
# Smernice 01/2022 o pravicah posameznikov, na katere se nanašajo osebni podatki – pravica do dostopa

## Različica 2.0

## Sprejete 28. marca 2023

Sprejeto

## Zgodovina različic

| | | |
|---|---|---|
| Različica 1.0 | 18. januar 2022 | Sprejetje smernic za javno posvetovanje |
| Različica 2.0 | 28. marec 2023 | Sprejetje smernic po javnem posvetovanju |

# POVZETEK

Pravica posameznikov, na katere se nanašajo osebni podatki, do dostopa je določena v členu 8 Listine EU o temeljnih pravicah. Ta pravica je od samega začetka del evropskega pravnega okvira za varstvo podatkov in je zdaj dodatno opredeljena z natančnejšimi in podrobnejšimi pravili iz člena 15 splošne uredbe o varstvu podatkov.

**Namen in splošna struktura pravice do dostopa**

Splošni namen pravice do dostopa je posameznikom zagotoviti zadostne, pregledne in lahko dostopne informacije o obdelavi njihovih osebnih podatkov, da se bodo lahko seznanili z obdelavo, preverili njeno zakonitost ter točnost obdelanih podatkov. To bo posameznikom olajšalo uveljavljanje drugih pravic, kot sta pravici do izbrisa ali popravka, ne bo pa pogoj za to.

V skladu z zakonodajo o varstvu podatkov je treba pravico do dostopa razlikovati od podobnih pravic, ki imajo druge cilje, na primer pravice dostopa do javnih dokumentov, katere cilj je zagotoviti preglednost pri odločanju javnih organov in dobro upravno prakso.

Vendar posamezniku, na katerega se nanašajo osebni podatki, ni treba navesti razlogov za zahtevo za dostop in ni naloga upravljavca, da analizira, ali bo zahteva dejansko pomagala posamezniku, na katerega se nanašajo osebni podatki, pri preverjanju zakonitosti zadevne obdelave ali uresničevanju drugih pravic. Upravljavec bo moral zahtevo obravnavati, razen če je jasno, da je bila predložena v skladu s pravili, ki niso pravila o varstvu podatkov.

Pravica do dostopa vključuje tri različne sestavne dele:

- potrditev, ali se podatki o osebi obdelujejo ali ne,
- dostop do teh osebnih podatkov in
- dostop do informacij o obdelavi, kot so namen, vrste podatkov in uporabnikov, trajanje obdelave, pravice posameznikov, na katere se nanašajo osebni podatki, in ustrezni zaščitni ukrepi v primeru prenosov v tretje države.

**Splošni premisleki o presoji zahteve posameznika, na katerega se nanašajo osebni podatki**

Upravljavec mora pri analizi vsebine zahteve presoditi, ali se zahteva nanaša na osebne podatke posameznika, ki je predložil zahtevo, ali spada na področje uporabe člena 15 in ali obstajajo druge, podrobnejše določbe, ki urejajo dostop v določenem sektorju. Presoditi mora tudi, ali se zahteva nanaša na vse obdelane podatke o posamezniku, na katerega se nanašajo osebni podatki, ali le njihove dele.

Glede oblike zahteve ni posebnih zahtev. Upravljavec bi moral zagotoviti ustrezne in uporabniku prijazne komunikacijske kanale, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, zlahka uporablja. Vendar posameznik, na katerega se nanašajo osebni podatki, ni dolžan uporabiti teh posebnih kanalov in lahko namesto tega zahtevo pošlje uradni kontaktni točki upravljavca. Upravljavcu ni treba ukrepati v zvezi z zahtevami, poslanimi na popolnoma naključne ali očitno nepravilne naslove.

Kadar upravljavec ne more opredeliti podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, le-tega o tem obvesti, in lahko dostop zavrne, razen če posameznik, na katerega se nanašajo osebni podatki, zagotovi dodatne informacije, ki omogočajo opredelitev. Poleg tega lahko upravljavec, če dvomi, da je posameznik, na katerega se nanašajo osebni podatki, res oseba, za katero se predstavlja, zahteva dodatne informacije, da potrdi njegovo identiteto. Zahteva za dodatne

informacije mora biti sorazmerna z vrsto obdelanih podatkov, morebitno škodo itd., da bi se izognili pretiranemu zbiranju podatkov.

**Obseg pravice do dostopa**

Obseg pravice do dostopa je določen s področjem uporabe pojma osebnih podatkov, opredeljenega v členu 4(1) splošne uredbe o varstvu podatkov. Poleg osnovnih osebnih podatkov, kot so ime, naslov, telefonska številka itd., lahko v to opredelitev spadajo različni podatki, kot so zdravniški izvidi, zgodovina nakupov, kazalniki kreditne sposobnosti, dnevniki dejavnosti, dejavnosti iskanja itd. Osebni podatki, ki so bili psevdonimizirani, so v nasprotju z anonimiziranimi podatki še vedno osebni podatki. Pravica do dostopa se nanaša na osebne podatke o osebi, ki predloži zahtevo. To se ne bi smelo razlagati preveč omejevalno in lahko vključuje podatke, ki bi se lahko nanašali tudi na druge osebe, na primer zgodovino komunikacije, ki vključuje prejeta in poslana sporočila.

Upravljavec mora poleg dostopa do osebnih podatkov zagotoviti tudi dodatne informacije o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki. Takšne informacije lahko temeljijo na podatkih, zbranih v evidenci dejavnosti obdelave (člen 30 splošne uredbe o varstvu podatkov) in izjavi o varstvu osebnih podatkov (člena 13 in 14 splošne uredbe o varstvu podatkov). Vendar bo te splošne informacije morda treba posodobiti ob predložitvi zahteve ali jih prilagoditi tako, da bodo odražale dejanja obdelave, ki se izvajajo v zvezi z osebo, ki je predložila zahtevo.

**Kako zagotoviti dostop**

Dostop se lahko zagotovi na različne načine, odvisno od količine podatkov in kompleksnosti obdelave, ki se izvaja. Če ni izrecno navedeno drugače, bi bilo treba zahtevo razumeti kot sklicevanje na *vse* osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, in kadar upravljavec obdeluje veliko količino podatkov, lahko od posameznika zahteva, naj podrobno opredeli zahtevo.

