Številka: 007-18/2022/2
Datum: 18. 7. 2022

Ministrstvo za javno upravo
Gp.mju@gov.si

ZADEVA: Predlog Izvajanje projekta ePredpisov – Javna obravnava osnutka Metodologije za oceno učinkov na različna družbena področja – MNENJE
ZVEZA: vaš dopis št. 010-64/2020/38, prejet dne 17. 6. 2022 ter priloženo gradivo

Spoštovani,

na podlagi vašega zaprosila, 48. člena Zakona o varstvu osebnih podatkov (v nadaljevanju ZVOP-1), 57. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba) in 76. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (Uradni list RS, št. 177/20, v nadaljevanju ZVOPOKD) posredujemo mnenje Informacijskega pooblaščenca (v nadaljevanju: IP) na osnutek Metodologije za oceno učinkov na različna družbena področja v okviru projekta ePredpisov (v nadaljevanju predlog metodologije).

Uvodoma izpostavljamo, da izkušnje Informacijskega pooblaščenca (v nadaljevanju IP) v zadnjih letih kažejo, da v okviru priprave predlogov predpisov pogosto predlagatelji premalo pozornosti posvetijo vprašanjem povezanim z novimi oblikami sistemskega urejanja množičnih obdelav osebnih podatkov, zlasti v okviru uvedbe novih tehnologij, ki imajo za posameznike lahko resne posledice, če se pravočasno ne prepoznajo in naslovijo vsa tveganja, ki jih takšne nove obdelave in tehnologije prinašajo. Hkrati pa ugotavljamo, da primeri dobrih praks posameznih predlagateljev, ki v okviru priprave predlogov predpisov področju varstva osebnih podatkov posvetijo ustrezno pozornost in posledično pravočasno prepoznajo in naslovijo ta tveganja, dokazujejo, da takšen pristop prinaša pomembne koristi tako pri kakovosti predlaganih rešitev in prihranku finančnih sredstev (zaradi pravočasne prepoznave in izbire optimalnih rešitev tako z vidika učinkovitosti kot varstva pravic) kot tudi morda najpomembneje v obliki večjega zaupanja posameznikov v nove rešitve.

V zvezi s tem bi radi izpostavili tri vidike, ki so pomembni za predlog metodologije, in sicer najprej **38. člen Ustave**, ki zahteva, da je vsaka obdelava osebnih podatkov primarno opredeljena z zakonom in ne podzakonskim aktom. To še posebej velja za urejanje področij uporabe informacijskih tehnologij, kjer je posameznik v bistveno podrejenem položaju nasproti organom države in nima resničnega vpliva na posledice, ki jih bo to zanj prineslo, hkrati pa so tovrstne obdelave v uradnih in drugih postopkih bistvenega pomena za njegovo življenje (npr. urejanje različnih formalnih postopkov, poslovanje z bankami in drugimi poslovnimi subjekti).

Druga pomembna točka je **pravočasna izvedba t.i. ocene učinkov predvidenih dejanj obdelave na varstvo osebnih podatkov, kot je predvidena v 35. členu Splošne uredbe in v 49. členu**

ZVOPOKD. Praksa namreč potrjuje, da mora biti prva faza ocene učinkov izvedena že v fazi snovanja predpisa, ko je namreč predpis sprejet, nejasnosti, nesorazmernosti obdelav ali neustreznosti predpisanih rešitev ni mogoče več reševati z naknadno oceno učinkov. Ob tem je pomembno, da je v številnih primerih takšna ocena učinkov obvezna pred začetkom obdelave, če ocena učinkov ni bila izvedena v okviru splošne ocene učinkov med sprejemanjem posameznega zakona, ki je pravna podlaga za obdelavo na podlagi točk c oz. e prvega odstavka 6. člena Splošne uredbe ali 6., 7. oz. 8. člena ZVOPOKD. Temu bi lahko zadostili z ustrezno obsežno dopolnitvijo predloga metodologije, kot predlagamo v nadaljevanju.

Tretji vidik je dosledna **uporaba terminologije, definicij in ureditev skladno z veljavnimi predpisi na področju varstva osebnih podatkov** npr. v točki 3 III. poglavja predloga metodologije definicija pojma posredovanja osebnih podatkov, vpogleda ali dostopa do podatkov v zbirki osebnih podatkov in pojma povezovanja. Metodologija ne more in ne sme posameznih pojmov opredeljevati drugače kot veljavni predpisi.

