



**Skupno mnenje EOVP in ENVP
03/2022 o predlogu
uredbe o
evropskem zdravstvenem podatkovnem prostoru**

Sprejeto 12. julija 2022

KAZALO

1	Ozadje	5
2	Področje uporabe mnenja	5
3	Ocena	6
3.1	Splošne pripombe	6
3.2	Medsebojni vpliv predloga in zakonodaje EU o varstvu podatkov	7
3.3	Medsebojni vpliv predloga ter akta o upravljanju podatkov, akta o podatkih in akta o umetni inteligenci	10
4	Splošne določbe (poglavje I).....	10
4.1	Člen 1: Predmet urejanja in področje uporabe predloga	11
4.2	Člen 2: Opredelitve pojmov	12
5	Primarna uporaba elektronskih zdravstvenih podatkov (poglavje II)	14
6	Sistemi za vodenje elektronskih zdravstvenih zapisov in aplikacije za dobro počutje (poglavje III) 19	
7	Sekundarna uporaba elektronskih zdravstvenih podatkov (poglavje IV).....	22
8	Dodatni ukrepi (poglavje V).....	25
8.1	Shranjevanje osebnih elektronskih zdravstvenih podatkov v EU in skladnost mednarodnih prenosov podatkov s poglavjem V Splošne uredbe o varstvu podatkov.....	26
8.2	Javno naročanje in financiranje Unije	29
8.3	Nacionalne kontaktne točke tretje države ali sistemi, vzpostavljeni na mednarodni ravni.	29
9	Evropsko upravljanje in usklajevanje (poglavje VI).....	30
10	Prenos pooblastila in postopek v odboru (poglavje VII)	31
11	Razno (poglavje VIII).....	32

Povzetek

Namen EOVP in ENVP s tem skupnim mnenjem je usmeriti pozornost na več splošnih pomislekov glede predloga o evropskem zdravstvenem podatkovnem prostoru ter pozvati zakonodajalca k odločnemu ukrepanju.

EOVP in ENVP ugotavljata, da je namen predloga podpreti posameznike pri prevzemanju nadzora nad svojimi zdravstvenimi podatki, podpreti uporabo zdravstvenih podatkov za boljše zagotavljanje zdravstvenega varstva, boljše raziskave, inovacije in oblikovanje politik ter omogočiti EU, da v celoti izrabi potencial varne in zanesljive izmenjave, uporabe in ponovne uporabe zdravstvenih podatkov. Dejansko bi lahko „olajšanje uporabe elektronskih zdravstvenih podatkov“, in to primarne ter sekundarne uporabe, pomembno pripomoglo k javnim interesom ter interesom posameznikov, na katere se nanašajo osebni podatki, oziroma posameznih pacientov.

Čeprav so prizadevanja za okrepitev nadzora, ki ga imajo posamezniki, na katere se nanašajo osebni podatki, nad svojimi osebnimi zdravstvenimi podatki, ter njihovih pravic dobrodošla, je treba poudariti, da ta predlog določa predvsem nekatere „dodatke“ k nekaterim pravicam posameznikov, na katere se nanašajo osebni podatki, ki so že določene v Splošni uredbi o varstvu podatkov. Dejansko bi lahko predlog celo zmanjšal varstvo pravic do zasebnosti in varstva podatkov, predvsem glede na kategorije osebnih podatkov in namene, ki so povezani s sekundarno uporabo podatkov.

EOVP in ENVP ugotavljata, da bodo določbe iz tega predloga dodale še eno plast k že tako kompleksni (večplastni) zbirki določb (iz zakonodaje EU in držav članic) o obdelavi zdravstvenih podatkov (v zdravstvenem sektorju). Medsebojni vpliv teh različnih zakonodajnih aktov mora biti (popolnoma) jasen.

EOVP in ENVP menita, da je zlasti pomembno pojasniti razmerje med določbami iz tega predloga ter določbami iz Splošne uredbe o varstvu podatkov in zakonov držav članic. EOVP in ENVP ugotavljata namero in prizadevanja, da bi se s tem predlogom o evropskem zdravstvenem podatkovnem prostoru upoštevali okviri Splošne uredbe o varstvu podatkov. To izhaja na primer iz dela, v katerem se na podlagi prava Unije vzpostavi pravna podlaga in/ali izjema za obdelavo zdravstvenih podatkov na podlagi prava Unije, ki ustreza strukturi Splošne uredbe o varstvu podatkov, predvideni v njenih členih 6 in 9. Potrebne pa bo še veliko dela (v smislu izboljšanja določb in dodatnih pojasnil), da bo dosežena želena jasnost navedenih določb, zlasti glede medsebojnega vpliva določb in predpisov držav članic na podlagi člena 9(4) Splošne uredbe o varstvu podatkov. Ti pomisleki so izraženi v pripombah glede poglavij II in IV predloga.

Glede področja uporabe predloga EOVP in ENVP priporočata, da se iz člena 33(1), točka (f), predloga izključijo aplikacije za dobro počutje in druge digitalne aplikacije ter podatki v zvezi z dobrim počutjem in vedenjem, pomembni za zdravje. Če bi se ti podatki ohranili, bi bilo treba za obdelavo za sekundarno uporabo osebnih podatkov, pridobljenih iz aplikacij za dobro počutje in drugih digitalnih aplikacij, zahtevati predhodno privolitev v smislu Splošne uredbe o varstvu podatkov. Poleg tega EOVP in ENVP opozarjata, da bi lahko taka obdelava spadala na področje uporabe Direktive 2002/58/ES (direktiva o zasebnosti in elektronskih komunikacijah).

EOVP in ENVP močno priporočata tudi, da se opusti razširitev področja uporabe izjem v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki, iz Splošne uredbe o varstvu podatkov na predlog in zlasti člen 38(2) predloga. Taka izjema ne krepi možnosti posameznikov, na katere se nanašajo osebni podatki, da izvajajo učinkovit nadzor nad svojimi osebnimi podatki, ampak jo zmanjšuje, zato se zdi, da je v nasprotju s ciljem iz člena 1(2), točka (a), predloga.

EOVP in ENVP pozdravljata dejstvo, da predlog vsebuje sklice na pravice iz Splošne uredbe o varstvu podatkov (na primer na pravico do brezplačnega dostopa in pravico do pridobitve kopije podatkov). Vendar ugotavljata, da opis pravic iz predloga ni skladen z opisom iz Splošne uredbe o varstvu podatkov. Kot je navedeno zgoraj, lahko to povzroči pravno negotovost pri posameznikih, na katere se nanašajo osebni podatki in ki morda ne morejo razlikovati med tema vrstama pravic. Zato in za preprečitev kompleksnosti praktičnega izvajanja EOVP in ENVP so zakonodajalca pozivata, naj zagotovita pravno jasnost glede medsebojnega vpliva pravic posameznikov, na katere se nanašajo osebni podatki, uvedenih s predlogom, in splošnih določb o pravicah navedenih posameznikov iz Splošne uredbe o varstvu podatkov.

EOVP in ENVP ugotavljata, da so določbe v poglavju III namenjene izboljšanju interoperabilnosti elektronskih zdravstvenih zapisov in olajšanju povezljivosti aplikacij za dobro počutje s takimi elektronskimi zdravstvenimi zapisi. Vendar menita, da te aplikacije ne bi smele biti vključene v sekundarno uporabo zdravstvenih podatkov na podlagi poglavja IV predloga. Prvič, za zdravstvene podatke, ki jih ustvarijo aplikacije za dobro počutje in druge digitalne zdravstvene aplikacije, ne veljajo iste zahteve glede kakovosti podatkov kot za podatke, ki jih ustvarijo medicinski pripomočki, niti nimajo enakih kakovostnih značilnosti. Poleg tega te aplikacije ustvarjajo ogromno podatkov in so lahko zelo vdorne, saj se podatki nanašajo na vsak korak posameznika v vsakdanjem življenju. Tudi če bi bilo mogoče ločiti zdravstvene podatke od drugih vrst podatkov, bi kljub temu bilo preprosto izpeljati sklepe, na primer o prehranjevalnih in drugih navadah, ki razkrivajo posebno občutljive informacije, kot je veroizpoved.

V zvezi z nameni sekundarne uporabe zdravstvenih podatkov, navedenimi v členu 34(1) predloga, EOVP in ENVP menita, da lahko člen 34(1), točki (f) in (g), predloga vključuje vsako obliko „razvojn[ih] in inovacijsk[ih] dejavnosti za izdelke ali storitve, ki prispevajo k javnemu zdravju ali socialni varnosti“, ali „usposabljanj[a], preskušanj[a] in vrednotenj[a] algoritmov, vključno z medicinskimi pripomočki, umetnointeligenčnimi sistemi in digitalnimi zdravstvenimi aplikacijami, ki prispevajo k javnemu zdravju ali socialni varnosti“. Menita, da bi bilo treba te namene v predlogu podrobneje opredeliti in določiti, kdaj je povezava z javnim zdravjem in/ali socialno varnostjo zadostna. To bo ključno za zagotovitev ravnotežja med ustreznim upoštevanjem ciljev predloga in varstvom osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki jih obdelava zadeva.

Poleg tega člen 34(1) predloga vsebuje več vrst sekundarne uporabe, ki bi spadale v različne kategorije razlogov za izjemo, predvidene v členu 9(2) Splošne uredbe o varstvu podatkov. Vendar EOVP in ENVP menita, da to ni izraženo v merilih, po katerih bi morali organi za dostop do zdravstvenih podatkov oceniti vloge za dostop do podatkov in sprejeti odločitev o njih (člen 45 predloga), da bi izdali dovoljenje za obdelavo podatkov (člen 46 predloga). Zato EOVP in ENVP poudarjata, da so merila, določena v zvezi s tem v členu 46 predloga, omejena na določbe in načela tega predloga, pri čemer ni jasno, kako so take določbe povezane z načeli in določbami Splošne uredbe o varstvu podatkov, zlasti njenim členom 9(2).

EOVP in ENVP glede poglavja V ugotavljata, da infrastruktura za izmenjavo elektronskih zdravstvenih podatkov, predvidena v tem predlogu o evropskem zdravstvenem podatkovnem prostoru, nikakor ni namenjena vzpostavitvi centralne zbirke zdravstvenih podatkov EU (niti se taka zbirka podatkov ne bi mogla vzpostaviti na podlagi navedene infrastrukture), ampak bo zgolj olajšala izmenjavo takih zdravstvenih podatkov iz decentraliziranih podatkovnih zbirk. Vendar EOVP in ENVP zaradi velike količine podatkov, ki bi se obdelovali, njihove zelo občutljive narave, tveganja nezakonitega dostopa in potrebe po tem, da se v celoti zagotovi učinkovit nadzor nad temi podatki, pozivata k dopolnitvi tega predloga z določbo, po kateri bi bilo treba osebne elektronske zdravstvene podatke hraniti v EU/EGP, vendar brez poseganja v nadaljnje prenose v skladu s poglavjem V Splošne uredbe o varstvu podatkov.

Nazadnje, kar zadeva model upravljanja, ki se oblikuje s predlogom, bi bilo treba naloge in pristojnosti novih javnih organov skrbno prilagoditi, zlasti ob upoštevanju nalog in pristojnosti nacionalnih nadzornih organov, EOVP in ENVP na področju obdelave osebnih (zdravstvenih) podatkov. Preprečiti bi bilo treba prekrivanje pristojnosti ter podrobno določiti področja sodelovanja in zahteve glede tega.

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta –

ob upoštevanju člena 42(2) Uredbe 2018/1725 z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES,

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018,

SPREJELA NASLEDNJE SKUPNO MNENJE:

1 OZADJE

1. Predlog uredbe Evropskega parlamenta in Sveta o evropskem zdravstvenem podatkovnem prostoru (v nadaljevanju: predlog) bo pripomogel k uresničitvi vizije Komisije za digitalno preobrazbo EU do leta 2030¹.
2. Evropski odbor za varstvo podatkov (EOVP) in Evropski nadzornik za varstvo podatkov (ENVP) ugotavljata, da po navedbah Komisije predlog „podpira posameznike pri prevzemanju nadzora nad lastnimi zdravstvenimi podatki; podpira uporabo zdravstvenih podatkov za boljše zagotavljanje zdravstvenega varstva, boljše raziskave, inovacije in oblikovanje politik ter omogoča EU, da v celoti izkoristi potencial varne in zanesljive izmenjave, uporabe in ponovne uporabe zdravstvenih podatkov“².
3. Kot je pojasnjeno v obrazložitvenem memorandumu, je predlog v skladu z glavnimi cilji EU. Ti cilji vključujejo vzpostavitev močnejše evropske zdravstvene unije, izvajanje evropskega stebra socialnih pravic, izboljšanje delovanja notranjega trga, spodbujanje sinergij z agendo EU za digitalni notranji trg ter izvajanje ambiciozne agende za raziskave in inovacije. Poleg tega bo zagotovil pomemben sklop elementov, ki bodo pripomogli k oblikovanju evropske zdravstvene unije s spodbujanjem inovacij in raziskav ter boljšim obvladovanjem prihodnjih zdravstvenih kriz.

2 PODROČJE UPORABE MNENJA

4. Komisija je 3. maja 2022 objavila predlog uredbe Evropskega parlamenta in Sveta o evropskem zdravstvenem podatkovnem prostoru (v nadaljevanju: predlog).

¹ Obrazložitveni memorandum, stran 3.

² https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_sl

5. Komisija je 4. maja 2022 zaprosila za skupno mnenje EOVP in ENVP o predlogu (v nadaljevanju: mnenje) na podlagi člena 42(2) Uredbe (EU) 2018/1725³.
6. Predlog je zlasti pomemben za varstvo temeljnih pravic in svoboščin posameznikov pri obdelavi njihovih osebnih podatkov. Področje uporabe mnenja je omejeno na vidike predloga v zvezi z osebnimi podatki, ki so eden od glavnih stebrov predloga.
7. EOVP in ENVP pozdravljata obrazložiten memorandum predloga, v katerem je navedeno: „Glede na to, da so velika količina elektronskih podatkov, do katerih bo mogoče dostopati v evropskem zdravstvenem podatkovnem prostoru, osebni zdravstveni podatki, ki se nanašajo na fizične osebe v EU, je predlog oblikovan popolnoma v skladu s splošno uredbo o varstvu podatkov in Uredbo (EU) 2018/1725 (uredba EU o varstvu podatkov)“.
8. Podobno EOVP in ENVP poudarjata, da je treba zagotoviti in podpreti spoštovanje ter uporabo pravnega reda EU na področju varstva podatkov. Pri obravnavi osebnih podatkov v okviru predloga se je v pravnem besedilu predloga nujno treba jasno izogniti vsaki neusklajenosti in morebitnemu nasprotju s Splošno uredbo o varstvu podatkov⁴, direktivo o zasebnosti in elektronskih komunikacijah⁵ ter uredbo EU o varstvu podatkov. To ne velja zgolj zaradi pravne varnosti, ampak tudi za preprečitev, da bi predlog neposredno ali posredno ogrozil temeljni pravici do zasebnosti in varstva osebnih podatkov, kot sta določeni v členih 7 in 8 Listine Evropske unije o temeljnih pravicah ter členu 16 Pogodbe o delovanju Evropske unije.
9. Kot je podrobno pojasnjeno v mnenju, predlog vzbuja več pomislekov glede varstva temeljnih pravic do zasebnosti in varstva osebnih podatkov, zato namen tega mnenja ni zagotoviti izčrpnega seznama vseh vprašanj niti niso v vseh primerih navedeni alternativni predlogi besedila. Namen mnenja je obravnavati glavne kritične točke predloga v zvezi z zasebnostjo in varstvom podatkov.

3 OCENA

3.1 Splošne pripombe

10. EOVP in ENVP ugotavljata, da je cilj predloga razširiti uporabo elektronskih zdravstvenih podatkov za zagotavljanje zdravstvenega varstva posamezniku, od katerega so bili ti podatki zbrani (primarna uporaba), ter izboljšati raziskave, inovacije, oblikovanje politik, varnost pacientov, personalizirano medicino, uradne statistične podatke ali regulativne dejavnosti (sekundarna uporaba). Poleg tega ugotavljata, da je cilj predloga izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira za razvoj, trženje in uporabo sistemov za vodenje elektronskih zdravstvenih zapisov.

³ Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21. 11. 2018, str. 39).

⁴ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (UL L 119, 4. 5. 2016, str. 1).

⁵ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (UL L 201, 31. 7. 2002, str. 37).

11. Ne glede na to EOVP in ENVP poudarjata, da je varstvo osebnih podatkov sestavni element zaupanja, ki naj bi ga posamezniki in organizacije imeli v razvoj digitalnega gospodarstva⁶, ter dostopa do pravičnega zdravstvenega varstva, zlasti v zvezi z obdelavo zdravstvenih podatkov v okviru evropskega zdravstvenega podatkovnega prostora.
12. Glede tega EOVP in ENVP poudarjata, da bo uspeh evropskega zdravstvenega podatkovnega prostora odvisen od zanesljive pravne podlage za obdelavo v skladu z zakonodajo EU o varstvu podatkov, vzpostavitve zanesljivega mehanizma za upravljanje podatkov ter učinkovitih zaščitnih ukrepov za pravice in interese fizičnih oseb, ki morajo biti popolnoma skladni s Splošno uredbo o varstvu podatkov. Zagotoviti bi bilo treba zadostna jamstva za zakonito, odgovorno in etično upravljanje na podlagi vrednot EU, vključno s spoštovanjem temeljnih pravic. V zvezi s tem EOVP in ENVP menita, da bi moral biti evropski zdravstveni podatkovni prostor zgled za preglednost, učinkovito odgovornost in ustrezno ravnovesje med interesi posameznikov, na katere se nanašajo osebni podatki, in skupnimi interesi celotne družbe.
13. Poglavja v nadaljevanju tega mnenja vsebujejo priporočila EOVP in ENVP za zagotovitev skladnosti ustreznih določb predloga s pravnim okvirom EU za varstvo podatkov pa tudi s sedanjo razlago sodne prakse Sodišča Evropske unije, ki se uporablja. Glede na širok obseg pravic in obveznosti, določenih v predlogu, v zvezi z dostopom, uporabo in souporabo posebnih kategorij osebnih podatkov, kot so zdravstveni podatki, splošni sklici na Splošno uredbo o varstvu podatkov in uredbo EU o varstvu podatkov morda ne zadostujejo. Glede tega EOVP in ENVP menita, da lahko obstaja tveganje napačne razlage ključnih določb v zvezi z varstvom podatkov, to pa lahko povzroči znižanje ravni varstva, ki ga posameznikom, na katere se nanašajo osebni podatki, zdaj zagotavlja veljavni pravni okvir EU za varstvo podatkov (Splošna uredba o varstvu podatkov, uredba EU o varstvu podatkov ter direktiva o zasebnosti in elektronskih komunikacijah). Zato menita, da so potrebne dodatne specifikacije, kot je podrobno opisano v preostalem delu tega mnenja.
14. EOVP in ENVP pozdravljata, da je namen predloga tudi pripomoči tudi k zmanjšanju sedanje razdrobljenosti pravil, ki se uporabljajo za obdelavo zdravstvenih podatkov in znanstvene raziskave. Hkrati pa dvomita, da so nekatere določbe poglavij II in IV predloga (predvsem glede dostopa zdravstvenih delavcev do omejenih osebnih elektronskih zdravstvenih podatkov, sistematično registracijo ustreznih zdravstvenih podatkov, ki jo opravijo zdravstveni delavci, ali obravnavo nepričakovanih ugotovitev organov za dostop do zdravstvenih podatkov o fizičnih osebah) v celoti združljive z zakonodajo držav članic o sektorju e-zdravja brez splošne zakonodajne pristojnosti EU za usklajitev na tem področju. Glede tega bi bilo treba opozoriti, da v skladu s členom 168 Pogodbe o delovanju Evropske unije Unija spodbuja sodelovanje med državami članicami na področjih javnega zdravja ter po potrebi podpira njihove ukrepe z dopolnjevanjem nacionalne politike, ob upoštevanju odgovornosti držav članic za opredelitev svoje zdravstvene politike ter za organizacijo in zagotavljanje zdravstvenih storitev in zdravstvene oskrbe.

3.2 Medsebojni vpliv predloga in zakonodaje EU o varstvu podatkov

15. EOVP in ENVP pozdravljata uvodno izjavo 4 predloga, v skladu s katero „[z]a obdelavo osebnih elektronskih zdravstvenih podatkov veljajo določbe Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta, za institucije in organe Unije pa Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta.

⁶ Skupno mnenje o aktu o upravljanju podatkov.

Sklicevanja na določbe Uredbe (EU) 2016/679 bi bilo treba po potrebi razumeti tudi kot sklicevanja na ustrezne določbe Uredbe (EU) 2018/1725 za institucije in organe Unije.“

16. Poleg tega je v obrazložitvenem memorandumu navedeno, da predlog temelji na členih 16 in 114 Pogodbe o delovanju Evropske unije. Člen 114 Pogodbe o delovanju Evropske unije je namenjen izboljšanju delovanja notranjega trga z ukrepi za približevanje nacionalnih pravil, predlog pa je namenjen razširitvi uporabe elektronskih zdravstvenih podatkov ob sočasni krepitvi pravic, ki izhajajo iz člena 16 Pogodbe o delovanju Evropske unije.
17. Glede tega EOVP in ENVP poudarjata, da v skladu s sodno prakso Sodišča EU člen 16 Pogodbe o delovanju Evropske unije zagotavlja ustrezno pravno podlago, kadar je varstvo osebnih podatkov eden od bistvenih ciljev ali sestavnih delov pravil, ki jih je sprejel zakonodajalec EU⁷. Poleg tega opozarjata, da uporaba člena 16 Pogodbe o delovanju Evropske unije vključuje tudi potrebo po zagotavljanju neodvisnega nadzora nad skladnostjo z zahtevami glede obdelave osebnih podatkov, kot se zahteva tudi v skladu s členom 8 Listine Evropske unije o temeljnih pravicah⁸.
18. V zvezi s trditvijo o neodvisnem nadzoru EOVP in ENVP poudarjata, da bi morali biti nadzorni organi v skladu z uvodno izjavo 43 predloga zadolženi za izvajanje ustreznih določb Splošne uredbe o varstvu podatkov in uredbe EU o varstvu podatkov, zlasti v zvezi z obdelavo osebnih podatkov za sekundarno uporabo v okviru poglavja IV predloga. EOVP in ENVP glede tega priporočata, da se ustrezna določba vključi v operativni del besedila.
19. V zvezi z uporabo člena 16 Pogodbe o delovanju Evropske unije kot pravno podlago (eno od dveh⁹) predloga EOVP in ENVP ugotavljata, da je **cilj** predloga določiti „dodatne pravno zavezujoče določbe in zaščitne ukrepe“¹⁰ glede varstva zdravstvenih podatkov. Take določbe se uporabljajo poleg tistih iz Splošne uredbe o varstvu podatkov. Predlog določa „specifične zahteve in standarde“¹¹, ki so prilagojeni obdelavi elektronskih zdravstvenih podatkov in namenjeni uresničenju „možnost[i], ki jo Splošna uredba o varstvu podatkov omogoča za zakonodajo EU za številne namene“¹².
20. V zvezi z **vsebino** predloga sta EOVP in ENVP pripravila dve splošni pripombi.
21. Prvič, predlog vsebuje predvsem pravila o obdelavi osebnih (zdravstvenih) podatkov za primarno ali sekundarno uporabo. EOVP in ENVP se ob upoštevanju vpliva teh določb na splošno težišče predloga strinjata, da je zaradi vsebine predloga člen 16 Pogodbe o delovanju Evropske unije potrebna pravna podlaga. To pa ne vpliva na pripombe v tem mnenju o medsebojnem vplivu več določb predloga in določb iz Splošne uredbe o varstvu podatkov, zaradi katerega so nujna dodatna pojasnila, v nekaterih primerih pa tudi dodaten premislek in preoblikovanje, kot je predstavljeno v nadaljevanju tega mnenja.
22. EOVP in ENVP ugotavljata tudi, da je v skladu z uvodno izjavo 37 namen tega predloga določiti pravo Unije ob uporabi izjem iz člena 9(2), točke (g), (i) in (j), Splošne uredbe o varstvu podatkov. Poleg tega ugotavljata, da predlog za sekundarno uporabo zdravstvenih podatkov določa obveznost v smislu

⁷ Mnenje z dne 26. julija 2017, PNR Kanada, postopek za izdajo mnenja 1/15, ECLI:EU:C:2017:592, točka 96.

⁸ Skupno mnenje o aktu o umetni inteligenci.

⁹ ENVP in EOVP v skladu s svojima mandatoma v tem mnenju ne obravnavata vprašanja utemeljitve uporabe dvojne pravne podlage, ampak zgolj uporabo člena 16 Pogodbe o delovanju Evropske unije.

¹⁰ Obrazložiteni memorandum k predlogu, str. 7.

¹¹ Prav tam.

¹² Prav tam.

člena 6(1), točka (c), Splošne uredbe o varstvu podatkov, v skladu s katero morajo imetniki podatkov osebne podatke razkriti organom za dostop do zdravstvenih podatkov. Ob tem razumeta, da predlog ni namenjen vzpostavitvi pravne podlage za prosilce za dostop do podatkov v zvezi s členom 6 Splošne uredbe o varstvu podatkov, niti ni namenjen spremembi zahtev po informacijah na podlagi Splošne uredbe o varstvu podatkov ali direktive o zasebnosti in elektronskih komunikacijah ali spremembi katerih koli pravic iz navedene uredbe oziroma direktive.

23. Drugič, EOVP in ENVP ugotavljata, da predlog vsebuje vsaj eno izrecno odstopanje od določbe Splošne uredbe o varstvu podatkov: v skladu s členom 38(2) predloga namreč nekaterim subjektom (organom za dostop do zdravstvenih podatkov) ni treba uporabljati določb člena 14 Splošne uredbe o varstvu podatkov v zvezi z informacijami, ki jih je treba zagotoviti posameznikom, na katere se nanašajo osebni podatki. EOVP in ENVP menita, da taka izjema ne krepí možnosti posameznikov, na katere se nanašajo osebni podatki, da izvajajo učinkovit nadzor nad svojimi osebnimi podatki, ampak jo zmanjšuje, zato se zdi, da je v nasprotju s ciljem iz člena 1(2), točka (a), predloga. Poleg tega dvomita, da je uvedba omejitve pravice do obveščенosti potrebna in utemeljena, kot je podrobneje pojasnjeno v točkah 26, 34, 96 in 97 tega mnenja, tudi ob upoštevanju člena 23 Splošne uredbe o varstvu podatkov.
24. EOVP in ENVP na splošno odsvetujeta zakonodajo, ki določa odstopanja od nalog in pooblastil nadzornih organov za varstvo podatkov ter pravil Splošne uredbe o varstvu podatkov, ki se na splošno uporabljajo, v skladu s členom 8 Listine Evropske unije o temeljnih pravicah. Taka zakonodaja nujno vpliva na središčnost horizontalnih pravil, sprejetih na podlagi člena 16 Pogodbe o delovanju Evropske unije, končno pa jo lahko sčasoma tudi ogrozi. Neodvisni nadzorni organi bi morali biti zadolženi za nadzor nad predlogom v zvezi z obdelavo osebnih podatkov.
25. EOVP in ENVP vsekakor dvomita, da je omejitev pravice do obveščенosti v okviru tega potrebna in utemeljena. V skladu s členom 14(5), točki (b) in (c), Splošne uredbe o varstvu podatkov upravljavcem v nekaterih primerih dejansko ni treba upoštevati njenega člena 14, in sicer kadar (1) se izkaže, da je zagotavljanje takih informacij nemogoče ali bi vključevalo nesorazmeren napor, zlasti pri obdelavi v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene, pod pogoji in ob upoštevanju zaščitnih ukrepov iz člena 89(1) ali kolikor bi obveznost iz odstavka 1 tega člena lahko onemogočila ali resno ovirala uresničevanje namenov te obdelave¹³, ter (2) je pridobitev ali razkritje osebnih podatkov izrecno določeno s pravom Unije ali pravom države članice, ki velja za upravljavca in s katerim so določeni ustrezni ukrepi za zaščito zakonitih interesov posameznika, na katerega se nanašajo osebni podatki. Če predlog o evropskem zdravstvenem podatkovnem prostoru izrecno določa pridobitev ali razkritje osebnih podatkov, bi bilo treba oceniti, ali vsebuje ustrezne ukrepe za zaščito zakonitih interesov posameznikov, na katere se nanašajo osebni podatki.
26. Nazadnje, EOVP in ENVP ugotavljata, da predlog vključuje tudi aplikacije za dobro počutje in druge digitalne zdravstvene aplikacije, vendar direktiva o zasebnosti in elektronskih komunikacijah ni vključena v člen 1(4) predloga. EOVP in ENVP imata pomisleke glede vključitve takih aplikacij na področje uporabe poglavja IV predloga, kot je pojasnjeno v naslednjem poglavju; če bi se v predlogu ohranile, pa priporočata, da se vključi še sklic na direktivo o zasebnosti in elektronskih komunikacijah.

¹³ V takih primerih upravljavec sprejme ustrezne ukrepe za zaščito pravic in svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, tudi tako, da informacije objavi.

27. Poleg tega bi moral člen 1(4) predloga vsebovati tudi sklic na uredbo EU o varstvu podatkov, v predlogu pa bi bilo treba izrecno navesti ustrezne določbe navedene uredbe¹⁴. Zdi se, da so izrecni sklici na ustrezne člene uredbe EU o varstvu podatkov v normativnem delu predloga povsem utemeljeni, saj bo Komisija delovala kot obdelovalec elektronskih zdravstvenih podatkov, posredovanih prek platforme Moje zdravje @ EU (MyHealth@EU) (člen 12(7) predloga), institucije, organi, uradi in agencije Unije lahko imajo reden dostop do elektronskih zdravstvenih podatkov (uvodna izjava 41 predloga), podatki, ki jih hranijo institucije EU, pa se lahko dajo na voljo tudi za sekundarno uporabo (uvodna izjava 46 predloga).

3.3 Medsebojni vpliv predloga ter akta o upravljanju podatkov, akta o podatkih in akta o umetni inteligenci

28. EOVP in ENVP ugotavljata, da v skladu s členom 1(4) predloga „uredba ne posega v druge pravne akte Unije v zvezi z dostopom do elektronskih zdravstvenih podatkov, njihovo souporabo ali sekundarno uporabo ali zahtevami glede obdelave podatkov, povezanih z elektronskimi zdravstvenimi podatki, zlasti v uredbi (EU) 2016/679, (EU) 2018/1725, [...] [akt o upravljanju podatkov, COM(2020) 767 final] in [...] [akt o podatkih, COM(2022) 68 final]“. Poleg tega v skladu s členom 1(5) predloga „uredba ne posega v uredbi (EU) 2017/745 in [...] [akt o umetni inteligenci, COM(2021) 206 final] v zvezi z varnostjo medicinskih pripomočkov in umetno-inteligenčnih sistemov, ki vzajemno delujejo s sistemi za vodenje elektronskih zdravstvenih zapisov“.
29. EOVP in ENVP sicer pozdravljata izrecno navedbo, da predlog ne posega v akt o upravljanju podatkov, akt o podatkih in akt o umetni inteligenci, vendar menita, da bi bilo treba bolje obravnavati specifični medsebojni vpliv predloga ter navedenih pobud v okviru digitalnega svežnja in uredbe o medicinskih pripomočkih¹⁵. Na primer predlog v členu 2(2), točka (y), vsebuje opredelitev pojma „imetnik podatkov“, ki morda ni skladna z opredelitvijo tega pojma iz akta o upravljanju podatkov in akta o podatkih. To lahko povzroči pravne negotovost glede tega, kateri subjekti bi ustrezali taki opredelitvi, čeprav je to osrednji vidik predloga, saj je od njega odvisno, za katere subjekte bo veljala obveznost dajanja elektronskih zdravstvenih podatkov na voljo za sekundarno uporabo.
30. EOVP in ENVP ugotavljata tudi, da je splošni cilj predloga zagotoviti, da imajo fizične osebe v EU večji nadzor nad svojimi elektronskimi zdravstvenimi podatki, tega cilja pa ni mogoče doseči, če medsebojni vpliv ustreznih predpisov ni jasno opredeljen. Pravna varnost je ključna za zagotovitev, da imajo različni deležniki občutek, da je varno ukrepati na podlagi novega okvira, in da so pravice fizičnih oseb zajamčene. Zato EOVP in ENVP priporočata, da se medsebojni vpliv predloga ter navedenih pobud in pravnih instrumentov dodatno pojasni.

