



**17/HR**

**WP 248 rev.01**

**Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik” u smislu Uredbe 2016/679**

**Donesene 4. travnja 2017.**

**Posljednji put revidirane i donesene 4. listopada 2017.**

Ova Radna skupina osnovana je na temelju članka 29. Direktive 95/46/EZ. To je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnosti. Njezini zadaci opisani su u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo djeluje u sklopu Uprave C (Temeljna prava i građanstvo Unije) Europske komisije, Glavna uprava za pravosuđe, B-1049 Bruxelles, Belgija, ured br. MO-59 03/075.

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

## **RADNA SKUPINA ZA ZAŠTITU POJEDINACA U VEZI S OBRADOM OSOBNIH PODATAKA**

osnovana Direktivom 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995.,

uzimajući u obzir članke 29. i 30. te Direktive,

uzimajući u obzir svoj Poslovnik,

**DONIJELA JE OVE SMJERNICE:**

## Sadržaj

<b>I.</b>	<b>UVOD.....</b>	<b>4</b>
<b>II.</b>	<b>PODRUČJE PRIMJENE SMJERNICA.....</b>	<b>5</b>
<b>III.</b>	<b>PROCJENA UČINKA NA ZAŠTITU PODATAKA: OBJAŠNJENJE UREDBE.....</b>	<b>7</b>
A.	NA ŠTO SE ODNOSI PROCJENA UČINKA NA ZAŠTITU PODATAKA? NA JEDAN POSTUPAK OBRADE ILI SKUP SLIČNIH POSTUPAKA OBRADE. 8	
B.	KOJI POSTUPCI OBRADE PODLIJEŽU PROCJENI UČINKA NA ZAŠTITU PODATAKA? OSIM U IZNIMNIM SLUČAJEVIMA, ONI KOJI ĆE VJEROJATNO PROUZROČITI VISOK RIZIK. ....	9
a)	<i>U kojim je slučajevima obvezno provođenje procjene učinka na zaštitu podataka? Ako će obrada vjerojatno prouzročiti visok rizik.....</i>	9
b)	<i>U kojim slučajevima nije potrebna procjena učinka na zaštitu podataka? Ako nije vjerojatno da će obrada vjerojatno prouzročiti visok rizik, ako postoji slična procjena učinka na zaštitu podataka, ako je obrada bila odobrena prije svibnja 2018., ako ima pravni temelj ili ako je na popisu postupaka obrade za koje procjena učinka na zaštitu podataka nije potrebna. ....</i>	14
C.	ŠTO JE S POSTOJEĆIM POSTUPCIMA OBRADE? PROCJENA UČINKA NA ZAŠTITU PODATAKA POTREBNA JE U NEKIM OKOLNOSTIMA. ....	15
D.	KAKO SE PROVODI PROCJENA UČINKA NA ZAŠTITU PODATAKA?.....	16
a)	<i>U kojem trenutku treba provesti procjenu učinka na zaštitu podataka? Prije obrade. ....</i>	16
b)	<i>Tko mora provesti procjenu učinka na zaštitu podataka? Voditelj obrade sa službenikom za zaštitu podataka i izvršiteljima obrade. ....</i>	16
c)	<i>Koja je metodologija za provođenje procjene učinka na zaštitu podataka? Postoje različite metodologije, ali kriteriji su im zajednički. ....</i>	17
d)	<i>Postoji li obveza objavljivanja procjene učinka na zaštitu podataka? Ne, ali objavom sažetka može se potaknuti povjerenje, dok cijela procjena učinka na zaštitu podataka mora biti dostavljena nadzornom tijelu u slučaju prethodnih konzultacija ili ako to zahtijeva tijelo za zaštitu podataka. ....</i>	20
E.	KADA JE POTREBNO SAVJETOVATI SE S NADZORNIM TIJELOM? U SLUČAJU VISOKIH PREOSTALIH RIZIKA. ....	20
<b>IV.</b>	<b>ZAKLJUČCI I PREPORUKE.....</b>	<b>21</b>
	<b>PRILOG 1. – PRIMJERI POSTOJEĆIH OKVIRA EU-A U POGLEDU PROCJENE UČINKA NA ZAŠTITU PODATAKA ...</b>	<b>23</b>
	<b>PRILOG 2. – KRITERIJI ZA PRIHVATLJIVU PROCJENU UČINKA NA ZAŠTITU PODATAKA .....</b>	<b>25</b>

## I. Uvod

Uredba 2016/679<sup>1</sup> (Opća uredba o zaštiti podataka) primjenjivat će se od 25. svibnja 2018. Člankom 35. Opće uredbe o zaštiti podataka uvodi se koncept procjene učinka na zaštitu podataka<sup>2</sup>, kao i Direktivom 2016/680<sup>3</sup>.

Procjena učinka na zaštitu podataka je postupak osmišljen za opisivanje obrade, procjenu njezine nužnosti i proporcionalnosti te pružanje pomoći u upravljanju rizicima za prava i slobode pojedinaca koji nastaju obradom osobnih podataka<sup>4</sup>, njihovom procjenom i određivanjem mjera za njihovo uklanjanje. Provođenje procjene učinka na zaštitu podataka važno je za odgovornost jer pomaže voditeljima obrade da se usklade sa zahtjevima Opće uredbe o zaštiti podataka i da dokažu da su poduzete potrebne mjere za osiguravanje usklađenosti s Uredbom (vidjeti i članak 24.)<sup>5</sup>. Drugim riječima, **procjena učinka na zaštitu podataka postupak je za uspostavu i dokazivanje usklađenosti.**

U skladu s Općom uredbom o zaštiti podataka neusklađenost sa zahtjevima procjene učinka na zaštitu podataka može rezultirati novčanim kaznama koje izriče nadležno nadzorno tijelo. Propust u provođenju procjene učinka na zaštitu podataka u slučaju da obrada podliježe njezinu provođenju (članak 35. stavci 1., 3. i 4.), neispravno provođenje procjene učinka na zaštitu podataka (članak 35. stavci 2., 7., 8. i 9.) ili nesavjetovanje s nadležnim nadzornim tijelom kad je to potrebno (članak 36. stavak 3. točka (e)) može rezultirati upravnim novčanim kaznama do najviše 10 milijuna EUR ili, u slučaju poduzeća, do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos viši.

---

<sup>1</sup> Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).

<sup>2</sup> Pojam „procjena učinka na privatnost” često se koristi i u drugim kontekstima za objašnjavanje istog koncepta.

<sup>3</sup> Isto tako, u članku 27. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka navodi se da je procjena učinka na privatnost potrebna jer je vjerojatno da će obrada „prouzročiti visok rizik za prava i slobode pojedinaca”.

<sup>4</sup> U Općoj uredbi o zaštiti podataka formalno se ne definira koncept procjene učinka na zaštitu podataka kao takve, ali

- njezin sadržaj, utvrđen u članku 35. stavku 7., obuhvaća barem sljedeće:
  - o (a) sustavan opis predviđenih postupaka obrade i svrha obrade, uključujući, ako je primjenjivo, legitimni interes voditelja obrade;
  - o (b) procjenu nužnosti i razmjernosti postupaka obrade povezanih s njihovim svrhama;
  - o (c) procjenu rizika za prava i slobode ispitanika iz stavka 1. i
  - o (d) mjere predviđene za rješavanje problema rizika, što uključuje zaštitne mjere, sigurnosne mjere i mehanizme za osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s ovom Uredbom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba;
- njezino značenje i njezina uloga pojašnjeni su u uvodnoj izjavi 84. kako slijedi: *Radi poboljšanja sukladnosti s ovom Uredbom kada postupci obrade vjerojatno mogu dovesti do visokog stupnja rizika za prava i slobode pojedinaca, voditelj obrade trebao bi biti odgovoran za provođenje procjene učinka na zaštitu podataka kako bi se osobito procijenili izvor, priroda, osobitost i ozbiljnost tog rizika.*

<sup>5</sup> Vidjeti i uvodnu izjavu 84.: *Ishod procjene trebao bi se uzeti u obzir pri utvrđivanju odgovarajućih mjera radi dokazivanja da je obrada osobnih podataka sukladna s ovom Uredbom.*

## II. Područje primjene Smjernica

Ovim se Smjernicama u obzir uzima sljedeće:

- Izjava Radne skupine za zaštitu podataka iz članka 29., 14/EN WP 218<sup>6</sup>,
- Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243<sup>7</sup>,
- Mišljenje Radne skupine za zaštitu podataka iz članka 29. o ograničavanju svrhe, 13/EN WP 203<sup>8</sup>,
- međunarodni standardi<sup>9</sup>.

U skladu s pristupom temeljenim na riziku, utvrđenim u Općoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obvezno za svaki postupak obrade. Procjena učinka na zaštitu podataka potrebna je ako će obrada *vjerojatno* prouzročiti *visok rizik za prava i slobode pojedinaca* (članak 35. stavak 1.). Kako bi se osiguralo dosljedno tumačenje okolnosti u kojima je procjena učinka na zaštitu podataka obvezna (članak 35. stavak 3.), ovim se Smjernicama prvenstveno nastoji pojasniti taj pojam i utvrditi kriteriji za popise koje će donijeti tijela za zaštitu podataka u skladu s člankom 35. stavkom 4.