Konkretno glede predloga metodologije ugotavljamo, da ne zajema ustrezno vseh vsebin ocene učinkov, kot so predvideni v ZVOPOKD in Splošni uredbi. Deloma so posamezni zelo ozki deli take ocene, ki se nanašajo na obstoj pravne podlage za obdelavo osebnih podatkov takih novih rešitev zajeti v točkah 5 in 6 III. poglavja predloga metodologije, ki se nanaša na Oceno administrativnih učinkov, ki vključuje tudi informacijske vidike, vendar pa ocenjujemo, da zgolj navedena vprašanja, ki se obravnavajo v okviru III. poglavja ne zadostijo zahtevam 36. člena Splošne uredbe oz. 49. člena ZVOPOKD. **Zato predlagamo, da se upoštevajoč navedene zakonske določbe (11. in 49. člen ZVOPOKD ter 35. člen Splošne uredbe) ter Seznam dejanj obdelav osebnih podatkov, za katere velja zahteva po izvedbi ocene učinka v zvezi z varstvom osebnih podatkov po 4. odstavku člena 35 Uredbe (EU) 2016/679[1] v predlogu metodologije izrecno opredeli primere, ko mora biti izvedba predhodne ocene učinkov po Splošni uredbi oz. ZVOPOKD obvezni del procesa priprave predpisov.**

V nadaljevanju v zvezi s tem podajamo konkretne predloge za oblikovanje takšne obvezne ocene učinkov pri pripravi zakonodajnih predlogov, pri čemer smo upoštevali obseg, pristop in strukturo ostalih ocen učinkov.

[1] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf

Ocena učinkov na varstvo osebnih podatkov

1) Uvod

Ocene učinkov v zvezi z varstvom osebnih podatkov (angl. DPIA) predstavljajo orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije. Ocene učinkov v zvezi z varstvom osebnih podatkov so se najprej uveljavile kot orodje pri snovalcih zakonodaje, politik in projektov v Kanadi, Avstraliji in ZDA, z določbami Splošne uredbe ter Direktive EU 2016/680 pa postajajo v določenih primerih obvezne tudi v evropskem prostoru. Ocene učinkov v zvezi z varstvom osebnih podatkov temeljijo na sistematični in pravočasni identifikaciji tveganj za nezakonita ravnanja z osebnimi podatki, s katerimi se lahko tveganja ustrezno upravlja - pravočasno identificira, odpravi, zmanjša ali sprejme.

2) Obrazložitev

Poleg ocene učinkov v zvezi z varstvom osebnih podatkov, ki jih pripravljajo upravljavci osebnih podatkov, so posebej pomembne ocene učinka glede varstva osebnih podatkov pri pripravi predpisov. Glede na to, da mora obdelavo osebnih podatkov določati zakon (kakor tudi upravljavce, namene, roke hrambe, evidence, morebitno povezovanje zbirk ipd.), je bistveno, da se tveganja glede varstva osebnih podatkov analizirajo že v času priprave predpisa, saj jih upravljavci kasneje, ko so bistveni elementi že določeni v predpisu, ne morejo spremeniti in njihove ocene učinka nimajo več takšnega pomena. Kakovostno in celovito izdelana ocena učinka na ravni predpisa lahko bistveno razbremeni upravljavce podatkov, ki bi nato morali izdelovati ločene ocene učinka (10. odstavek 35. člena Splošne uredbe oz. 3. odstavek 49. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj - ZVOPOKD).

Ocena učinka v zvezi z varstvom osebnih podatkov lahko v fazi snovanja predpisa zagotovi upoštevanje temeljnih načel varstva osebnih podatkov: poštenosti, preglednosti in zakonitosti, minimizacije obdelave, namenskosti, ažurnosti, rokov hrambe ter določitev ustreznih zaščitnih ukrepov in varovalk – njen cilj je celovit premislek o tem, katere podatke se bo zbiralo in za katere namene, kakšne so možnosti minimizacije nabora in obsega obdelave, katere evidence bodo vsebovale katere podatke in kdo bo z njimi upravljal, ali gre pri tem morda za skupno upravljanje, ali je predvideno povezovanje evidenc, kakšne so relevantne pravice posameznika, kateri so najkrajši možni roki hrambe, komu se bodo določeni podatki posredovali, ali prihaja do prenosa osebnih podatkov v tretje države ipd.

Izjemnega pomena so zlasti pri uvajanju sistematičnih novih obsežnih nacionalnih zbirk osebnih podatkov, novih policijskih pooblastil in pristojnosti, na področju obdelave posebej občutljivih podatkov (kot npr. podatki o zdravstvenem stanju, podatki o kazenskih in prekrškovnih postopkih, genski, biometrijski podatki ipd.), pri opredeljevanju ukrepov, ki zadevajo široko populacijo ali specifične družbene segmente, saj z analizo tveganj in učinkov na posameznika in družbo omogočajo javni diskurz o sprejemljivosti, primernosti, učinkovitosti ter nujnosti določenih ukrepov v demokratični družbi.