4 SPLOŠNE DOLOČBE (POGLAVJE I)

¹⁴ V skladu z uvodno izjavo 4 predloga bi bilo treba sklicevanja na določbe Splošne uredbe o varstvu podatkov razumeti tudi kot sklicevanja na ustrezne določbe uredbe EU o varstvu podatkov. Čeprav je namen uvodne izjave 4 jasn, EOVP in ENVP močno priporočata, da se v normativnem delu predloga izrecno navedejo ustrezne določbe uredbe EU o varstvu podatkov kot take.

¹⁵ Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5. 5. 2017, str. 1).

4.1 Člen 1: Predmet urejanja in področje uporabe predloga

31. EOVP in ENVP pozdravljata cilj predloga, da se med drugim okrepijo pravice fizičnih oseb v zvezi z dostopnostjo do njihovih elektronskih zdravstvenih podatkov in nadzorom nad njimi.
32. EOVP in ENVP se zavedata, da je pandemija covid-19 močno pospešila uporabo medicinskih pripomočkov, aplikacij za dobro počutje ali nosljivih naprav v splošni populaciji. Vendar taka tehnologija ustvarja ogromne količine podatkov, pogosto posebne kategorije osebnih podatkov, in je lahko zelo vdorna. Namesto spremljanja dejanj in odločitev ljudi je zdaj mogoče spremljati telesa, misli in čustva ljudi v obsegu, v katerem tega niti ljudje sami morda ne morejo početi. Ti podatki se nato lahko uporabljajo za predvidevanje dejanj ljudi in manipulacijo njihovega ravnanja, tudi na ravni skupin.
33. EOVP in ENVP ugotavljata, da je prvi cilj predloga okrepiti pravice fizičnih oseb glede dostopnosti do njihovih elektronskih zdravstvenih podatkov in nadzorom nad njimi, kot je določeno v členu 1(2), točka (a), predloga. Hkrati pa ugotavljata, da v nasprotju s primarno uporabo, v primeru katere lahko fizične osebe v skladu s predlogom omejijo dostop do svojih osebnih podatkov, te možnosti v zvezi s sekundarno uporabo podatkov nimajo. Poleg tega v skladu s členom 38(2) predloga „[o]rgani za dostop do zdravstvenih podatkov niso dolžni posredovati posebnih informacij iz člena 14 Uredbe (EU) 2016/679 vsaki fizični osebi v zvezi z uporabo njihovih podatkov za projekte, za katere velja dovoljenje za obdelavo podatkov [...]“. EOVP in ENVP poudarjata, da sta pravica do obveščeniosti in pravica do ugovora neločljivo povezani. Zato menita, da predlog z omejevanjem pravice do obveščeniosti iz Splošne uredbe o varstvu podatkov morda ne bo dosegel ciljev iz člena 1(2), točka (a), predloga. Dejansko se zdi, da predvideni pristop ogroža pravici fizičnih oseb do zasebnosti in varstva osebnih podatkov, zlasti ob upoštevanju zelo široke opredelitve sekundarne uporabe in minimalnih kategorij elektronskih podatkov za sekundarno uporabo, uvedenih s predlogom, pri čemer sekundarna uporaba ni omejena zgolj na znanstvene raziskave, ampak vključuje tudi druge namene, kot so inovacije.
34. EOVP in ENVP ugotavljata še, da se predlog v skladu s členom 1(3), točka (a), uporablja za „proizvajalce in dobavitelje **sistemov za vodenje elektronskih zdravstvenih zapisov in aplikacij za dobro počutje**, ki so dani na trg in v uporabo v Uniji, ter uporabnike takih proizvodov“, v skladu s členom 33(1), točki (f) in (n), predloga pa minimalne kategorije elektronskih podatkov za sekundarno uporabo vključujejo elektronske zdravstvene podatke, ki jih ustvari oseba, vključno s podatki **medicinskih pripomočkov, aplikacij za dobro počutje ali drugih digitalnih zdravstvenih aplikacij, ter podatke v zvezi dobrim počutjem in vedenjem, pomembne za zdravje** (poudarek dodan). Prvič, področje uporabe predloga ni skladno s kategorijami podatkov, navedenimi v členu 33(1), točka (f), predloga: področje uporabe se nanaša le na proizvajalce in dobavitelje sistemov za vodenje elektronskih zdravstvenih zapisov in aplikacij za dobro počutje, navedeni člen pa poleg aplikacij za dobro počutje in drugih digitalnih zdravstvenih aplikacij vključuje še medicinske pripomočke. EOVP in ENVP sklepata, da področje uporabe predloga vključuje tudi medicinske pripomočke. Zato zaradi pravne jasnosti priporočata, da se v členu 1(3), točka (a), predloga dodajo tudi proizvajalci in dobavitelji medicinskih pripomočkov.
35. EOVP in ENVP poudarjata še, da za zdravstvene podatke, ki jih ustvarijo aplikacije za dobro počutje in druge digitalne zdravstvene aplikacije, ne veljajo iste zahteve glede kakovosti podatkov kot za podatke, ki jih ustvarijo medicinski pripomočki (za katere se uporabljajo veljavni specifični standardi in zakonodaja), niti nimajo enakih kakovostnih značilnosti. Opozoriti je treba tudi, da lahko digitalne zdravstvene aplikacije zbirajo osebne podatke, ki presegajo zdravstvene podatke: na primer zbrani

osebni podatki v zvezi s prehranjevalnimi in drugimi navadami lahko posredno razkrijejo posebno občutljive informacije, kot je veroizpoved.

36. Ob upoštevanju tega ozadja EOVP in ENVP sicer razumeta, da je morda treba vključiti medicinske pripomočke na področje uporabe predloga, vendar **priporočata, da se iz člena 33(1), točki (f) in (n), predloga izključijo aplikacije za dobro počutje in druge digitalne aplikacije oziroma podatki v zvezi z dobrim počutjem in vedenjem, pomembni za zdravje**. Če bi se ti podatki ohranili, bi bilo treba za obdelavo za sekundarno uporabo osebnih podatkov, pridobljenih iz aplikacij za dobro počutje in drugih digitalnih aplikacij, zahtevati predhodno privolitev v smislu Splošne uredbe o varstvu podatkov. Poleg tega EOVP in ENVP opozarjata, da bi lahko taka obdelava spadala na področje uporabe Direktive 2002/58/ES (direktiva o zasebnosti in elektronskih komunikacijah).
37. EOVP in ENVP ugotavljata, da v skladu s členom 2(2) predloga opredelitev pojma „imetnik podatkov“ izrecno vključuje institucije EU. Vendar **so lahko institucije EU upravljavci osebnih podatkov in podatkov, povezanih z zdravjem (s tem pa tudi imetniki podatkov), ter uporabniki osebnih podatkov in podatkov, povezanih z zdravjem**¹⁶. To je pojasnjeno v uvodni izjavi 41 ter členih 34, 45 in 48 predloga. Zato in zaradi pravne varnosti EOVP in ENVP **priporočata, da se pojasni, ali opredelitev pojma „uporabnik podatkov“ vključuje tudi institucije EU**. Nazadnje, EOVP in ENVP opozarjata, da nacionalne jurisdikcije ne veljajo za institucije, organe, urade in agencije Unije, zato je treba izrecno pojasniti kazni, ki jih lahko naložijo organi za dostop do zdravstvenih podatkov v skladu s členom 43 predloga.

4.2 Člen 2: Opredelitve pojmov

38. EOVP in ENVP ugotavljata, da člen 2 predloga vsebuje ustrezne opredelitve pojmov za razumevanje celotne uredbe. Vendar menita, da je več opredelitev zelo širokih in dopuščajo različne razlage, to pa bi lahko povzročilo pravno negotovost.
39. Prvič, v členu 2(1), točka (a), predloga je navedeno, da se uporabljajo **opredelitve pojmov iz Uredbe (EU) 2016/679**. Hkrati pa predlog določa nove opredelitve in vsebuje sklice na specifične koncepte iz drugih aktov, kot je akt o podatkih. Na primer predlog določa opredelitev pojma „prejemnik podatkov“, čeprav je ta opredelitev že določena v členu 4(9) Splošne uredbe o varstvu podatkov. Ker je namen predloga dopolniti nekatere določbe Splošne uredbe o varstvu podatkov, EOVP in ENVP priporočata, da se zaradi pravne varnosti pojasni, zakaj so potrebne dodatne opredelitve pojmov, v skrajnem primeru pa navedejo opredelitve pojmov iz Splošne uredbe o varstvu podatkov, ki se izjemoma ne uporabljajo.

¹⁶ Institucije, organi in agencije EU obdelujejo podatke, povezane z zdravjem, predvsem v naslednjih primerih:

1. zaposlovanje (zdravniški pregled pred zaposlitvijo);
2. zdravje pri delu (letni zdravniški pregled)/zdravje in varnost pri delu;
3. povračilo stroškov zdravljenja (skupni sistem zdravstvenega zavarovanja);
4. bolniški dopusti (zdravniška potrdila) in postopki za ugotavljanje invalidnosti ter
5. opravljanje naloge, zaupane instituciji EU (na primer Evropski center za preprečevanje in obvladovanje bolezni ter Evropska agencija za zdravila).

Postopki obdelave, ki vključujejo zdravstvene podatke, verjetno povzročajo specifična in večja tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki ter ki so uslužbenci, začasni uslužbenci, pogodbeni uslužbenci, nacionalni strokovnjaki, pripravniki pri teh organih, kandidati za navedena delovna mesta in obiskovalci institucij EU. Ta tveganja so podobna tveganjem, s katerimi se srečujejo posamezniki, na katere se nanašajo osebni podatki, kadar njihove zdravstvene podatke obdelujejo upravljavci, ki niso institucije EU.

40. V skladu s členom 2(2), točka (a), predloga „**osebni elektronski zdravstveni podatki**“ pomenijo elektronsko obdelane podatke v zvezi z zdravstvenimi in genskimi podatki, kot so opredeljeni v Splošni uredbi o varstvu podatkov, ter podatke, ki se nanašajo na dejavnike zdravja, ali podatke, obdelane v zvezi z zagotavljanjem zdravstvenih storitev. Glede tega je treba opozoriti, da uvodna izjava 35 Splošne uredbe o varstvu podatkov že vključuje „informacije [...], zbrane med [...] zagotavljanjem [storitev zdravstvenega varstva]“. Poleg tega se uvodna izjava 54 predloga sklicuje na „determinante, ki vplivajo na zdravstveno stanje“, zlasti v povezavi z obdelavo takih podatkov v zvezi z zdravjem iz razlogov javnega interesa. Za zagotovitev čim večje usklajenosti s Splošno uredbo o varstvu podatkov EOVP in ENVP priporočata, da se opredelitev iz člena 2(2), točka (a), predloga spremeni tako, da se bo nanašala zgolj na „elektronsko obdelane podatke v zvezi z zdravstvenimi in genskimi podatki, kot so opredeljeni v Uredbi (EU) 2016/679“.
41. Po drugi strani so v skladu s členom 2(2), točka (b), predloga „**neosebni elektronski zdravstveni podatki**“ opredeljeni kot podatki v zvezi z zdravstvenimi in genskimi podatki v elektronski obliki, ki ne ustrezajo opredelitvi osebnih podatkov iz člena 4(1) Splošne uredbe o varstvu podatkov. Glede tega EOVP in ENVP znova poudarjata¹⁷, da je razlika med kategorijami osebnih in neosebnih podatkov v praksi težko uporabljati. Iz kombinacije neosebnih podatkov je dejansko mogoče izpeljati ali pridobiti osebne podatke, tj. podatke, ki se nanašajo na določenega ali določljivega posameznika, zlasti kadar so neosebni podatki pridobljeni z anonimizacijo osebnih podatkov, še bolj pa v okviru obdelave zdravstvenih podatkov. Ob upoštevanju tega EOVP in ENVP opozarjata na tveganje ponovne identifikacije, ki je navedeno v uvodni izjavi 64 predloga, ter priporočata, da se izrecneje navede, da se v primeru mešanih podatkovnih naborov (ko so osebni in neosebni podatki „neločljivo povezani“) uporabljajo zaščitni ukrepi v zvezi z osebnimi elektronskimi zdravstvenimi podatki iz Splošne uredbe o varstvu podatkov in predloga.
42. V členu 2(2), točki (d) in (e), predloga sta opredeljena pojma „**primarna uporaba elektronskih zdravstvenih podatkov**“ in „**sekundarna uporaba elektronskih zdravstvenih podatkov**“. EOVP in ENVP menita, da bi lahko ti opredelitvi ter zlasti opredelitev sekundarne uporabe elektronskih zdravstvenih podatkov povzročili pravno negotovost in neusklajenost s Splošno uredbo o varstvu podatkov. V drugem delu člena 2(2), točka (e), predloga je navedeno: „Uporabljeni podatki lahko vključujejo osebne elektronske zdravstvene podatke, ki so bili prvotno zbrani v okviru primarne uporabe, ter elektronske zdravstvene podatke, zbrane za namen sekundarne uporabe.“ Ker Splošna uredba o varstvu podatkov ne vsebuje koncepta „sekundarne uporabe osebnih podatkov“, EOVP in ENVP menita, da drugi del opredelitve pojma „sekundarna uporaba elektronskih zdravstvenih podatkov“ odstopa od koncepta „nadaljnje obdelave osebnih podatkov“ iz Splošne uredbe o varstvu podatkov. Dejansko je treba zadnje navedeni koncept razumeti v povezavi z namenom, za katerega je posamezni upravljavec prvotno zbral podatke, ne glede na njihove kvalitativne vidike. Zato EOVP in ENVP priporočata, da se take opredelitve popravijo ob upoštevanju Splošne uredbe o varstvu podatkov ter zlasti da se pojasni povezava med opredelitvijo sekundarne uporabe elektronskih zdravstvenih podatkov v smislu predloga in konceptom „nadaljnje uporabe osebnih podatkov“ v smislu Splošne uredbe o varstvu podatkov, predvsem ob upoštevanju posebne ureditve za znanstvene raziskave, določene s Splošno uredbo o varstvu podatkov.
43. V skladu s členom 2(2), točka (f), predloga „**interoperabilnost**“ pomeni „sposobnost organizacij ter programskih aplikacij ali naprav istega proizvajalca ali različnih proizvajalcev, da prek podprtih procesov vzajemno delujejo pri doseganju vzajemno koristnih ciljev, ki vključujejo izmenjavo

¹⁷ Skupno mnenje EOVP in ENVP o aktu o upravljanju podatkov, točka 58.

informacij in znanja brez spreminjanja vsebine podatkov med temi organizacijami, programskimi aplikacijami ali napravami“. EOVP in ENVP glede tega menita, da bi bilo morda treba to opredelitev dodatno pojasniti v zvezi z medsebojnim vplivom navedene opredelitve in obstoječih opredelitev interoperabilnosti iz drugih zakonodajnih aktov, kot sta akt o upravljanju podatkov in uredba eIDAS.