Upravljavec bo moral iskati osebne podatke v vseh informacijskih sistemih ter zbirkah, ki ne temeljijo na informacijski tehnologiji, na podlagi iskalnih meril, ki odražajo način, na katerega so informacije strukturirane, kot sta na primer ime in številka stranke. Podatke in druge informacije o obdelavi je treba sporočiti v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. Natančnejše zahteve v zvezi s tem so odvisne od okoliščin obdelave podatkov ter zmožnosti posameznika, na katerega se nanašajo osebni podatki, da dojame in razume sporočilo (na primer, če je posameznik, na katerega se nanašajo osebni podatki, otrok ali oseba s posebnimi potrebami, se to upošteva). Če so podatki sestavljeni iz kod ali drugih neobdelanih podatkov, jih je morda treba pojasniti, da bi bili za posameznika, na katerega se nanašajo osebni podatki, smiselni.

Glavni način zagotavljanja dostopa je, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovi kopija njegovih podatkov, vendar so lahko predvideni tudi drugi načini (kot sta ustna predložitev informacij in dostop na kraju samem), če to zahteva posameznik, na katerega se nanašajo osebni podatki. Podatki se lahko pošljejo po elektronski pošti, če se upoštevajo vsi potrebni zaščitni ukrepi, na primer narava podatkov, ali na druge načine, na primer s samopostrežnim orodjem.

Včasih, kadar je količina podatkov velika in bi posameznik, na katerega se nanašajo osebni podatki, težko razumel informacije, če bi bile vse zagotovljene v enem kosu, zlasti v spletnem okolju, bi bil najprimernejši ukrep večdelni pristop. Zagotavljanje informacij po različnih delih lahko posamezniku, na katerega se nanašajo osebni podatki, olajša razumevanje podatkov. Upravljavec mora biti zmožen dokazati, da ima večdelni pristop za posameznika, na katerega se nanašajo osebni podatki, dodano vrednost, in hkrati zagotoviti vse dele, če se posameznik, na katerega se nanašajo osebni podatki, tako odloči.

Kopijo podatkov in dodatne informacije bi bilo treba zagotoviti v trajni obliki, kot je pisno besedilo, ki bi lahko bilo v elektronski obliki, ki je splošno uporabljana, da ga lahko posameznik, na katerega se nanašajo osebni podatki, zlahka prenese. Podatki se lahko zagotovijo v obliki prepisa ali zbirni obliki, če so vključene vse informacije ter se s tem ne spremeni vsebina informacij.

Zahtevo je treba izpolniti čim prej, v vsakem primeru pa v enem mesecu od njenega prejema. Ta rok se lahko po potrebi podaljša za dva meseca, pri čemer se upoštevata kompleksnost in število zahtev. Posameznika, na katerega se nanašajo osebni podatki, je treba nato obvestiti o razlogu za zamudo. Upravljavec mora izvesti potrebne ukrepe za čim prejšnjo obravnavo zahtev in jih prilagoditi okoliščinam obdelave. Kadar se podatki hranijo le zelo kratko obdobje, je treba sprejeti ukrepe, da se podatki med obravnavo zahteve ne bi izbrisali. Kadar se obdeluje velika količina podatkov, bo moral upravljavec vzpostaviti postopke in mehanizme, prilagojene kompleksnosti obdelave.

Presoja zahteve bi morala odražati stanje v trenutku, ko je upravljavec prejel zahtevo. Predložiti bo treba tudi podatke, ki so morda nepravilni ali nezakonito obdelani. Predložiti ni mogoče podatkov, ki so že bili izbrisani, na primer v skladu s politiko hrambe, in zato upravljavcu niso več na voljo.

**Omejitve**

Splošna uredba o varstvu podatkov dovoljuje nekatere omejitve pravice do dostopa. Dodatnih izjem ali odstopanj ni. Pravica do dostopa je brez splošnega pridržka glede sorazmernosti v zvezi s prizadevanji, ki jih mora upravljavec vložiti v izpolnitev zahteve posameznika, na katerega se nanašajo osebni podatki.

V skladu s členom 15(4) pravica do pridobitve kopije ne sme negativno vplivati na pravice in svoboščine drugih. Evropski odbor za varstvo podatkov meni, da je treba te pravice upoštevati ne le pri odobritvi dostopa z zagotovitvijo kopije, temveč tudi, če se dostop do podatkov zagotovi z drugimi sredstvi (na primer dostop na kraju samem). Vendar se člen 15(4) ne uporablja za dodatne informacije o obdelavi, kot je navedeno v členu 15(1), točke (a) do (h). Upravljavec mora biti zmožen dokazati, da bi v konkretnem primeru to negativno vplivalo na pravice ali svoboščine drugih. Uporaba člena 15(4) ne bi smela povzročiti, da se zahteva posameznika, na katerega se nanašajo osebni podatki, v celoti zavrne; posledica bi bila le, da bi se deli, ki bi lahko negativno vplivali na pravice in svoboščine drugih, izključili ali naredili nečitljive.

Člen 12(5) splošne uredbe o varstvu podatkov upravljavcem omogoča, da zavrnejo zahteve, ki so očitno neutemeljene ali pretirane, ali za take zahteve zaračunajo razumno pristojbino. Te pojme je treba razlagati ozko. Ker je v zvezi z zahtevami za dostop zelo malo predpogojev, se zahteva obravnava kot očitno neutemeljena v precej omejenem obsegu. Pretirane zahteve so odvisne od posebnosti sektorja, v katerem upravljavec deluje. Čim pogostejše so spremembe v podatkovni zbirki upravljavca, tem pogosteje se lahko posamezniku, na katerega se nanašajo osebni podatki, dovoli, da zahteva dostop, ne da bi bilo to pretirano. Upravljavec se lahko odloči, da bo namesto zavrnitve dostopa posamezniku, na katerega se nanašajo osebni podatki, zaračunal pristojbino. To bi bilo ustrezno le v primeru pretiranih zahtev za kritje upravnih stroškov, ki bi jih take zahteve lahko povzročile. Upravljavec mora biti zmožen dokazati, da je zahteva očitno neutemeljena ali pretirana.