3) Opredelitev pojmov

- **osebni podatki** pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;
- **obdelava** pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;
- **omejitev obdelave** pomeni označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;
- **oblikovanje profilov** pomeni vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;
- **psevdonimizacija** pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;
- **zbirka** pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
- **upravljavec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;
- **obdelovalec** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
- **uporabnik** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
- **tretja oseba** pomeni fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
- **privolitev posameznika**, na katerega se nanašajo osebni podatki pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj;
- **kršitev varnosti osebnih podatkov** pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
- **genski podatki** pomeni osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;
- **biometrični podatki** pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;
- **podatki o zdravstvenem stanju** pomeni osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;

- **glavna ustanovitev** pomeni: | (a) | v zvezi z upravljavcem, ki ima ustanovitve v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugi ustanovitvi upravljavca v Uniji in ima ta ustanovitev pooblastila za izvajanje takih odločitev, ustanovitev, ki sprejema take odločitve; | (b) | v zvezi z obdelovalcem, ki ima ustanovitve v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, če obdelovalec nima osrednje uprave v Uniji, ustanovitev obdelovalca v Uniji, kjer se izvajajo glavne dejavnosti obdelave v okviru dejavnosti ustanovitve obdelovalca, kolikor za obdelovalca veljajo posebne obveznosti iz Splošne uredbe;
- **predstavnik** pomeni fizično ali pravno osebo z ustanovitvijo v Uniji, ki jo pisno imenuje upravljavec ali obdelovalec v skladu s 27. členom in ki predstavlja upravljavca ali obdelovalca v zvezi z njegovimi obveznostmi iz Splošne uredbe;
- **podjetje** pomeni fizično ali pravno osebo, ki opravlja gospodarsko dejavnost, ne glede na njeno pravno obliko, vključno s partnerstvi ali združenji, ki redno opravljajo gospodarsko dejavnost;
- **povezana družba** pomeni obvladujočo družbo in njene odvisne družbe;
- **zavezujoča poslovna pravila** pomeni politike na področju varstva osebnih podatkov, ki jih upravljavec ali obdelovalec z ustanovitvijo na ozemlju države članice spoštuje pri prenosih ali nizih prenosov osebnih podatkov upravljavcu ali obdelovalcu povezane družbe ali skupine podjetij, ki opravljajo skupno gospodarsko dejavnost, v eni ali več tretjih državah;
- **čezmejna obdelava osebnih podatkov** pomeni bodisi: | (a) | obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti ustanovitev upravljavca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec ustanovitev v več kot eni državi članici, bodisi | (b) | obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edine ustanovitve upravljavca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;
- **ustrezen in utemeljen ugovor** pomeni ugovor osnutku odločitve glede tega, ali je bila Splošna uredba kršena, oziroma glede tega, ali je predvideno ukrepanje v zvezi z upravljavcem ali obdelovalcem v skladu s Splošno uredbo, kar jasno navede pomen tveganja, ki ga predstavlja osnutek odločitve, kar zadeva temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in – kjer je to ustrezno – prosti pretok osebnih podatkov v Uniji;
- **storitev informacijske družbe** pomeni storitev, kakor je opredeljena v točki (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta (19);
- **mednarodna organizacija** pomeni organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo ali kateri koli drugo telo, ustanovljeno s sporazumom med dvema ali več državami ali na podlagi takega sporazuma.

Tabela X: Ocena učinkov v zvezi z varstvom osebnih podatkov

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
1. Ali predpis predvideva nove ali spremenjene obdelave osebnih podatkov?	1.1. Ali se bo vzpostavil nov register, evidenca, razvid ali druga zbirka osebnih podatkov?	Poseben premislek mora biti opravljen pri uvajanju novih centraliziranih zbirk osebnih podatkov, pri informatizaciji obstoječih centraliziranih nacionalnih zbirk osebnih podatkov in uvedbi novih načinov zbiranja ali pridobivanja osebnih podatkov od posameznikov ali iz drugih nacionalnih zbirk preko različnih spletnih obrazcev, glede novega povezovanja zbirk osebnih podatkov in na specifičnih področjih (npr. nova policijska pooblastila in pristojnosti organov kazenskega pregona, množičnem zbiranju in posredovanju osebnih podatkov različnih subjektov kot npr. na področju preprečevanja pranja denarja in financiranja terorizma). Cilji in nameni morajo biti natančno definirani upoštevajoč načelo sorazmernosti.
	1.2. Ali je določanje novih obdelav osebnih podatkov ustrezno utemeljeno?	Iz obrazložitve predlaganih ukrepov in rešitev mora izhajati: - ocena stanja na področju urejanja, - utemeljitev potrebe po zbiranju osebnih podatkov oz. določenem načinu obdelave, - obrazložitev, kako točno naj bi predvidena oblika obdelave osebnih podatkov zadovoljila te potrebe, - obrazložitev, kako je bilo upoštevano načelo sorazmernosti pri opredelitvi nabora podatkovin zakaj ciljev zbiranja ni mogoče doseči z blažjimi posegi v pravice posameznikov (npr. z obdelavo anonimiziranih podatkov).
	1.3. Ali je bila izvedena primerjava z ureditvami v tujini?	Pri pravno-primerjalni analizi rešitev je ključno, da se iz tuje prakse prenesejo ne le ideje o tem, kaj vse je mogoče, ampak tudi že izoblikovane in utemeljene pravne omejitve ter dejanske izkušnje pri uporabi določene tehnologije, rešitev oziroma ukrepov. Pri tem je bistvenega pomena, da se pridobijo tudi informacije o morebitnih negativnih učinkih uporabe določenih tehnologij ali oblik zbiranja in obdelave osebnih podatkov ter načinih naslavljanja teh učinkov.
2. Ali je podan sistematičen opis obdelave?	2.1. Ali so upoštevani narava, obseg, okoliščine in nameni obdelave?	Pri snovanju predpisa je treba upoštevati naravo, obseg, okoliščine in namene obdelave, zlasti ko so možna velika tveganje za pravice in svoboščine posameznikov. Take vrste dejanj obdelave so lahko tiste, ki zlasti vključujejo uporabo novih tehnologij, predvidevajo množično obdelavo in/ali obdelavo posebnih vrst osebnih podatkov. Pri pripravi zakonske ureditve mora biti jasno opredeljen celoten podatkovni tok obdelave v vseh stopnjah od postopka zbiranja, vseh faz obdelave, tudi morebitne nadaljnje obdelave ter hrambe in vseh namenov obdelave v različnih