44. V skladu s členom 2(2), točka (y), predloga „**imetnik podatkov**“ pomeni „fizično ali pravno osebo, ki je subjekt ali organ v zdravstvenem sektorju ali sektorju oskrbe ali izvaja raziskave v zvezi s tema sektorjema, ter ustanove, organe, urade in agencije Unije, ki imajo pravico ali dolžnost v skladu s to uredbo, veljavno zakonodajo Unije ali nacionalno zakonodajo, s katero se izvaja pravo Unije, ali v primeru neosebni podatkov, z nadzorom tehnične zasnove izdelka in povezanih storitev, zmožnost dajanja na voljo določenih podatkov, vključno z njihovo registracijo, zagotavljanjem, omejevanjem dostopa ali izmenjavo“. Kot je že poudarjeno v točki 29 zgoraj, je to osrednja opredelitev, ki pa je tako široka, da ni mogoče jasno ugotoviti, kdo bi izpolnjeval pogoje za imetnika podatkov, niti razumeti, kakšen je medsebojni vpliv te opredelitve in opredelitve imetnika podatkov iz akta o podatkih in akta o upravljanju podatkov. Če v tej določbi ni jasno navedeno, na koga se opredelitev pojma nanaša, lahko to povzroči pravno negotovost glede tega, kdo mora dati podatke na voljo za sekundarno uporabo na podlagi členov 33(1) in člena 44 predloga, to pa lahko ogrozi pravici posameznikov, na katere se nanašajo osebni podatki, do zasebnosti in varstva podatkov. Poleg tega opredelitev pojma ni usklajena s členom 3(8) predloga, ki vsebuje tudi sklic na sektor socialne varnosti, ta pa zdaj ni zajet z navedeno opredelitvijo iz člena 2(2), točka (y), predloga. Zato EOVP in ENVP menita, da je zaradi pravne varnosti pomembno, da se pojem pojasni.
45. V skladu s členom 2(2), točka (z), predloga „**uporabnik podatkov**“ pomeni „fizično ali pravno osebo, ki ima zakonit dostop do osebnih ali neosebni elektronskih zdravstvenih podatkov za sekundarno uporabo“. EOVP in ENVP glede tega menita, da povezava opredelitve pojma z opredelitvijo pojma „prejemnik podatkov“ iz člena 2(2), točka (k), predloga in opredelitvijo pojma „uporabnik“ iz Splošne uredbe o varstvu podatkov ni jasna. Taka nejasnost velja tudi za medsebojni vpliv te opredelitve in pojma „uporabnik podatkov“ iz akta o upravljanju podatkov. EOVP in ENVP opozarjata tudi na priporočilo v zvezi z vključitvijo institucij EU v to opredelitev iz točke 37 tega mnenja. Nazadnje, EOVP in ENVP menita, da bi bilo namesto navedbe, da ima pravna oseba zakonit dostop do osebnih elektronskih zdravstvenih podatkov, ustrezneje navesti, ali je mogoče tak dostop pridobiti in pod katerimi pogoji.

5 PRIMARNA UPORABA ELEKTRONSKIH ZDRAVSTVENIH PODATKOV (POGLAVJE II)

46. EOVP in ENVP ugotavljata, da je treba pri primarni uporabi elektronskih zdravstvenih podatkov, kot je določena v predlogu, doseči ravnotežje med olajševanjem razpoložljivosti elektronskih zapisov na nacionalni, EU ali mednarodni ravni ter vplivom na pravice in svoboščine posameznikov na splošno ter na pravice iz Splošne uredbe o varstvu podatkov. EOVP in ENVP menita, da bi morala sozakonodajalca za doseg tega cilja upoštevati vidike predloga, navedene v nadaljevanju.

47. EOVP in ENVP ugotavljata, da se člen 3 predloga nanaša na pravice fizičnih oseb v zvezi s primarno uporabo njihovih osebnih elektronskih zdravstvenih podatkov¹⁸. EOVP in ENVP imata velike pomisleke glede medsebojnega vpliva takih novo uvedenih pravic in pravic iz členov 15 do 22 Splošne uredbe o varstvu podatkov. Zlasti imata pomisleke glede prekrivanja pravic, predvidenih v predlogu, s pravicami iz Splošne uredbe o varstvu podatkov ter tveganja pravne negotovosti, ki ga to lahko povzroči v zvezi s posamezniki, na katere se nanašajo osebni podatki. Zato zaradi pravne varnosti so zakonodajalca pozivata, naj pojasnita razmerje med temi pravicami in preprečita, da bi (neposredno ali posredno) omejile obseg pravic posameznikov na podlagi zakonodaje EU o varstvu podatkov.
48. V skladu s členom 3 predloga se uvedejo pravica fizičnih oseb do takojšnjega dostopa, pravica, da omogočijo dostop ali zahtevajo posredovanje svojih podatkov izbranim prejemnikom, ter pravica omejiti dostop zdravstvenih delavcev do vseh ali dela svojih elektronskih zdravstvenih podatkov ter pridobiti informacije o izvajalcih zdravstvenih storitev in zdravstvenih delavcih, ki so v okviru zdravstvenega varstva dostopali do njihovih elektronskih zdravstvenih podatkov. Kot je navedeno v uvodni izjavi 1 predloga, je „[c]ilj te uredbe [...] vzpostaviti evropski zdravstveni podatkovni prostor, da se izboljšata dostop fizičnih oseb do lastnih osebnih elektronskih zdravstvenih podatkov in nadzor nad njimi v okviru zdravstvenega varstva (primarna uporaba elektronskih zdravstvenih podatkov) [...]“. V uvodni izjavi 6 predloga je pojasnjeno, da evropski zdravstveni podatkovni prostor temelji na pravicah posameznikov, na katere se nanašajo osebni podatki, iz Splošne uredbe o varstvu podatkov in jih dodatno razvija, hkrati pa podpira dosledno izvajanje teh pravic, kot se uporabljajo za elektronske zdravstvene podatke.
49. V okviru tega EOVP in ENVP poudarjata, da do priprave tega mnenja ocena učinka predloga v zvezi z varstvom podatkov¹⁹ še ni bila opravljena. Zato ni bila opravljena ocena morebitnega vpliva predvidenih sprememb na pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, niti povezanega tveganja.
50. EOVP in ENVP pozdravljata dejstvo, da predlog vsebuje sklice na pravice iz Splošne uredbe o varstvu podatkov (na primer pravico do brezplačnega dostopa in pravico do pridobitve kopije podatkov)²⁰. Vendar ugotavljata, da opis pravic iz predloga ni skladen z opisom iz Splošne uredbe o varstvu podatkov. Kot je navedeno zgoraj, lahko to povzroči pravno negotovost pri posameznikih, na katere se nanašajo osebni podatki in ki morda ne morejo razlikovati med tema vrstama pravic. Zato in za preprečitev kompleksnosti praktičnega izvajanja EOVP in ENVP so zakonodajalca pozivata, naj zagotovita pravno jasnost pri medsebojnem vplivu pravic posameznikov, na katere se nanašajo osebni

¹⁸ Na primer v zvezi z novo pravico posameznika, na katerega se nanašajo osebni podatki, da omeji dostop zdravstvenih delavcev do vseh ali dela svojih elektronskih zdravstvenih podatkov, ki je določena v členu 3(9) predloga, ni jasno, ali se pri pravilih in posebnih zaščitnih ukrepih, ki se v skladu z navedenimi določbami določijo v pravo države članice, upoštevajo pravila o pravici do omejitve obdelave podatkov iz člena 18(2) in (3) Splošne uredbe o varstvu podatkov.

¹⁹ V zvezi s tem je predlogu priložen delovni dokument služb Komisije – ocena učinka (dokument 8751/22, ADD 3 z dne 6. maja 2022), ki vsebuje le splošen pregled treh možnosti politike glede vpliva na temeljne pravice. To ne pomeni ocene učinka v zvezi z varstvom podatkov v smislu Splošne uredbe o varstvu podatkov, ki bi bila nepogrešljiva za temeljito analizo tveganja, ki bi ga vključevala obdelava posebnih kategorij podatkov v zelo velikem obsegu, ter določitev potrebnih ukrepov za zmanjšanje tveganja in zaščitnih ukrepov.

²⁰ V zvezi z obstojem pravice dostopa in pravice do pridobitve kopije podatkov glej na primer člen 15(1) in (3) Splošne uredbe o varstvu podatkov, člen 12(5) navedene uredbe pa določa, da se pravice uveljavljajo brezplačno.

podatki, uvedenih s predlogom, in splošnih določb o pravicah navedenih posameznikov iz Splošne uredbe o varstvu podatkov.

51. To je še pomembneje za zagotovitev, da se posameznikom, na katere se nanašajo osebni podatki ter ki imajo omejeno zmožnost dostopa do digitalnih storitev in njihove uporabe, ni treba zanašati na tretje osebe za uveljavljanje svojih temeljnih pravic ter jim tako ni treba izpostaviti zasebnosti in osebnih podatkov drugim fizičnim osebam, da bi lahko zahtevali dostop do svojih podatkov v skladu s členom 3(5), točka (b), predloga.
52. EOVP in ENVP opozarjata, da mora zastopanje posameznika, na katerega se nanašajo osebni podatki, pri uveljavljanju njegovih pravic do varstva podatkov izpolnjevati nekatere zahteve glede pravne varnosti. Koncept pooblastitve, uveden s členom 3(5) predloga v zvezi s splošnimi posredniškimi storitvami za dostop, morda ne bo dovolj za zagotovitev, da posameznik, na katerega se nanašajo osebni podatki, ni bil kakor koli prisiljen v to, da je izbranim drugim fizičnim osebam omogočil dostop do svojih podatkov v svojem imenu²¹.
53. EOVP in ENVP poudarjata še, da tako širok koncept pooblastitve brez vsakršnih zaščitnih ukrepov dopušča možnost zlorabe pravice dostopa do elektronskih zdravstvenih podatkov. Dejansko ni nujno, da se z zahtevo, v skladu s katero je lahko zastopnik samo fizična oseba, prepreči, da bi do podatkov dostopala zasebna podjetja. Zato EOVP in ENVP za preprečitev take morebitne zlorabe priporočata, da se vzpostavijo dodatni zaščitni ukrepi, ki bodo dopolnjevali tak mehanizem pooblastitve.
54. Glede pravice do popravka iz člena 3(7) predloga EOVP in ENVP ugotavljata, da iz predloga ni jasno razvidno, kdo bo pristojen za zagotavljanje popravka podatkov. To pomeni težavo, saj v okviru tega obstaja več virov in prejemnikov osebnih podatkov na nacionalni ravni, ravni EU in celo na mednarodni ravni. EOVP in ENVP poudarjata, da ima v skladu s Splošno uredbo o varstvu podatkov tako obveznost upravljavec podatkov. Ker pa v zadevnem primeru elektronske zdravstvene podatke, ki se dajo na voljo, prispeva več upravljavcev, EOVP in ENVP sozakonodajalca pozivata, naj v predlogu pojasnita, kako se bo v praksi zagotavljalo spoštovanje pravice do popravka.
55. EOVP in ENVP ugotavljata, da imajo fizične osebe v skladu s členom 3(8) predloga pravico imetniku podatkov iz zdravstvenega sektorja ali sektorja socialne varnosti omogočiti dostop do elektronskih podatkov ali od njega zahtevati, da nemudoma in brezplačno posreduje njihove zdravstvene podatke prejemniku podatkov po lastni izbiri iz zdravstvenega sektorja ali sektorja socialne varnosti, ne da bi jih oviral imetnik podatkov ali proizvajalci sistemov, ki jih uporablja navedeni imetnik. Glede tega poudarjata, da mora sistem ustrezno identificirati prejemnika podatkov, pri čemer je treba med drugim dokazati, da je subjekt, ki prejme podatke, iz zdravstvenega sektorja ali sektorja socialne varnosti.
56. EOVP in ENVP menita, da bi bilo treba s členom 3(8) poleg možnosti posameznika, na katerega se nanašajo osebni podatki, da sam določi, kateremu prejemniku podatkov se njegovi podatki dajo na voljo, zagotoviti tudi možnost, da sam določi, kateri podatki se posredujejo, podobno kot je to predvideno v členu 3(9) predloga. Zlasti poudarjata, da bi bilo treba z zahtevo po sprejetju tehničnih

²¹ Upoštevati je treba, da se v nekaterih državah članicah to lahko zakonito izvede samo prek notarja, ne glede na to, ali je oseba, ki pridobi dostop, zakoniti skrbnik ali ne. Opozoriti je treba, da je razlog za posredovanje notarja povezan s potrebo po zagotovitvi svobodnega izražanja želja posameznikov, na katere se nanašajo osebni podatki.

ukrepov za vgrajeno zasebnost v predlogu določiti možnost, da se posredujejo samo podatki, potrebni za zadevni namen, da bi se upoštevalo načelo najmanjšega obsega podatkov.

57. Nazadnje, EOVP in ENVP ugotavljata, da se v skladu s členom 3(8) predloga uvaja nova pravica posameznika, na katerega se nanašajo osebni podatki, da posreduje svoje elektronske zdravstvene podatke izbranemu prejemniku podatkov, izrecna ustrezna obveznost imetnika podatkov, da to stori, pa ni določena. Ker v skladu s členom 9(1) Splošne uredbe o varstvu podatkov obdelava osebnih podatkov v zvezi z zdravjem in genskih podatkov načeloma ni dovoljena, razen če se uporablja ena od izjem iz člena 9(2) navedene uredbe, EOVP in ENVP sozakonodajalcema priporočata, da uskladita člen 3(8) predloga s členoma 6 in 9(2) Splošne uredbe o varstvu podatkov ter pojasnita medsebojni vpliv te določbe in morebitnih dodatnih pogojev, tudi omejitev, glede obdelave zdravstvenih ali genskih podatkov, ki jih lahko ohranijo ali uvedejo države članice v skladu s členom 9(4) Splošne uredbe o varstvu podatkov.
58. EOVP in ENVP pozdravljata določbe člena 3(10) predloga, saj zagotavljajo, da imajo posamezniki, na katere se nanašajo osebni podatki, učinkovit nadzor nad svojimi osebnimi podatki in lahko ugotovijo morebiten nezakoniti dostop do svojih zdravstvenih podatkov. Ne glede na to pa menita, da ni jasno, ali se pravica do pridobitve informacije v vseh primerih dostopa do podatkov izvaja s postopkom samodejnega obveščanja ali samo na zahtevo. EOVP in ENVP menita, da je prva možnost najustreznejša rešitev za krepitev vloge posameznika, na katerega se nanašajo osebni podatki. Zato priporočata, da sozakonodajalca to upoštevata in da se ustrezno pojasni.
59. EOVP in ENVP glede člena 4(1) predloga ugotavljata, da zdravstveni delavci (a) imajo dostop do elektronskih zdravstvenih podatkov fizičnih oseb, ki se zdravijo, ne glede na državo članico zdravstvenega zavarovanja in državo članico zdravljenja ter (b) zagotovijo, da osebni elektronski zdravstveni podatki fizičnih oseb, ki jih zdravijo, vsebujejo posodobljene informacije v zvezi z opravljenimi zdravstvenimi storitvami. EOVP in ENVP opozarjata, da se lahko dostop do osebnih elektronskih zdravstvenih podatkov obravnava in ureja že na nacionalni ravni, zato priporočata, da sozakonodajalca pojasnita razmerje med to določbo in nacionalnimi zakoni, s katerimi se to vprašanje že ureja.
60. Prvič, EOVP in ENVP v zvezi s členom 4(1) predloga poudarjata, da v skladu s členom 9(1) Splošne uredbe o varstvu podatkov obdelava osebnih podatkov v zvezi z zdravjem in genskih podatkov načeloma ni dovoljena, razen če se uporablja ena od izjem iz njenega člena 9(2). Zato priporočata, da se člen 4(1) predloga uskladi s členom 9(2), točka (h), Splošne uredbe o varstvu podatkov.
61. Drugič, EOVP in ENVP menita, da ta določba ni skladna z načeloma najmanjšega obsega podatkov in omejitve namena iz Splošne uredbe o varstvu podatkov, saj se dostop ne omogoči le, kadar je potreben in v skladu s potrebo po seznanitvi. Zato in za zagotovitev ustreznih zaščitnih ukrepov za posameznike, na katere se nanašajo osebni podatki, priporočata, da se navede, da se tak dostop omogoči samo na podlagi potrebe po seznanitvi.
62. Tretjič, EOVP in ENVP poudarjata, da pojem „zdravstveni delavec“ vključuje številne poklice, ki so zelo različni in vključujejo različne vrste sodelovanja, odločanja in odgovornosti (na primer zdravniki, medicinske sestre, laboratorijski tehniki in tehniki za slikanje, strokovnjaki za prehrano, fizioterapevti, psihologi, farmacevti). Zato priporočata, da se prepreči, da bi se vsi zdravstveni podatki dajali na voljo vsem zdravstvenim delavcem brez razlikovanja, ampak samo tistim, za katere se šteje, da dostop potrebujejo zaradi opravljanja specifične naloge. Ob upoštevanju tega poudarjata pomen načel nujnosti in sorazmernosti v zvezi s tem. EOVP in ENVP ugotavljata, da v skladu s členom 4(2) predloga države članice ob upoštevanju načela najmanjšega obsega podatkov določijo pravila za določitev

kategorij osebnih elektronskih zdravstvenih podatkov, ki jih zahtevajo različni zdravstveni poklici. Ob tem opozarjata, da se v skladu s predlogom ta odgovornost izrecno prenese na države članice, saj je v skladu z njim obvezna. V ta namen priporočata, da se beseda „lahko“ črta in tako zagotovi, da bodo taka pravila določile države članice.