U skladu s člankom 70. stavkom 1. točkom (e) Europski odbor za zaštitu podataka moći će izdati smjernice, preporuke i primjere najbolje prakse kako bi poticao dosljednu primjenu Opće uredbi o zaštiti podataka. Ovim se dokumentom nastoji predvidjeti takav budući rad Europskog odbora za zaštitu podataka i stoga pojasniti relevantne odredbe Opće uredbi o zaštiti podataka kako bi se voditelji obrade mogli lakše uskladiti sa zakonodavstvom te kako bi se pružila pravna sigurnost onim voditeljima obrade koji su dužni provesti procjenu učinka na zaštitu podataka.

Isto tako, cilj ovih Smjernica promicanje je razvoja:

- zajedničkog popisa Europske unije onih postupaka obrade za koje je obvezno provođenje procjene učinka na zaštitu podataka (članak 35. stavak 4.),
- zajedničkog popisa Europske unije onih postupaka obrade za koje provođenje procjene učinka na zaštitu podataka nije potrebno (članak 35. stavak 5.),
- zajedničkih kriterija u pogledu metodologije provođenja procjene učinka na zaštitu podataka (članak 35. stavak 5.),

---

<sup>6</sup> Izjava Radne skupine za zaštitu podataka iz članka 29. o ulozi pristupa pravnim okvirima za zaštitu podataka temeljenog na riziku, 14/EN WP 218, donesena 30. svibnja 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> Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243, donesene 13. prosinca 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> Mišljenje 03/2013 Radne skupine za zaštitu podataka iz članka 29. o ograničavanju svrhe, 13/EN WP 203, doneseno 2. travnja 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> Npr. ISO 31000:2009, *Upravljanje rizicima – načela i smjernice*, Međunarodna organizacija za normizaciju (ISO); ISO/IEC 29134 (projekt), *Informacijske tehnologije – Sigurnosne tehnike – Procjena učinka na privatnost – Smjernice*, Međunarodna organizacija za normizaciju (ISO).

- zajedničkih kriterija za utvrđivanje slučajeva u kojima je potrebno savjetovati se s nadzornim tijelom (članak 36. stavak 1.),
- prema potrebi, preporuka utemeljenih na iskustvu stečenom u državama članicama EU-a.

### III. Procjena učinka na zaštitu podataka: Objašnjenje Uredbe

Općom se uredbom o zaštiti podataka od voditelja obrade zahtijeva provedba prikladnih mjera radi osiguravanja i dokazivanja usklađenosti s Općom uredbom o zaštiti podataka uzimajući u obzir među ostalim „rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca” (članak 24. stavak 1.). Obvezu provođenja procjene učinka na zaštitu podataka u određenim okolnostima koju imaju voditelji obrade treba tumačiti u kontekstu njihove opće obveze primjerenog upravljanja rizicima<sup>10</sup> koje predstavlja obrada osobnih podataka.

„Rizik” je scenarij koji opisuje događaj i njegove posljedice procijenjene s obzirom na ozbiljnost i vjerojatnost. S druge strane, „upravljanje rizicima” može se definirati kao koordinirane aktivnosti usmjeravanja i kontroliranja organizacije u pogledu rizika.

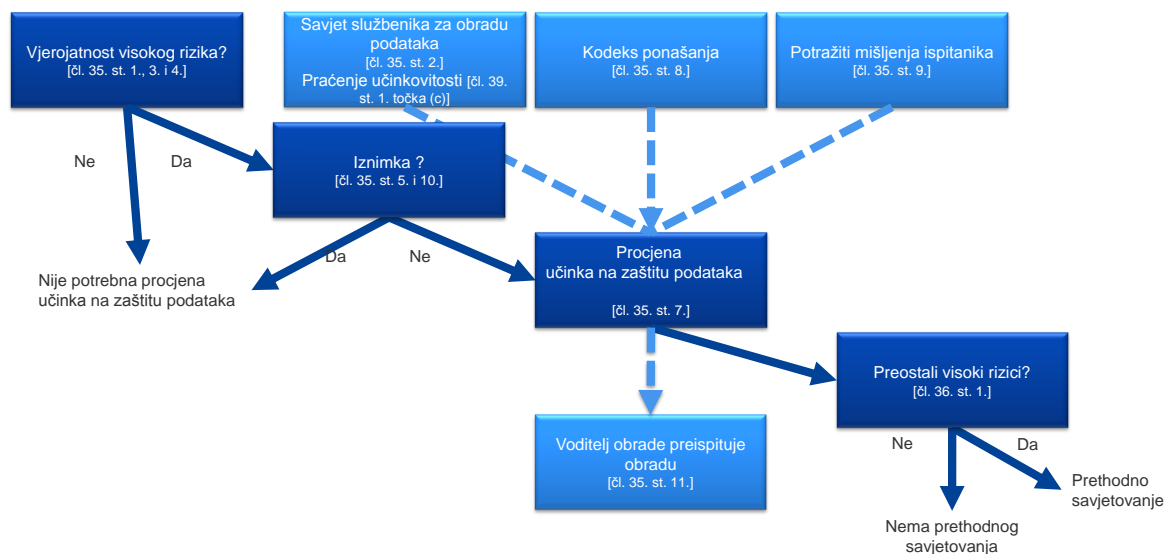
Članak 35. odnosi se na vjerojatni visoki rizik „za prava i slobode pojedinaca”. Kao što je navedeno u Izjavi Radne skupine za zaštitu podataka iz članka 29. o ulozi pristupa pravnim okvirima za zaštitu podataka temeljenog na riziku, upućivanje na „prava i slobode” ispitanika odnosi se prvenstveno na prava na zaštitu podataka i privatnosti, ali može obuhvaćati i druga temeljna prava poput slobode govora, slobode mišljenja, slobode kretanja, zabrane diskriminacije te prava na slobodu savjesti i vjeroispovijesti.

U skladu s pristupom temeljenim na riziku, utvrđenim u Općoj uredbi o zaštiti podataka, provođenje procjene učinka na zaštitu podataka nije obvezno za svaki postupak obrade. Umjesto toga, procjena učinka na zaštitu podataka potrebna je ako će obrada „vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca” (članak 35. stavak 1.). Međutim, sama činjenica da uvjeti kojima se nameće obveza provedbe procjene učinka na zaštitu podataka još nisu ispunjeni ne umanjuje opću obvezu voditelja obrade da provedu mjere za primjereno upravljanje rizicima za prava i slobode ispitanika. To u praksi znači da voditelji moraju kontinuirano procjenjivati rizike nastale njihovim aktivnostima obrade kako bi utvrdili kada će neka vrsta obrade „vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca”.

---

<sup>10</sup> Potrebno je naglasiti da se rizici moraju identificirati, analizirati, procijeniti, ocijeniti, obraditi (npr. umanjiti...) i redovito preispitivati kako bi se smanjili rizici za prava i slobode pojedinaca. Voditelji obrade ne mogu izbjeći odgovornost pokrivanjem rizika policama osiguranja.

Na dijagramu u nastavku prikazana su osnovna načela povezana s procjenom učinka na zaštitu podataka u Općoj uredbi o zaštiti podataka:



A. Na što se odnosi procjena učinka na zaštitu podataka? Na jedan postupak obrade ili skup sličnih postupaka obrade.

**Procjena učinka na zaštitu podataka može se odnositi na jedan postupak obrade podataka.** Međutim, u članku 35. stavku 1. navodi se da se „jedna procjena može odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike”. U uvodnoj izjavi 92. dodaje se da „u nekim okolnostima može biti razumno i ekonomično da procjena učinka na zaštitu podataka obuhvaća više od jednog projekta i tematski šire područje, na primjer ako tijela javne vlasti ili javna tijela namjeravaju uspostaviti zajedničku aplikaciju ili platformu za obradu ili ako nekoliko voditelja obrade namjerava uvesti zajedničku aplikaciju ili okruženje za obradu u cijeli jedan industrijski sektor ili segment ili za horizontalnu djelatnost široke uporabe”.

**Jedna procjena učinka na zaštitu podataka može se upotrijebiti za procjenu višestrukih postupaka obrade koji su slični** s obzirom na prirodu, opseg, kontekst, svrhu i rizike. Doista, cilj procjene učinka na zaštitu podataka jest sustavno proučavanje novih situacija koje mogu dovesti do visokih rizika za prava i slobode pojedinaca te nema potrebe za provođenjem procjene učinka na zaštitu podataka u slučajevima (npr. postupci obrade provedeni u specifičnom kontekstu i u specifične svrhe) koji su već proučeni. To može biti slučaj ako se koristi slična tehnologija za prikupljanje iste vrste podataka u iste svrhe. Na primjer, skupina općinskih tijela, od kojih svako postavlja sličan sustav kamera televizije zatvorenog kruga (CCTV), može provesti jednu procjenu učinka na zaštitu podataka koja obuhvaća postupke pojedinačnih voditelja obrade ili željeznički prijevoznik (jedan voditelj obrade) može jednom procjenom učinka na zaštitu podataka obuhvatiti sve nadzorne kamere na svim željezničkim postajama. To može biti primjenjivo i u sličnim postupcima obrade koje provode razni voditelji obrade podataka. U tim je slučajevima referentnu procjenu učinka na zaštitu podataka potrebno zajednički upotrebljavati ili učiniti javno dostupnom, moraju se provesti mjere opisane u procjeni učinka na zaštitu podataka, a provođenje jedne procjene učinka na zaštitu podataka potrebno je obrazložiti.