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
		fazah.
	2.2. Ali je opredeljen nabor podatkov, upravljavci in uporabniki ter roki hrambe?	Predpis mora natančno določati upravljavce ali skupne upravljavce osebnih podatkov (slednje glej 26. člen Splošne uredbe), kolikor je mogoče izčrpno nabor osebnih podatkov, uporabnike, ki se jim posredujejo osebni podatki ter roke hrambe. Jasno morajo biti opredeljene različne vloge posameznih deležnikov, ki so vključeni v postopke zbiranja in obdelave, zlasti v primeru skupnega upravljanja. Morebitno povezovanje zbirk osebnih podatkov mora opredeljevati zbirke, ki se povezujejo, uporabljen povezovalni znak in namene povezovanja.
	2.3. Ali je podan opis podatkovnih tokov in udeleženih subjektov?	Iz obrazložitve predpisa in kot je ustrezno v samih določbah predpisa mora jasno izhajati, kako se bodo osebni podatki zbirali, kdo jih bo zbiral in komu bodo posredovani ter pod kakšnimi pogoji in na kakšne načine, kje in kako se bodo hranili. Kjer je ustrezno morajo biti opredeljeni načini zbiranja (na papirju, prek spleta…), morebitne zahteve glede avtentikacije posameznikov (npr. brez, s predložitvijo osebnega dokumenta, z digitalnimi certifikati) ter dostopa do podatkov.
	2.4. Ali je podan osnoven opis sredstev obdelave (strojne in programske opreme, omrežij, človeških virov in uporabljenih komunikacijskih sredstev)?	Podrobne tehnično-izvedbene podrobnosti postopka obdelave sicer ne sodijo v samo zakonsko besedilo. Izkušnje pa kažejo, da je treba zaradi vsebinskih in obsežnih finančnih posledic različnih tehničnih rešitev že v fazi snovanja predpisa poznati osnovne tehnične okvire sredstev obdelave. Zlasti se v praksi odsotnost tega razmisleka pri pripravi predpisov kaže v neustrezni opredelitvi namenov obdelave, vlog posameznih upravljavcev/skupnih upravljavcev ter nabora osebnih podatkov. Zato IP priporoča osnovni razmislek o tem ter vključitev IT strokovnjakov kot obvezni sestavni del snovanja predpisa.

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
3. Ali so bila upoštevana vsa temeljna načela varstva osebnih podatkov?	3.1. Ali je upoštevano načelo zakonitosti, poštenosti in preglednosti obdelave (člen 5(1a))? Ali je natančno in pravilno opredeljena pravna podlaga za obdelavo osebnih podatkov (člen 6)?	V zakonu naj bi bili opredeljeni splošni pogoji iz Splošne uredbe, ki urejajo zakonitost obdelave osebnih podatkov, določena natančnejša pravila za določitev upravljavca, vrst osebnih podatkov, ki se obdelujejo, zadevnih posameznikov, na katere se nanašajo osebni podatki, subjektov, katerim se osebni podatki lahko razkrijejo, omejitve namena, roka hranjenja in drugih ukrepov za zagotovitev zakonite in poštene obdelave. Prav tako je naloga prava držav članic, da določi, ali upravljavec nalogo izvaja v javnem interesu ali pri izvajanju javne oblasti, ali gre za javni organ ali drugo fizično ali pravno osebo, za katero velja javno pravo, ali, kadar to upravičuje javni interes. Obdelava osebnih podatkov mora potekati na eni izmed pravnih podlag, ki jih določata 6. oz. v primeru zbiranja posebnih vrst osebnih podatkov 9. člen Splošne uredbe, pri tem je treba upoštevati, da niso vse pravne podlage primerne v vseh primerih (privolitev npr. samo v situacijah, kjer je odločitev posameznika resnično popolnoma prostovoljna; upoštevati je treba pogoje za veljavnost privolitve). Privolitev se ne bi smela šteti za prostovoljno, če posameznik nima možnosti dejanske ali prostovoljne izbire ali privolitve ne more zavrniti ali preklicati brez škode. To je zlasti pomembno v primeru zbiranja osebnih podatkov v okviru delovnih razmerij in pri zbiranju osebnih podatkov s strani javnega sektorja za javne in druge oblastne naloge. Načini zbiranja, uporabe, pregledovanja ali drug način obdelave ter obseg obdelave ali prihodnje obdelave osebnih podatkov bi morali za posameznike biti pregledni. Načelo preglednosti zahteva, da so vse informacije in sporočila, ki se nanašajo na obdelavo teh osebnih podatkov, lahko dostopni in razumljivi ter izraženi v jasnem in preprostem jeziku. To načelo zadeva zlasti informacije za posameznike o istovetnosti upravljavca in namenih obdelave ter dodatne informacije za zagotovitev poštene in pregledne obdelave glede zadevnih posameznikov in njihove pravice do pridobitve potrditve in sporočila o obdelavi osebnih podatkov v zvezi z njimi. Posameznike bi bilo treba opozoriti na tveganja, pravila, zaščitne ukrepe in pravice v zvezi z obdelavo njihovih osebnih podatkov ter na to, kako lahko uresničujejo njihove pravice v zvezi s tako obdelavo.