63. EOVP in ENVP ugotavljata, da se v skladu s členom 4(3) predloga zdravstvenim delavcem omogoči dostop vsaj do prednostnih kategorij elektronskih podatkov iz člena 5 predloga, pri čemer pa ni določeno, ali imajo vsi zdravstveni delavci dostop do vseh prednostnih kategorij. Kot je navedeno zgoraj, EOVP in ENVP menita, da bi bilo treba omogočiti dostop samo ob upoštevanju tistega, kar je potrebno za namene zdravljenja. Menita, da bi bilo treba v predlogu dodatno pojasniti razmerje med odstavkoma 2 in 3 člena 4 predloga.
64. Člen 4(4) predloga zagotavlja možnost odstopanja od omejitev dostopa, za katere se odloči posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 3(9) predloga, kadar je dostop potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe. Glede tega EOVP in ENVP sozakonodajalcema priporočata, da naj pravica fizičnih oseb, da pridobijo informacije o dostopu zdravstvenih delavcev do njihovih elektronskih zdravstvenih podatkov, določena v členu 3(10), vključuje dostop do omejenih informacij iz člena 3(9) predloga.
65. V skladu s členom 7 predloga morajo države članice zagotoviti, da zdravstveni delavci v elektronski obliki „sistematično“ registrirajo ustrezne zdravstvene podatke v zvezi z zdravstvenimi storitvami, ki jih zagotavljajo fizičnim osebam, v sistemu za vodenje elektronskih zdravstvenih zapisov. EOVP in ENVP imata pomisleke glede take sistematične registracije, saj se zdi, da ni v skladu z načelom najmanjšega obsega podatkov iz Splošne uredbe o varstvu podatkov. Zato predlagata, da se besedilo predloga spremeni tako, da se beseda „sistematično“ črta, da bi se določba uskladila z načelom najmanjšega obsega podatkov.
66. EOVP in ENVP pozdravljata določbe o upravljanju elektronske identitete iz člena 9 predloga, saj menita, da sta varna identifikacija in avtentikacija fizičnih oseb in zdravstvenih delavcev, ki uporabljajo elektronske zdravstvene storitve ali dostopajo do osebnih zdravstvenih podatkov, med osrednjimi elementi varstva pravic zadevnih posameznikov, na katere se nanašajo osebni podatki. Glede tega poudarjata, da je morda treba določiti drugačen mehanizem identifikacije in avtentikacije za zdravstvene delavce, odvisno od tega, ali imajo dostop kot zdravstveni delavci ali v zasebne namene.
67. V zvezi z določitvijo organa za digitalno zdravje iz člena 10 predloga imata EOVP in ENVP pomisleke zaradi dejstva, da bi se lahko nekatere naloge organa prekrivale z nalogami nadzornih organov za varstvo podatkov na podlagi Splošne uredbe o varstvu podatkov, zlasti v zvezi s pravicami posameznika, na katerega se nanašajo osebni podatki, in varnostjo obdelave. Zaradi pravne varnosti in izboljšanja berljivosti pravnega besedila predlagata, da se določba iz zadnjega stavka člena 3(11) predloga izvzame iz navedenega člena in vstavi v člen 10 predloga.
68. EOVP in ENVP glede člena 11 predloga, ki določa pravico fizičnih in pravnih oseb, da vložijo pritožbo pri organu za digitalno zdravje, menita, da zgolj obveščanje organov za varstvo podatkov o obstoju pritožbe ne zadostuje za to, da bi lahko navedeni organi ocenili in preiskali vidike pritožbe, povezane z varstvom podatkov. Zato priporočata, da se pojasni, da organ za digitalno zdravje ustreznemu nadzornemu organu za varstvo podatkov pošlje kopijo pritožbe, če se ta kakor koli nanaša na varstvo podatkov, tudi če se njena vsebina nanaša na nove pravice fizičnih oseb, uvedene s členom 3 predloga.
69. Na splošno EOVP in ENVP predlagata, da se uvedeta obvezno posvetovanje in dolžnost sodelovanja z organi za varstvo podatkov v zvezi z oceno pritožb in izvajanjem predloga v vseh primerih, ko so

prisotni vidiki varstva podatkov. Poleg tega poudarjata, da so organi za varstvo podatkov edini organi, pristojni za vprašanja varstva podatkov, zato bi morali ostati edina kontaktna točka za posameznika, na katerega se nanašajo osebni podatki, v zvezi z navedenimi vprašanji, med drugim, da se prepreči morebitna zmeda navedenih posameznikov glede načinov, kako lahko uveljavljajo svoje pravice do varstva podatkov.

70. V skladu s členom 13 predloga je predvidena možnost, da se dodatne čezmejne digitalne zdravstvene storitve zagotavljajo prek platforme Moje zdravje @ EU (MyHealth@EU), ki omogoča tudi izmenjavo podatkov z drugimi infrastrukturami ali storitvami na področju zdravstva, oskrbe ali socialne varnosti. V skladu z navedeno določbo morajo države članice in Komisija zagotoviti interoperabilnost platforme Moje zdravje @ EU (MyHealth@EU) s tehnološkimi sistemi, vzpostavljenimi na mednarodni ravni za izmenjavo elektronskih zdravstvenih podatkov.
71. EOVP in ENVP ugotavljata, da so take možnosti opredeljene splošno in da je dokaj nejasno, v katerih okoliščinah in pod katerimi pogoji se lahko elektronski zdravstveni podatki souporabljajo z udeleženci v tretjih državah. Ob upoštevanju zaščitnih ukrepov, ki se v skladu s poglavjem V Splošne uredbe o varstvu podatkov zahtevajo za mednarodne prenose podatkov, EOVP in ENVP so zakonodajalca priporočata, da se pojasni, da preverjanje skladnosti nacionalne kontaktne točke tretje države ali sistema, vzpostavljenega na mednarodni ravni, ki ga Komisija opravi pred sprejetjem izvedbenega akta, ki določa, da je taka nacionalna kontaktna točka ali sistem skladen z zahtevami platforme Moje zdravje @ EU (MyHealth@EU) za namene izmenjave elektronskih zdravstvenih podatkov, vključuje tudi izpolnjevanje zahtev poglavja V Splošne uredbe o varstvu podatkov.

6 SISTEMI ZA VODENJE ELEKTRONSKIH ZDRAVSTVENIH ZAPISOV IN APLIKACIJE ZA DOBRO POČUTJE (POGLAVJE III)

72. Poglavje III predloga je osredinjeno na izvajanje obvezne sheme samocertifikacije za sisteme za vodenje elektronskih zdravstvenih zapisov, pri čemer morajo taki sistemi izpolnjevati bistvene zahteve glede interoperabilnosti in varnosti iz Priloge II k predlogu. Kot je poudarjeno v obrazložitvenem memorandumu, je „[t]a pristop [...] potreben, da se zagotovi združljivost elektronskih zdravstvenih zapisov med posameznimi sistemi in omogoči enostaven prenos elektronskih zdravstvenih podatkov med njimi“. EOVP in ENVP pozdravljata dejstvo, da je treba v skladu s členoma 15 in 17 predloga v zvezi s sistemi za vodenje elektronskih zdravstvenih zapisov opraviti predhodni postopek ugotavljanja skladnosti, preden se lahko ti sistemi dajo na trg ali drugače dajo v uporabo v EU.
73. Vendar EOVP in ENVP ugotavljata, da se nekatere bistvene zahteve iz Priloge II k predlogu nanašajo na vidike, povezane z varstvom osebnih podatkov, kot so vidiki v zvezi z izvajanjem pravic fizičnih oseb, kot so določene v poglavju II predloga, ali varno obdelavo elektronskih zdravstvenih podatkov²². Poleg tega lahko skupne specifikacije v zvezi z bistvenimi zahtevami iz Priloge II, ki jih Komisija sprejme z izvedbenimi akti v skladu s členom 23(3) predloga, vključujejo elemente v zvezi z varstvom podatkov, kot so zahteve glede kakovosti podatkov, vključno s popolnostjo in točnostjo elektronskih zdravstvenih

²² Glej na primer točko 1.3 in zahteve glede varnosti iz točke 3 Priloge II, kot so točka 3.1 o preprečevanju nepooblaščenega dostopa; točka 3.2 o mehanizmih za identifikacijo in avtentikacijo; točka 3.3 o mehanizmih za nadzor dostopa; točka 3.4 o mehanizmih beleženja dostopa do podatkov ter točka 3.5 o mehanizmih za omejitev dostopa zdravstvenih delavcev.

podatkov, ter zahteve in načela glede varnosti, zaupnosti, celovitosti, varnosti pacientov in varstva elektronskih zdravstvenih podatkov²³.

74. Prvič, EOVP in ENVP poudarjata, da skladnost sistemov za vodenje elektronskih zdravstvenih zapisov z bistvenimi zahtevami v zvezi z interoperabilnostjo in varnostjo iz Priloge II k predlogu ne pomeni nujno, da so postopki obdelave, na katerih temelji delovanje navedenih sistemov, sami po sebi zakoniti, saj mora upravljavec morda izpolniti dodatne zahteve, ki izhajajo iz zakonodaje EU o varstvu podatkov. EOVP in ENVP sicer razumeta, da navedene bistvene zahteve in skupne specifikacije niso neposredno povezane z zakonodajo EU o varstvu podatkov, vendar lahko nekatere od njih znatno vplivajo na vidike, pomembne za varstvo osebnih podatkov zadevnih posameznikov, na katere se nanašajo osebni podatki. Glede tega ugotavljata, da se zdi, da se pri teh zahtevah ne upoštevata ustrezno načeli najmanjšega obsega podatkov in vgrajenega varstva podatkov kot ključna vidika, ki ju je treba upoštevati pri načrtovanju sistema za vodenje elektronskih zdravstvenih zapisov, da se ustrezno zaščitijo interesi in pravice posameznikov, na katere se nanašajo osebni podatki, v zvezi z varstvom podatkov in zasebnostjo. Poleg tega se pri zahtevah glede obdobja hrambe in pravicami dostopa iz točke 3.8 Priloge II k predlogu ne upošteva specifični namen postopkov obdelave podatkov kot ključni element, ki ga je treba upoštevati poleg „izvora in kategorij elektronskih zdravstvenih podatkov“ pri načrtovanju lastnosti shranjevanja sistemov za vodenje elektronskih zdravstvenih zapisov.
75. Ob upoštevanju tveganj, ki jih prinašajo določbe o obvezni razpoložljivosti, čezmejni souporabi in nadaljnji uporabi elektronskih zdravstvenih podatkov, ki jih vsebujejo sistemi za vodenje elektronskih zdravstvenih zapisov, ter dostopu do njih, ter vpliva na zadevne posameznike EOVP in ENVP menita, da bi bilo za krepitev zaščite posameznikov in njihovega zaupanja v te sisteme najustreznejše, če bi se za sisteme za vodenje elektronskih zdravstvenih zapisov uvedel postopek ugotavljanja skladnosti, ki ga izvaja tretja oseba²⁴, pri čemer bi priglašeni organi sodelovali pri oceni ukrepov, ki jih sprejme proizvajalec za izpolnitev zahtev glede interoperabilnosti in varnosti iz Priloge II k predlogu, vključno s tehničnimi rešitvami. Glede tega menita, da je dobrodošlo, da bo to vprašanje predmet posebne ocene v okviru ocene in pregleda predloga, ki ju Komisija opravi pet let po začetku njegove veljavnosti.
76. EOVP in ENVP priporočata tudi, da se predlog spremeni in pojasni razmerje med obvezno shemo samocertifikacije za sisteme za vodenje elektronskih zdravstvenih zapisov in zahtevami glede varstva podatkov. Opozoriti je treba tudi, da bi bilo treba vselej, kadar skupne specifikacije iz člena 23 predloga vplivajo na zahteve glede varstva podatkov, ki se uporabljajo za sisteme za vodenje zdravstvenih elektronskih zapisov, v zvezi z izvedbenimi akti, ki jih sprejme Komisija v skladu s členom 23 predloga, opraviti posvetovanje z EOVP in ENVP v skladu s členom 42(2) uredbe EU o varstvu podatkov. Isti premisleki veljajo za prostovoljno označevanje aplikacij za dobro počutje, ki prav tako temeljijo na bistvenih zahtevah iz Priloge II k predlogu in skupnih specifikacijah iz člena 23 predloga.
77. Glede obravnave tveganj, ki jih pomenijo sistemi za vodenje elektronskih zdravstvenih zapisov, in hudih incidentov ter izvajanja korektivnih ukrepov v skladu s členom 29 predloga EOVP in ENVP priporočata, da se določi dolžnost obveščanja organov za varstvo podatkov in sodelovanja z njimi,

²³ Glej člen 23(3), točki (c) in (e), predloga ter člen 10(2), točka (h), predloga.

²⁴ Glej na primer postopek ugotavljanja skladnosti, ki ga izvaja tretja oseba, določen v Uredbi (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS.

kadar je ustrezno. Dejansko ni jasno, ali lahko sklic na tveganje „za druge vidike zaščite javnega interesa“, navedeno med tveganji, ki jih lahko prinaša sistem za vodenje elektronskih zdravstvenih zapisov, zaradi česar je potrebno posredovanje organa za nadzor trga, vključuje varstvo osebnih podatkov. Poleg tega ni mogoče izključiti, da je hud incident, ki vključuje sistem za vodenje elektronskih zdravstvenih zapisov²⁵, posledica okvar ali poslabšanj lastnosti ali učinkovitosti sistema za vodenje elektronskih zdravstvenih zapisov, ki vplivajo tudi na varstvo osebnih podatkov.