Ako postupak obrade uključuje zajedničke voditelje obrade, oni trebaju precizno definirati svoje obveze. U njihovoj procjeni učinka na zaštitu podataka treba biti utvrđena stranka koja je odgovorna



za različite mjere osmišljene za postupanje s rizicima i zaštitu prava i sloboda ispitanika. Svaki voditelj obrade podataka treba navesti svoje potrebe i podijeliti korisne informacije bez otkrivanja tajni (npr. zaštita poslovnih tajni, intelektualnog vlasništva, povjerljivih poslovnih informacija) ili slabosti.

**Procjena učinka na zaštitu podataka može biti korisna i u procjeni učinka nekog tehnološkog proizvoda na zaštitu podataka**, na primjer neke opreme ili nekog računalnog programa, koje će različiti voditelji obrade podataka vjerojatno upotrebljavati za provođenje različitih postupaka obrade. Naravno, voditelj obrade podataka koji upotrebljava proizvod i dalje mora provesti vlastitu procjenu učinka na zaštitu podataka s obzirom na specifičnu provedbu, ali te se informacije mogu nalaziti i u procjeni učinka na zaštitu podataka koju prema potrebi priprema dobavljač proizvoda. Kao primjer može poslužiti odnos između proizvođača pametnih brojlara i komunalnih poduzeća. Svaki dobavljač proizvoda ili izvršitelj obrade treba podijeliti korisne informacije bez otkrivanja tajni ili uzrokovanja sigurnosnih rizika otkrivanjem slabosti.

**B. Koji postupci obrade podliježu procjeni učinka na zaštitu podataka? Osim u iznimnim slučajevima, oni koji će vjerojatno prouzročiti visok rizik.**

U ovom se odjeljku opisuje u kojim je slučajevima procjena učinka na zaštitu podataka obvezna i kada je nije potrebno provesti.

**Osim ako postupak obrade ispunjava zahtjeve za iznimku (III.B.a), nužno je provesti procjenu učinka na zaštitu podataka ako će postupak obrade vjerojatno prouzročiti visok rizik (III.B.b).**

a) U kojim je slučajevima obvezno provođenje procjene učinka na zaštitu podataka? Ako će obrada *vjerojatno prouzročiti visok rizik*.

Općom se uredbom o zaštiti podataka ne zahtijeva provođenje procjene učinka na zaštitu podataka za svaki postupak obrade koji može prouzročiti rizike za prava i slobode pojedinaca. Provođenje procjene učinka na zaštitu podataka obvezno je samo ako će obrada *vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca* (članak 35. stavak 1., objašnjeno u članku 35. stavku 3. i nadopunjeno člankom 35. stavkom 4.). Ta je procjena posebno važna pri uvođenju nove tehnologije za obradu podataka<sup>11</sup>.

Ako nije jasno je li procjena učinka na zaštitu podataka potrebna, Radna skupina za zaštitu podataka iz članka 29. preporučuje da se ona ipak provede jer voditeljima obrade olakšava usklađivanje sa zakonodavstvom o zaštiti podataka.

Iako procjena učinka na zaštitu podataka može biti potrebna i u drugim okolnostima, u članku 35. stavku 3. navode se primjeri u kojima će postupak obrade *vjerojatno prouzročiti visok rizik*, odnosno u slučaju:

- (a) *sustavne i opsežne procjene osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca*<sup>12</sup>;

<sup>11</sup> Za dodatne primjere vidjeti uvodne izjave 89. i 91. te članak 35. stavke 1. i 3.

<sup>12</sup> Vidjeti uvodnu izjavu 71.: *osobito analiza ili predviđanje aspekata u vezi s učinkom na poslu, ekonomskim stanjem, zdravljem, osobnim preferencijama ili interesima, pouzdanošću ili ponašanjem, lokacijom ili kretanjem kako bi se izradili ili upotrebljavali osobni profili.*

- (b) opsežne obrade posebnih kategorija osobnih podataka iz članka 9. stavka 1. ili podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.<sup>13</sup> ili
- (c) sustavnog praćenja javno dostupnog područja u velikoj mjeri.

Riječ *osobito* u uvodnoj rečenici članka 35. stavka 3. Opće uredbe o zaštiti podataka upućuje na neiscrpan popis. Mogu postojati postupci obrade „visokog rizika” koji nisu navedeni na popisu, ali predstavljaju usporedivo visoke rizike. Ti postupci obrade isto bi tako trebali podlijevati procjeni učinka na zaštitu podataka. Stoga kriteriji utvrđeni u nastavku ponekad nadilaze jednostavno objašnjenje onoga što se podrazumijeva pod trima primjerima navedenima u članku 35. stavku 3. Opće uredbe o zaštiti podataka.

Kako bi se se osigurao konkretniji skup postupaka obrade koji zahtijevaju provođenje procjene učinka na zaštitu podataka zbog svojstvenog visokog rizika, uzimajući u obzir pojedine elemente članka 35. stavka 1., članka 35. stavka 3. točaka od (a) do (c), popis koji je potrebno donijeti na nacionalnoj razini u skladu s člankom 35. stavkom 4. i uvodnim izjavama 71., 75. i 91., kao i druga upućivanja iz Opće uredbe o zaštiti podataka na postupke obrade koji će *vjerojatno prouzročiti visok rizik*<sup>14</sup>, potrebno je razmotriti sljedećih devet kriterija.

1. Procjena ili bodovanje, uključujući izradu profila i predviđanje, osobito na temelju *aspekata ispitaničkovog učinka na poslu, ekonomskog stanja, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja* (uvodne izjave 71. i 91.). Primjeri mogu obuhvaćati financijsku instituciju koja provjerava svoje klijente u referentnoj bazi podataka o kreditnoj sposobnosti, u bazama podataka o suzbijanju pranja novca i financiranja terorizma ili u bazi podataka o prijevarama; biotehnološko poduzeće koje izravno svojim kupcima nudi genetska testiranja radi procjene i predviđanja bolesti/zdravstvenih rizika ili poduzeće koje izrađuje bihevioralne i marketinške profile utemeljene na upotrebi ili pregledavanju njihove internetske stranice.
2. Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom: obrada čiji je cilj donošenje odluka o ispitanicima proizvođači *pravne učinke koji se odnose na pojedinca ili na sličan način značajno utječu na pojedinca* (članak 35. stavak 3. točka (a)). Na primjer, obrada može rezultirati isključivanjem ili diskriminacijom pojedinaca. Obrada čiji je učinak na pojedince neznatan ili nikakav ne odgovara ovom specifičnom kriteriju. Ovi će pojmovi biti dodatno pojašnjeni u predstojećim smjernicama Radne skupine za zaštitu podataka iz članka 29. o profiliranju.
3. Sustavno praćenje: obrada koja se koristi za promatranje, praćenje ili kontrolu ispitanika, uključujući podatke prikupljene putem mreža ili „*sustavnog praćenja javno dostupnog područja*” (članak 35. stavak 3. točka (c))<sup>15</sup>. Ova je vrsta praćenja jedan od kriterija jer se

<sup>13</sup> Vidjeti uvodnu izjavu 75.: *ako se obrađuju osobni podaci koji odaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i ako je riječ o obradi genetičkih podataka, podataka koji se odnose na zdravlje ili spolni život ili kaznene osude i kažnjiva djela ili s tim povezane sigurnosne mjere.*

<sup>14</sup> Vidjeti npr. uvodne izjave 75., 76., 92. i 116.

<sup>15</sup> Radna skupina za zaštitu podataka iz članka 29. smatra da pojam *sustavno* može imati jedno značenje ili više njih, kako je navedeno u nastavku (vidjeti Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243):

- odvija se u skladu sa sustavom,
- planirano, organizirano ili metodično,
- odvija se kao dio općeg plana za prikupljanje podataka,

osobni podaci mogu prikupljati u situacijama u kojima ispitanici nisu svjesni tko prikuplja njihove podatke i u koje će svrhe ti podaci biti upotrijebljeni. Usto, pojedinci možda neće moći izbjeći takvu obradu na javnim (ili javno dostupnim) mjestima.