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
	3.2. Ali je upoštevano načelo določenosti, izrecnosti in zakonitosti namenov (člen 5(1b))?	Nameni obdelave morajo biti zakonu jasno in natančno opredeljeni. Zlasti posebni nameni, za katere se osebni podatki obdelujejo, bi morali biti izrecni in zakoniti ter določeni v času zbiranja osebnih podatkov. Nameni zbiranja morajo biti sorazmerni s cilji obdelave, pri čemer mora biti upoštevano, da se ne zbira osebnih podatkov, če je cilje možno doseči brez zbiranja osebnih podatkov. Analizirati je treba tveganja v povezavi z možnostjo uporabe podatkov v druge namene (t.i. function creep) – večje kot so zbirke podatkov in bolj kot vsebujejo zanimive podatke (npr. finančni podatki, komunikacijski podatki, zdravstveni podatki) večje so nevarnosti, da bi se lahko kdaj kasneje podatke uporabilo za druge namene, še posebej če je to tehnično izvedljivo. Zato je treba predvideti ustrezne varovalke, kot npr. izrecne zakonske prepovedi, sorazmerno kratke roke hrambe, omejenost dostopov na nujno potrebne in druge omejitve ter tehnične ukrepe za preprečevanje uporabe v druge namene.
	3.3. Ali je upoštevano načelo, da bo obdelava ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki (člen 5(1c))?	Zbirati in drugače obdelovati se smejo samo tisti osebni podatki, ki so nujni za doseganje vnaprej opredeljenih zakonitih namenov. Kolikor je cilje mogoče doseči brez obdelave osebnih podatkov (npr. z anonimnimi podatki), je treba predvideti takšno rešitev. Posebej je treba biti pri tem pozoren na razlikovanje med psevdonimiziranimi podatki, ki so še vedno v celoti varovani osebni podatki (četudi to morda na prvi pogled ni videti tako), in anonimnimi podatki. Poleg samega obsega podatkov se sorazmernost nanaša tudi na uporabo manj občutljivih podatkov od tistih, katerih narava oziroma zloraba ima večjo težo (psevdonimi so boljši kot navadni podatki, govoreče šifre so slabše od naključnih nizov ipd.). Upošteva se pravilo, da se zbira osebne podatke tistih oseb, od katerih so potrebni, takrat, ko so potrebni in v obsegu, ki je potreben in ne obratno – nesorazmerno bi bilo zbiranje vseh podatkov, vseh oseb, vnaprej in na zalogo.
	3.4. Ali je upoštevano načelo točnosti in ažurnosti (člen 5(1d))?	Analizirati je treba tveganja, da bo bodo zbrani oz. obdelovani podatki netočni, pomanjkljivi, nepopolni, napačni, zastareli. Do napak pogosto prihaja pri prepisovanju in pretipkavanju podatkov, ko so dolžnosti upravljavca razdeljene med več institucij. V primeru skupnih upravljavcev je treba določiti, kdo je odgovoren za zagotavljanje točnosti in ažurnosti podatkov in kdo lahko izvaja popravke v primeru ugotovljenih nepravilnosti. Premisliti je treba o možnih ukrepih in kontrolnih mehanizmih ter postopkih za zagotovitev točnosti podatkov (npr. logične kontrole pri vnosu podatkov, kot so EMŠO ali davčna številka), sistem štirih oči, kjer je ustrezno ipd.).

