvezi z varstvom podatkov, ki jo pripravi ponudnik proizvoda, če je ustrezno. Primer je lahko odnos med proizvajalcem inteligentnih števec in komunalno družbo. Vsak ponudnik proizvodov ali obdelovalec bi moral ponuditi uporabne informacije, pri tem pa ne bi smel ogroziti ohranitve skrivnosti ali povzročiti varnostnih tveganj z razkritjem ranljivosti.

B. Za katera dejanja obdelave je treba izvesti oceno učinka v zvezi z varstvom podatkov? Kadar „je verjetno, da [bodo] povzročila veliko tveganje“, razen v primerih izjem.

V tem oddelku je opisano, kdaj je ocena učinka v zvezi z varstvom podatkov obvezna in kdaj je ni treba izvesti.

**Oceno učinka v zvezi z varstvom podatkov je treba izvesti, kadar je „verjetno, da [bo dejanje obdelave] povzročilo veliko tveganje“ (III.B.b.), razen če za dejanje obdelave velja izjema (III.B.a).**

a) Kdaj je ocena učinka v zvezi z varstvom podatkov obvezna? Kadar „je verjetno, da [bo obdelava] povzročila veliko tveganje“.

V skladu s splošno uredbo o varstvu podatkov ocene učinka v zvezi z varstvom podatkov ni treba izvesti za vsako dejanje obdelave, ki bi lahko povzročilo tveganja za pravice in svoboščine posameznikov. Ocena učinka v zvezi z varstvom podatkov je obvezna le, kadar „je verjetno, da [bo obdelava] povzročila veliko tveganje za pravice in svoboščine posameznikov“ (člen 35(1), kar ponazarja člen 35(3) in dopolnjuje člen 35(4)). To je še zlasti pomembno, kadar se uvaja nova tehnologija za obdelavo podatkov<sup>11</sup>.

Če ni jasno, ali je v posameznem primeru ocena učinka v zvezi z varstvom podatkov obvezna, Delovna skupina iz člena 29 priporoča, naj se vseeno izvede, saj je uporabno orodje, ki je upravljavcem v pomoč pri zagotavljanju skladnosti s pravom o varstvu podatkov.

Člen 35(3) določa nekatere primere, v katerih „je verjetno, da [bo dejanje obdelave] povzročilo veliko tveganje“, čeprav se ocena učinka v zvezi z varstvom podatkov lahko zahteva tudi v drugih okoliščinah:

- “(a) sistematičn[o] in obsežn[o] vrednotenj[e] osebnih vidikov v zvezi s posamezniki, ki temelji na avtomatizirani obdelavi, vključno z oblikovanjem profilov, in je osnova za

---

<sup>11</sup> Za več primerov glej uvodni izjavi (89) in (91) ter člen 35(1) in (3).

odločitve, ki imajo pravne učinke v zvezi s posameznikom ali nanj na podoben način znatno vplivajo<sup>12</sup>;

- (b) obsežne obdelave posebnih vrst podatkov iz člena 9(1) ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz člena 10<sup>13</sup>, ali
- (c) obsežn[o] sistematičn[o] spremljanj[e] javno dostopnega območja“.

Kot izhaja iz besede „zlasti“ v uvodnem stavku člena 35(3) splošne uredbe o varstvu podatkov, ta seznam ni izčrpen. Obstajajo lahko dejanja obdelave z „velikim tveganjem“, ki niso zajeta v seznamu, vendar pomenijo podobno veliko tveganje. Tudi za navedena dejanja obdelave bi se morala izvesti ocena učinka v zvezi z varstvom podatkov. Zato spodaj navedena merila, ki so bila razvita, včasih presegajo zgolj preprosto razlago, kaj naj se razume s tremi primeri iz člena 35(3) splošne uredbe o varstvu podatkov.

Upoštevati bi bilo treba naslednjih devet meril, da se zagotovi konkretnější niz dejanj obdelave, za katera se zahteva ocena učinka v zvezi z varstvom podatkov zaradi velikega tveganja, ki je z njimi neločljivo povezano, pri čemer bi bilo treba upoštevati posamezne elemente iz člena 35(1) in 35(3)(a) do (c), seznam, ki ga je treba sprejeti na nacionalni ravni na podlagi člena 35(4) in uvodnih izjav (71), (75) in (91), ter drugih primerov dejanj obdelave, za katere „je verjetno, da [bodo] povzročila veliko tveganje“, ki so navedeni v splošni uredbi o varstvu podatkov<sup>14</sup>.

1. Vrednotenje ali točkovanje, vključno z oblikovanjem profilov in predvidevanjem, zlasti na podlagi vidikov, ki se nanašajo na uspešnost posameznikov, na katere se nanašajo podatki, pri delu, ekonomski položaj, zdravje, osebni okus ali interese, zanesljivost ali vedenje, lokacijo ali gibanje (uvodni izjavi (71) in (91)). Primeri tega lahko zajemajo finančno institucijo, ki pregleduje svoje stranke glede na kreditno referenčno podatkovno zbirko ali glede na podatkovne zbirke za preprečevanje pranja denarja in preprečevanje financiranja terorizma ali goljufij, ali družbo na področju biotehnologije, ki ponuja genske teste neposredno potrošnikom, da se ocenijo in predvidijo tveganja za bolezni in zdravstvena tveganja, ali družba, ki gradi vedenjske ali tržne profile na podlagi uporabe ali navigacije po svojem spletišču.
2. Avtomatizirano odločanje, ki ima pravne ali podobno pomembne učinke: obdelava, katere cilj je sprejemanje odločitev o posameznikih, na katere se nanašajo osebni podatki, in ki ima „pravne učinke v zvezi s posameznikom“ ali ki „nanj na podoben način znatno vplivajo“ (člen 35(3)(a)). Posledica obdelave je na primer lahko izključitev posameznikov ali diskriminacija zoper njih. Obdelava, ki ima majhen učinek na posameznike ali ga sploh nima, ne ustreza temu posebnemu merilu. Več pojasnil v zvezi s temi pojmi bo zagotovljenih v prihodnjih smernicah Delovne skupine iz člena 29 o oblikovanju profilov.
3. Sistematično spremljanje: obdelava, ki se uporablja za opazovanje, spremljanje ali nadzor posameznikov, na katere se nanašajo osebni podatki, vključno s podatki, zbranimi prek

<sup>12</sup> Glej uvodno izjavo (71): „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“.

<sup>13</sup> Glej uvodno izjavo (75): „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“.

<sup>14</sup> Glej na primer uvodne izjave (75), (76), (92) in (116).

omrežij ali z obsežnim sistematičnim spremljanjem javno dostopnega območja (člen 35(3)(c))<sup>15</sup>. Ta vrsta spremljanja je merilo, ker je osebne podatke mogoče zbirati v okoliščinah, v katerih se posamezniki, na katere se nanašajo osebni podatki, morda ne zavedajo, kdo zbira njihove podatke in kako bodo uporabljeni. Poleg tega se je posameznikom morda nemogoče izogniti taki obdelavi na javnih (ali javno dostopnih) območjih.