4. Osjetljivi podaci ili podaci vrlo osobne naravi: to uključuje posebne kategorije osobnih podataka, kako je utvrđeno u članku 9. (na primjer informacije o političkim mišljenjima pojedinaca), kao i osobne podatke koji se odnose na kaznene osude ili kažnjiva djela, kako je utvrđeno u članku 10. Primjer je opća bolnica koja čuva medicinsku dokumentaciju pacijenata ili privatni istražitelj koji čuva pojedinosti o prijestupnicima. Osim onoga što je obuhvaćeno odredbama Opće uredbe o zaštiti podataka, za neke se kategorije podataka može smatrati da povećavaju mogući rizik za prava i slobode pojedinaca. Ti osobni podaci smatraju se osjetljivima (kako se uobičajeno i shvaća ovaj pojam) jer su povezani s kućanstvom i privatnim aktivnostima (poput elektronske komunikacije čija povjerljivost treba biti zaštićena) ili zato što utječu na ostvarivanje temeljnog prava (poput lokacijskih podataka čije prikupljanje dovodi u pitanje slobodu kretanja) ili zato što njihova povreda očito podrazumijeva ozbiljne učinke na svakodnevni život ispitanika (poput financijskih podataka koji mogu biti upotrijebljeni za prijevaru u platnom prometu). U tom pogledu može biti važno je li te podatke već javno objavio ispitanik ili treća strana. Činjenica da su osobni podaci javno dostupni može se smatrati čimbenikom u procjeni ako se očekivalo daljnje korištenje tim podacima u određene svrhe. Taj kriterij može obuhvaćati i podatke poput osobnih dokumenata, e-pošte, dnevnika, bilježaka s e-čitača na kojima se mogu praviti bilješke i vrlo osobnih informacija sadržanih u aplikacijama za bilježenje životnih događaja.
5. Opsežna obrada podataka: u Općoj uredbi o zaštiti podataka nije određeno što obuhvaća pojam „opsežno”, ali se u uvodnoj izjavi 91. nalaze određene smjernice. U svakom slučaju, Radna skupina za zaštitu podataka iz članka 29. preporučuje da se, pri utvrđivanju je li obrada opsežna, posebno razmotre slijedeći čimbenici<sup>16</sup>:
  - a. broj uključenih ispitanika, bilo kao određeni broj ili udio relevantnog stanovništva;
  - b. količina podataka i/ili niz različitih podataka koji se obrađuju;
  - c. trajanje ili stalnost postupka obrade podataka;
  - d. zemljopisni opseg aktivnosti obrade.
6. Podudarajući ili kombinirani skupovi podataka, na primjer oni koji potječu iz dva postupka obrade ili više njih, a koji su provedeni u različite svrhe i/ili koje su proveli različiti voditelji obrade podataka na način koji može premašiti razumna očekivanja ispitanika<sup>17</sup>.
7. Podaci koji se odnose na osjetljive ispitanike (uvodna izjava 75.): obrada ove vrste podataka jest kriterij zbog povećane neravnoteže moći između ispitanika i voditelja obrade podataka, što znači da pojedinci ne mogu jednostavno dati suglasnost ili se usprotiviti obradi svojih podataka ili ostvarivati svoja prava. Osjetljivi ispitanici mogu biti djeca (smatra se da ne mogu svjesno i promišljeno dati pristanak ili se usprotiviti obradi podataka), zaposlenici, osjetljivije skupine stanovništva koje trebaju posebnu zaštitu (osobe s duševnim smetnjama, tražitelji

---

- provedeno kao dio strategije.

Radna skupina za zaštitu podataka iz članka 29. tumači pojam *javno dostupno područje* kao svaki prostor dostupan svakom građaninu, na primjer trg, trgovački centar, ulica, tržnica, željeznička postaja ili javna knjižnica.

<sup>16</sup> Vidjeti Smjernice Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243.

<sup>17</sup> Vidjeti objašnjenje u Mišljenju Radne skupine za zaštitu podataka iz članka 29. o ograničavanju svrhe, 13/EN WP 203, str. 24.

azila ili starije osobe, pacijenti itd.). Time su obuhvaćene i situacije u kojima se može utvrditi neravnoteža između položaja ispitanika i voditelja obrade.

8. Inovativna upotreba ili primjena novih tehnoloških ili organizacijskih rješenja, poput kombiniranja otisaka prstiju i prepoznavanja lica radi poboljšane kontrole fizičkog pristupa itd. Iz Opće je uredbе o zaštiti podataka jasno (članak 35. stavak 1. i uvodne izjave 89. i 91.) da upotreba nove tehnologije, definirane u skladu s postignutom razinom tehnološkog znanja (uvodna izjava 91.) može dovesti do potrebe za provođenjem procjene učinka na zaštitu podataka. To je zato što upotreba takve tehnologije može obuhvaćati inovativne oblike prikupljanja i upotrebe podataka s mogućim visokim rizikom za prava i slobode pojedinaca. Doista, osobne i društvene posljedice implementacije nove tehnologije još nisu posve poznate. Procjena učinka na zaštitu podataka pomoći će voditelju obrade podataka u razumijevanju takvih rizika i postupanju s njima. Na primjer, određene aplikacije „interneta stvari” mogu znatno utjecati na svakodnevni život i privatnost pojedinaca; stoga je potrebno provesti procjenu učinka na zaštitu podataka.
9. Situacija u kojoj sama obrada sprečava ispitanike u ostvarivanju prava ili upotrebi usluge i ugovora (članak 22. i uvodna izjava 91.). To uključuje i postupke obrade kojima se ispitanicima dopušta, mijenja ili odbija pristup pojedinoj usluzi ili sklapanje ugovora. Primjer je banka koja provjerava klijente u referentnoj bazi podataka o kreditnoj sposobnosti pri odlučivanju o dodjeli kredita.

U većini slučajeva, voditelj obrade podataka može smatrati da obrada koja ispunjava dva kriterija zahtijeva provođenje procjene učinka na zaštitu podataka. Općenito, Radna skupina za zaštitu podataka iz članka 29. smatra da što je više kriterija ispunjeno obradom, to je veća mogućnost da ona predstavlja visok rizik za prava i slobode ispitanika i stoga je nužno provođenje procjene učinka na zaštitu podataka, bez obzira na mjere koje voditelj obrade namjerava donijeti.

Međutim, u određenim slučajevima **voditelj obrade podataka može smatrati da je zbog obrade koja ispunjava samo jedan od tih kriterija nužno provesti procjenu učinka na zaštitu podataka.**

U slijedećim je primjerima prikazano na koji se način trebaju upotrijebiti kriteriji kako bi se procijenilo je li za određeni postupak obrade nužno provesti procjenu učinka na zaštitu podataka:

Primjeri obrade	Mogući relevantni kriteriji	Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna?
Bolnica koja obrađuje genetske i zdravstvene podatke svojih pacijenata (bolnički informacijski sustav).	<ul style="list-style-type: none"> <li>- <u>Osjetljivi podaci ili podaci vrlo osobne naravi.</u></li> <li>- Podaci koji se odnose na osjetljive ispitanike.</li> <li>- Opsežne obrade podataka.</li> </ul>	Da
Upotreba sustava nadzornih kamera za praćenje ponašanja vozača na autocestama. Voditelj obrade	<ul style="list-style-type: none"> <li>- Sustavno praćenje.</li> <li>- Inovativna upotreba ili primjena</li> </ul>	

Primjeri obrade	Mogući relevantni kriteriji	Hoće li procjena učinka na zaštitu podataka vjerojatno biti potrebna?
namjerava upotrijebiti sustav pametne video analize za izdvajanje automobila i automatsko prepoznavanje registarskih tablica.	tehnoloških ili organizacijskih rješenja.	
Poduzeće sustavno prati aktivnosti svojih zaposlenika, uključujući praćenje radne stanice, aktivnost na internetu itd.	<ul style="list-style-type: none"> <li>- Sustavno praćenje.</li> <li>- Podaci koji se odnose na osjetljive ispitanike.</li> </ul>	
Prikupljanje podataka s javnih društvenih medija za izradu profila.	<ul style="list-style-type: none"> <li>- Procjena ili bodovanje.</li> <li>- Opsežna obrada podataka.</li> <li>- Podudarajući ili kombinirani skupovi podataka.</li> <li>- <u>Osjetljivi podaci ili podaci vrlo osobne naravi:</u></li> </ul>	
Institucija koja uspostavlja bazu podataka kreditnog rejtinga ili prijevara na nacionalnoj razini.	<ul style="list-style-type: none"> <li>- Procjena ili bodovanje.</li> <li>- Automatizirano donošenje odluka s pravnim ili sličnim znatnim učinkom.</li> <li>- Sprečava ispitanika u ostvarivanju prava, korištenju uslugom ili ugovorom.</li> <li>- <u>Osjetljivi podaci ili podaci vrlo osobne naravi:</u></li> </ul>	
Pohrana u svrhu arhiviranja pseudonimiziranih osobnih osjetljivih podataka koji se odnose na osjetljive ispitanike u okviru istraživačkih projekata ili kliničkih ispitivanja.	<ul style="list-style-type: none"> <li>- Osjetljivi podaci.</li> <li>- Podaci koji se odnose na osjetljive ispitanike.</li> <li>- Sprečava ispitanike u ostvarivanju prava, korištenju uslugom ili ugovorom.</li> </ul>	
Obrada „osobnih podataka pacijenata ili klijenata pojedinih liječnika, zdravstvenih djelatnika ili odvjetnika” (uvodna izjava 91.).	<ul style="list-style-type: none"> <li>- <u>Osjetljivi podaci ili podaci vrlo osobne naravi.</u></li> <li>- Podaci koji se odnose na osjetljive ispitanike.</li> </ul>	Ne
Internetski časopis čiji se urednici koriste popisom adresa za slanje generičkih dnevnih novosti svojim pretplatnicima.	<ul style="list-style-type: none"> <li>- Opsežna obrada podataka.</li> </ul>	
Internetska stranica e-trgovine koja prikazuje reklame za dijelove oldtajmera, što obuhvaća i ograničenu izradu profila na temelju pregleda ili kupnji na vlastitoj internetskoj stranici.	<ul style="list-style-type: none"> <li>- Procjena ili bodovanje.</li> </ul>	

**S druge strane, postupak obrade može odgovarati prethodno navedenim slučajevima, a da voditelj obrade ipak ne smatra da će „vjerojatno prouzročiti visok rizik”. U takvim slučajevima**

**voditelj obrade treba opravdati i dokumentirati razloge za neprovođenje procjene učinka na zaštitu podataka te uključiti/zabilježiti mišljenje službenika za zaštitu podataka.**

Usto, kao dio načela odgovornosti, svaki voditelj obrade podataka *vodi evidenciju aktivnosti obrade za koje je odgovoran*, uključujući među ostalim svrhe obrade, opis kategorija podataka i primatelja podataka i *ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera iz članka 32. stavka 1.* (članak 30. stavak 1.) te mora procijeniti vjerojatnost visokog rizika, čak i ako konačno odluči da neće provesti procjenu učinka na zaštitu podataka.