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
	3.5. Ali je upoštevano načelo omejitve shranjevanja – določenost rokov hrambe (člen 5(1e))?	Gre za sorazmernost s časovnega vidika – kateri je najkrajši možni rok, ki omogoča doseganje zastavljenih ciljev. Roki hrambe morajo biti opredeljeni dovolj določno (ne npr. „dokler je to potrebno“ ali „trajno“ – če to ni posebej utemeljeno in izjemoma). Ko natančnega roka ni mogoče določiti, se opredeli kriterije, ki na to vplivajo (npr. do preklica privolitve, x let po prenehanju obveznosti ipd.). Po dosegu namena oziroma po preteku zakonsko ali drugače določenega roka je treba osebne podatke izbrisati, uničiti ali anonimizirati. Iz zakona mora jasno izhajati kdo od morebitnih skupnih upravljavcev je pristojen za izbris. Prav tako je treba že v fazi snovanja predpisa razmisliti, kako bo upravljavec dobil podatke, ki mu bodo omogočali odločiti o izbrisu, če s temi podatki ne razpolaga sam upravljavec.
	3.6. Ali je upoštevano načelo celovitosti, zaupnosti in razpoložljivosti podatkov (člen 5(1f))?	Obdelava osebnih podatkov mora potekati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo in sicer z ustreznimi tehničnimi ali organizacijskimi ukrepi. Več pojasnil o zahtevah z vidika informacijske varnosti je na voljo v smernicah IP, smiselno je uporabiti tudi priporočila mednarodnih standardov informacijske varnosti (npr. ISO/IEC 27001). Ključni varnostni ukrepi in morebitna delitev odgovornosti zanje med skupnimi upravljavci bi morali biti opredeljeni v predpisu, podrobnosti pa lahko določajo podzakonski akti.
4. Ali so bile upoštevane pravice posameznika?	4.1. Ali je bila upoštevana dolžnost informiranja posameznika o obdelavi podatkov (12., 13. in 14. člen Splošne uredbe in 23. člen ZVOPOKD)?	Upravljavci osebnih podatkov morajo posameznike informirati o obdelavi osebnih podatkov. Splošna uredba o varstvu podatkov v 13. in 14. členu tako določa, katere so informacije, ki jih mora upravljavec zagotoviti posameznikom, odvisno od tega, ali so bili osebni podatki pridobljeni s strani posameznika ali iz drugega vira. Informacije morajo biti podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. V primeru skupnega upravljavstva je treba določiti, kdo je odgovoren za podajo teh informacij. Tehnično izvedbene podrobnosti in obrazce za podajo informacij, pa naj določajo podzakonski akti. Prav tako mora v primeru omejitev pravic posameznika po 23. členu Splošne uredbe oz. 14., 20. in 25. člena ZVOPOKD takšne omejitve določati zakon.
	4.2. Ali je bila upoštevana pravica do seznanitve in prenosljivosti podatkov (15. in 20. člen Splošne uredbe in 24. člen ZVOPOKD)?	Oceniti je treba, ali je zadevna pravica relevantna v konkretnem primeru, ali je dejansko potrebna kakšna specifična ureditev ali natančnejša opredelitev postopka uresničevanja pravice, udeleženih subjektov, časovnih okvirov. Pravice posameznika že opredeljuje Splošna uredba in ZVOPOKD. Načeloma zato ni potrebe po posebnem dodatnem urejanju v področnih predpisih (nevarnost nesistemskih rešitev,

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
		omejitev zaračunavanja stroškov), po drugi strani je lahko pomembno v primeru delitve nalog upravljavcev (npr. en organ vnaša in popravlja, drug organ odgovoren za ostale naloge upravljavca) z vidika preglednosti in jasne razmejitve odgovornosti. Prav tako mora tudi v primeru omejitev pravic posameznika po 23. členu Splošne uredbe oz. 14., 20. in 25. člena ZVOPOKD takšne omejitve določati zakon.
	4.3. Ali je bila upoštevana pravica do popravka in izbrisa podatkov (16., 17. in 19. člen Splošne uredbe in 26. člen ZVOPOKD)?	Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave, pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave.
	4.4. Ali je bila upoštevana pravica do ugovora in omejitve obdelave (18., 19. in 21. člen Splošne uredbe in 26. člen ZVOPOKD)?	Oceniti je treba, ali je zadevna pravica relevantna v konkretnem primeru, ali je dejansko potrebna kakšna specifična ureditev ali natančnejša opredelitev postopka uresničevanja pravice, udeleženih subjektov, časovnih okvirov. Načeloma ni potrebe po posebnem dodatnem urejanju v področnih predpisih (nevarnost nesistemskih rešitev, omejitev zaračunavanja stroškov), po drugi strani je lahko pomembno v primeru delitve nalog upravljavcev (npr. en organ vnaša in popravlja, drug organ odgovoren za ostale naloge upravljavca) z vidika preglednosti in jasne razmejitve odgovornosti.