Omejitve pravice do dostopa lahko obstajajo tudi v nacionalnem pravu držav članic v skladu s členom 23 splošne uredbe o varstvu podatkov in tam določenimi odstopanji. Upravljavci, ki se nameravajo sklicevati na takšne omejitve, morajo skrbno preveriti zahteve nacionalnih določb in upoštevati morebitne posebne pogoje. Primer takšnega pogoja je, da se pravica do dostopa le začasno odloži ali da se omejitev uporablja samo za nekatere vrste podatkov.

# Kazalo

## Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[1],

ob upoštevanju členov 12 in 22 svojega poslovnika,

ob upoštevanju, da so se pri pripravi teh smernic zbirali prispevki deležnikov v pisni obliki in na posebnem dogodku deležnikov o pravicah posameznikov, na katere se nanašajo osebni podatki, namenjenem opredelitvi izzivov in težav pri razlagi, s katerimi se srečujejo pri uporabi ustreznih določb splošne uredbe o varstvu podatkov –

**SPREJEL NASLEDNJE SMERNICE:**

# 1 UVOD – SPLOŠNE UGOTOVITVE

1. V današnji družbi javni in zasebni subjekti med številnimi dejavnostmi obdelujejo osebne podatke za najrazličnejše namene in na mnoge različne načine. Posamezniki so lahko pogosto v slabšem položaju v smislu razumevanja načina obdelave njihovih osebnih podatkov, vključno s tehnologijo, ki se uporablja v posameznem primeru, ne glede na to, ali podatke obdeluje zasebni ali javni subjekt. Za varstvo osebnih podatkov fizičnih oseb v teh primerih se je s splošno uredbo o varstvu podatkov vzpostavil skladen in trden pravni okvir, ki se na splošno uporablja za različne vrste obdelave, vključno s posebnimi določbami v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki.

2. Pravica do dostopa do osebnih podatkov je poleg drugih pravic ena od pravic posameznikov, na katere se nanašajo osebni podatki, iz poglavja III splošne uredbe o varstvu podatkov, kot so na primer pravica do popravka in izbrisa, pravica do omejitve obdelave, pravica do prenosljivosti, pravica do ugovora ali pravica, da se ne uporablja avtomatizirano sprejemanje posameznih odločitev, vključno z oblikovanjem profilov[2]. Pravica posameznika, na katerega se nanašajo osebni podatki, do dostopa je zapisana v Listini EU o temeljnih pravicah (v nadaljnjem besedilu: Listina)[3] in členu 15 splošne uredbe o varstvu podatkov, kjer je natančno opredeljena kot pravica do dostopa do osebnih podatkov in drugih povezanih informacij.

3. V skladu s splošno uredbo o varstvu podatkov je pravica do dostopa sestavljena iz treh sestavnih delov, in sicer potrditve, ali se osebni podatki obdelujejo ali ne, dostopa do njih in informacij o sami obdelavi. Posameznik, na katerega se nanašajo osebni podatki, lahko pridobi tudi kopijo obdelanih osebnih podatkov, pri čemer ta možnost ni njegova dodatna pravica, temveč način zagotavljanja dostopa do

[1] Sklicevanja na „države članice“ v tem dokumentu je treba razumeti kot sklicevanja na „države članice EGP“.
[2] Člena 15 in 22 splošne uredbe o varstvu podatkov.
[3] V skladu s členom 8(1) Listine Evropske unije o temeljnih pravicah ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. V skladu z drugim stavkom člena 8(2) ima vsakdo pravico do dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo.

podatkov. Pravico do dostopa je torej mogoče razumeti kot možnost posameznika, na katerega se nanašajo osebni podatki, da upravljavca vpraša, ali se obdelujejo osebni podatki o njem, ter kot možnost dostopa do teh podatkov in njihovega preverjanja. Upravljavec posamezniku, na katerega se nanašajo osebni podatki, na podlagi njegove zahteve zagotovi informacije, ki spadajo na področje uporabe člena 15(1) in (2) splošne uredbe o varstvu podatkov.

4. Pravica do dostopa se uresničuje v okviru zakonodaje o varstvu podatkov v skladu s cilji zakonodaje o varstvu podatkov in natančneje v okviru „temeljnih pravic in svoboščin posameznikov ter zlasti njihove pravice do varstva osebnih podatkov“, kot je določeno v členu 1(2) splošne uredbe o varstvu podatkov. Pravica do dostopa je pomemben element celotnega sistema varstva podatkov.

5. Cilj pravice do dostopa je omogočiti posameznikom nadzor nad njihovimi osebnimi podatki v praksi[4]. Da bi se ta cilj učinkovito uresničil v praksi, je namen splošne uredbe o varstvu podatkov to uresničevanje olajšati s številnimi jamstvi, ki posamezniku, na katerega se nanašajo osebni podatki, omogočajo enostavno uresničevanje te pravice brez nepotrebnih omejitev, v razumnih časovnih presledkih in brez pretiranega odlašanja ali stroškov. Vse to bi moralo voditi k učinkovitejšemu uresničevanju pravice posameznika, na katerega se nanašajo osebni podatki, do dostopa v digitalni dobi, pri čemer sta v širšem smislu del te pravice tudi pravica posameznika, na katerega se nanašajo osebni podatki, do vložitve pritožbe pri nadzornem organu in pravica do učinkovitega sodnega varstva[5].