Napomena: nadzorna tijela trebaju uspostaviti, objaviti i Europskom odboru za zaštitu podataka dostaviti popis postupaka obrade zbog kojih je nužno provesti procjenu učinka na zaštitu podataka (članak 35. stavak 4.)<sup>18</sup>. Prethodno utvrđeni kriteriji pomoći će nadzornim tijelima u izradi takvog popisa i prema potrebi u pravodobnom dodavanju konkretnijeg sadržaja. Na primjer, obrada bilo koje vrste biometričkih podataka ili podataka o djeci može se isto tako smatrati relevantnom za razvoj popisa u skladu s člankom 35. stavkom 4.

- b) U kojim slučajevima nije potrebna procjena učinka na zaštitu podataka? Ako nije vjerojatno da će obrada *vjerojatno prouzročiti visok rizik*, ako postoji slična procjena učinka na zaštitu podataka, ako je obrada bila odobrena prije svibnja 2018., ako ima pravni temelj ili ako je na popisu postupaka obrade za koje procjena učinka na zaštitu podataka nije potrebna.

Radna skupina za zaštitu podataka iz članka 29. smatra da procjena učinka na zaštitu podataka nije potrebna u slijedećim slučajevima:

- **ako obrada vjerojatno neće prouzročiti visok rizik za prava i slobode pojedinaca** (članak 35. stavak 1.),
- **ako su priroda, opseg, kontekst i svrhe obrade jako slični obradi za koju je procjena učinka na zaštitu podataka bila provedena.** U takvim slučajevima, mogu se koristiti rezultati procjene učinka na zaštitu podataka za slične obrade (članak 35. stavak 1.<sup>19</sup>),
- ako je postupke obrade provjerilo nadzorno tijelo prije svibnja 2018. u posebnim uvjetima koji se nisu promijenili<sup>20</sup> (vidjeti III.C),
- **ako postupak obrade**, u skladu sa člankom 6. stavkom 1. točkom (c) ili (e), **ima pravni temelj** u zakonodavstvu EU-a ili države članice, ako je zakonodavstvom uređen poseban postupak obrade **i ako je procjena učinka na zaštitu podataka već bila provedena** kao dio uspostave tog pravnog temelja (članak 35. stavak 10.)<sup>21</sup>, osim ako je država članica zahtijevala provođenje procjene učinka na zaštitu podataka prije aktivnosti obrade,

<sup>18</sup> U tom kontekstu *nadležno nadzorno tijelo primjenjuje mehanizam konzistentnosti iz članka 63. kada takvi popisi obuhvaćaju aktivnosti obrade koje su povezane s ponudom robe ili usluga ispitanicima ili s praćenjem njihova ponašanja u nekoliko država članica ili koje mogu znatno utjecati na slobodno kretanje osobnih podataka unutar Unije* (članak 35. stavak 6).

<sup>19</sup> *Jedna procjena može se odnositi na niz sličnih postupaka obrade koji predstavljaju slične visoke rizike.*

<sup>20</sup> *Donesene odluke Komisije i odobrenja nadzornih tijela koja se temelje na Direktivi 95/46/EZ ostaju na snazi dok ih se ne izmijeni, zamijeni ili stavi izvan snage* (uvodna izjava 171.).

<sup>21</sup> Ako se procjena učinka na zaštitu podataka provodi u razdoblju pripreme zakonodavstva kojim se pruža pravni temelj za obradu, vjerojatno je da su potrebna preispitivanja prije samog početka provedbe jer se doneseno zakonodavstvo može razlikovati od prijedloga u smislu da može utjecati na pitanja povezana s privatnošću i zaštitom podataka. Nadalje, moguće je da je količina dostupnih tehničkih detalja koji se odnose na obradu u vrijeme donošenja zakonodavstva nedostatna, čak i ako je popraćena procjenom učinka na zaštitu

- **ako je obrada uvrštena na fakultativni popis postupaka obrade (koji je uspostavilo nadzorno tijelo)** za koje nije potrebna procjena učinka na zaštitu podataka (članak 35. stavak 5.). Takav popis može sadržavati aktivnosti obrade koje odgovaraju uvjetima koje je utvrdilo to nadzorno tijelo, posebno smjernicama, posebnim odlukama ili odobrenjima, pravilima o usklađivanju itd. (npr. u Francuskoj su to odobrenja, izuzeća, pojednostavnjena pravila, paketi usklađenosti...). U takvim slučajevima i podložno ponovnoj procjeni koju provodi nadležno nadzorno tijelo, procjena učinka na zaštitu podataka nije potrebna, ali samo ako je obrada strogo obuhvaćena područjem primjene relevantnog postupka s popisa i ako je i dalje u potpunosti usklađena sa svim relevantnim zahtjevima Opće uredbe o zaštiti podataka.

C. Što je s postojećim postupcima obrade? Procjena učinka na zaštitu podataka potrebna je u nekim okolnostima.

**Obveza provođenja procjene učinka na zaštitu podataka primjenjuje se na postojeće postupke obrade, koji će vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca i u pogledu kojih je došlo do promjene rizika, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade.**

Procjena učinka na zaštitu podataka nije potrebna za postupke obrade koje je provjerilo nadzorno tijelo ili službenik za zaštitu podataka, u skladu s člankom 20. Direktive 95/46/EZ, i koji su se provodili na isti način od prethodne provjere. Doista, *donesene odluke Komisije i odobrenja nadzornih tijela koja se temelje na Direktivi 95/46/EZ ostaju na snazi dok ih se ne izmijeni, zamijeni ili stavi izvan snage* (uvodna izjava 171.).

S druge strane, to znači da bilo koja obrada podataka čiji su se uvjeti provedbe (opseg, svrha, prikupljeni osobni podaci, identitet voditelja obrade podataka ili primatelja, razdoblje čuvanja podataka, tehničke i organizacijske mjere itd.) promijenili od prethodne provjere koju je provelo nadzorno tijelo ili službenik za zaštitu podataka i koja će vjerojatno prouzročiti visok rizik, treba biti podvrgnuta procjeni učinka na zaštitu podataka.

Nadalje, procjena učinka na zaštitu podataka vjerojatno će biti potrebna nakon promjene rizika koji proizlaze iz postupaka obrade<sup>22</sup>, npr. zbog uvođenja nove tehnologije ili zbog korištenja osobnim podacima u druge svrhe. Postupci obrade podataka mogu se brzo razviti i mogu se pojaviti nove slabosti. Stoga, treba napomenuti da revizija procjene učinka na zaštitu podataka nije korisna samo za kontinuirana poboljšanja, nego je i ključna za održavanje razine zaštite podataka u okruženju koje se s vremenom mijenja. Procjena učinka na zaštitu podataka može postati neophodna jer se promijenio organizacijski ili društveni kontekst aktivnosti obrade, npr. jer su učinci određenih automatiziranih odluka postali važniji ili jer su nove kategorije ispitanika postale podložne diskriminaciji. Svaki od ovih primjera može postati element koji dovodi do promjena rizika proizašlih iz dotičnih aktivnosti obrade.

S druge strane, određene promjene isto tako mogu smanjiti rizike. Na primjer, postupak obrade može se razviti tako da odluke više nisu automatizirane ili ako aktivnosti povezane s praćenjem više nisu

---

podataka. U takvim je slučajevima i dalje neophodno provođenje posebne procjene učinka na zaštitu podataka prije provođenja konkretnih aktivnosti obrade.

<sup>22</sup> U smislu konteksta, prikupljenih podataka, svrha, funkcionalnosti, obrađenih osobnih podataka, primatelja, kombinacija podataka, rizika (pomoćna sredstva, izvori rizika, potencijalni učinci, prijetnje itd.), sigurnosnih mjera i međunarodnih prijenosa.

sustavne. U tom slučaju, preispitivanje analize rizika može pokazati da provođenje procjene učinka na zaštitu podataka više nije potrebno.

Kao pitanje dobre prakse, **procjena učinka na zaštitu podataka trebala bi se stalno preispitivati i redovito ponovno procjenjivati**. Stoga, čak i ako procjena učinka na zaštitu podataka nije potrebna na dan 25. svibnja 2018., bit će neophodno da voditelj obrade pravodobno provede takvu procjenu učinka na zaštitu podataka u okviru svojih općih obveza odgovornosti.

D. Kako se provodi procjena učinka na zaštitu podataka?

a) U kojem trenutku treba provesti procjenu učinka na zaštitu podataka? Prije obrade.

**Procjenu učinka na zaštitu podataka treba provesti prije obrade (članak 35. stavci 1. i 10., uvodne izjave 90. i 93.)<sup>23</sup>. To je u skladu s načelima tehničke i integrirane zaštite podataka (članak 25. i uvodna izjava 78.). Procjena učinka na zaštitu podataka pomoćni je alat za donošenje odluka o obradi.**

S provođenjem procjene učinka na zaštitu podataka potrebno je započeti što je prije moguće tijekom planiranja postupka obrade, čak i ako su neki postupci obrade još uvijek nepoznati. Ažuriranjem procjene učinka na zaštitu podataka tijekom trajanja projekta osigurat će se da se vodi računa o zaštiti podataka i privatnosti i potaknut će se iznalaženje rješenja kojima se potiče usklađenost. Pojedine će korake procjene možda biti potrebno ponoviti u tijeku postupka razvoja jer odabir određenih tehničkih ili organizacijskih mjera može utjecati na ozbiljnost i vjerojatnost rizika koje predstavlja obrada.