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
	4.5. Ali so predvidene kakršne koli omejitve pravic posameznika?	Pravice posameznika se lahko v primeru obdelav zavezancev po Splošni uredbi omejijo le z zakonom, in sicer če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje (23. člen Splošne uredbe): (a) državne varnosti; (b) obrambe; (c) javne varnosti; (d) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem; (e) drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo; (f) varstva neodvisnosti sodstva in sodnega postopka; (g) preprečevanja, preiskovanja, odkrivanja in pregona kršitev etike v zakonsko urejenih poklicih; (h) spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti v primerih iz točk (a) do (e) in (g); (i) varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih; (j) uveljavljanja civilnopravnih zahtevkov. Vsak zakonodajni ukrep, ki določa omejitev pravic posameznika mora vsebovati posebne določbe vsaj, kjer je ustrezno, glede: (a) namenov obdelave ali vrst obdelave; (b) vrst osebnih podatkov; (c) obsega uvedenih omejitev; (d) zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa; (e) natančnejše ureditve upravljavca ali vrst upravljavcev; (f) obdobij hrambe in veljavnih zaščitnih ukrepov, pri čemer se upoštevajo narava, obseg in nameni obdelave ali vrste obdelave. (g) tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter (h) pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve. Določene omejitve pravic posameznikov v primeru obdelav po ZVOPOKD opredeljuje že sam ZVOPOKD (14., 20. In 25. člen ZVOPOKD). Za druge primere 25. člen ZVOPOKD določa, da se lahko pravica posameznika do dostopa do lastnih osebnih

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
		podatkov ob upoštevanju njegovih človekovih pravic in temeljnih svoboščin ter zakonitih interesov z zakonom delno ali popolnoma omeji glede posameznih obdelav ali posameznih kategorij obdelav, če in dokler je to nujno in sorazmerno: 1. da se onemogoči oviranje ali vplivanje na uradne postopke, katerih nameni so določeni v prvem odstavku 1. člena tega zakona; 2. da se onemogoči oviranje ali vplivanje na druge uradne postopke, povezane s prejšnjo točko; 3. zaradi zagotavljanja javne varnosti; 4. zaradi zagotavljanja varnosti države ali obrambe države; 5. zaradi varstva ali uresničevanja človekovih pravic in temeljnih svoboščin tretjih oseb.
5. Ali so obvladovana tveganja za pravice in svoboščine posameznika?	5.1. Ali je podana ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84 Splošne uredbe)?	Vprašati se je treba, kaj gre lahko narobe pri pripravi predpisa? Identifikacija tveganj je bistvenega pomena – tveganja, ki jih predlagatelj ob pripravi predloga predpisa morebiti ne bi identificiral, utegnejo kasneje izpostaviti splošna in/ali strokovna javnost oziroma sodna presoja. Rezultat nepravočasno ali nepopolno identificiranih in naslovljenih tveganj je lahko odpor strokovne in splošne javnosti – in to kljub temu, da bi bil ob ustrezni analizi tveganj ukrep sicer povsem sprejemljiv. V interesu predlagatelja je zato, da vsa tveganja pravočasno identificira in obravnava. Tveganja je priporočljivo ovrednotiti po temeljnih načelih varstva osebnih podatkov (zakonitost, sorazmernost, namenskost…). Primeri tveganj so na voljo v smernicah IP o ocenah učinka.
	5.2. Ali so upoštevani možni učinki na pravice posameznika v primeru nezakonitega dostopa, spremembe ali izgube podatkov (uvodna določba 84 Splošne uredbe)?	Kršitev varnosti osebnih podatkov lahko, če se ne obravnava ustrezno in pravočasno, zadevnim posameznikom povzroči fizično, premoženjsko ali nepremoženjsko škodo, kot je izguba nadzora nad njihovimi osebnimi podatki ali omejitev njihovih pravic, diskriminacija, kraja ali zloraba identitete, finančna izguba, neodobrena reverzija psevdonimizacije, okrnitev ugleda, izguba zaupnosti osebnih podatkov, zaščitenih s poklicno skrivnostjo, ali katera koli druga znatna gospodarska ali socialna škoda.
	5.3. Ali sta ocenjeni verjetnost in resnost tveganj (uvodna določba 90 Splošne uredbe)?	Splošne uredba ne predpisuje uporabe določene metodologije za ocenjevanje tveganj in upravljavcem pušča določeno mero fleksibilnosti glede izbire in uporabe metodologije. Skupna raven tveganja predstavlja kombinacijo verjetnosti, da se bo tveganje uresničilo, in resnosti oziroma teže posledic, ki jih bo imela uresničitev tveganja. Metodologija za ocenjevanje tveganja se običajno opira na tabele oz. matrike (najpogosteje 2x2, 3x3 ali 5x5), ki omogočajo izračun in prikaz skupne ravni tveganja.