4. Občutljivi podatki ali zelo osebni podatki: to zajema posebne kategorije osebnih podatkov, kot so opredeljeni v členu 9 (na primer informacije o posameznikovem političnem prepričanju), ter osebne podatke, ki se nanašajo na kazenske obsodbe ali prekrške, kot je opredeljeno v členu 10. Primer bi bila splošna bolnišnica, ki hrani zdravstveno dokumentacijo pacientov, ali zasebni preiskovalec, ki hrani podatke o kršitelju. Poleg teh določb splošne uredbe o varstvu podatkov je za nekatere kategorije podatkov mogoče šteti, da povečujejo morebitno tveganje za pravice in svoboščine posameznikov. Šteje se, da so ti osebni podatki občutljivi (ker je ta izraz splošno razumljiv), ker so povezani z dejavnostmi v gospodinjstvu in zasebnimi dejavnostmi (na primer elektronske komunikacije, katerih zaupnost bi bilo treba varovati), ali ker vplivajo na izvrševanje temeljne pravice (na primer lokacijski podatki, zaradi zbiranja katerih se dvomi o svobodi gibanja), ali ker ima njihova kršitev očitno resne posledice za vsakodnevno življenje posameznika, na katerega se nanašajo osebni podatki (na primer finančni podatki, ki bi lahko bili uporabljeni za goljufijo v zvezi s plačili). V tem smislu je morda pomembno, ali je podatke že javno objavil posameznik, na katerega se nanašajo osebni podatki, ali tretja oseba. Dejstvo, da so osebni podatki javno dostopni, je lahko dejavnik pri oceni, ali se je pričakovalo, da bodo podatki nadalje uporabljeni za nekatere namene. To merilo lahko zajema tudi podatke, kot so osebni dokumenti, elektronska sporočila, dnevniki, zapisi v elektronskih bralnikih, ki imajo funkcijo zapisovanja opomb, in zelo osebne informacije, ki jih vsebujejo aplikacije za vsakodnevno spremljanje.
5. Podatki, ki se obdelujejo v velikem obsegu: v splošni uredbi o varstvu podatkov ni opredeljeno, kaj pomeni v velikem obsegu, vendar nekaj smernic zagotavlja uvodna izjava (91). Delovna skupina iz člena 29 vsekakor priporoča, naj se pri opredeljevanju, ali se obdelava izvaja v velikem obsegu, upoštevajo zlasti naslednji dejavniki<sup>16</sup>:
  - a. število zadevnih posameznikov, na katere se nanašajo osebni podatki, bodisi kot konkretno število bodisi kot delež zadevne populacije;
  - b. obseg podatkov in/ali razpon različnih postavk podatkov, ki se obdelujejo;
  - c. trajanje ali stalnost dejavnosti obdelave podatkov;
  - d. geografski obseg dejavnosti obdelave.
6. Usklajeni ali združeni nabori podatkov, ki izhajajo na primer iz dveh ali več dejanj obdelave podatkov, izvedenih za različne namene in/ali s strani različnih upravljavcev podatkov na

---

<sup>15</sup> Delovna skupina iz člena 29 si besedo „sistematično“ razlaga tako, da pomeni eno ali več od naslednjega (glej smernice 16/EN (WP 243) Delovne skupine iz člena 29 o pooblaščenim osebam za varstvo podatkov):

- se pojavlja po sistemu,
- je vnaprej urejeno, organizirano ali metodično,
- se izvaja kot del splošnega načrta zbiranja podatkov,
- je izvedeno kot del strategije.

Delovna skupina iz člena 29 si izraz „javno dostopno območje“ razlaga tako, da pomeni vsak prostor, ki je odprt za vsakega člana javnosti, na primer trg, nakupovalno središče, ulica, tržnica, železniška postaja ali javna knjižnica.

<sup>16</sup> Glej Smernice 16/EN (WP 243) Delovne skupine za varstvo podatkov iz člena 29 o pooblaščenim osebam za varstvo podatkov.

način, ki presega razumna pričakovanja posameznika, na katerega se nanašajo osebni podatki<sup>17</sup>.

7. Podatki o ranljivih posameznikih, na katere se nanašajo osebni podatki (uvodna izjava (75)): obdelava te vrste podatkov je merilo zaradi povečanega neravnovesja moči med posamezniki, na katere se nanašajo osebni podatki, in upravljavcem podatkov, kar pomeni, da posamezniki morda ne morejo zlahka privoliti v obdelavo svojih podatkov, tej nasprotovati ali izvrševati svojih pravic. Med ranljive posameznike, na katere se nanašajo osebni podatki, so lahko zajeti otroci (lahko se šteje, da ne morejo vede in premišljeno nasprotovati obdelavi svojih podatkov ali vanjo privoliti), zaposleni in ranljivejši deli prebivalstva, ki potrebujejo posebno zaščito (duševno bolne osebe, prosilci za azil, starejši, pacienti itd.), vsekakor pa mednje spadajo posamezniki, na katere se nanašajo podatki, kadar je mogoče opredeliti neravnovesje v odnosu med položajem takega posameznika in upravljavcem.
8. Inovativna uporaba ali uporaba novih tehnoloških ali organizacijskih rešitev, kot je združevanje uporabe prstnih odtisov in prepoznavanja obraza za izboljššan nadzor nad fizičnim dostopom itd. Iz splošne uredbe o varstvu podatkov jasno izhaja (člen 35(1) ter uvodni izjavi (89) in (91)), da lahko uporaba nove tehnologije, opredeljene „v skladu z doseženo stopnjo tehnološkega znanja“ (uvodna izjava (91)), sproži potrebo po izvedbi ocene učinka v zvezi z varstvom podatkov. Uporaba take tehnologije lahko namreč zajema nove oblike zbiranja in uporabe podatkov, po možnosti z velikim tveganjem za pravice in svoboščine posameznika. Osebnostne in družbene posledice začetka uporabe nove tehnologije so lahko neznane. Ocena učinka v zvezi z varstvom podatkov bo upravljavcu podatkov v pomoč pri razumevanju in obravnavi takih tveganj. Nekatere aplikacije interneta stvari lahko na primer pomembno vplivajo na vsakodnevno življenje posameznikov in njihovo zasebnost, zato je zanje potrebna ocena učinka v zvezi z varstvom podatkov.
9. Kadar sama obdelava „posameznikom preprečujejo uresničevanje pravice ali uporabo storitve ali pogodbe“ (člen 22 in uvodna izjava (91)). To zajema tudi dejanja obdelave, katerih cilj je omogočanje, spreminjanje ali zavrnitev dostopa posameznikov, na katere se nanašajo osebni podatki, do storitve ali sklenitve pogodbe. Primer tega je banka, ki svoje stranke preverja glede na kreditno referenčno podatkovno zbirko, da se lahko odloči, ali naj jim ponudi posojilo.

V večini primerov lahko upravljavec podatkov meni, da je ocena učinka v zvezi z varstvom podatkov potrebna, če obdelava izpolnjuje dve merili. Delovna skupina iz člena 29 na splošno meni, da čim več meril obdelava izpolnjuje, tem večja je verjetnost, da pomeni veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, zato je zanj potrebna ocena učinka v zvezi z varstvom podatkov, ne glede na ukrepe, ki jih namerava sprejeti upravljavec.

V nekaterih primerih pa **se lahko upravljavec podatkov odloči, da je ocena učinka v zvezi z varstvom podatkov potrebna tudi za obdelavo, ki izpolnjuje le eno od teh meril.**

Iz naslednjih primerov izhaja, kako naj se merila uporabijo pri oceni, ali je za posamezno dejanje obdelave ocena učinka v zvezi z varstvom podatkov potrebna:

---

<sup>17</sup> Glej pojasnilo v Mnenju 13/EN (WP 203) Delovne skupine za varstvo podatkov iz člena 29 o omejitvi namena, str. 24.