Činjenica da će procjena učinka na zaštitu podataka možda trebati biti ažurirana nakon što obrada stvarno započne nije valjan razlog za odgodu ili neprovođenje procjene učinka na zaštitu podataka. Procjena učinka na zaštitu podataka kontinuiran je proces, posebno ako je postupak obrade dinamičan i podložan stalnim promjenama. **Procjena učinka na zaštitu podataka provodi se kontinuirano, a ne jednom.**

b) Tko mora provesti procjenu učinka na zaštitu podataka? Voditelj obrade sa službenikom za zaštitu podataka i izvršiteljima obrade.

**Voditelj obrade odgovoran je za osiguravanje provođenja procjene učinka na zaštitu podataka (članak 35. stavak 2.).** Procjenu učinka na zaštitu podataka može provesti i druga osoba unutar i izvan organizacije, ali odgovornost za tu zadaću u potpunosti preuzima voditelj obrade.

**Voditelj obrade mora se savjetovati sa službenikom za zaštitu podataka**, ako je imenovan (članak 35. stavak 2.), što, uz odluke voditelja obrade, mora biti zabilježeno u procjeni učinka na zaštitu podataka. Službenik za zaštitu podataka mora pratiti provođenje procjene učinka na zaštitu podataka (članak 39. stavak 1. točka (c)). Daljnje smjernice navedene su u Smjernicama Radne skupine za zaštitu podataka iz članka 29. o službeniku za zaštitu podataka, 16/EN WP 243.

Ako obradu u cijelosti ili djelomično provodi izvršitelj obrade podataka, **on bi trebao pomoći voditelju obrade u provođenju procjene učinka na zaštitu podataka** i pružiti sve potrebne informacije (u skladu s člankom 28. stavkom 3. točkom (f)).

---

<sup>23</sup> Osim ako je riječ o postojećoj obradi koju je prethodno provjerilo nadzorno tijelo. U tom je slučaju procjenu učinka na zaštitu podataka potrebno provesti prije nego što se načine znatne promjene.



**Nužno je da voditelj obrade *prema potrebi od ispitanika ili njihovih predstavnika traži mišljenje* (članak 35. stavak 9.).** Stajalište Radne skupine za zaštitu podataka iz članka 29. sljedeće je:

- ta se mišljenja mogu prikupljati različitim sredstvima, ovisno o kontekstu (npr. generičkim studijama koje se odnose na svrhu i sredstva postupka obrade, upućivanjem pitanja predstavnicima osoblja ili uobičajenim anketama koje se šalju budućim klijentima voditelja obrade podataka), i na taj se način osigurava da voditelj obrade ima pravni temelj za obradu bilo kojih osobnih podataka obuhvaćenih prikupljanjem takvih mišljenja. Ipak, potrebno je napomenuti da pristanak na obradu očito nije način za prikupljanje mišljenja ispitanika,
- ako se konačna odluka voditelja obrade podataka razlikuje od mišljenja ispitanika, razlozi za nastavak ili prekid obrade moraju biti zabilježeni,
- ako voditelj obrade odluči da nije potrebno tražiti mišljenje ispitanika, npr. ako bi se time ugrozila povjerljivost poslovnih planova poduzeća ili ako bi to bilo nerazmjerno ili neizvedivo, svoje obrazloženje isto tako mora zabilježiti.

Konačno, dobra je praksa ako se definiraju i zabilježe druge specifične uloge i odgovornosti, ovisno o unutarnjoj politici, procesima i pravilima, npr.:

- ako određene poslovne jedinice mogu predložiti provođenje procjene učinka na zaštitu podataka, te bi jedinice u tom slučaju trebale pridonijeti procjeni učinka na zaštitu podataka i biti uključene u postupak vrednovanja procjene učinka na zaštitu podataka,
- prema potrebi, preporučuje se zatražiti savjet neovisnih stručnjaka različitih zanimanja<sup>24</sup> (odvjetnika, stručnjaka za IT, stručnjaka za sigurnost, sociologa, etičara itd.),
- uloge i odgovornosti izvršitelja obrade moraju biti definirane u ugovoru; izvršitelj obrade obvezno pomaže voditelju obrade u provođenju procjene učinka na zaštitu podataka, uzimajući u obzir prirodu obrade i informacije koje su mu dostupne (članak 28. stavak 3. točka (f)),
- glavni službenik za informacijsku sigurnost, ako je imenovan, kao i službenik za zaštitu podataka, mogu predložiti da voditelj obrade provede procjenu učinka na zaštitu podataka određenog postupka obrade, a dionicima bi trebali pomoći u utvrđivanju metodologije, ocjeni kvalitete procjene rizika i prihvatljivosti preostalog rizika te razvijati znanje potrebno voditeljima obrade podataka,
- glavni službenik za informacijsku sigurnost, ako je imenovan, i/ili informatička služba, trebaju pružiti pomoć voditelju obrade i mogu predložiti provođenje procjene učinka na zaštitu podataka određenog postupka obrade, ovisno o sigurnosnim ili operativnim potrebama.

- c) Koja je metodologija za provođenje procjene učinka na zaštitu podataka? Postoje različite metodologije, ali kriteriji su im zajednički.

---

<sup>24</sup> Preporuke za okvir procjene učinka na privatnost u Europskoj uniji, Izvješće D3:  
[http://www.piafproject.eu/ref/PIAF\\_D3\\_final.pdf](http://www.piafproject.eu/ref/PIAF_D3_final.pdf).

Općom se uredbom o zaštiti podataka utvrđuje da procjena učinka na zaštitu podataka sadržava barem (članak 35. stavak 7. i uvodne izjave 84. i 90.):

- *sustavan opis predviđenih postupaka obrade i svrha obrade,*
- *procjenu nužnosti i proporcionalnosti postupaka obrade,*
- *procjenu rizika za prava i slobode ispitanika,*
- *mjere predviđene za:*
  - o *„rješavanje problema rizika,*
  - o *dokazivanje sukladnosti s ovom Uredbom.*

Na sljedećem je dijagramu prikazan opći iterativan postupak provedbe procjene učinka na zaštitu podataka<sup>25</sup>:



Pri procjeni učinka postupka obrade podataka u obzir se mora uzeti (članak 35. stavak 8.) usklađenost s kodeksom ponašanja (članak 40.). To može biti korisno pri dokazivanju odabira ili provedbe prikladnih mjera, pod uvjetom da kodeks ponašanja odgovara postupku obrade. U obzir bi se trebali uzeti potvrde, pečati i oznake kojima se dokazuje da su postupci obrade koje provode voditelji obrade i izvršitelji obrade u skladu s Općom uredbom o zaštiti podataka (članak 42.), kao i obvezujuća korporativna pravila.

Svim se relevantnim zahtjevima utvrđenima u Općoj uredbi o zaštiti podataka omogućuje širok, opći okvir za oblikovanje i provođenje procjene učinka na zaštitu podataka. Praktična provedba procjene učinka na zaštitu podataka ovisi o zahtjevima utvrđenima u Općoj uredbi o zaštiti podataka, koji se

<sup>25</sup> Treba napomenuti da je iterativan i ovdje opisani postupak: u praksi je moguće da se svaka faza ponovi više puta prije nego što procjena učinka na zaštitu podataka može biti dovršena.

moгу dopuniti detaljnijim praktičnim smjernicama. Stoga je provedba procjene učinka na zaštitu podataka prilagodljiva. To znači da i maleni voditelj obrade podataka može oblikovati i provoditi procjenu učinka na zaštitu podataka koja je prikladna za njegove postupke obrade.

U uvodnoj izjavi 90. Opće uredbe o zaštiti podataka navodi se niz dijelova procjene učinka na zaštitu podataka koji se preklapaju s dobro definiranim dijelovima upravljanja rizicima (npr. ISO 31000<sup>26</sup>). U smislu upravljanja rizicima, procjena učinka na zaštitu podataka usmjerena je prema „upravljanju rizicima” za prava i slobode pojedinaca, uz upotrebu sljedećih postupaka:

- uspostava konteksta: *uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade te izvore rizika,*
- procjena rizika: *procjene osobite vjerojatnosti i ozbiljnosti visokog rizika,*
- postupanje s rizicima: *umanjivanje tog rizika i osiguravanje zaštite osobnih podataka i dokazivanje sukladnosti s ovom Uredbom.*

Napomena: procjena učinka na zaštitu podataka iz Opće uredbe o zaštiti podataka alat je za upravljanje rizicima za prava ispitanika promatrajući situaciju iz njihove perspektive, kao što je slučaj i u određenim područjima (npr. društvena sigurnost). S druge strane, upravljanje rizicima u drugim područjima (npr. informacijska sigurnost) usmjereno je na organizaciju.

Općom se uredbom o zaštiti podataka voditeljima obrade podataka omogućuje fleksibilnost u utvrđivanju točne strukture i oblika procjene učinka na zaštitu podataka kako bi se uklopila u postojeće radne prakse. Unutar EU-a i u cijelom svijetu uspostavljen je niz različitih postupaka u okviru kojih se u obzir uzimaju dijelovi opisani u uvodnoj izjavi 90. Međutim, bez obzira na oblik, procjenom učinka na zaštitu podataka moraju se zaista procijeniti rizici omogućavajući voditeljima obrade da poduzmu mjere za njihovo uklanjanje.