6. V zvezi z razvojem pravice do dostopa, ki je del pravnega okvira za varstvo podatkov, je treba poudariti, da je že od samega začetka del evropskega sistema za varstvo podatkov. V primerjavi z Direktivo 95/46/ES je bil standard pravic posameznikov, na katere se nanašajo osebni podatki, določen v splošni uredbi o varstvu podatkov, izboljšan in okrepljen; to velja tudi za pravico do dostopa. Ker so načini za uresničevanje pravice do dostopa zdaj natančneje določeni v splošni uredbi o varstvu podatkov, je ta pravica za posameznika, na katerega se nanašajo osebni podatki, in za upravljavca tudi bolj poučna s stališča pravne varnosti. Poleg tega mora biti upravljavec glede na posebno besedilo člena 15 in natančen rok za zagotovitev podatkov iz člena 12(3) splošne uredbe o varstvu podatkov pripravljen na poizvedbe posameznikov, na katere se nanašajo osebni podatki, in sicer tako, da pripravi postopke za obravnavo zahtev.

7. Pravice do dostopa ne bi smeli obravnavati ločeno, saj je tesno povezana z drugimi določbami splošne uredbe o varstvu podatkov, zlasti z načeli varstva podatkov, vključno s poštenostjo in zakonitostjo obdelave, obveznostjo upravljavca glede preglednosti in drugimi pravicami posameznikov, na katere se nanašajo osebni podatki, iz poglavja III splošne uredbe o varstvu podatkov.

8. V okviru pravic posameznikov, na katere se nanašajo osebni podatki, je pomembno poudariti tudi pomen člena 12 splošne uredbe o varstvu podatkov, ki določa zahteve za ustrezne ukrepe upravljavca pri zagotavljanju informacij iz členov 13 in 14 splošne uredbe o varstvu podatkov ter sporočil iz členov 15–22 in 34 splošne uredbe o varstvu podatkov; te zahteve na splošno določajo obliko, način in rok za odgovore posamezniku, na katerega se nanašajo osebni podatki, in zlasti za morebitne informacije, namenjene otroku.

9. Evropski odbor za varstvo podatkov meni, da so potrebne natančnejše smernice o tem, kako je treba v različnih razmerah izvajati pravico do dostopa. Namen teh smernic je analizirati različne vidike pravice do dostopa. Natančneje, naslednji oddelek je namenjen splošnemu pregledu in pojasnitvi vsebine

[4] Glej uvodne izjave 7, 68, 75 in 85 splošne uredbe o varstvu podatkov.
[5] Glej člene 77, 78 in 79 poglavja VIII splošne uredbe o varstvu podatkov.

člena 15, medtem ko oddelki, ki mu sledijo, vsebujejo poglobljeno analizo najpogostejših praktičnih vprašanj in težav v zvezi z izvajanjem pravice do dostopa.

# 2 NAMEN PRAVICE DO DOSTOPA, STRUKTURA ČLENA 15 SPLOŠNE UREDBE O VARSTVU PODATKOV IN SPLOŠNA NAČELA

## 2.1 Namen pravice do dostopa

10. Pravica do dostopa je torej namenjena temu, da se posameznikom omogoči nadzor nad njihovimi osebnimi podatki, saj jim omogoča, da se „seznani[jo] z obdelavo in preveri[jo] njeno zakonitost“[6]. Natančneje, namen pravice do dostopa je posameznikom, na katere se nanašajo osebni podatki, omogočiti razumevanje načina obdelave njihovih osebnih podatkov in posledic take obdelave ter preverjanje točnosti obdelanih podatkov, ne da bi jim bilo treba upravičiti svoj namen. Z drugimi besedami, namen pravice do dostopa je posameznikom zagotoviti zadostne, pregledne in lahko dostopne informacije o obdelavi podatkov, ne glede na uporabljene tehnologije, ter jim omogočiti, da preverijo različne vidike posamezne dejavnosti obdelave v skladu s splošno uredbo o varstvu podatkov (npr. zakonitost, točnost).

11. Razlaga splošne uredbe o varstvu podatkov v teh smernicah temelji na dosedanji sodni praksi Sodišča Evropske unije. Glede na pomen pravice do dostopa se lahko pričakuje, da se bo povezana sodna praksa v prihodnosti znatno razvila.

12. V skladu s sklepi Sodišča Evropske unije[7] je namen pravice do dostopa zagotoviti varstvo pravice posameznikov, na katere se nanašajo osebni podatki, do zasebnosti in varstva podatkov v zvezi z obdelavo podatkov, ki se nanje nanašajo,[8] ter lahko olajša uresničevanje njihovih pravic, ki izhajajo na primer iz členov 16 do 19, 21 in 22 ter 82 splošne uredbe o varstvu podatkov. Vendar je uresničevanje pravice do dostopa pravica posameznika in ni pogojena z uresničevanjem drugih navedenih pravic, uresničevanje drugih navedenih pravic pa ni odvisno od uresničevanja pravice do dostopa.

13. Glede na splošni namen pravice do dostopa ni primerno, da bi upravljavec pri presojanju zahteve za dostop namen pravice do dostopa analiziral kot predpogoj za uresničevanje pravice do dostopa. Zato upravljavci ne bi smeli presojati, „zakaj“ posameznik, na katerega se nanašajo osebni podatki, zahteva dostop, temveč samo, „kaj“ zahteva posameznik, na katerega se nanašajo osebni podatki (glej oddelek 3 o analizi zahteve), in ali imajo osebne podatke, ki se nanašajo na tega posameznika (glej oddelek 4). Upravljavec zato posamezniku, na katerega se nanašajo osebni podatki, ne bi smel zavrniti dostopa, ker bi slednji lahko zahtevane podatke uporabil za obrambo na sodišču v primeru odpovedi pogodbe o zaposlitvi ali gospodarskega spora z upravljavcem ali zaradi suma, da bi se to lahko zgodilo[9]. Glede omejitev pravice do dostopa glej oddelek 6.

**Primer 1**: Delodajalec je odpustil posameznika. Teden zatem se posameznik odloči, da bo zbral dokaze in proti nekdanjemu delodajalcu vložil tožbo zaradi odpovedi pogodbe o zaposlitvi. Zato posameznik od nekdanjega delodajalca zahteva dostop do vseh osebnih podatkov, ki se nanašajo nanj kot posameznika, na katerega se nanašajo osebni podatki, ki jih prejšnji delodajalec kot upravljavec obdeluje.