Primeri obdelave	Morebitna upoštevana merila	Ali je verjetno, da je potrebna ocena učinka v zvezi z varstvom podatkov?
Bolnišnica, ki obdeluje genetske in zdravstvene podatke pacientov (bolnišnični informacijski sistem).	<ul style="list-style-type: none"> <li>- <u>Občutljivi podatki ali zelo osebni podatki.</u></li> <li>- Podatki, ki se nanašajo na ranljive posameznike.</li> <li>- Podatki se obdelujejo v velikem obsegu.</li> </ul>	Da
Uporaba sistema kamer za spremljanje vedenja voznikov na avtocesti. Upravljalavec namerava uporabiti inteligentni sistem videoanalize za opredelitev posameznih avtomobilov in samodejno prepoznavanje registrskih tablic.	<ul style="list-style-type: none"> <li>- Sistematično spremljanje.</li> <li>- Inovativna uporaba ali uporaba tehnoloških ali organizacijskih rešitev.</li> </ul>	
Družba sistematično spremlja dejavnosti svojih zaposlenih, vključno s spremljanjem delovnega mesta zaposlenih, dejavnosti na spletu itd.	<ul style="list-style-type: none"> <li>- Sistematično spremljanje.</li> <li>- Podatki, ki se nanašajo na ranljive posameznike.</li> </ul>	
Zbiranje podatkov na javnih družbenih omrežjih za oblikovanje profilov.	<ul style="list-style-type: none"> <li>- Vrednotenje ali točkovanje.</li> <li>- Podatki se obdelujejo v velikem obsegu.</li> <li>- Usklajevanje ali združevanje naborov podatkov.</li> <li>- <u>Občutljivi podatki ali zelo osebni podatki:</u></li> </ul>	
Institucija, ki ustvari podatkovno zbirko bonitetnih ocen ali goljufij na nacionalni ravni.	<ul style="list-style-type: none"> <li>- Vrednotenje ali točkovanje.</li> <li>- Avtomatizirano odločanje, ki ima pravne ali podobno pomembne učinke.</li> <li>- Posamezniku, na katerega se nanašajo osebni podatki, preprečuje uresničevanje pravice ali uporabo storitve ali pogodbe.</li> <li>- <u>Občutljivi podatki ali zelo osebni podatki:</u></li> </ul>	
Shranjevanje za arhiviranje psevdonimiziranih občutljivih osebnih podatkov o ranljivih posameznikih, na katere se nanašajo osebni podatki, v raziskovalnih projektih ali kliničnih študijah.	<ul style="list-style-type: none"> <li>- Občutljivi podatki.</li> <li>- Podatki, ki se nanašajo na ranljive posameznike.</li> <li>- Posameznikom, na katere se nanašajo osebni podatki, preprečuje uresničevanje pravice ali uporabo storitve ali pogodbe.</li> </ul>	
Obdelava „osebnih podatkov pacientov ali strank s strani posameznega zdravnika, drugega zdravstvenega delavca ali odvetnika“ (uvodna izjava (91)).	<ul style="list-style-type: none"> <li>- <u>Občutljivi podatki ali zelo osebni podatki.</u></li> <li>- Podatki, ki se nanašajo na ranljive posameznike.</li> </ul>	Ne
Spletna revija, ki uporablja dopisni seznam za pošiljanje generičnih dnevnih novic svojim naročnikom.	<ul style="list-style-type: none"> <li>- Podatki se obdelujejo v velikem obsegu.</li> </ul>	

Primeri obdelave	Morebitna upoštevna merila	Ali je verjetno, da je potrebna ocena učinka v zvezi z varstvom podatkov?
Spletišče e-trgovine, ki prikazuje oglase za dele starodobnih avtomobilov na podlagi omejenega oblikovanja profilov glede na ogledane ali kupljene predmete na zadevnem spletišču.	- Vrednotenje ali točkovanje.	

**Po drugi strani pa lahko dejanje obdelave ustreza zgoraj navedenim primerov, vendar upravljavec kljub temu meni, da ni „verjetno, da [bi] povzročil[o] veliko tveganje“. V takih primerih bi moral upravljavec utemeljiti in dokumentirati razloge za neizvedbo ocene učinka v zvezi z varstvom podatkov ter vključiti/evidentirati tudi stališča pooblaščenice osebe za varstvo podatkov.**

Poleg tega mora v skladu z načelom odgovornosti vsak upravljavec podatkov „vodi[ti] evidenco dejavnosti obdelave osebnih podatkov v okviru svoje odgovornosti“, med drugim vključno z nameni obdelave, opisom kategorij podatkov in prejemnikov podatkov, in „kadar je mogoče, splošni[m] opis[om] tehničnih in organizacijskih varnostnih ukrepov iz člena 32(1)“ (člen 30(1)), poleg tega pa mora oceniti, ali obstaja verjetnost za nastanek velikega tveganja, tudi če se nazadnje ne odloči za izvedbo ocene učinka v zvezi z varstvom podatkov.

Opomba: nadzorni organi morajo določiti, objaviti in Evropskemu odboru za varstvo podatkov posredovati seznam dejanj obdelave, za katere je potrebna ocena učinka v zvezi z varstvom podatkov (člen 35(4))<sup>18</sup>. Zgornja merila so lahko nadzornim organom v pomoč pri pripravi takega seznama, če je ustrezno, pa se mu lahko sčasoma doda podrobnejša vsebina. Obdelava katere koli vrste biometričnih podatkov ali podatkov otrok se na primer tudi lahko šteje za pomembno za razvoj seznama v skladu s členom 35(4).

- b) Kdaj ocena učinka v zvezi z varstvom podatkov ni potrebna? Kadar ni „verjetno, da [bi obdelava] povzročila veliko tveganje“, ali kadar obstaja podobna ocena učinka v zvezi z varstvom podatkov, ali če je bila odobrena pred majem 2018, ali če obstaja pravna podlaga, ali če je na seznamu dejanj obdelave, za katere ocena učinka v zvezi z varstvom podatkov ni potrebna.

Delovna skupina iz člena 29 meni, da ocena učinka v zvezi z varstvom podatkov ni potrebna v naslednjih primerih:

<sup>18</sup> V tem smislu „pristojni nadzorni organ [...] uporabi mehanizem za skladnost iz člena 63, kadar taki seznam vključujejo dejavnosti obdelave, ki so povezane z nudenjem blaga ali storitev posameznikom, na katere se nanašajo osebni podatki, ali s spremljanjem njihovega ravnanja v več državah članicah ali pa lahko znatno vplivajo na prosti pretok osebnih podatkov v Uniji“ (člen 35(6)).