Različite se metodologije (vidjeti Prilog 1. za primjere zaštite podataka i metodologije procjene učinka na privatnost) mogu koristiti radi olakšavanja provedbe osnovnih zahtjeva utvrđenih u Općoj uredbi o zaštiti podataka. Kako bi se omogućili ti različiti pristupi, a da pritom voditelji obrade mogu djelovati u skladu s Općom uredbom o zaštiti podataka, utvrđeni su zajednički kriteriji (vidjeti Prilog 2.). Njima se pojašnjavaju osnovni zahtjevi ove Uredbe ostavljajući dovoljno prostora za različite oblike provedbe. Ti se kriteriji mogu koristiti kao dokaz da je određena metodologija procjene učinka na zaštitu podataka usklađena sa standardima koji se zahtijevaju Općom uredbom o zaštiti podataka. **Voditelj obrade podataka mora odabrati metodologiju, ali ta metodologija mora biti usklađena s kriterijima iz Priloga 2.**

Radna skupina za zaštitu podataka iz članka 29. potiče razvoj okvira procjene učinka na zaštitu podataka specifičnih za pojedine sektore. To je zbog toga što mogu iskoristiti znanje koje posjeduju u pojedinim sektorima, što znači da se procjenom učinka na zaštitu podataka mogu obuhvatiti pojedinosti određene vrste postupka obrade (npr.: određene vrste podataka, zajednička imovina, potencijalni učinci, prijetnje, mjere). To znači da se procjenom učinka na zaštitu podataka mogu riješiti pitanja koja se javljaju u određenom gospodarskom sektoru ili pri upotrebi određenih tehnologija ili provedbi određenih vrsta postupaka obrade.

---

<sup>26</sup> Postupci upravljanja rizicima: komunikacija i konzultacije, uspostava konteksta, procjena rizika, postupanje s rizicima, praćenje i pregled (vidjeti izraze i definicije te sadržaj u pregledu norme ISO 31000: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>).

Konačno, prema potrebi *voditelj obrade provodi preispitivanje kako bi procijenio je li obrada provedena u skladu s procjenom učinka na zaštitu podataka barem onda kada postoji promjena u razini rizika koji predstavljaju postupci obrade.* (članak 35. stavak 11.<sup>27</sup>).

- d) Postoji li obveza objavljivanja procjene učinka na zaštitu podataka? Ne, ali objavom sažetka može se potaknuti povjerenje, dok cijela procjena učinka na zaštitu podataka mora biti dostavljena nadzornom tijelu u slučaju prethodnih konzultacija ili ako to zahtijeva tijelo za zaštitu podataka.

**Objava procjene učinka na zaštitu podataka nije propisana Općom uredbom o zaštiti podataka, nego o tome odlučuje voditelj obrade. Ipak, voditelji obrade trebali bi razmisliti o objavi pojedinih dijelova, kao što je sažetak ili zaključak njihove procjene učinka na zaštitu podataka.**

Time se želi potaknuti povjerenje u postupke obrade koje provodi voditelj obrade te dokazati odgovornost i transparentnost. Objava procjene učinka na zaštitu podataka vrlo je dobra praksa ako postupak obrade utječe na javnost. To je osobito slučaj ako tijelo javne vlasti provodi procjenu učinka na zaštitu podataka.

Objavljena procjena učinka na zaštitu podataka ne treba sadržavati cijelu procjenu, posebno ako bi se u procjeni učinka na zaštitu podataka mogle nalaziti određene informacije koje se odnose na sigurnosne rizike za voditelja obrade podataka ili ako bi se objavljivanjem mogle odati poslovne tajne ili osjetljive poslovne informacije. U tim okolnostima, objavljena verzija može se sastojati samo od sažetka glavnih zaključaka procjene učinka na zaštitu podataka ili čak samo od izjave da je provedena procjena učinka na zaštitu podataka.

Dakle, ako se procjenom učinka na zaštitu podataka otkriju visoki preostali rizici, voditelj obrade podataka mora se prije obrade savjetovati s nadzornim tijelom (članak 36. stavak 1.). U okviru toga nužno je dostaviti čitavu procjenu učinka na zaštitu podataka (članak 36. stavak 3. točka (e)). Nadzorno tijelo može dati svoj savjet<sup>28</sup>, čime se neće ugroziti sigurnost poslovnih tajni ili razotkriti sigurnosne slabosti, u skladu s načelima javnog pristupa službenim dokumentima primjenjivima u svakoj državi članici.

**E. Kada je potrebno savjetovati se s nadzornim tijelom? U slučaju visokih preostalih rizika.**

Kao što je prethodno objašnjeno:

- procjena učinka na zaštitu podataka potrebna je ako će obrada podataka *vjerojatno prouzročiti visok rizik za prava i slobode pojedinaca* (članak 35. stavak 1., vidjeti III.B.a). Na primjer, smatra se da će opsežna obrada zdravstvenih podataka rezultirati visokim stupnjem rizika i da je potrebna procjena učinka na zaštitu podataka,
- zatim je voditelj obrade podataka dužan procijeniti rizike za prava i slobode ispitanika i utvrditi predviđene mjere<sup>29</sup> za smanjenje tih rizika na prihvatljivu razinu i dokazivanje sukladnosti s Općom uredbom o zaštiti podataka (članak 35. stavak 7., vidjeti III.C.c). Kao

<sup>27</sup> U članku 35. stavku 10. izričito se isključuje samo primjena članka 35. stavaka od 1. do 7.

<sup>28</sup> Savjetovanje voditelja obrade pisanim putem neophodno je samo ako nadzorno tijelo smatra da obrada nije u skladu s Uredbom, kako je utvrđeno u članku 36. stavku 2.

<sup>29</sup> Među ostalim uzimajući u obzir postojeće smjernice Europskog odbora za zaštitu podataka i nadzornih tijela, kao i najnovija dostignuća i troškove provedbe kao što je propisano člankom 35. stavkom 1.

primjer moglo bi se navesti pohranjivanje osobnih podataka u prijenosno računalo uz upotrebu prikladnih tehničkih i organizacijskih sigurnosnih mjera (učinkovito šifriranje cijelog diska, sigurno upravljanje ključem, prikladni nadzor pristupa, zaštićene sigurnosne kopije itd.) uz postojeće politike (obavijest, privola, pravo pristupa, pravo na prigovor itd.).

U prethodno navedenom primjeru prijenosnog računala, ako voditelj obrade podataka smatra da je rizik dovoljno umanjen te u skladu s tekstem članka 36. stavka 1. i uvodnih izjava 84. i 94., obrada se može nastaviti bez savjetovanja s nadzornim tijelom. Samo u slučajevima u kojima utvrđene rizike voditelj obrade podataka ne može ukloniti na odgovarajući način, (tj. preostali rizici su i dalje visoki), voditelj obrade podataka mora potražiti savjet nadzornog tijela.

Primjer neprihvatljivog visokog preostalog rizika uključuje slučajeve u kojima se ispitanici mogu suočiti sa znatnim ili čak nepopravljivim posljedicama, koje možda neće moći ukloniti (npr.: neovlašteni pristup podacima kojim se može ugroziti život ispitanika, otpuštanje, financijski rizik) i/ili ako je očito da će doći do pojave rizika (npr.: ako se ne može smanjiti broj osoba koje pristupaju podacima zbog razmjene podataka, njihove upotrebe ili načina distribucije ili ako dobro poznata slabost nije uklonjena).

**Ako voditelj obrade podataka ne može pronaći odgovarajuće mjere za smanjenje rizika na prihvatljivu razinu (tj. ako su preostali rizici i dalje visoki), mora se savjetovati s nadzornim tijelom<sup>30</sup>.**

Osim toga, voditelj obrade morat će se savjetovati s nadzornim tijelom kad god se pravom države članice propisuje da se voditelji obrade savjetuju s nadzornim tijelom i/ili da od njega moraju dobiti prethodno odobrenje u pogledu obrade koju obavlja voditelj obrade za izvršenje zadaće koju voditelj obrade provodi u javnom interesu, uključujući obradu u vezi sa socijalnom zaštitom i javnim zdravljem (članak 36. stavak 5.).

Trebalo bi međutim istaknuti da, bez obzira na to je li savjetovanje s nadzornim tijelom potrebno s obzirom na razinu preostalog rizika, čuvanje zapisa o procjeni učinka na zaštitu podataka i pravodobno ažuriranje procjene učinka na zaštitu podataka i dalje su nužni.

#### **IV. Zaključci i preporuke**

Procjena učinka na zaštitu podataka koristan je način da voditelji obrade podataka primjene sustave za obradu podataka usklađene s Općom uredbom o zaštiti podataka koji mogu biti obvezni za neke vrste postupaka obrade. Oni su prilagodljivi i mogu biti u različitim oblicima, no ipak, Općom se uredbom o zaštiti podataka utvrđuju osnovni zahtjevi učinkovite procjene učinka na zaštitu podataka. Voditelji obrade podataka moraju biti svjesni da je procjena učinka na zaštitu podataka korisna i pozitivna aktivnost kojom se olakšava pravna usklađenost.