Upravljavec ne presoja namena posameznika, na katerega se nanašajo osebni podatki, slednjemu pa ni treba navesti razloga za zahtevo. Če zahteva izpolnjuje vse druge zahteve (glej oddelek 3), jo mora

[6] Uvodna izjava 63 splošne uredbe o varstvu podatkov.
[7] Sodišče Evropske unije, C-434/16, Nowak, in združeni zadevi C-141/12 in C-372/12, YS in drugi.
[8] Sodišče Evropske unije, C-434/16, Nowak, točka 56.
[9] Vprašanja v zvezi s to temo se obravnavajo v zadevi, ki je trenutno pred Sodiščem Evropske unije (C-307/22).

upravljavec izpolniti, razen če se izkaže, da je očitno neutemeljena ali pretirana v skladu s členom 12(5) splošne uredbe o varstvu podatkov (glej oddelek 6.3), kar mora upravljavec dokazati.

**Različica**: Posameznik, na katerega se nanašajo osebni podatki, med pravdnim postopkom uveljavlja pravico do dostopa do osebnih podatkov, ki se nanašajo nanj. Vendar nacionalno pravo države članice, ki ureja delovno razmerje med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki, vsebuje nekatere določbe, ki omejujejo obseg informacij, ki jih je treba zagotoviti ali izmenjati med strankami v tekočih ali morebitnih sodnih postopkih, in se uporabljajo za tožbo o nezakoniti odpovedi delovnega razmerja, ki jo je vložil posameznik, na katerega se nanašajo osebni podatki. V tem okviru in pod pogojem, da so te nacionalne določbe skladne z zahtevami iz člena 23 splošne uredbe o varstvu podatkov[10], posameznik, na katerega se nanašajo osebni podatki, nima pravice od upravljavca prejeti več informacij, kot je določeno v določbah nacionalnega prava države članice, ki urejajo izmenjavo informacij med strankami v pravnih sporih.

14. Čeprav je namen pravice do dostopa širok, je Sodišče Evropske unije ponazorilo tudi omejitve pristojnosti zakonodaje o varstvu podatkov in pravice do dostopa. Sodišče Evropske unije je na primer ugotovilo, da je treba cilj pravice do dostopa, ki jo zagotavlja zakonodaja EU o varstvu podatkov, razlikovati od cilja pravice do dostopa do javnih dokumentov, ki jo določata zakonodaja EU in nacionalna zakonodaja, pri čemer je slednja namenjena „zagotavljanju preglednosti procesa odločanja javnih organov ter spodbujanju dobre upravne prakse“[11], kar pa ni cilj zakonodaje o varstvu podatkov. Sodišče Evropske unije je sklenilo, da se pravica do dostopa do osebnih podatkov uporablja ne glede na to, ali se uporablja druga vrsta pravice do dostopa z drugačnim namenom, na primer v okviru postopka pregleda.

## 2.2 Struktura člena 15 splošne uredbe o varstvu podatkov

15. Da bi se odgovorilo na zahtevo za dostop in zagotovilo, da se upoštevajo vsi njeni vidiki, je treba najprej razumeti strukturo člena 15 in sestavne dele pravice do dostopa, določene v tem členu.

16. Člen 15 se lahko razčleni na osem različnih elementov, ki so navedeni v spodnji preglednici:

| | | |
|---|---|---|
| 1. | Potrditev, ali upravljavec obdeluje osebne podatke v zvezi osebo, ki je predložila zahtevo | Člen 15(1), prva polovica stavka |
| 2. | Dostop do osebnih podatkov v zvezi z osebo, ki je predložila zahtevo | Člen 15(1), druga polovica stavka (prvi del) |
| 3. | Dostop do naslednjih informacij o obdelavi:<br>(a) nameni obdelave;<br>(b) vrste osebnih podatkov;<br>(c) uporabniki ali kategorije uporabnikov;<br>(d) predvideno trajanje obdelave ali merila za določitev trajanja;<br>(e) obstoj pravic do popravka, izbrisa, omejitve obdelave in ugovora obdelavi;<br>(f) pravica do vložitve pritožbe pri nadzornem organu;<br>(g) vse razpoložljive informacije o viru podatkov, kadar niso zbrani pri posamezniku, na katerega se nanašajo; | Člen 15(1), druga polovica stavka (drugi del) |

[10] Smernice Evropskega odbora za varstvo podatkov 10/2020 o omejitvah na podlagi člena 23 splošne uredbe o varstvu podatkov, različica za javno posvetovanje, 18. december 2020.
[11] Sodišče Evropske unije, združeni zadevi C-141/12 in C-372/12, YS in drugi, točka 47.

| | | |
|---|---|---|
| | (h) obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov, in drugih informacij v zvezi s tem. | |
| 4. | Informacije o zaščitnih ukrepih v skladu s členom 46, kadar se osebni podatki prenesejo v tretjo državo ali mednarodno organizacijo | Člen 15(2) |
| 5. | Obveznost upravljavca, da zagotovi kopijo osebnih podatkov, ki se obdelujejo | Člen 15(3), prvi stavek |
| 6. | Zaračunavanje razumne pristojbine s strani upravljavca ob upoštevanju upravnih stroškov za vse dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki | Člen 15(3), drugi stavek |
| 7. | Zagotavljanje informacij v elektronski obliki | Člen 15(3), tretji stavek |
| 8. | Upoštevanje pravic in svoboščin drugih | Člen 15(4) |

Medtem ko vsi elementi člena 15(1) in (2) skupaj opredeljujejo vsebino pravice do dostopa, člen 15(3) poleg splošnih zahtev iz člena 12 splošne uredbe o varstvu podatkov obravnava načine dostopa. Člen 15(4) dopolnjuje omejitve, določene v členu 12(5) splošne uredbe o varstvu podatkov za vse pravice posameznikov, na katere se nanašajo osebni podatki, s posebnim poudarkom na pravicah in svoboščinah drugih v okviru dostopa.