78. EOVP in ENVP načeloma pozdravljata člen 31 predloga o prostovoljnem označevanju aplikacij za dobro počutje, saj se lahko z njim zagotovi preglednost za uporabnike navedenih aplikacij glede njihovih ključnih lastnosti, s tem pa podprejo odločitve uporabnikov za zanesljive aplikacije za dobro počutje. Vendar se s členoma 31 in 32 predloga obravnava samo interoperabilnost aplikacij za dobro počutje s sistemi za vodenje elektronskih zdravstvenih zapisov ter vzpostavi mehanizem za prostovoljno skladnost, omejen na zahteve glede interoperabilnosti in varnosti iz Priloge II k predlogu, da se zagotovi, da lahko aplikacije za dobro počutje posredujejo elektronske zdravstvene podatke sistemom za vodenje elektronskih zdravstvenih zapisov.
79. Glede tega EOVP in ENVP poudarjata, da oznaka, priložena aplikacijam za dobro počutje v skladu s členom 31 predloga, ne pomeni nujno, da so postopki obdelave, na katerih temelji delovanje navedenih aplikacij, sami po sebi zakoniti in jih lahko uporabnik uporablja kot take. Upravljavec bo moral izpolniti dodatne zahteve, ki izhajajo iz zakonodaje EU o varstvu podatkov. EOVP in ENVP priporočata, da se to pojasni v predlogu, tudi v uvodni izjavi. V uvodni izjavi 35 predloga je navedeno: „Uporabnike aplikacij za dobro počutje, kot so mobilne aplikacije, bi bilo treba obvestiti o zmožnosti takih aplikacij, da se povežejo in posredujejo podatke sistemom za vodenje elektronskih zdravstvenih zapisov ali nacionalnim elektronskim zdravstvenim rešitvam, kadar so podatki, pridobljeni z aplikacijami za dobro počutje, koristni za zdravstvene namene.“ Vendar v predlogu niso določeni pogoji, pod katerimi se lahko take aplikacije za dobro počutje zakonito povežejo s sistemi za vodenje elektronskih zdravstvenih zapisov (ali nacionalnimi elektronskimi zdravstvenimi rešitvami) in jim posredujejo podatke v skladu z zakonodajo o varstvu podatkov. Na podlagi seznama minimalnih kategorij elektronskih podatkov za sekundarno uporabo iz člena 33 predloga se zdi jasno, da osebni podatki, ki jih ustvarijo aplikacije za dobro počutje, posredno (ko se naložijo v sistem za vodenje elektronskih zdravstvenih zapisov²⁶) ali neposredno (kolikor jih zbirajo in/ali obdelujejo subjekti, ki ustrezajo opredelitvi imetnikov podatkov iz člena 2(2), točka (y), predloga²⁷) spadajo v te kategorije, zato zanje velja obveznost imetnikov podatkov, da jih dajo na voljo za sekundarno uporabo v skladu z določbami poglavja IV predloga.
80. Obvezno razpoložljivost elektronskih zdravstvenih podatkov, ki jih ustvarijo medicinski pripomočki, aplikacije za dobro počutje ali druge digitalne zdravstvene aplikacije, je treba oceniti glede na hiter tehnološki razvoj na področju tehnologije mobilnih in nosljivih naprav ter vse večje priljubljenosti aplikacij in naprav za „samosledenje“, ki ljudem omogočajo, da beležijo vse vrste vidikov o svoji osebnosti, mislih, telesu, vedenjskih vzorcih in lokacijah. Jasno je, da je treba tem vrstam obdelave podatkov nameniti precejšnjo pozornost, saj jih zadevni posamezniki, na katere se nanašajo osebni podatki, ne morejo preprosto prepoznati kot obdelavo zdravstvenih podatkov. Hkrati pa to prinaša dejanska tveganja za zasebnost, zlasti v primeru, ko se taki podatki obdelujejo za dodatne namene in/ali združijo z drugimi podatki ali posredujejo tretjim osebam. Te vrste obdelave podatkov lahko

²⁵ Glej opredelitev pojma iz člena 2(2), točka (q), predloga.

²⁶ Glej člen 3(6) in člen 33(1), točka (a), predloga.

²⁷ Glej člen 33(1), točki (f) in (n), predloga.

ustvarijo specifična tveganja, vključno s tveganjem neenake ali nepravilne obravnave na podlagi podatkov o domnevem ali dejanskem zdravstvenem stanju osebe, pridobljenih na primer z oblikovanjem profilov na podlagi zelo intimnih podrobnosti o zasebnem življenju navedene osebe, in to ne glede na to, ali so sklepi o njenem zdravstvenem stanju točni ali ne. Dejansko so lahko ta tveganja povezana tudi z zanesljivostjo in točnostjo podatkov, ki jih ustvarijo medicinski pripomočki, aplikacije za dobro počutje ali druge digitalne zdravstvene aplikacije. Ob upoštevanju tega EOVP in ENVP ugotavljata, da je člen 33(3) namenjen opredelitvi, kateri podatki, ki jih ustvarijo medicinski pripomočki, aplikacije za dobro počutje ali druge digitalne zdravstvene aplikacije, se dajo na voljo za sekundarno uporabo. Vendar poudarjata, da še vedno ni jasno, kateri podatki spadajo v to kategorijo in kdo bi ocenjeval njihovo veljavnost ter kakovost potem, ko jih posamezniki vnesejo v svoj elektronski zdravstveni zapis v skladu s členoma 3(6) in 33(1), točka (a), predloga ali ko jih imetniki podatkov neposredno dajo na voljo v skladu s členom 33(1), točki (f) in (n), predloga.

81. Glede tega EOVP in ENVP priporočata, da se aplikacije za dobro počutje in druge digitalne aplikacije izključijo s področja uporabe poglavja IV predloga. Poudarjata pa, da morajo imeti uporabniki, če se ti podatki ohranijo na področju uporabe poglavja IV, še naprej možnost, da se sami odločijo, ali se njihovi osebni podatki, ki jih ustvarijo aplikacije za dobro počutje in druge digitalne aplikacije – ne glede na dejstvo, da so jih naložili v svoje elektronske zdravstvene zapise – souporabljajo z drugimi prejemniki in nadalje obdelajo za sekundarne uporabe ter kateri. Zato EOVP in ENVP priporočata, da se predlog spremeni, da bi se zagotovilo, da so posamezniki, na katere se nanašajo osebni podatki, ustrezno obveščeni o možnostih glede morebitne nadaljnje uporabe njihovih elektronskih zdravstvenih podatkov, vključno s podatki, ki jih ustvarijo aplikacije za dobro počutje in druge digitalne aplikacije. Poleg tega je treba v skladu z zakonodajo o varstvu podatkov jasno določiti specifične pogoje za nadaljnjo obdelavo takih osebnih podatkov in vzpostaviti ustrezne mehanizme za zagotovitev spoštovanja želje posameznikov, na katere se nanašajo osebni podatki, v zvezi z nadaljnjo obdelavo njihovih osebnih zdravstvenih podatkov, ki jih ustvarijo aplikacije za dobro počutje in druge digitalne aplikacije.

7 SEKUNDARNA UPORABA ELEKTRONSKIH ZDRAVSTVENIH PODATKOV (POGLAVJE IV)

82. EOVP in ENVP ugotavljata, da je poglavje IV predloga namenjeno olajšanju sekundarne uporabe elektronskih zdravstvenih podatkov, in pozdravljata dejstvo, da ima lahko taka sekundarna uporaba precejšnje koristi za javno dobro. Vendar menita, da take dejavnosti nadaljnje obdelave vključujejo tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.
83. EOVP in ENVP ugotavljata, da v skladu z uvodno izjavo 37 predloga „uredba zagotavlja pravno podlago v skladu s členom 9(2), točke (g), (h) [...] in (j), Uredbe (EU) 2016/679 za sekundarno uporabo zdravstvenih podatkov, določa zaščitne ukrepe za obdelavo v smislu zakonitih namenov, zaupanja vredno upravljanje za zagotavljanje dostopa do zdravstvenih podatkov (prek organov za dostop do zdravstvenih podatkov) in obdelavo v varnem okolju ter načine obdelave podatkov, določene v dovoljenju za obdelavo podatkov“. V zvezi s tem je v tej uvodni izjavi navedeno, da mora prosilec za dostop do podatkov dokazati pravno podlago v skladu s členom 6 Splošne uredbe o varstvu podatkov, na podlagi katere bi lahko zaprosil za dostop do podatkov v skladu s predlogom, vendar to ni nujno izraženo v operativnem delu predloga. Po drugi strani EOVP in ENVP ugotavljata, da člen 34(1) predloga vsebuje seznam namenov, za katere se lahko elektronski zdravstveni podatki obdelujejo za

sekundarno uporabo, ti pa med drugim vključujejo znanstvene raziskave v zvezi z zdravstvenim sektorjem ali sektorjem oskrbe.

84. EOVP in ENVP imata glede tega tri glavne pomisleke.
85. **Prvič**, EOVP in ENVP ugotavljata, da nameni, za katere se lahko elektronski zdravstveni podatki nadalje obdelujejo, kot so navedeni v členu 34(1) predloga, niso ustrezno opredeljeni, predvsem pa imata pomisleke v zvezi s točkama (f) in (g) navedenega člena, ki po možnosti vključujeta vse oblike „razvojn[ih] in inovacijsk[ih] dejavnosti za izdelke ali storitve, ki prispevajo k javnemu zdravju ali socialni varnosti“ ali „usposabljanj[a], preskušanj[a] in vrednotenj[a] algoritmov, vključno z medicinskimi pripomočki, umetnointeligentnimi sistemi in digitalnimi zdravstvenimi aplikacijami, ki prispevajo k javnemu zdravju ali socialni varnosti“. EOVP in ENVP močno priporočata, da se ti nameni v predlogu podrobneje opredelijo in da se določi, kdaj je povezava z javnim zdravjem in/ali socialno varnostjo zadostna, da bi se doseglo ravnotežje med ustreznim upoštevanjem ciljev predloga in varstvom osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki jih obdelava zadeva.
86. **Drugič**, EOVP in ENVP ob upoštevanju teh ugotovitev in kljub besedilu uvodne izjave 37 predloga menita, da je treba predlog dodatno izboljšati, da se zagotovi skladnost s členom 9 Splošne uredbe o varstvu podatkov.
87. Nameni, za katere se lahko elektronski zdravstveni podatki obdelujejo za sekundarno uporabo, iz člena 34(1) predloga dejansko vsebujejo več vrst sekundarne uporabe, ki bi spadale v različne kategorije razlogov za izjemo, predvidene v členu 9(2) Splošne uredbe o varstvu podatkov. Vendar EOVP in ENVP menita, da to ni izraženo v merilih, v skladu s katerimi bi morali organi za dostop do zdravstvenih podatkov oceniti vloge za dostop do podatkov in sprejeti odločitve o njih (člen 45 predloga), da bi izdali dovoljenje za obdelavo podatkov (člen 46 predloga). Zato EOVP in ENVP poudarjata, da so merila, določena v zvezi s tem v členu 46 predloga, omejena na določbe in načela tega predloga, pri čemer ni jasno, kako so take določbe povezane z načeli in določbami Splošne uredbe o varstvu podatkov, zlasti njenim členom 9(2).
88. Poleg tega EOVP in ENVP menita, da bi bilo treba pojasniti, kako in v katerih okoliščinah bi se člen 9(2), točka (j), Splošne uredbe o varstvu podatkov uporabljal v primeru obdelave zdravstvenih podatkov za „namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene“ (na podlagi prava Unije ali prava države članice), ter „ustrezne zaščitne ukrepe“, kot se zahtevajo v skladu s členom 89(1) Splošne uredbe o varstvu podatkov.
89. **Tretjič**, EOVP in ENVP obravnavata, kako se lahko ta izjema iz člena 9(2) Splošne uredbe o varstvu podatkov, ki se razlaga na podlagi prava Unije, uskladi z njenim členom 9(4) ter možnostjo držav članic, da uvedejo dodatne pogoje, tudi omejitve, glede obdelave genskih podatkov, biometričnih podatkov ali podatkov v zvezi z zdravjem. Glede tega menita, da bi se lahko v predlogu pojasnilo, kako naj bi se izjema od člena 9(1) Splošne uredbe o varstvu podatkov, ki sicer izhaja iz predloga, vendar v njegovih določbah še ni izrecno določena, uskladila z vsemi različnimi nacionalnimi zakoni držav članic.
90. Na podlagi tega **EOVP in ENVP pozivata, naj se s predlogom zagotovi popolna združljivost s členom 9(2) Splošne uredbe o varstvu podatkov, zlasti glede njegove uporabe v zvezi z nameni iz člena 34(1), točki (f) in (g), predloga.** Poleg tega priporočata, da se člen 46 predloga ustrezno spremeni, da se primerno vključijo in upoštevajo razlike v ciljih in zahtevah za sekundarno uporabo elektronskih zdravstvenih podatkov.

91. V zvezi z **minimalnimi kategorijami elektronskih zdravstvenih podatkov za sekundarno uporabo** EOVP in ENVP ugotavljata, da iz člena 33(1) predloga izhaja pravna obveznost imetnikov podatkov, da v skladu s pravom Unije dajo na voljo specifične kategorije elektronskih zdravstvenih podatkov za sekundarno uporabo. EOVP in ENVP ugotavljata, da v skladu s členom 41(1) predloga ta (nova) pravna obveznost dopolnjuje morebitne druge pravne obveznosti, ki so (že) predvidene v drugi zakonodaji Unije ali nacionalni zakonodaji, s katero se izvaja pravo Unije. Prav tako ugotavljata, da bi v skladu z uvodno izjavo 37 predloga člen 33(1) predloga zagotavljal pravno podlago v skladu s členom 6(1), točka (c), Splošne uredbe o varstvu podatkov in izvzetje iz prepovedi iz člena 9(1) navedene uredbe, da bi imetnik podatkov obdeloval (ter tako dal na voljo in zagotovil) osebne elektronske zdravstvene podatke. Čeprav glede tega priznavata, da taka pravna obveznost imetnikov podatkov načeloma ustreza sistemu Splošne uredbe o varstvu podatkov, bi lahko povzročila pravno negotovost.
92. Glede tega člen 33(5) predloga določa: „Kadar nacionalna zakonodaja zahteva privolitve fizične osebe, se organi za dostop do zdravstvenih podatkov opirajo na obveznosti iz tega poglavja za zagotavljanje dostopa do elektronskih zdravstvenih podatkov.“ EOVP in ENVP menita, da ni jasno, na katere „zahteve glede privolitve“ iz nacionalnega prava se določba nanaša. Zlasti **poudarjata, da ni jasno, v kateri fazi postopka, predvidenega v predlogu v zvezi s sekundarno uporabo elektronskih zdravstvenih podatkov, lahko organi za dostop do zdravstvenih podatkov opustijo upoštevanje takih zahtev iz nacionalne zakonodaje**, zlasti kadar temeljijo na členu 9(4) Splošne uredbe o varstvu podatkov. Poleg tega priporočata dodatno pojasnitev in podrobnejšo določitev v zvezi s členom 46(6), točka (f), predloga, v skladu s katerim lahko organi za dostop do zdravstvenih podatkov določijo „posebn[e] pogoji[e] v izdanem dovoljenju za obdelavo podatkov“.
93. V skladu s členom 36 predloga se **določijo organi za dostop do zdravstvenih podatkov**. Glede tega EOVP in ENVP poudarjata, da bo organ za dostop do zdravstvenih podatkov potreboval ustrezno strokovno znanje s pravnega področja, da oceni pravno podlago, ki jo predlaga uporabnik podatkov. EOVP in ENVP ugotavljata, da v členu 36 predloga to še ni izrecno navedeno. Vendar poudarjata, da lahko ustrezní organ za varstvo podatkov vselej pregleda in po potrebi razveljavi oceno pravne podlage, ki jo je opravil organ za dostop do podatkov. Zato pozivata k zagotovitvi jasnosti glede medsebojnega vpliva vloge organa za dostop do zdravstvenih podatkov in ustreznega organa za varstvo podatkov v primeru vprašanj, povezanih z varstvom podatkov.
94. Potreba po pojasnitvi razmerja med predlogom in zakonodajo držav članic je razvidna tudi iz primera **vlog za dovoljenje za obdelavo podatkov v zvezi s čezmejním dostopom do osebnih elektronskih zdravstvenih podatkov za sekundarno uporabo** (oddelek 4, členi 52 do 54 predloga). EOVP in ENVP ugotavljata, da je predlog sicer namenjen olajšanju čezmejne sekundarne uporabe z določitvijo „nacionalnih kontaktnih točk“ in vzpostavitvijo čezmejne infrastrukture (Zdravstveni podatki @ EU (HealthData@EU)), vendar bodo uporabniki podatkov morda kljub temu morali predložiti vlogo ustreznim organom za dostop do zdravstvenih podatkov v vsaki državi članici. EOVP in ENVP menita, da člen 45(3) predloga dejansko določa zgolj omejeno usklajevanje med vključenimi organi za dostop do zdravstvenih podatkov za pridobitev dovoljenja za obdelavo podatkov. Pri tem pa menita, da v predlogu ni ustrezno pojasnjeno, katero specifično nacionalno pravo se bo uporabljalo v zvezi s čezmejnimi dovoljenji za obdelavo podatkov (nacionalno pravo zadevnega organa za dostop do zdravstvenih podatkov ali nacionalno pravo prosilca za dostop do podatkov), vključno s pravno podlago, ki jo bo treba opredeliti (ki jo opredeli prosilec za dostop do podatkov) in oceniti (ki jo oceni organ za dostop do zdravstvenih podatkov). Glede tega bi bilo nazadnje treba opozoriti tudi, da lahko na strani organa za dostop do zdravstvenih podatkov in uporabnika podatkov obstajajo (precejšnje)

vrzeli v strokovnem znanju za reševanje težav pri opredelitvi in upoštevanju razlik (glede določenih zahtev, ki jih je treba izpolniti) v zakonih držav članic v zvezi s (tako) pravno podlago.