U članku 24. stavku 1. navode se osnovne obveze voditelja obrade u pogledu usklađenosti s Općom uredbom o zaštiti podataka: *Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi*

---

<sup>30</sup> Napomena: *pseudonimizacija i enkripcija osobnih podataka* (kao i minimizacija podataka, mehanizmi nadzora itd.) nisu nužno odgovarajuće mjere. Riječ je samo o primjerima. Odgovarajuće mjere ovise o kontekstu i rizicima koji su specifični za postupke obrade.

*odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju.*

Procjena učinka na zaštitu podataka ključan je dio usklađivanja s Uredbom ako se planira ili provodi obrada podataka visokog rizika. To znači da se voditelji obrade podataka trebaju koristiti kriterijima utvrđenima u ovom dokumentu kako bi odredili mora li se provesti procjena učinka na zaštitu podataka. Unutarnja politika voditelja obrade podataka može nadilaziti pravne zahtjeve Opće uredbe o zaštiti podataka. To bi trebalo dovesti do većeg povjerenja ispitanika i drugih voditelja obrade podataka.

Ako se planira obrada koja će vjerojatno prouzročiti visok rizik, voditelj obrade podataka mora:

- odabrati prikladnu metodologiju procjene učinka na zaštitu podataka (primjeri su navedeni u Prilogu 1.) koja zadovoljava kriterije iz Priloga 2. ili navesti i provesti sustavan postupak procjene učinka na zaštitu podataka koji je:
  - o usklađen s kriterijima iz Priloga 2.,
  - o integriran u postojeće postupke oblikovanja, razvoja, promjene, utvrđivanja rizika i operativnog preispitivanja u skladu s unutarnjim postupcima, kontekstom i kulturom i
  - o u koji su uključene odgovarajuće zainteresirane strane, čije su odgovornosti jasno definirane (voditelj obrade, službenik za zaštitu podataka, ispitanici ili njihovi predstavnici, poslovni subjekti, tehničke službe, izvršitelji obrade, službenik za informacijsku sigurnost itd.),
- dostaviti izvješće o procjeni učinka na zaštitu podataka odgovarajućem nadzornom tijelu ako je to potrebno,
- savjetovati se s nadzornim tijelom ako nije uspio utvrditi mjere dostatne za ublažavanje visokih rizika,
- povremeno preispitivati procjenu učinka na zaštitu podataka i obradu koja se njome procjenjuje, barem ako se promijeni rizik koji predstavlja obrada aktivnosti,
- zabilježiti donesene odluke.

## Prilog 1. – Primjeri postojećih okvira EU-a u pogledu procjene učinka na zaštitu podataka

U Općoj uredbi o zaštiti podataka ne navodi se koji se postupak procjene učinka na zaštitu podataka mora slijediti, nego se voditeljima obrade podataka omogućuje uvođenje okvira usklađenog s postojećim radnim praksama, pod uvjetom da se u obzir uzmu dijelovi opisani u članku 35. stavku 7. Takav okvir može biti namijenjen voditelju obrade podataka ili se isti okvir može zajednički upotrebljavati u određenoj industriji. Prethodno objavljeni okviri koje su razvila tijela EU-a za zaštitu podataka i okviri EU-a specifični za pojedine sektore među ostalim uključuju sljedeće:

Primjeri općih okvira EU-a:

- Njemačka: Standardni model zaštite podataka, V.1.0 – probna verzija, 2016.<sup>31</sup>  
[https://www.datenschutzzentrum.de/uploads/SDM-Methodology\\_V1\\_EN1.pdf](https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf)
- Španjolska: *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)
- Francuska: *Procjena učinka na privatnost*, Commission nationale de l'informatique et des libertés (CNIL), 2015.  
<https://www.cnil.fr/fr/node/15798>
- Ujedinjena Kraljevina: *Primjena kodeksa postupanja tijekom provedbe procjene učinka na privatnost*, Ured povjerenika za pravo na pristup informacijama (ICO), 2014.  
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Primjeri okvira EU-a specifičnih za pojedine sektore:

- okvir procjene učinka na privatnost i zaštitu podataka za aplikacije za radiofrekvencijsku identifikaciju (RFID)<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)
- obrazac za procjenu učinka na zaštitu podataka za pametne mreže i pametne mjerne sustave<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> Jednoglasno prihvaćen i priznat (Bavarija suzdržana) na 92. konferenciji neovisnih tijela za zaštitu podataka središnje vlade i saveznih pokrajina u Kuhlungsbornu, održanoj od 9. do 10. studenoga 2016.

<sup>32</sup> Vidjeti i:

- Preporuku komisije od 12. svibnja 2009. o provedbi načela zaštite podataka i privatnosti u aplikacijama koji se oslanjaju na radiofrekvencijsku identifikaciju  
<https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles>
- Mišljenje 9/2011 o revidiranom prijedlogu industrije za okvir procjene učinka na zaštitu podataka i privatnosti za aplikacije za radiofrekvencijsku identifikaciju.  
[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> Vidjeti i Mišljenje 07/2013 o Obrascu za procjenu utjecaja na zaštitu podataka za pametne mreže i pametne mjerne sustave („Obrazac PUZP”) koji je pripremila Stručna skupina 2 Radne skupine Komisije za pametne mreže. [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209\\_hr.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_hr.pdf)

Isto tako, u međunarodnom standardu pružit će se smjernice za metodologije koje se koriste za provođenje procjene učinka na zaštitu podataka (ISO/IEC 29134<sup>34</sup>).

---

<sup>34</sup> ISO/IEC 29134 (projekt), *Informacijske tehnologije – Sigurnosne tehnike – Procjena učinka na privatnost – Smjernice*, Međunarodna organizacija za normizaciju (ISO).



## **Prilog 2. – Kriteriji za prihvatljivu procjenu učinka na zaštitu podataka**

Radna skupina za zaštitu podataka iz članka 29. predlaže slijedeće kriterije kojima se voditelji obrade podataka mogu koristiti kako bi procijenili je li procjena učinka na zaštitu podataka ili metodologija za provođenje procjene učinka na zaštitu podataka dostatno opsežna za potrebe usklađivanja s Općom uredbom o zaštiti podataka:

- ☐ procjena sadržava sustavan opis obrade (članak 35. stavak 7. točka (a)):
  - ☐ u obzir su uzeti priroda, opseg, kontekst i svrhe obrade (uvodna izjava 90.);
  - ☐ zabilježeni su osobni podaci, primatelji i razdoblje pohrane osobnih podataka;
  - ☐ naveden je funkcionalni opis postupka obrade;
  - ☐ utvrđena su sredstva o kojima ovise osobni podaci (oprema, računalni programi, mreže, osobe, dokumenti u papirnatom obliku ili kanali za slanje dokumenata u papirnatom obliku);
  - ☐ u obzir je uzeta i usklađenost s odobrenim kodeksima ponašanja (članak 35. stavak 8.);
- ☐ procijenjene su nužnost i proporcionalnost (članak 35. stavak 7. točka (b)):
  - ☐ određene su mjere predviđene za usklađivanje s Uredbom (članak 35. stavak 7. točka (d) i uvodna izjava 90.), uzimajući u obzir:
    - ☐ mjere koje pridonose proporcionalnosti i nužnosti obrade na temelju:
      - ☐ posebnih, izričitih i zakonitih svrha (članak 5. stavak 1. točka (b));
      - ☐ zakonitosti obrade (članak 6.);
      - ☐ primjerenih i relevantnih osobnih podataka, ograničenih na ono što je nužno (članak 5. stavak 1. točka (c));
      - ☐ ograničenog trajanja pohrane (članak 5. stavak 1. točka (e));
    - ☐ mjere koje pridonose pravima ispitanika:
      - ☐ informacije pružene ispitaniku (članak 12., 13. i 14.);
      - ☐ pravo na pristup i prenosivost podataka (članci 15. i 20.);
      - ☐ pravo na ispravak i brisanje (članci 16., 17. i 19.);
      - ☐ pravo na prigovor i ograničavanje obrade (članci 18., 19. i 21.);
      - ☐ odnosi s izvršiteljima obrade (članak 28.);
      - ☐ zaštitne mjere koje se odnose na međunarodni prijenos (poglavlje V.);
      - ☐ prethodno savjetovanje (članak 36.).
- ☐ kontrolirani su rizici za prava i slobode ispitanika (članak 35. stavak 7. točka (c)):
  - ☐ uvaženi su izvor, priroda, osobitost i ozbiljnost rizika (vidjeti uvodnu izjavu 84.) ili detaljnije, za svaki rizik (neovlašteni pristup, neželjene izmjene i nestanak podataka) iz perspektive ispitanika:
    - ☐ u obzir su uzeti izvori rizika (uvodna izjava 90.);
    - ☐ mogući učinci na prava i slobode ispitanika utvrđeni su među ostalim u slučaju neovlaštenog pristupa, neželjene izmjene i nestanka podataka;
    - ☐ utvrđene su prijetnje koje mogu dovesti do neovlaštenog pristupa, neželjene izmjene i nestanka podataka;
    - ☐ procijenjene su vjerojatnost i ozbiljnost (uvodna izjava 90.);
  - ☐ određene su mjere predviđene za uklanjanje tih rizika (članak 35. stavak 7. točka (d) i uvodna izjava 90.);
- ☐ uključene su zainteresirane strane:
  - ☐ zatražen je savjet službenika za zaštitu podataka (članak 35. stavak 2.);
  - ☐ prema potrebi zatražena su mišljenja ispitanika ili njihovih predstavnika (članak 35. stavak 9.).