### 2.2.1 Opredelitev vsebine pravice do dostopa

17. Člen 15(1) in (2) vsebuje naslednje tri vidike: prvič, potrditev, ali se obdelujejo osebni podatki osebe, ki je predložila zahtevo, drugič, če je odgovor pritrdilen, dostop do teh podatkov in tretjič, informacije o obdelavi. Lahko se obravnavajo kot trije različni sestavni deli, ki skupaj tvorijo pravico do dostopa.

#### 2.2.1.1 Potrditev, „ali“ se osebni podatki obdelujejo ali ne

18. Ko posamezniki, na katere se nanašajo osebni podatki, predložijo zahtevo za dostop do osebnih podatkov, morajo najprej vedeti, ali upravljavec obdeluje podatke, ki se nanašajo nanje. Zato so te informacije prvi sestavni del pravice do dostopa v skladu s členom 15(1). Kadar upravljavec ne obdeluje osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki in ki zahteva dostop, bi bile informacije, ki jih je treba zagotoviti, omejene na potrditev, da se osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ne obdelujejo. Kadar upravljavec obdeluje podatke v zvezi z osebo, ki je predložila zahtevo, mora to dejstvo tej osebi potrditi. Ta potrditev se lahko sporoči ločeno ali kot del informacij o osebnih podatkih, ki se obdelujejo (glej spodaj).

#### 2.2.1.2 Dostop do osebnih podatkov, ki se obdelujejo

19. Dostop do osebnih podatkov je drugi sestavni del pravice do dostopa iz člena 15(1) in je osrednji element te pravice. Nanaša se na pojem osebnih podatkov, kot je opredeljen v členu 4(1) splošne uredbe o varstvu podatkov. Poleg osnovnih osebnih podatkov, kot sta ime in naslov, lahko v to opredelitev spadajo neomejeni različni podatki, pod pogojem, da so zajeti v stvarnem področju uporabe splošne uredbe o varstvu podatkov, zlasti kar zadeva način obdelave (člen 2 splošne uredbe o varstvu podatkov). Dostop do osebnih podatkov pomeni dostop do dejanskih osebnih podatkov, ne le splošnega opisa podatkov ali zgolj sklicevanja na vrste osebnih podatkov, ki jih obdeluje upravljavec.

Če se ne uporabljajo nobene omejitve[12], imajo posamezniki, na katere se nanašajo osebni podatki, pravico do dostopa do vseh podatkov, ki se obdelujejo v zvezi z njimi, ali njihovih delov, odvisno od obsega zahteve (glej oddelek 2.3.1). Obveznost zagotavljanja dostopa do podatkov ni odvisna od vrste ali vira teh podatkov. Uporablja se v celotnem obsegu tudi v primerih, ko je oseba, ki je predložila zahtevo, prvotno zagotovila podatke upravljavcu, saj je njen namen seznaniti posameznika, na katerega se nanašajo osebni podatki, o dejanski obdelavi teh podatkov, ki jo izvaja upravljavec. Obseg osebnih podatkov iz člena 15 je podrobno pojasnjen v oddelkih 4.1 in 4.2.

#### 2.2.1.3 Informacije o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki

20. Tretji sestavni del pravice do dostopa so informacije o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki, ki jih mora upravljavec zagotoviti v skladu s členom 15(1)(a)–(h) in členom 15(2). Takšne informacije bi lahko na primer temeljile na besedilu iz izjave upravljavca[13] o varstvu osebnih podatkov ali iz evidence upravljavca o dejavnostih obdelave iz člena 30 splošne uredbe o varstvu podatkov, vendar jih bo morda treba posodobiti in prilagoditi zahtevi posameznika, na katerega se nanašajo osebni podatki. Vsebina in stopnja podrobne opredelitve informacij sta natančneje opredeljeni v oddelku 4.3.

### 2.2.2 Določbe o načinih

21. Člen 15(3) dopolnjuje zahteve glede načinov odgovora na zahteve za dostop iz člena 12 splošne uredbe o varstvu podatkov z nekaterimi podrobnimi opredelitvami v okviru zahtev za dostop.

#### 2.2.2.1 Zagotovitev kopije

22. Upravljavec v skladu s prvim stavkom člena 15(3) splošne uredbe o varstvu podatkov zagotovi brezplačno kopijo osebnih podatkov, s katerimi je povezana obdelava. Kopija se torej nanaša le na drugi sestavni del pravice do dostopa („dostop do obdelanih osebnih podatkov“, glej zgoraj). Upravljavec mora zagotoviti, da je prva kopija brezplačna, tudi če meni, da so stroški reprodukcije visoki (primer: stroški zagotovitve kopije posnetka telefonskega pogovora).

23. Obveznost zagotovitve kopije se ne sme razumeti kot dodatna pravica posameznika, na katerega se nanašajo osebni podatki, temveč kot način zagotavljanja dostopa do podatkov. Krepi pravico do dostopa do podatkov[14] in pomaga pri razlagi te pravice, saj jasno določa, da dostop do podatkov v skladu s členom 15(1) zajema popolne informacije o vseh podatkih in ga ni mogoče razumeti kot zagotovitev zgolj povzetka podatkov. Hkrati obveznost zagotovitve kopije ni namenjena razširitvi obsega pravice do dostopa: nanaša se (samo) na kopijo osebnih podatkov, ki se obdelujejo, in ne nujno na reprodukcijo izvirnih dokumentov (glej odstavek 152 oddelka 5). Na splošno posamezniku, na katerega se nanašajo osebni podatki, ob zagotovitvi kopije ni treba predložiti nobenih dodatnih informacij: obseg informacij, ki jih mora vsebovati kopija, je obseg dostopa do podatkov iz člena 15(1) (drugi sestavni del pravice do dostopa, kot je navedeno zgoraj, glej odstavek 19), ki vključuje vse potrebne informacije, da lahko posameznik, na katerega se nanašajo osebni podatki, razume obdelavo in preveri njeno zakonitost[15].

---

[12] Glej oddelek 6 teh smernic.

[13] Za informacije o tem glej Smernice o preglednosti na podlagi Uredbe 2016/679 delovne skupine iz člena 29, WP 260 rev. 01, 11. april 2018, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov).