95. EOVP in ENVP ugotavljata, da v skladu s členom 38(2) predloga organi za dostop do zdravstvenih podatkov niso dolžni posredovati posebnih informacij iz člena 14 Splošne uredbe o varstvu podatkov vsaki fizični osebi v zvezi z uporabo njihovih podatkov za projekte, za katere velja dovoljenje za obdelavo podatkov. Glede tega menita, da ima lahko uvedena izjema zaradi neobstoja konkretnih pogojev, pod katerimi bi se uporabljala, nenamerne posledice za temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.
96. EOVP in ENVP opozarjata tudi na pomen obveznosti glede preglednosti v zvezi s posamezniki, na katere se nanašajo osebni podatki, in sozakonodajalca pozivata, naj opredelita specifične primere, da se organom za dostop do zdravstvenih podatkov prepreči sistematično zanašanje na tako določbo. Zato priporočata, da se določba ustrezno spremeni, ob upoštevanju, da se zahteve iz člena 14 Splošne uredbe o varstvu podatkov ne smejo sistematično razveljaviti brez zadovoljive in ustrezne ocene ter utemeljitve potrebe po uporabi take izjeme²⁸. Če bi se omejitev pravice do obveščenosti ohranila, EOVP in ENVP sozakonodajalca opozarjata na potrebo po upoštevanju pogojev iz člena 23 Splošne uredbe o varstvu podatkov.
97. V členu 40 predloga je opredeljen in določen podatkovni altruizem v zvezi z zdravjem. EOVP in ENVP glede tega menita, da je določba nejasna, zlasti glede medsebojnega vpliva te določbe in ustrezne določbe iz akta o upravljanju podatkov. Zato priporočata, da se določba ustrezno pojasni.
98. EOVP in ENVP pozdravljata določbo člena 44(3) predloga, po kateri uporabniki podatkov v primerih, ko morajo organi za dostop do zdravstvenih podatkov omogočiti dostop do podatkov v psevdonimizirani obliki, ne smejo ponovno identificirati elektronskih zdravstvenih podatkov, posredovanih v navedeni obliki (informacije, potrebne za razveljavitev psevdonimizacije, so na voljo samo organom za dostop do zdravstvenih podatkov). Poleg tega pozdravljata dejstvo, da se v skladu z navedeno določbo v zvezi z uporabnikom podatkov sprejmejo ustrezni zaščitni ukrepi, če ne spoštuje ukrepov organa za dostop do zdravstvenih podatkov, ki zagotavljajo psevdonimizacijo.
99. Nazadnje, v skladu s členom 48 predloga organi javnega sektorja ter institucije, organi, uradi in agencije Unije z odstopanjem od člena 46 predloga ne potrebujejo dovoljenja za obdelavo podatkov za dostop do elektronskih zdravstvenih podatkov na podlagi člena 48 predloga. EOVP in ENVP menita, da bi se moralo zahtevati dovoljenje, da se lahko preveri, ali so izpolnjene vse ustrezne zahteve, vključno z zakonitostjo in potrebnostjo. Poleg tega menita, da je tako dovoljenje pomembno za spodbujanje preglednosti, saj je v predlogu predvideno, da organi za dostop do zdravstvenih podatkov zagotavljajo splošne javne informacije o vseh dovoljenjih za obdelavo podatkov, izdanih v skladu s členom 46.

8 DODATNI UKREPI (POGLAVJE V)

²⁸ Glej tudi točko 25 zgoraj.

8.1 Shranjevanje osebnih elektronskih zdravstvenih podatkov v EU in skladnost mednarodnih prenosov podatkov s poglavjem V Splošne uredbe o varstvu podatkov

100. Cilj poglavja V predloga je predlagati druge ukrepe za spodbujanje krepitve zmogljivosti držav članic, kar bi spremljalo razvoj evropskega zdravstvenega podatkovnega prostora. Poleg tega se s tem poglavjem urejajo mednarodni dostop do *neosebnih* elektronskih (zdravstvenih) podatkov in njihov prenos ter mednarodni dostop do *osebnih* elektronskih zdravstvenih podatkov in njihov prenos.
101. V zvezi z mednarodnim dostopom do *osebnih* elektronskih zdravstvenih podatkov in njihovim prenosom je v členu 63 predloga določeno, da „lahko države članice ohranijo ali uvedejo nadaljnje pogoje, vključno z omejitvami, v skladu s členom 9(4) Uredbe (EU) 2016/679 in njegovimi pogoji“.
102. **Prvič**, EOVP in ENVP opozarjata, da je Sodišče EU v sodbi v zadevi *Digital Rights Ireland* navedlo, da neobstoj zahteve po hrambi podatkov v EU pomeni, da „[...] ni mogoče šteti, da je v celoti zagotovljen nadzor neodvisnega organa, izrecno zahtevan v členu 8(3) Listine, nad spoštovanjem zahtev glede varovanja in varnosti [...]. Tak nadzor, ki se izvaja na podlagi prava Unije, pa je bistven element varstva oseb pri obdelavi osebnih podatkov [...].“²⁹ Povedano drugače, Sodišče EU je v obravnavani zadevi izrecno navedlo, da nadzora neodvisnega nadzornega organa nad izpolnjevanjem zahtev glede varstva in varnosti ni mogoče v celoti zagotoviti, če zahteva po hrambi zadevnih podatkov v EU ne obstaja. Opustitev zahteve po hrambi podatkov v EU je bila eden od elementov, na podlagi katerih je Sodišče EU sklenilo, da je zakonodajalec EU presegel meje, ki jih določa spoštovanje načela sorazmernosti z vidika členov 7 in 8 ter člena 52(1) Listine Evropske unije o temeljnih pravicah³⁰.
103. Potreba po določitvi zahteve, v skladu s katero je treba osebne podatke v nekaterih specifičnih primerih hraniti v EU, je bila nato potrjena in dopolnjena v sodbi v zadevi *Tele 2*, v kateri je Sodišče EU navedlo: „Glede na količino hranjenih podatkov, občutljivost teh podatkov in tveganje za nezakonit dostop do teh podatkov morajo ponudniki elektronskih komunikacijskih storitev, da zagotovijo celovitost in zaupnost teh podatkov, zagotoviti zelo visoko raven varstva in varnosti z ustreznimi tehničnimi in organizacijskimi ukrepi. Zlasti mora nacionalna ureditev določiti hrambo na ozemlju Unije in nepreklicno uničenje teh podatkov po koncu obdobja njihove hrambe [...]“ (poudarek dodan)³¹. Sodišče EU je tako znova poudarilo, da **je treba** v zadevni zakonodaji zahtevati, da se podatki hranijo v EU, da se zagotovi potrebna raven varnosti in varstva zadevnih podatkov.

²⁹ Sodba Sodišča (veliki senat) z dne 8. aprila 2014, *Digital Rights Ireland Ltd*, združeni zadevi C-293/12 in C-594/12, ECLI:EU:C:2014:238, točka 68. Glej tudi točki 78 in 79 sklepnih predlogov generalnega pravobranilca Cruza Villalóna z dne 12. decembra 2013 v isti zadevi, v katerih je navedeno, da neobstoj določbe, v skladu s katero je treba „podatke, ki jih je treba hraniti, [...] hrani[ti] na ozemlju, ki je v pristojnosti države članice“, „povečuje [...] tveganje za uporabo, ki ni v skladu z zahtevami, povezanimi s pravico do spoštovanja zasebnega življenja“ in „precej povečuje tveganje, da bi bili lahko podatki dostopni ali razkriti v nasprotju s temi predpisi“.

³⁰ Sodba Sodišča (veliki senat) z dne 8. aprila 2014, *Digital Rights Ireland Ltd*, združeni zadevi C-293/12 in C-594/12, ECLI:EU:C:2014:238, točka 69.

³¹ Sodba Sodišča (veliki senat) z dne 21. decembra 2016, *Tele2 Sverige AB proti Post- och telestyrelsen in Secretary of State for the Home Department proti Tomu Watsonu in drugim*, združeni zadevi C-203/15 in C-698/15, ECLI:EU:C:2016:970, točka 122. Glej tudi sklepne predloge generalnega pravobranilca H. Saugmandsgaarda Øja, predstavljene 19. julija 2016, *Tele2 Sverige AB proti Post- och telestyrelsen in Secretary of State for the Home Department proti Tomu Watsonu in drugim*, združeni zadevi C-203/15 in C-698/15, točke 239 do 241.

104. EOVP in ENVP menita, da so ugotovitve Sodišča EU v teh dveh prelomnih sodbah pomembne tudi v zvezi s predlogom, saj se bo uporabljal za (i) obdelavo velikih količin osebnih podatkov, (ii) ki so zelo občutljive narave in (iii) v zvezi s katerimi ni objektivnega elementa za sklep, da je tveganje nezakonitega dostopa manjše od tveganja, ugotovljenega v okviru navedenih sodb³². EOVP in ENVP poudarjata zlasti, da ugotovitev Sodišča še zlasti velja za zadevne podatke, saj se zdravstveni podatki verjetno štejejo za še občutljivejše kot telekomunikacijski podatki (tj. zadevni podatki v navedenih sodbah).
105. Glede tega imata EOVP in ENVP enake pomisleke kot Sodišče v zvezi s potrebo po zmanjšanju tveganja nezakonitega dostopa in neučinkovitega nadzora glede nekaterih vrst podatkov in postopkov obdelave. Zlasti ugotavljata, da nadzor nadzornega organa EU za varstvo podatkov nad skladnostjo s pravili EU o varstvu podatkov morda ni vselej v celoti zagotovljen, kadar je infrastruktura za obdelavo v državi nečlanici EU/EGP.
106. EOVP in ENVP ugotavljata še, da je Komisija nedavno predlagala zahteve glede shranjevanja podatkov v drugih okoliščinah: dejansko se v skladu s členom 17(1), točka (c), nedavnega predloga uredbe Evropskega parlamenta in Sveta o informacijski varnosti v institucijah, organih, uradih in agencijah Unije „občutljivi netajni podatki [...] hranijo in obdelujejo v Uniji“³³. Na splošno EOVP in ENVP ugotavljata, da pravo EU že vključuje več primerov veljavnih zakonodajnih aktov, v skladu s katerimi je treba osebne podatke hraniti v EU in ki običajno poleg tega še omejujejo prenos³⁴. Zato sklepata, da pravo EU zahteva, da se v nekaterih specifičnih primerih določi, da je treba podatke hraniti v EU, da se zmanjša tveganje nezakonitega dostopa in zagotovi učinkovit nadzor.
107. **Drugič**, EOVP in ENVP ugotavljata, da člen 62 predloga o mednarodnem dostopu do neosebne elektronske zdravstvene podatke, „ki se hranijo v Uniji“, in zdi se, da to izraža splošno domnevo, da bi bilo treba to kategorijo podatkov hraniti v EU. EOVP in ENVP menita, da bi bilo treba isti pristop sprejeti v zvezi z osebnimi podatki, ki spadajo na področje uporabe predloga, saj se zdi, da bi bilo težko utemeljiti obstoj zahteve po shranjevanju neosebne elektronske zdravstvene podatke v EU brez iste zahteve za osebne elektronske zdravstvene podatke.

³² EOVP in ENVP ugotavljata, da je tveganje nezakonitega dostopa takšno, da je Komisija dejansko namenila posebno določbo vprašanju, kaj se nanaša na neosebne podatke (člen 62 predloga).

³³ Predlog uredbe Evropskega parlamenta in Sveta o informacijski varnosti v institucijah, organih, uradih in agencijah Unije,

COM(2022) 119 final; <https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX:52022PC0119>.

³⁴ Glej na primer člen 6(8) Direktive (EU) 2016/681 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o uporabi podatkov iz evidence podatkov o potnikih (PNR) za preprečevanje, odkrivanje, preiskovanje in pregon terorističnih in hudih kaznivih dejanj: „Enota za informacije o potnikih hrani, obdeluje in analizira podatke PNR izključno na varni lokaciji ali lokacijah na ozemlju držav članic“; člen 3 Uredbe (ES) št. 767/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o vizumskem informacijskem sistemu (VIS) in izmenjavi podatkov med državami članicami o vizumih za kratkoročno prebivanje (Uredba VIS); člen 41 Uredbe (EU) 2017/2226 Evropskega parlamenta in Sveta z dne 30. novembra 2017 o vzpostavitvi sistema vstopa/izstopa (SVI) za evidentiranje podatkov o vstopu in izstopu ter podatkov o zavrnitvi vstopa državljanov tretjih držav pri prehajanju zunanjih meja držav članic in določitvi pogojev za dostop do SVI zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter o spremembi Konvencije o izvajanju Schengenskega sporazuma in uredb (ES) št. 767/2008 ter (EU) št. 1077/2011; člen 39 Uredbe (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II).

108. **Tretjič**, EOVP in ENVP želita glede tega pojasniti, da obveznost hrambe osebnih podatkov v EU ne izključuje prenosa osebnih elektronskih zdravstvenih podatkov v tretje države ali mednarodne organizacije. Dejansko je mogoče uskladiti splošno zahtevo po hrambi osebnih podatkov v EU z možnostjo specifičnih prenosov v skladu s poglavjem V Splošne uredbe o varstvu podatkov (na primer v okviru znanstvenih raziskav, zagotavljanja oskrbe, mednarodnega sodelovanja). Zato EOVP in ENVP menita, da bi bila obveznost hrambe podatkov v EU sorazmerna in ne bi presegala tistega, kar je potrebno za doseganje postavljenega cilja, tj. določiti dodaten zaščitni ukrep za zmanjšanje tveganja nezakonitega dostopa in neučinkovitega nadzora nad zadevnimi podatki zaradi njihove zelo občutljive narave.
109. **Četrtrič**, EOVP in ENVP ugotavljata tudi, da lahko države članice v skladu s členom 63 predloga ohranijo ali uvedejo nadaljnje pogoje, vključno z omejitvami, v skladu s členom 9(4) Splošne uredbe o varstvu podatkov in njegovimi pogoji. Take omejitve, določene na nacionalni ravni, lahko vključujejo obveznost hrambe podatkov v EU. EOVP in ENVP opozarjata na dejstvo, da se taka obveznost že uporablja v več državah članicah, ter menita, da bi več držav članic verjetno naložilo ali še naprej nalagalo podobne obveznosti, če se vprašanje ne uskladi na ravni EU.
110. Glede na to EOVP in ENVP menita, da se je nujno treba izogniti nedoslednemu in razdrobljenemu pristopu po vsej EU, ki bi privedel do različnih ravni varstva posameznikov, na katere se nanašajo osebni podatki, kar bi bilo v nasprotju z enim od ključnih ciljev Splošne uredbe o varstvu podatkov³⁵. Zato menita, da bi bilo treba dodatne obveznosti, vključno s hrambo osebnih elektronskih zdravstvenih podatkov v EU, kolikor je mogoče obravnavati na ravni EU, tj. v predlogu, da bi se zagotovila enotna visoka raven varstva posameznikov, na katere se nanašajo osebni podatki, v vsej EU in ohranilo ustrezno delovanje notranjega trga v skladu s členom 114 Pogodbe o delovanju Evropske unije, na katerem temelji predlog.
111. Zaradi vseh navedenih razlogov in ob upoštevanju zelo občutljive narave zadevnih osebnih podatkov **EOVP in ENVP menita, da bi bilo treba v skladu s členom 63 predloga od upravljavcev in obdelovalcev s sedežem v EU, ki obdelujejo osebne elektronske zdravstvene podatke na področju uporabe predloga, zahtevati, da te podatke hranijo v EU.** Kot je pojasnjeno zgoraj, taka zahteva po hrambi osebnih elektronskih zdravstvenih podatkov v EU **ne bi smela vplivati na možnost prenosa osebnih elektronskih zdravstvenih podatkov v skladu s poglavjem V Splošne uredbe o varstvu podatkov**³⁶. EOVP in ENVP priporočata tudi, da se v preambuli opozori, da se v zvezi z upravljavci in obdelovalci, ki obdelujejo osebne elektronske zdravstvene podatke, še naprej uporablja člen 48 Splošne uredbe o varstvu podatkov v zvezi s prenosi ali razkritji, ki jih pravo EU ne dovoljuje, ter da bi morali upoštevati to določbo v primeru zahtevka za dostop, poslanega iz tretje države³⁷.