- kadar ni „verjetno, da [bi obdelava] povzročila veliko tveganje za pravice in svoboščine posameznikov“ (člen 35(1));
- kadar so narava, obseg, okoliščine in nameni obdelave zelo podobni obdelavi, za katero je bila ocena učinka v zvezi z varstvom podatkov izvedena. V takih primerih je mogoče uporabiti rezultate ocene učinka v zvezi z varstvom podatkov za podobno obdelavo (člen 35(1)<sup>19</sup>);
- kadar je nadzorni organ pred majem 2018 dejanja obdelave preveril v posebnih razmerah, ki se niso spremenile<sup>20</sup> (glej III.C);
- kadar ima dejanje obdelave v skladu s točko (c) ali (e) člena 6(1) pravno podlago na podlagi prava EU ali prava države članice, kadar pravo ureja posamezna dejanja obdelave in kadar je bila ocena učinka v zvezi z varstvom podatkov že izvedena v okviru vzpostavitve navedene pravne podlage (člen 35(10))<sup>21</sup>, razen če je država članica določila, da je treba oceno učinka v zvezi z varstvom podatkov izvesti pred izvedbo dejavnosti obdelave;
- kadar je obdelava uvrščena na neobvezni seznam dejanj obdelave (ki ga pripravi nadzorni organ), za katera ocena učinka v zvezi z varstvom podatkov ni potrebna (člen 35(5)). Tak seznam lahko vsebuje dejavnosti obdelave, ki so skladne s pogoji, ki jih navede ta organ, zlasti prek smernic, posameznih odločitev ali dovoljenj, pravil o skladnosti itd. (na primer v Franciji dovoljenja, izjeme, poenostavljena pravila, paketi skladnosti ...). V takih primerih in na podlagi ponovne ocene, ki jo izvede pristojni nadzorni organ, ocena učinka v zvezi z varstvom podatkov ni potrebna, vendar le, če obdelava spada izključno na področje uporabe zadevnega postopka, navedenega na seznamu, in še naprej v celoti izpolnjuje vse ustrezne zahteve iz splošne uredbe o varstvu podatkov.

C. Kaj pa glede že obstoječih dejanj obdelave? Ocena učinka v zvezi z varstvom podatkov je potrebna v nekaterih okoliščinah.

**Zahteva za izvedbo ocene učinka v zvezi z varstvom podatkov se nanaša na obstoječa dejanja obdelave, za katera je verjetno, da bodo povzročila veliko tveganje za pravice in svoboščine posameznikov, in glede katerih se je tveganje spremenilo, pri čemer se upoštevajo narava, obseg, okoliščine in nameni obdelave.**

Ocena učinka v zvezi z varstvom podatkov ni potrebna za dejanja obdelave, ki jih je preveril nadzorni organ ali pooblaščen oseba za varstvo podatkov v skladu s členom 20 Direktive 95/46/ES in ki se izvajajo na način, ki se od predhodnega preverjanja ni spremenil. Velja, da so „odločitve, ki jih je na podlagi Direktive 95/46/ES sprejela Komisija, in dovoljenja s strani nadzornih organov [...] veljavni, dokler se ne spremenijo, nadomestijo ali prekličejo“ (uvodna izjava (171)).

Po drugi strani pa to pomeni, da bi bilo treba oceno učinka v zvezi z varstvom podatkov izvesti za vsako obdelavo podatkov, pri kateri so se pogoji izvajanja (obseg, namen, zbrani osebni podatki,

<sup>19</sup> „V eni oceni je lahko obravnavan niz podobnih dejanj obdelave, ki predstavljajo podobna velika tveganja.“

<sup>20</sup> „Odločitve, ki jih je na podlagi Direktive 95/46/ES sprejela Komisija, in dovoljenja s strani nadzornih organov so veljavni, dokler se ne spremenijo, nadomestijo ali prekličejo.“ (uvodna izjava (171)).

<sup>21</sup> Kadar se ocena učinka v zvezi z varstvom podatkov izvede v fazi priprave zakonodaje, ki daje pravno podlago za obdelavo, je verjetno, da jo bo treba pred začetkom delovanja pregledati, saj se lahko sprejeta zakonodaja razlikuje od predlagane na načine, ki vplivajo na vprašanja zasebnosti in varstva podatkov. Poleg tega ob sprejetju zakonodaje morda niso na voljo zadostni tehnični podatki o dejanski obdelavi, čeprav jo spremlja ocena učinka v zvezi z varstvom podatkov. V takih primerih bo morda pred izvedbo dejanskih dejavnosti obdelave kljub temu treba izvesti posebno oceno učinka v zvezi z varstvom podatkov.

identiteta upravljavcev ali prejemnikov podatkov, obdobje hrambe podatkov, tehnični in organizacijski ukrepi itd.) spremenili, odkar jih je nadzorni organ ali pooblaščen oseba za varstvo podatkov predhodno preveril, in za katero je verjetno, da bo povzročila veliko tveganje.

Poleg tega je lahko ocena učinka v zvezi z varstvom podatkov potrebna po spremembi tveganj, ki izhajajo iz dejanj obdelave<sup>22</sup>, na primer ker se je začela uporabljati nova tehnologija ali ker se osebni podatki uporabljajo za druge namene. Dejanja obdelave podatkov se lahko hitro razvijajo in s tem se lahko hitro pojavijo tudi nove ranljivosti. Zato je treba poudariti, da je pregled ocene učinka v zvezi z varstvom podatkov koristen ne le za stalno izboljševanje, ampak je tudi ključnega pomena za ohranjanje ravni varstva podatkov v okolju, ki se skozi čas spreminja. Ocena učinka v zvezi z varstvom podatkov lahko postane potrebna tudi zaradi spremembe organizacijskih ali družbenih okoliščin dejavnosti obdelave, na primer ker so postali učinki nekaterih avtomatiziranih odločitev pomembnejši ali ker postanejo ranjive za diskriminacijo nove kategorije posameznikov, na katere se nanašajo osebni podatki. Vsak od teh primerov je lahko element, zaradi katerega se spremeni tveganje, ki izhaja iz zadevne dejavnosti obdelave.

Po drugi strani pa se lahko tveganje zaradi nekaterih sprememb tudi zmanjša. Dejanje obdelave se lahko razvije tako, da odločitve niso več avtomatizirane ali da dejavnost spremljanja ni več sistematična. V takem primeru lahko pregleda analize tveganja pokaže, da izvedba ocene učinka v zvezi z varstvom podatkov ni več potrebna.

V skladu z dobro prakso **bi se morala ocena učinka v zvezi z varstvom podatkov stalno pregledovati in redno ponovno presoјati**. Tudi če torej ocena učinka v zvezi z varstvom podatkov 25. maja 2018 ni potrebna, bo moral upravljavec ob ustreznem času tako oceno izvesti kot del svojih splošnih obveznosti glede odgovornosti.

D. Kako izvesti oceno učinka v zvezi z varstvom podatkov?

a) Kdaj je treba izvesti oceno učinka v zvezi z varstvom podatkov? Pred obdelavo.

**Oceno učinka v zvezi z varstvom podatkov bi bilo treba izvesti „pred obdelavo“ (člen 35(1) in 35(10), uvodni izjavi (90) in (93))<sup>23</sup>. To je skladno z načeloma vgrajenega in privzetega varstva podatkov (člen 25 in uvodna izjava (78)). Oceno učinka v zvezi z varstvom podatkov bi bilo treba razumeti kot orodje, ki pomaga pri sprejemanju odločitev glede obdelave.**

Oceno učinka v zvezi z varstvom podatkov bi bilo treba začeti takoj, ko je to v zasnovi dejanja obdelave izvedljivo, čeprav nekatera dejanja obdelave še niso znana. Posodabljanje ocene učinka v zvezi z varstvom podatkov skozi celotno trajanje projekta bo zagotovilo upoštevanje varstva podatkov in zasebnosti ter spodbudilo ustvarjanje rešitev, ki spodbujajo skladnost. Morda bo ob napredovanju postopka razvoja treba posamezne korake ocene ponoviti, saj lahko izbor nekaterih tehničnih ali organizacijskih ukrepov vpliva na resnost ali verjetnost tveganj, ki izhajajo iz obdelave.