[14] Obveznost zagotovitve kopije ni bila omenjena v Direktivi o varstvu podatkov 95/46/ES.

[15] Vprašanja v zvezi s temo tega odstavka se obravnavajo v zadevi, ki je trenutno pred Sodiščem Evropske unije (C-487/21).

24. Glede na navedeno je obveznost zagotovitve kopije iz člena 15(3) izpolnjena, če se dostop do podatkov v smislu člena 15(1) omogoči z zagotovitvijo kopije. Obveznost zagotovitve kopije podpira cilje pravice do dostopa, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči, da se seznani z obdelavo in preveri njeno zakonitost (uvodna izjava 63). Za dosego teh ciljev bo posamezniku, na katerega se nanašajo osebni podatki, v večini primerov treba zagotoviti več kot le začasen vpogled v te informacije. Zato bo moral posameznik, na katerega se nanašajo osebni podatki, pridobiti dostop do informacij s prejemom kopije osebnih podatkov.

25. Pojem kopije je treba glede na navedeno razlagati v širšem smislu in če je kopija popolna (tj. vključuje vse zahtevane osebne podatke) ter jo posameznik, na katerega se nanašajo osebni podatki, lahko hrani, zajema različne vrste dostopa do osebnih podatkov. Zahteva za zagotovitev kopije torej pomeni, da se informacije o osebnih podatkih v zvezi z osebo, ki predloži zahtevo, zagotovijo posamezniku, na katerega se nanašajo osebni podatki, na način, ki temu posamezniku omogoča, da vse informacije hrani in si jih znova ogleda.

26. Kljub temu širokemu razumevanju kopije in glede na to, da je to glavni način zagotavljanja dostopa, bi lahko bili v nekaterih okoliščinah primerni tudi drugi načini. Dodatna pojasnila o kopijah in drugih načinih zagotavljanja dostopa so navedena v oddelku 5, zlasti 5.2.2 do 5.2.5.

#### 2.2.2.2 Zagotavljanje dodatnih kopij

27. Drugi stavek člena 15(3) se nanaša na primere, ko posameznik, na katerega se nanašajo osebni podatki, od upravljavca zahteva več kot eno kopijo, na primer če se je prva kopija izgubila ali poškodovala ali če želi posameznik, na katerega se nanašajo osebni podatki, kopijo posredovati drugi osebi ali nadzornemu organu. Ker mora upravljavec na zahtevo posameznika, na katerega se nanašajo osebni podatki, zagotoviti dodatne kopije, je v členu 15(3) določeno, da lahko za vsako dodatno zahtevano kopijo zaračuna razumno pristojbino ob upoštevanju upravnih stroškov (drugi stavek člena 15(3)).

28. Če posameznik, na katerega se nanašajo osebni podatki, po predložitvi prve zahteve zahteva dodatno kopijo, se lahko pojavijo vprašanja, ali bi bilo treba to obravnavati kot novo zahtevo ali pa želi posameznik, na katerega se nanašajo osebni podatki, dodatno kopijo podatkov v smislu drugega stavka člena 15(3); v slednjem primeru se lahko zaračuna pristojbina za dodatno kopijo. Odgovor na ta vprašanja je odvisen izključno od vsebine zahteve: zahtevo bi bilo treba razlagati kot zahtevo po dodatni kopiji, če se z vidika časa in obsega nanaša na isto obdelavo osebnih podatkov kot prva zahteva. Če pa želi posameznik, na katerega se nanašajo osebni podatki, pridobiti informacije o podatkih, ki niso bili obdelani v isti obdelavi ali se nanašajo na drugačen niz podatkov, kot se je prvotno zahteval, ponovno velja pravica do brezplačne kopije v skladu s členom 15(3). To velja tudi v primerih, ko je posameznik, na katerega se nanašajo osebni podatki, malo pred tem vložil prvo zahtevo. Posameznik, na katerega se nanašajo osebni podatki, lahko uresničuje svojo pravico do dostopa z naknadno zahtevo in pridobi brezplačno kopijo, razen če se zahteva šteje za pretirano v skladu s členom 12(5), pri čemer se lahko zaračuna razumna pristojbina v skladu s členom 12(5)(a) (glede pretiranih zahtev, ki se ponavljajo, glej oddelek 6).

**Primer 2:** Stranka trgovski družbi predloži zahtevo za dostop. Ista stranka leto po odgovoru družbe spet vloži zahtevo za dostop v skladu s členom 15. Drugo zahtevo je treba obravnavati kot novo, ne glede na to, ali sta od predložitve prejšnje zahteve stranki sklenili nove poslovne transakcije ali imeli druge stike. Tudi če ni prišlo do sprememb obdelave podatkov v družbi – s čimer posameznik, na katerega se nanašajo osebni podatki, ni nujno seznanjen –, ima posameznik, na katerega se nanašajo osebni podatki, pravico do brezplačne kopije podatkov.

**Različica 1**: Tudi če stranka v navedenih primerih predloži novo zahtevo na primer le en teden po prvi zahtevi, se to lahko šteje za novo zahtevo v skladu s členom 15(1) in prvim stavkom člena 15(3), če je ni mogoče razlagati zgolj kot opomnik o prvi zahtevi. Zaradi kratkega časovnega razmaka in glede na posebne okoliščine nove zahteve je vprašljivo, ali je v skladu s členom 12(5) (glej oddelek 6) pretirana.

**Različica 2**: Zahtevo za „novo kopijo“ informacij, ki so že bile dane v obliki kopije v odgovor na predhodno zahtevo, na primer če je stranka prej prejeto kopijo izgubila, bi bilo treba praviloma obravnavati kot zahtevo za dodatno kopijo, saj se nanaša na isti obseg in čas obdelave kot prejšnja zahteva.

29. Če posameznik, na katerega se nanašajo osebni podatki, prvo zahtevo za dostop ponovi z obrazložitvijo, da prejeti odgovor ni bil popoln ali da zavrnitev ni bila obrazložena, se ta zahteva ne šteje za novo zahtevo, saj gre zgolj za opozorilo o prvi neizpolnjeni zahtevi.