³⁵ Glej uvodno izjavo 53 Splošne uredbe o varstvu podatkov v zvezi s členom 9(4) navedene uredbe: „To pa ne bi smelo ovirati prostega pretoka osebnih podatkov v Uniji, kadar ti pogoji veljajo za čezmejno obdelavo takih podatkov.“

³⁶ In če so izpolnjeni drugi pogoji Splošne uredbe o varstvu podatkov, zlasti člen 6 o obveznosti zagotovitve zakonitosti obdelave.

³⁷ Člen 48 Splošne uredbe o varstvu podatkov: „Sodba sodišča in odločba upravnega organa tretje države, ki od upravljavca ali obdelovalca zahteva prenos ali razkritje osebnih podatkov, se lahko prizna ali izvrši na kateri koli način le, če temelji na mednarodnem sporazumu, kot je pogodba o medsebojni pravni pomoči, sklenjenem med

8.2 Javno naročanje in financiranje Unije

112. EOVP in ENVP ugotavljata, da se v členu 60 predloga obravnava vprašanje dodatnih zahtev za javna naročila in financiranje Unije. EOVP in ENVP menita, da bi se zgoraj navedena priporočila (v zvezi s hrambo podatkov v EU ter skladnostjo s poglavjem V in zlasti členom 48 Splošne uredbe o varstvu podatkov) najbolje operacionalizirala, če bi se vključila v zgodnji fazi javnega naročanja³⁸ ali financiranja storitev upravljavcev in obdelovalcev s sedežem v EU, ki obdelujejo osebne elektronske zdravstvene podatke.
113. Zato **EOVP in ENVP priporočata, da se v členu 60 predloga kot pogoj za javno naročanje ali financiranje storitev upravljavcev in obdelovalcev s sedežem v EU, ki obdelujejo osebne elektronske zdravstvene podatke, določi, da morajo taki upravljavci in obdelovalci (i) hraniti te podatke v EU in (ii) ustrezno dokazati, da se zanje ne uporablja zakonodaja tretje države, ki je v nasprotju s pravili EU o varstvu podatkov.**

8.3 Nacionalne kontaktne točke tretje države ali sistemi, vzpostavljeni na mednarodni ravni

114. EOVP in ENVP ugotavljata, da člena 13(3) in 52(5) predloga zagotavljata možnost, da se prizna skladnost nacionalnih kontaktnih točk tretje države ali sistemov, vzpostavljenih na mednarodni ravni, z zahtevami platforme Moje zdravje @ EU (MyHealth@EU) oziroma infrastrukture Zdravstveni podatki @ EU (HealthData@EU). EOVP in ENVP opozarjata, da bi moral biti prenos, ki temelji na povezavi s platformo Moje zdravje @ EU (MyHealth@EU) in infrastrukturo Zdravstveni podatki @ EU (HealthData@EU) ter njuni uporabi, skladen s poglavjem V Splošne uredbe o varstvu podatkov.
115. EOVP in ENVP ugotavljata, da člena 13(3) in 52(5) predloga zagotavljata možnost, da se prizna skladnost nacionalnih kontaktnih točk tretje države ali sistemov, vzpostavljenih na mednarodni ravni, z zahtevami platforme Moje zdravje @ EU (MyHealth@EU) oziroma infrastrukture Zdravstveni podatki @ EU (HealthData@EU). EOVP in ENVP opozarjata, da bi moral biti prenos, ki temelji na povezavi s platformo Moje zdravje @ EU (MyHealth@EU) in infrastrukturo Zdravstveni podatki @ EU (HealthData@EU) ter njuni uporabi, skladen s poglavjem V Splošne uredbe o varstvu podatkov.
116. EOVP in ENVP ugotavljata zlasti, da se člena 13(3) in 52(5) predloga nanašata na preverjanja skladnosti, ki jih Komisija opravi pred izdajo izvedbenega akta, ki določa, da je nacionalna kontaktna točka tretje države ali sistem, vzpostavljen na mednarodni ravni, skladen z zahtevami platforme Moje zdravje @ EU (MyHealth@EU) oziroma infrastrukture Zdravstveni podatki @ EU (HealthData@EU). Poleg tega ugotavljata, da se uvodna izjava 26 predloga v zvezi s platformo Moje zdravje @ EU (MyHealth@EU) nanaša na potrebo po tem, da se preveri, „ali nacionalna kontaktna točka izpolnjuje tehnične specifikacije, pravila o varstvu podatkov in druge zahteve [...]“. **Glede tega EOVP in ENVP priporočata, da se neposredno v členih 13(3) in 52(5) predloga pojasni, da je treba s preverjanjem skladnosti zagotoviti skladnost s poglavjem V Splošne uredbe o varstvu podatkov pri povezavi nacionalne**

tretjo državo prosilko in Unijo ali državo članico, brez poseganja v druge podlage za prenos v skladu s tem poglavjem.“

³⁸ V zvezi s tem je v uvodni izjavi 78 Splošne uredbe o varstvu podatkov navedeno: „Načeli vgrajenega in privzetega varstva podatkov bi morali biti upoštevani tudi pri javnih razpisih.“ Poleg tega je v uvodni izjavi 77 Direktive 2014/24/EU o javnem naročanju navedeno: „Javni naročniki bi morali pri oblikovanju tehničnih specifikacij upoštevati zahteve, ki izhajajo iz prava Unije na področju varstva podatkov, zlasti v zvezi z načrtovanjem obdelave osebnih podatkov (vgrajeno varstvo podatkov).“

kontaktne točke tretje države ali sistema, vzpostavljenega na mednarodni ravni, s platformo Moje zdravje @ EU (MyHealth@EU) ali infrastrukturo Zdravstveni podatki @ EU (HealthData@EU).

9 EVROPSKO UPRAVLJANJE IN USKLAJEVANJE (POGLAVJE VI)

117. EOVP in ENVP ugotavljata, da se v skladu s členom 64 predloga ustanovi odbor za evropski zdravstveni podatkovni prostor, tj. organ za usklajevanje, ki si prizadeva olajšati sodelovanje in izmenjavo informacij med državami članicami. Poleg tega ugotavljata, da bodo odbor za evropski zdravstveni podatkovni prostor sestavljali predstavniki organov za digitalno zdravje in organov za dostop do zdravstvenih podatkov vseh držav članic ter da **mu bo predsedovala Komisija**. EOVP in ENVP ugotavljata, da se lahko v skladu s predlogom na sestanke povabijo predstavniki EOVP in ENVP, ko se obravnavajo vprašanja varstva podatkov. **EOVP in ENVP menita, da bi morali biti njuni predstavniki stalni člani odbora za evropski zdravstveni podatkovni prostor (torej ne le priložnostno povabljeni udeleženci) ter bi morali sodelovati pri vseh razpravah o vprašanjih varstva osebnih podatkov**, da bi se zagotovila dosledna razlaga in uporaba določb, uvedenih s predlogom, v zvezi z določbami Splošne uredbe o varstvu podatkov.
118. V členu 65(1) predloga so opredeljene naloge odbora za evropski zdravstveni podatkovni prostor, povezane s primarno uporabo elektronskih zdravstvenih podatkov. EOVP in ENVP ugotavljata, da bo lahko Komisija izdajala pisne prispevke in si izmenjevala najboljše prakse o zadevah, povezanih z izvajanjem predloga, zlasti glede določb iz poglavij II in III predloga (člen 65(1), točka (b)(i)) ter vseh vidikov primarne uporabe elektronskih zdravstvenih podatkov (člen 65(1), točka (b)(iii)). Ker so v poglavju II predloga določene podobne pravice do varstva podatkov kot v Splošni uredbi o varstvu podatkov (glej točko 28), EOVP in ENVP menita, da odbor za evropski zdravstveni podatkovni prostor ne bi smel imeti možnosti, da izdaja pisne prispevke v zvezi z vprašanji pravic do varstva podatkov. **EOVP in ENVP poudarjata, da sicer obstaja tveganje, da bo predlog povzročil odstopanje od razlage ali uporabe pravic do varstva podatkov**, kot jo določata EOVP in ENVP. Poleg tega ugotavljata, da bo ta določba ustvarila pravno negotovost, ki bo tudi v nasprotju s ciljem predloga, da se izboljša delovanje notranjega trga z določitvijo **enotnega pravnega okvira** (uvodna izjava 1 predloga). Poleg tega so v členu 65(2) predloga opredeljene naloge odbora za evropski zdravstveni podatkovni prostor, povezane s sekundarno uporabo elektronskih zdravstvenih podatkov. EOVP in ENVP ponavljata opozorilo glede pristojnosti odbora za evropski zdravstveni podatkovni prostor, da objavi pisne prispevke o vprašanjih, povezanih s pravicami do varstva podatkov v zvezi s sekundarno uporabo elektronskih zdravstvenih podatkov.
119. V zvezi s členom 65(1), točka (d), in členom 65(2), točka (d), predloga EOVP in ENVP ugotavljata, da si bo lahko odbor za evropski zdravstveni podatkovni prostor izmenjeval informacije o tveganjih in incidentih na področju varstva podatkov, povezanih s primarno in sekundarno uporabo elektronskih zdravstvenih podatkov, ter informacije o njihovem obvladovanju. **EOVP in ENVP znova poudarjata, da obstaja tveganje, da bo predlog povzročil razhajanje med EOVP in ENVP ter odborom za evropski zdravstveni podatkovni prostor v zvezi z ugotavljanjem ali obravnavanjem kršitev varnosti podatkov**, saj si bo lahko odbor izmenjeval informacije o tem, kako bi se lahko obravnavali incidenti na področju varstva podatkov. Poleg tega ni jasno, kdo so prejemniki informacij, ki si jih bo izmenjeval odbor za evropski zdravstveni podatkovni prostor. Na splošno EOVP in ENVP so zakonodajalcema priporočata, da podrobno določita vzajemno delovanje EOVP in ENVP ter odbora za evropski

zdravstveni podatkovni prostor glede vprašanj varstva podatkov, ki bi morala ostati v izključni pristojnosti organov za varstvo podatkov.

120. EOVP in ENVP glede tega poglavja ugotavljata, da v skladu s členom 66 predloga Komisija ustanovi dve podskupini, odgovorni za skupno upravljanje čezmejnih infrastruktur Moje zdravje @ EU (MyHealth@EU) in Zdravstveni podatki @ EU (HealthData@EU) (člena 12 oziroma 52 predloga). **EOVP in ENVP ugotavljata, da naloge skupin za skupno upravljanje niso jasno opredeljene in se lahko prekrivajo z nalogami odbora za evropski zdravstveni podatkovni prostor** iz člena 65 predloga. Na splošno priporočata, da se jasno opredeli vzajemno delovanje različnih organov, skupin in organizacij, navedenih v predlogu.
121. EOVP in ENVP ugotavljata še nekatere neuskkljenosti med nalogami podskupin in pristojnostjo Komisije, da sprejme izvedbene ali delegirane akte o istih temah. Na primer v skladu s členom 52(13) predloga lahko Komisija z izvedbenimi akti določi zahteve, tehnične specifikacije, arhitekturo IT infrastrukture Zdravstveni podatki @ EU (HealthData@EU), medtem ko tudi ena od podskupin sprejema odločitve v zvezi z razvojem in delovanjem iste infrastrukture. **Zato EOVP in ENVP priporočata, da se pojasni vzajemno delovanje Komisije in teh podskupin.**

10 PRENOS POOBLASTILA IN POSTOPEK V ODBORU (POGLAVJE VII)

122. V skladu s poglavjem VII predloga lahko Komisija sprejme delegirane akte o več konkretnih vidikih, ki se urejajo s predlogom. Glede tega EOVP in ENVP ugotavljata, da ima Komisija kljub sodelovanju držav članic pri odločanju zaradi svojega pooblastila za odločanje o spremembi ali razširitvi nekaterih bistvenih vprašanj, ki se obravnavajo v predlogu, vendarle precejšnji manevrski prostor za spremembo ali razširitev področja uporabe predloga na način, ki bi lahko vplival na pravice do varstva podatkov in izključno pristojnost držav članic, da opredelijo svoje nacionalne zdravstvene politike.
123. EOVP in ENVP zlasti menita, da člena 5(2) in 33(7) predloga vzbujata pomisleke, saj se na Komisijo prenese pooblastilo za spremembo seznama prednostnih kategorij elektronskih zdravstvenih podatkov, do katerih se dostopa in ki se izmenjujejo med državami članicami za primarno uporabo, ter seznama elektronskih zdravstvenih podatkov, ki morajo biti na voljo in dostopni tretjim osebam za sekundarno uporabo. Ker je lahko za morebitno spremembo takih kategorij osebnih podatkov, zlasti posebnih kategorij podatkov, potrebna vnovična ocena tveganj za temeljne pravice in interese zadevnih posameznikov, so ta vprašanja vsebinska in bi jih bilo treba šteti za bistvene elemente v skladu s členom 290 Pogodbe o delovanju Evropske unije.
124. Zato EOVP in ENVP menita, da se taka vprašanja ne bi smela izključiti z zakonodajne ravni, na kateri bi bilo treba jasno določiti morebitno omejitev temeljnih pravic, da se doseže nepogrešljiva predvidljivost pravnega instrumenta, s sprejetjem delegiranih aktov pa bi bilo treba dodati samo podrobnejša podatkovna polja (podkategorije podatkov), ki spadajo v že opredeljene kategorije podatkov iz členov 5(1) in 33(1) predloga.

125. EOVP in ENVP ugotavljata še, da se zdi, da so merila iz člena 5(2), točka (b), predloga, po katerih naj bi Komisija odločala o prednostnih kategorijah elektronskih zdravstvenih podatkov, ki se dodajo seznamu iz člena 5(1) predloga, ohlapna in bi jih bilo treba podrobneje opredeliti³⁹.
126. Nazadnje, čeprav je v členu 67(4) predloga navedeno, da se Komisija posvetuje s strokovnjaki, ki jih imenujejo države članice in lahko imajo določeno strokovno znanje na področju varstva podatkov, EOVP in ENVP priporočata, da se navede jasen sklic na člen 42 uredbe EU o varstvu podatkov in pojasni, da se po potrebi opravi posvetovanje z EOVP in ENVP, kadar se predlagajo taki delegirani akti.

11 RAZNO (POGLAVJE VIII)

127. EOVP in ENVP ugotavljata, da so v skladu s poglavjem VIII predloga za določitev kazni za kršitve uredbe pristojne države članice EU. Zaradi različnih višin kazni ter precej različnih najnižjih in najvišjih zneskov, ki jih lahko določijo posamezne države članice, EOVP in ENVP menita, da bi to lahko povzročilo precej pravne negotovosti v zvezi z ustreznim izvajanjem pravil, določenih s predlogom, v posameznih državah članicah. Glede tega opozarjata, da bi bilo treba določiti usklajena pravila o kaznih, da se zagotovi pravično in varno izvrševanje, zlasti v okviru čezmejnih primerov.
128. Nazadnje, EOVP in ENVP v skladu s prejšnjimi pripombami glede samocertifikacije sistemov za vodenje elektronskih zdravstvenih zapisov ugotavljata, da so obdobja za oceno in pregled iz člena 70 predloga predolga, da bi se zagotovila pravočasna izvedba.

³⁹ Merila se nanašajo na kategorijo, ki se po najnovejših informacijah „uporablja v številnih sistemih za vodenje elektronskih zdravstvenih zapisov, ki se uporabljajo v državah članicah“.

Za Evropskega nadzornika za varstvo podatkov

Evropski nadzornik za varstvo podatkov

(Wojciech Wiewiorowski)

Za Evropski odbor za varstvo podatkov

predsednica

(Andrea Jelinek)