---

<sup>22</sup> V smislu okoliščin, zbranih podatkov, namenov, funkcionalnosti, obdelanih osebnih podatkov, prejemnikov, kombinacij podatkov, tveganj (podporna sredstva, viri tveganj, morebitni učinki, grožnje itd.), varnostnih ukrepov in mednarodnih prenosov.

<sup>23</sup> Razen pri že obstoječi obdelavi, ki jo je že preveril nadzorni organ – v takem primeru bi bilo treba oceno učinka v zvezi z varstvom podatkov izvesti pred uvedbo pomembnih sprememb.



Dejstvo, da bo oceno učinka v zvezi z varstvom podatkov morda treba posodobiti, ko se bo obdelava dejansko začela, ni upošteven razlog za odlog ocene učinka v zvezi z varstvom podatkov ali njeno neizvedbo. Ocena učinka v zvezi z varstvom podatkov je stalen proces, zlasti kadar je dejanje obdelave dinamično in se stalno spreminja. **Izvajanje ocene učinka v zvezi z varstvom podatkov je stalen proces, ne enkratni dogodek.**

- b) Kdo mora izvesti oceno učinka v zvezi z varstvom podatkov? Upravljavec skupaj s pooblaščen osebo za varstvo podatkov in obdelovalci.

**Upravljavec mora zagotoviti, da se ocena učinka v zvezi z varstvom podatkov izvede (člen 35(2)).** Oceno učinka v zvezi z varstvom podatkov lahko izvede kdo drug v organizacije ali zunaj nje, vendar je za navedeno nalogo nazadnje odgovoren upravljavec.

**Upravljavec mora za mnenje zaprositi tudi pooblaščen osebo za varstvo podatkov,** kadar je ta imenovana (člen 35(2)), njeno mnenje in svojo odločitev pa navesti v oceni učinka v zvezi z varstvom podatkov. Pooblaščen oseba za varstvo podatkov bi morala tudi spremljati izvajanje ocene učinka v zvezi z varstvom podatkov (člen 39(1)(c)). Več smernic je navedenih v Smernicah 16/EN (WP 243) Delovne skupine za varstvo podatkov iz člena 29 o pooblaščenih osebah za varstvo podatkov.

Če obdelavo v celoti ali delno izvaja obdelovalec podatkov, **bi moral pomagati upravljavcu pri izvedbi ocene učinka v zvezi z varstvom podatkov** in zagotoviti vse potrebne informacije (v skladu s členom 28(3)(f)).

**Upravljavec „po potrebi [...] zaprosi za mnenje posameznikov, na katere se nanašajo osebni podatki, ali njihovih predstavnikov“ (člen 35(9)).** Delovna skupina iz člena 29 meni, da:

- je za mnenje mogoče zaprositi na več načinov, odvisno od okoliščin (na primer generična študija, povezana z namenom in načini dejanja obdelave, vprašanje predstavniku osebja ali običajne ankete, ki se pošljejo prihodnjim strankam upravljavca podatkov), pri čemer je treba zagotoviti, da ima upravljavec zakonito podlago za obdelavo katerih koli osebnih podatkov, ki so zajeti v tako prošnjo za mnenje. Treba pa je poudariti, da privolitev v obdelavo očitno ni način, kako se posameznike, na katere se nanašajo osebni podatki, prosi za mnenje;
- če se končna odločitev upravljavca podatkov razlikuje od mnenja posameznikov, na katere se nanašajo osebni podatki, bi moral upravljavec dokumentirati razloge za nadaljevanje ali nenadaljevanje postopka;
- upravljavec bi moral tudi dokumentirati svojo utemeljitev, zakaj posameznikov, na katere se nanašajo osebni podatki, ni prosil za mnenje, če se odloči, da to ni potrebno, na primer če bi to kršilo zaupnost poslovnih načrtov družbe ali če bi bilo nesorazmerno ali neizvedljivo.

Nazadnje je stvar dobre prakse, da se opredelijo in dokumentirajo druge posebne vloge in odgovornosti, odvisno od notranje politike, postopkov in pravil, na primer:

- kadar posamezne poslovne enote predlagajo izvedbo ocene učinka v zvezi z varstvom podatkov, bi te enote morale zagotoviti podatke zanje in biti vključene v postopek potrjevanja ocene učinka v zvezi z varstvom podatkov;
- kadar je ustrezno, se priporoča, da se za nasvet prosijo neodvisni strokovnjaki različnih poklicev<sup>24</sup> (pravniki, strokovnjaki s področja informacijske tehnologije ali varnosti, sociologi, etiki itd.).

---

<sup>24</sup> Priporočila za Evropsko unijo glede okvira ocene učinka na zasebnost, rezultat D3:

- vloge in odgovornosti obdelovalcev morajo biti pogodbeno opredeljene, ocena učinka v zvezi z varstvom podatkov pa mora biti izvedena s pomočjo obdelovalca ter ob upoštevanju narave obdelave in informacij, ki so na voljo obdelovalcu (člen 28(3)(f));
- direktor za varnost informacij, če je imenovan, in pooblaščen oseb za varstvo podatkov lahko predlagata, naj upravljavec izvede oceno učinka v zvezi z varstvom podatkov glede posameznega dejanja obdelave, pri čemer bi morala zainteresiranim stranem pomagati pri metodologiji, ocenjevanju kakovosti ocene tveganja in odločanju, ali je preostalo tveganje sprejemljivo, ter razviti znanje, ki se nanaša na posebne okoliščine upravljavca podatkov;
- direktor za varnost informacij, če je imenovan, in/ali oddelek IT bi morala upravljavcu pomagati, pri čemer lahko predlagata izvedbo ocene učinka v zvezi z varstvom podatkov glede posameznega dejanja obdelave, odvisno od varnostnih ali operativnih potreb.

c) Katero metodologijo uporabiti za izvedbo ocene učinka v zvezi z varstvom podatkov?  
Različne metodologije, vendar skupna merila.

Splošna uredba o varstvu podatkov določa minimalne značilnosti ocene učinka v zvezi z varstvom podatkov (člen 35(7) ter uvodni izjavi (84) in (90)):

- „opis predvidenih dejanj obdelave in namenov obdelave“,
- „ocen[a] potrebnosti in sorazmernosti dejanj obdelave“,
- „ocen[a] tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki“,
- „ukrep[i] za:
  - o „obravnavanje tveganj“,
  - o „za dokazovanje skladnosti s to uredbo“.

Naslednja slika prikazuje generični ponavljajoči se postopek za izvajanje ocene učinka v zvezi z varstvom podatkov<sup>25</sup>:



Pri oceni učinka dejanja obdelave podatkov je treba upoštevati (člen 35(8)) skladnost s kodeksom ravnanja (člen 40). To je lahko koristno pri dokazovanju, da so bili sprejeti ali vzpostavljeni ustrezni ukrepi, če je kodeks ravnanja ustrezen glede na dejanje obdelave. Prav tako bi bilo treba upoštevati potrjevanja, pečate in označbe, da se dokaže skladnost dejanj obdelave, ki jih izvajajo upravljavci in obdelovalci, s splošno uredbo o varstvu podatkov (člen 42), in zavezujoča poslovna pravila.