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
	5.4. Ali so opredeljeni ukrepi za obvladovanje tveganj (točka d 7. odstavka 35. člena Splošne uredbe in uvodna določba 90 Splošne uredbe)?	Pri pripravi predpisa je treba opraviti premislek o možnih ukrepih za obvladovanje tveganj - identificirana tveganja se upravlja z ustreznimi varovalkami (kavtelami), npr. s sodno avtorizacijo, anonimizacijo, depersonalizacijo, višji dokazni standard, minimizacijski postopki, kratki roki hrambe, zapisniki, z različnimi kontrolnimi mehanizmi (logične in fizične kontrole pri vnosu podatkov), z organizacijskimi in tehničnimi ukrepi za varnost podatkov itd. Primeri ukrepov so na voljo v smernicah IP o ocenah učinka.
6. Ali so bile v pripravo predpisa vključene zainteresirane strani?	6.1. Ali je bilo pridobljeno mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov?	Po določbi 37. člena Splošne uredbe morajo javni organ ali telesa, razen sodišč, kadar delujejo kot sodni organ, imenovati pooblaščeno osebo za varstvo osebnih podatkov (DPO), katere naloga je med drugim svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja (točka c prvega odstavka 39. člena Splošne uredbe). Podobno ureja obvezno imenovanje pooblaščene osebe za varstvo osebnih podatkov 55. člen ZVOPOKD.
	6.2. Ali so bila pridobljena mnenja posameznikov oziroma predstavnikov posameznikov, kjer je to primerno (9. odstavek 35. člena Splošne uredbe)?	Mnenje posameznikov, na katere se nanašajo osebni podatki, ali njihovih predstavnikov je mogoče pridobiti 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). Zlasti pomembno je pri tem ustrezno posvetovanje z nevladnimi organizacijami in strokovnimi javnostmi. Če se končna odločitev pripravljavca predpisa razlikuje od mnenja posameznikov, bi moral pripravljavec dokumentirati razloge za nadaljevanje ali nenadaljevanje postopka oziroma dokumentirati svojo utemeljitev, zakaj posameznikov, ni prosil za mnenje, če se odloči, da to ni potrebno, npr. če bi bilo to nesorazmerno ali neizvedljivo.
7. Ali je bil izveden zaključni test sorazmernosti?	7.1. Ali je ukrep nujen za dosego (ustavno dopustnega) zadanega cilja? Ali je zakonska dikcija jasna in nedvoumna ter je obdelava določena z zakonom?	Posegi v človekove pravice ali temeljne svoboščine so po ustaljeni ustavnosodni presoji dopustni, če so v skladu z načelom sorazmernosti. Na podlagi vseh zbranih informacij se izvede strogi test sorazmernosti, kot ga že poznamo v naši ustavnosodni praksi. Poseg v pravico do zasebnosti, ki ga prinaša vsako zbiranje in obdelava osebnih podatkov mora biti primeren, nujen in sorazmeren v ožjem smislu v demokratični družbi. Šele na podlagi uspešno prestanega testa sorazmernosti velja pripraviti zakonsko

VPRAŠANJA	PODVPRAŠANJA	POJASNILA
		besedilo predlaganega ukrepa, da bo ukrep učinkovit, zakonit, uporabljiv pred sodišči, ter sprejet s strani javnosti. Pri opredelitvi obdelav osebnih podatkov je treba upoštevati omejitve 38. člena Ustave, iz katerega med drugim izhaja, da mora zakon (in ne podzakonski akt) jasno in nedvoumno opredeliti namen zbiranja in obdelave ter nabor osebnih podatkov, ki naj bodo predmet zbiranja in obdelave. To je ob presoji skladnosti ukrepov v zvezi z omejevanjem epidemije nedavno ponovno potrdilo tudi Ustavno sodišče.
	7.2. Ali je ukrep primeren za dosego zadanega cilja?	Če ukrep ni primeren, gre iskati drug primernejši ukrep. Pretehtati je treba npr. ali je resnično potrebno ustvariti novo centralno zbirko podatkov, ali je povezava določenih osebnih podatkov iz posameznih zbirk res potrebna in primerna zaradi izvrševanja javnega interesa, ali so predvidene določbe res jasne ter natančne ipd.
	7.3. Ali je ukrep učinkovit v doseganju zadanega cilja?	Preveriti je treba, ali bomo s predvidenimi ukrepi dejansko dosegli zasledovane cilje. Primer: zakonodaja o obveznih hrambi podatkov v prometu elektronskih komunikacij (t.i. data retention), po kateri so se beležili prometni podatki o vseh opravljenih klici in poslana sms sporočila za namen boja proti terorizmu, je bila razveljavljena, saj se je izkazalo, da praktično ni bila učinkovita.
	7.4. Ali je ukrep sorazmeren glede na zadani cilj (ali morda preveč posega v pravice posameznikov)?	Nesorazmerni ukrepi lahko padejo na ustavnodsodnem testu sorazmernosti. Primer: zakonodaja o obveznih hrambi podatkov v prometu elektronskih komunikacij (t.i. data retention), po kateri so se beležili prometni podatki o vseh opravljenih klicih in poslana sms sporočila za namen boja proti terorizmu, je bila nesorazmerna – vnaprej so se hranili podatkih o klicih vseh oseb za obdobje do 24 mesecev. Ukrep je posegel v pravice vsakega posameznika, pri čemer velika večina ni imela nobene povezave s terorizmom ali hujšimi kaznivimi dejanji. Velike baze podatkov na zalogo so pomenile visoke stroške za operaterje in prinesle obsežna tveganja za zlorabe. Ukrep ni bil omejen na hujša kazniva dejanja.

S spoštovanjem,

Mojca Prelesnik, univ. dipl. prav.,
informacijska pooblaščenka

Pripravila:
Alenka Jerše, univ. dipl. prav.,
namestnica informacijske pooblaščenke

mag. Andrej Tomšič,
namestnik informacijske pooblaščenke