Vse ustrezne zahteve, določene v splošni uredbi o varstvu podatkov, zagotavljajo širok in generičen okvir za zasnovo in izvajanje ocene učinka v zvezi z varstvom podatkov. Praktično izvajanje ocene učinka v zvezi z varstvom podatkov bo odvisno od zahtev iz splošne uredbe o varstvu podatkov, ki jih

<sup>25</sup> Poudariti je treba, da je tu prikazani postopek ponavljajoč: v praksi je verjetno, da se vsak korak večkrat ponovi, preden se ocena učinka v zvezi z varstvom podatkov lahko zaključi.

lahko dopolnjujejo podrobnejše praktične smernice. Izvajanje ocene učinka v zvezi z varstvom podatkov je torej stopnjevano. To pomeni, da lahko tudi mali upravljavec podatkov zasnuje in izvede oceno učinka v zvezi z varstvom podatkov, ki je primerna za njegova dejanja obdelave.

V uvodni izjavi (90) splošne uredbe o varstvu podatkov je orisanih več sestavnih delov ocene učinka v zvezi z varstvom podatkov, ki se prekrivajo z dobro opredeljenimi sestavnimi deli obvladovanja tveganja (na primer ISO 31000<sup>26</sup>). V smislu obvladovanja tveganja je cilj ocene učinka v zvezi z varstvom podatkov „obvladovanje tveganj“ za pravice in svoboščine posameznikov z uporabo naslednjih postopkov:

- opredelitev okoliščin: upoštevanje narave, obsega, okoliščin in namena obdelave ter izvora tveganja,
- ocena tveganj: ocena posebne verjetnosti in resnosti velikega tveganja,
- obravnava tveganj: „ublažitev tega tveganja“ in „zagotavljanje varstva osebnih podatkov“ ter „dokazovanje skladnosti s to uredbo“.

Opomba: ocena učinka v zvezi z varstvom podatkov je na podlagi splošne uredbe o varstvu podatkov orodje za obvladovanje tveganj za pravice posameznikov, na katere se nanašajo osebni podatki, zato izhaja iz njihovega vidika, kot to velja na nekaterih področjih (na primer družbena varnost). Po drugi strani pa se obvladovanje tveganja na drugih področjih (na primer informacijska varnost) osredotoča na organizacijo.

Splošna uredba o varstvu podatkov upravljavcem podatkov omogoča prožnost pri določitvi natančne strukture in oblike ocene učinka v zvezi z varstvom podatkov, da se ta lahko sklada z obstoječimi delovnimi postopki. V EU in po svetu obstaja več različnih vzpostavljenih postopkov, v katerih se upoštevajo sestavni deli, opisani v uvodni izjavi (90). Ne glede na svojo obliko pa mora biti ocena učinka v zvezi z varstvom podatkov resnična ocena tveganj, ki upravljavcem omogoča sprejetje ukrepov za njihovo obravnavo.

V pomoč pri izvajanju osnovnih zahtev iz splošne uredbe o varstvu podatkov se lahko uporabijo različne metodologije (glej Prilogo 1 za primere metodologij varstva podatkov in ocene učinka na zasebnost). Opredeljena so bila skupna merila (glej Prilogo 2), da bi se omogočil obstoj tem različnim pristopom in da bi se upravljavcem omogočila skladnost s splošno uredbo o varstvu podatkov. V njih so pojasnjene osnovne zahteve iz Uredbe, obenem pa omogočajo dovolj prostora za različne oblike izvajanja. Ta merila je mogoče uporabiti kot dokaz, da posamezna metodologija ocene učinka v zvezi z varstvom podatkov ustreza standardom, zahtevanim v splošni uredbi o varstvu podatkov.

**Upravljavec lahko izbere metodologijo, vendar mora biti ta skladna z merili iz Priloge 2.**

Delovna skupina iz člena 29 spodbuja razvoj okvirov ocen učinka v zvezi z varstvom podatkov, prilagojenih posameznemu sektorju. Tako se lahko uporabi posebno znanje iz posameznega sektorja, zaradi česar se lahko v oceni učinka v zvezi z varstvom podatkov obravnavajo posebnosti posamezne vrste dejanj obdelave (na primer posebne vrste podatkov, korporativna sredstva, morebitni učinki, grožnje, ukrepi). To pomeni, da se lahko v oceni učinka v zvezi z varstvom podatkov obravnavajo vprašanja, ki se pojavljajo v posameznem gospodarskem sektorju, ali ob uporabi določenih tehnologij, ali ob izvajanju določenih vrst dejanj obdelave.

---

<sup>26</sup> Postopki obvladovanja tveganja: komunikacija in posvetovanje, opredelitev okoliščin, ocena tveganja, obravnava tveganja, spremljanje in pregled (glej izraze in opredelitve pojmov ter kazalo v predogledu dokumenta ISO 31000: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>).

Nazadnje, „upravljavec po potrebi opravi pregled, 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“ (člen 35(11)<sup>27</sup>).

- d) Ali je treba oceno učinka v zvezi z varstvom podatkov objaviti? Ne, vendar bi lahko objava povzetka spodbudila zaupanje, celotno oceno učinka v zvezi z varstvom podatkov pa je treba nadzornemu organu sporočiti v primeru predhodnega posvetovanja ali če tako zahteva organ za varstvo podatkov.

**Splošna uredba o varstvu podatkov ne vsebuje pravne zahteve po objavi ocene učinka v zvezi z varstvom podatkov, odločitev o tem je prepuščena upravljavcu. Upravljavcem pa se vseeno priporoča, da razmislijo o objavi vsaj delov ocene, na primer povzetka ali sklepnih ugotovitev.**

Namen takega postopka bi bil spodbujati zaupanje v upravljavčeva dejanja obdelave ter dokazati odgovornost in preglednost. Dobra praksa je zlasti objaviti oceno učinka v zvezi z varstvom podatkov, kadar dejanje obdelave vpliva na člane javnosti. To še zlasti velja, kadar oceno učinka v zvezi z varstvom podatkov izvede javni organ.

Ni treba, da objavljena ocena učinka v zvezi z varstvom podatkov vsebuje celotno oceno, zlasti kadar bi lahko vsebovala posebne informacije glede varnostnih tveganj za upravljavca podatkov ali razkrivala poslovne skrivnosti ali poslovno občutljive informacije. V teh okoliščinah lahko objavljena različica vsebuje le povzetek glavnih ugotovitev ocene učinka v zvezi z varstvom podatkov ali celo zgolj izjavo, da je bila ocena izvedena.

Poleg tega velja, da se mora upravljavec o obdelavi predhodno posvetovati z nadzornim organom, kadar iz ocene učinka v zvezi z varstvom podatkov izhaja veliko preostalo tveganje (člen 36(1)). Pri tem mora predložiti celotno oceno učinka v zvezi z varstvom podatkov (člen 36(3)(e)). Nadzorni organ lahko svetuje<sup>28</sup> in ne sme razkriti poslovnih skrivnosti ali varnostnih ranljivosti, pri čemer se upoštevajo načela, ki veljajo v posamezni državi članici glede dostopa javnosti do uradnih dokumentov.

E. Kdaj se je treba posvetovati z nadzornim organom? Kadar je preostalo tveganje veliko.

Kot je pojasnjeno zgoraj:

- ocena učinka v zvezi z varstvom podatkov je potrebna, kadar „je možno, da bi [dejanje obdelave lahko] povzročil[o] veliko tveganje za pravice in svoboščine posameznikov“ (člen 35(1), glej III.B.a). Za obdelavo zdravstvenih podatkov v velikem obsegu se na primer šteje, da bi lahko povzročila veliko tveganje, zato je zanjo potrebna ocena učinka v zvezi z varstvom podatkov;
- upravljavec podatkov mora nato oceniti tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in opredeliti ukrepe<sup>29</sup>, predvidene za zmanjšanje navedenih tveganj na sprejemljivo raven, ter dokazati skladnost s splošno uredbo o varstvu podatkov (člen 35(7), glej III.C.c). Primer tega bi bil, da se pri shranjevanju osebnih podatkov na

<sup>27</sup> S členom 35(10) je izrecno izvzeta le uporaba odstavkov 1–7 člena 35.

<sup>28</sup> Nadzorni organ mora upravljavcu pisno svetovati le, kadar meni, da nameravana obdelava ni v skladu z Uredbo, kakor je navedeno v členu 36(2).

<sup>29</sup> Vključno z upoštevanjem obstoječih smernic Evropskega odbora za varstvo podatkov in nadzornih organov ter najsodobnejše tehnologije in stroškov izvajanja, kot je določeno v členu 35(1).

prenosnih računalnikov poleg obstoječih politik (obvestilo, privolitve, pravica do dostopa, pravica do ugovora itd.) uporabijo ustrezni tehnični in organizacijski varnostni ukrepi (učinkovito šifriranje celotnega diska, zanesljivo upravljanje ključev, ustrezen nadzor nad dostopom, zaščitene varnostne kopije itd.).

V zgornjem primeru s prenosnim računalnikom velja, da če je upravljavec podatkov štel, da so tveganja zadosti zmanjšana, se lahko glede na razlago člena 36(1) ter uvodnih izjav (84) in (94) obdelava nadaljuje brez posvetovanja z nadzornim organom. Upravljavec podatkov se mora z nadzornim organom posvetovati v primerih, ko opredeljenih tveganj ne more ustrezno obravnavati (tj. preostala tveganja ostajajo velika).

Med nesprejemljivo veliko preostalo tveganje spadajo primeri, ko lahko posameznika, na katerega se nanašajo osebni podatki, doletijo pomembne ali celo nepopravljive posledice, ki jih ta ne more odpraviti (na primer nezakonit dostop do podatkov, zaradi katerega je ogroženo življenje posameznikov, na katere se nanašajo osebni podatki, ali zaradi katerega je lahko posameznik odpuščen ali v finančnih težavah), in/ali kadar se zdi očitno, da se bo navedeno tveganje uresničilo (na primer ker ne bo mogoče zmanjšati števila oseb, ki imajo dostop do podatkov, zaradi načinov njihove izmenjave, uporabe ali razširjanja, ali kadar znana ranljivost ni odpravljena).

**Upravljavec podatkov se mora posvetovati z nadzornim organom vedno, kadar ne najde zadostnih ukrepov za zmanjšanje tveganj na sprejemljivo raven (tj. preostala tveganja so še vedno visoka)<sup>30</sup>.**

Poleg tega se mora upravljavec posvetovati z nadzornim organom vedno, kadar je to potrebno v skladu s pravom države članice in/ali kadar mora v skladu z njim pridobiti predhodno dovoljenje nadzornega organa glede obdelave za izvajanje naloge, ki jo upravljavec izvede v javnem interesu, vključno z obdelavo v zvezi s socialno zaščito in javnim zdravjem (člen 36(5)).

Navesti pa je treba, da obveznost hrambe evidence ocene učinka v zvezi z varstvom podatkov in njenega posodabljanja ostaja, ne glede na to, ali je glede na raven preostalega tveganja posvetovanje z nadzornim organom potrebno ali ne.

#### **IV. Sklepne ugotovitve in priporočila**

Ocene učinka v zvezi z varstvom podatkov so uporaben način, kako lahko upravljavci podatkov izvajajo sisteme obdelave podatkov, ki so skladni s splošno uredbo o varstvu podatkov, za nekatere vrste dejanj obdelave pa so lahko te ocene obvezne. Ocene so stopnjevale in so lahko različnih oblik, splošna uredba o varstvu podatkov pa določa osnovne zahteve za učinkovito oceno učinka v zvezi z varstvom podatkov. Upravljavci podatkov bi morali v izvajanju ocene učinka v zvezi z varstvom podatkov prepoznati uporabno in pozitivno dejavnost, ki pripomore k pravni skladnosti.

Člen 24(1) določa osnovno odgovornost upravljavca v smislu zagotavljanja skladnosti s splošno uredbo o varstvu podatkov: „ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, upravljavec

---

<sup>30</sup> Opomba: „psevdonimizacija in šifriranje osebnih podatkov“ (ter najmanjši obseg podatkov, mehanizmi nadzora itd.) niso nujno ustrezni ukrepi. So le primeri. Kaj je ustrezen ukrep, je odvisno od okoliščin in tveganj, značilnih za posamezno dejanje obdelave.

izvede ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s to uredbo. Ti ukrepi se pregledajo in dopolnijo, kjer je to potrebno.“

Ocena učinka v zvezi z varstvom podatkov je ključni del zagotavljanja skladnosti z Uredbo, kadar se načrtuje ali izvaja obdelava podatkov z velikim tveganjem. To pomeni, da bi morali upravljavci podatkov uporabiti merila iz tega dokumenta za opredelitev, ali je treba oceno učinka v zvezi z varstvom podatkov izvesti ali ne. Notranja politika upravljavca podatkov lahko ta seznam razširi, tako da niso zajete samo pravne zahteve iz splošne uredbe o varstvu podatkov. Posledica tega bi moralo biti večje zaupanje in gotovost posameznikov, na katere se nanašajo osebni podatki, in drugih upravljavcev podatkov.

Kadar se načrtuje obdelava, pri kateri je mogoče veliko tveganje, mora upravljavec podatkov:

- izbrati metodologijo ocene učinka v zvezi z varstvom podatkov (primeri so v Prilogi 1), ki izpolnjuje merila iz Priloge 2, ali pa opredeliti in izvesti sistematičen postopek ocene učinka v zvezi z varstvom podatkov, ki:
  - o je skladen z merili iz Priloge 2;
  - o je vključen v obstoječe postopke pregleda zasnove, razvoja, sprememb, tveganj in delovanja, v skladu z notranjimi postopki, okoliščinami in kulturo;
  - o vključuje ustrezne zainteresirane strani in jasno opredeljuje njihove odgovornosti (upravljavec, pooblaščen oseba za varstvo podatkov, posamezniki, na katere se nanašajo osebni podatki, ali njihovi zastopniki, podjetje, tehnične službe, obdelovalci, pooblaščen oseba za varstvo zaupnosti podatkov itd.);
- poročilo o oceni učinka v zvezi z varstvom podatkov predložiti pristojnemu nadzornemu organu, kadar se to od njega zahteva;
- se posvetovati z nadzornim organom, kadar ne more opredeliti zadostnih ukrepov za ublažitev velikih tveganj;
- redno pregledovati oceno učinka v zvezi z varstvom podatkov in obdelavo, ki se z njo ocenjuje, vsaj kadar se spremeni tveganje, ki izhaja iz obdelave dejanja;
- dokumentirati sprejete odločitve.

## **Priloga 1: Primeri obstoječih okvirov EU glede ocene učinka v zvezi z varstvom podatkov**

V splošni uredbi o varstvu podatkov ni določeno, katere postopke v okviru ocene učinka v zvezi z varstvom podatkov je treba izvesti, ampak lahko upravljavci podatkov sami določijo okvir, ki ustreza njihovim obstoječim delovnim postopkom, če se pri tem upoštevajo sestavni deli, opisani v členu 35(7). Tak okvir se lahko nanaša le na posameznega upravljavca podatkov ali pa je skupen celotni panogi. Med že objavljenimi okviri, ki so jih razvili organi EU za varstvo podatkov, in okviri EU, ki se nanašajo na posamezne panoge, so med drugim (seznam ni izčrpen):

Primeri generičnih okvirov EU:

- DE: Standardni model varstva podatkov, V.1.0 – poskusna različica, 2016<sup>31</sup>.  
[https://www.datenschutzzentrum.de/uploads/SDM-Methodology\\_V1\\_EN1.pdf](https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf)
- ES: *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/Guia\\_EIPD.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf)
- FR: *Ocena učinka na zasebnost*, Commission nationale de l'informatique et des libertés (CNIL), 2015.  
<https://www.cnil.fr/fr/node/15798>
- UK: *Conducting privacy impact assessments code of practice (Kodeks ravnanja glede izvajanja ocen učinka na zasebnost)*, urad informacijskega pooblaščenca, 2014.  
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Okviri EU, ki se nanašajo na posamezne panoge:

- Okvir ocene učinka v zvezi z varstvom podatkov in ocene učinka na zasebnost v aplikacijah, podprtih z radiofrekvenčno identifikacijo<sup>32</sup>.  
[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180\\_annex\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf)
- Predloga ocene učinka na varstvo podatkov za inteligentna omrežja in inteligentne merilne sisteme<sup>33</sup>.  
[http://ec.europa.eu/energy/sites/ener/files/documents/2014\\_dpia\\_smart\\_grids\\_forces.pdf](http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf)

<sup>31</sup> Soglasno sprejet in potrjen (ob vzdržanju Bavarske) na 92. konferenci neodvisnih zveznih organov za varstvo podatkov in organov v posameznih zveznih državah, ki je 9. in 10. novembra 2016 potekala v Kühlungsbornu.

<sup>32</sup> Glej tudi:

- Priporočilo Komisije z dne 12. maja 2009 o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčno identifikacijo.  
<https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles>
- Mnenje 9/2011 o revidiranem predlogu industrije glede okvira ocene učinka v zvezi z varstvom podatkov in ocene učinka na zasebnost v aplikacijah, podprtih z radiofrekvenčno identifikacijo.  
[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf)

<sup>33</sup> Glej tudi Mnenje 7/2013 o predlogi ocene učinka na varstvo podatkov za inteligentna omrežja in inteligentne merilne sisteme (v nadaljnjem besedilu: predloga ocene učinka v zvezi z varstvom podatkov), ki ga je pripravila strokovna skupina 2 v okviru projektne skupine Komisije za inteligentna omrežja.  
[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf)



Tudi mednarodni standard bo zagotovil smernice za metodologije, ki se uporabljajo za izvedbo ocene učinka v zvezi z varstvom podatkov (ISO/IEC 29134<sup>34</sup>).

---

<sup>34</sup> ISO/IEC 29134 (projekt), Information technology – Security techniques – Privacy impact assessment – Guidelines (Informacijska tehnologija – varnostne tehnike – ocena učinka na zasebnost – smernice), Mednarodna organizacija za standardizacijo (ISO).

## **Priloga 2: Merila za sprejemljivost ocene učinka v zvezi z varstvom podatkov**

Delovna skupina iz člena 29 predlaga naslednja merila, ki jih lahko uporabijo upravljavci podatkov pri presoji, ali je ocena učinka v zvezi z varstvom podatkov oziroma metodologija za njeno izvedbo dovolj izčrpna za zagotovitev skladnosti s splošno uredbo o varstvu podatkov:

- ☐ zagotovljen je sistematičen opis obdelave (člen 35(7)(a)):
  - ☐ upoštevani so narava, obseg, okoliščine in namen obdelave (uvodna izjava (90));
  - ☐ evidentirajo se osebni podatki, prejemniki in obdobje, za katero se shranijo osebni podatki;
  - ☐ zagotovljen je funkcionalen opis dejanj obdelave;
  - ☐ opredeljena so sredstva, na katerih temeljijo osebni podatki (strojna in programska oprema, omrežja, posamezniki, tiskani dokumenti ali kanali za njihovo pošiljanje);
  - ☐ upošteva se skladnost z odobrenimi kodeksi ravnanja (člen 35(8));
- ☐ ocenita se potrebnost in sorazmernost (člen 35(7)(b)):
  - ☐ opredeljeni so načrtovani ukrepi za zagotovitev skladnosti z Uredbo (člen 35(7)(d) in uvodna izjava (90)), pri čemer se upoštevajo:
    - ☐ ukrepi, ki prispevajo k sorazmernosti in potrebnosti obdelave, na podlagi:
      - ☐ določenih, izrecnih in zakonitih namenov (člen 5(1)(b));
      - ☐ zakonitosti obdelave (člen 6);
      - ☐ ustreznih in relevantnih podatkov, ki so omejeni na to, kar je potrebno (člen 5(1)(c));
      - ☐ omejenega trajanja shranjevanja (člen 5(1)(e));
    - ☐ ukrepi, ki prispevajo k pravicam posameznikov, na katere se nanašajo osebni podatki:
      - ☐ informacije, ki se zagotovijo posameznikom, na katere se nanašajo osebni podatki (členi 12, 13 in 14);
      - ☐ pravica do dostopa in prenosljivosti podatkov (člena 15 in 20);
      - ☐ pravica do popravka in izbrisa (členi 16, 17 in 19);
      - ☐ pravica do ugovora in omejitve obdelave (členi 18, 19 in 21);
      - ☐ odnosi z obdelovalci (člen 28);
      - ☐ zaščitni ukrepi glede mednarodnih prenosov (poglavje V);
      - ☐ predhodno posvetovanje (člen 36);
- ☐ obvladujejo se tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki (člen 35(7)(c)):
  - ☐ upoštevajo se izvor, narava, posebnost in resnost tveganj (glej uvodno izjavo (84)) ali – še podrobneje – vsakega tveganja (nezakonit dostop, neželeno spreminjanje, izginotje podatkov) z vidika posameznikov, na katere se nanašajo osebni podatki:
    - ☐ upoštevajo se viri tveganj (uvodna izjava (90));
    - ☐ opredelijo se morebitni učinki na pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, v primeru dogodkov, ki vključujejo nezakonit dostop, neželeno spreminjanje in izginotje podatkov;
    - ☐ opredeljene so grožnje, ki bi lahko vodile do nezakonitega dostopa, neželenega spreminjanja in izginotja podatkov;
    - ☐ opredeljeni sta verjetnost in resnost (uvodna izjava (90));
  - ☐ opredeljeni so načrtovani ukrepi za obravnavo navedenih tveganj (člen 35(7)(d) in uvodna izjava (90));
- ☐ vključene so zainteresirane strani:
  - ☐ zaprosi se za mnenje pooblaščen osebe za varstvo podatkov (člen 35(2));
  - ☐ kadar je ustrezno, se zaprosi za mnenje posameznikov, na katere se nanašajo osebni podatki, ali njihovih predstavnikov (člen 35(9)).