30. V zvezi z dodelitvijo stroškov v primerih zahtev za dodatno kopijo člen 15(3) določa, da lahko upravljavec zaračuna razumno pristojbino ob upoštevanju upravnih stroškov, ki nastanejo zaradi zahteve. To pomeni, da so upravni stroški upoštevno merilo za določitev višine pristojbine. Hkrati bi morala biti pristojbina ustrezna ob upoštevanju pomena pravice do dostopa kot temeljne pravice posameznika, na katerega se nanašajo osebni podatki. Upravljavec režijskih ali drugih splošnih stroškov ne bi smel prenesti na posameznika, na katerega se nanašajo osebni podatki, temveč bi se moral osredotočiti na posebne stroške, ki so nastali zaradi zagotovitve dodatne kopije. Upravljavec bi moral pri organizaciji tega postopka učinkovito uporabiti svoje človeške in materialne vire, da bi ohranil nizke stroške kopije, tudi če uporablja zunanjo podporo.

31. Če se upravljavec odloči, da bo zaračunal pristojbino, bi moral to sporočiti vnaprej in – kolikor je mogoče natančno – navesti znesek stroškov, ki jih namerava zaračunati posamezniku, na katerega se nanašajo osebni podatki, da bi se ta lahko odločil, ali bo zahtevo ohranil ali umaknil.

#### 2.2.2.3 Zagotavljanje informacij v elektronski obliki, ki je splošno uporabljana

32. V primeru zahteve v elektronski obliki se informacije zagotovijo z elektronskimi sredstvi, kadar je to mogoče in razen če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače (glej člen 12(3) splošne uredbe o varstvu podatkov). Tretji stavek člena 15(3) dopolnjuje to zahtevo v okviru zahtev za dostop z navedbo, da mora upravljavec poleg tega odgovoriti v elektronski obliki, ki je splošno uporabljana, če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače. Člen 15(3) predpostavlja, da bodo upravljavci, ki lahko prejmejo zahteve v elektronski obliki, nanje lahko odgovorili v elektronski obliki, ki je splošno uporabljana (za podrobnosti glej oddelek 5.2.5). Ta določba se nanaša na vse informacije, ki jih je treba zagotoviti v skladu s členom 15(1) in (2). Če posameznik, na katerega se nanašajo osebni podatki, zahtevo za dostop predloži z elektronskimi sredstvi, je treba vse informacije zagotoviti v elektronski obliki, ki je splošno uporabljana. Vprašanja glede oblike so podrobneje opredeljena v oddelku 5. Upravljavec bi moral kot vedno uvesti ustrezne varnostne ukrepe, zlasti pri obravnavi posebne vrste osebnih podatkov (glej oddelek 2.3.4 v nadaljevanju).

### 2.2.3 Morebitna omejitev pravice do dostopa

33. V zvezi s pravico do dostopa je v členu 15(4) predvidena posebna omejitev. Navaja, da je treba upoštevati morebiten negativen vpliv na pravice in svoboščine drugih. Vprašanja glede področja uporabe in posledic te omejitve ter dodatnih omejitev iz člena 12(5) splošne uredbe o varstvu podatkov ali člena 23 splošne uredbe o varstvu podatkov so pojasnjena v oddelku 6.

## 2.3 Splošna načela pravice do dostopa

34. Kadar posamezniki, na katere se nanašajo osebni podatki, vložijo zahtevo za dostop do svojih podatkov, je treba informacije iz člena 15 splošne uredbe o varstvu podatkov načeloma vedno zagotoviti v celoti. V skladu s tem upravljavec, kadar obdeluje podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, zagotovi vse informacije iz člena 15(1) in po potrebi informacije iz člena 15(2). Upravljavec mora sprejeti ustrezne ukrepe za zagotovitev, da so informacije popolne, pravilne in posodobljene ter čim bolj ustrezajo stanju obdelave podatkov v času prejema zahteve[16]. Kadar podatke skupaj obdelujeta dva ali več upravljavcev, dogovor skupnih upravljavcev o njihovih odgovornostih v zvezi z uresničevanjem pravic posameznika, na katerega se nanašajo osebni podatki, zlasti v zvezi z odgovorom na zahteve za dostop, ne vpliva na pravice posameznikov, na katere se nanašajo osebni podatki, v razmerju do upravljavca, na katerega naslovijo svojo zahtevo[17].

### 2.3.1 Popolnost informacij

35. Posamezniki, na katere se nanašajo osebni podatki, imajo pravico, da razen izjem, navedenih v nadaljevanju, pridobijo popolno razkritje vseh podatkov, ki se nanašajo nanje (za podrobnosti o področju uporabe glej oddelek 4.2). Če posameznik, na katerega se nanašajo osebni podatki, izrecno ne zahteva drugače, se zahteva za uresničevanje pravice do dostopa razume na splošno in zajema vse osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki[18]. Omejitev dostopa do dela informacij pride v poštev v naslednjih primerih:

a) posameznik, na katerega se nanašajo osebni podatki, je izrecno omejil zahtevo na podniz. Da bi se izognil zagotavljanju nepopolnih informacij, lahko upravljavec to omejitev zahteve posameznika, na katerega se nanašajo osebni podatki, upošteva le, če je prepričan, da ta razlaga ustreza želji posameznika, na katerega se nanašajo osebni podatki (za več podrobnosti glej odstavek 51 oddelka 3.1.1). Posamezniku, na katerega se nanašajo osebni podatki, načeloma ni treba ponoviti zahteve za posredovanje vseh podatkov, do katerih je upravičen.

b) Kadar upravljavec obdeluje veliko količino podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, lahko dvomi, da je zelo splošno izražena zahteva za dostop dejansko namenjena pridobivanju podrobnih informacij o vseh vrstah podatkov, ki se obdelujejo, ali o vseh dejavnostih upravljavca. Do tega lahko pride zlasti v primerih, kadar posamezniku, na katerega se nanašajo osebni podatki, ni bilo mogoče zagotoviti orodij za opredelitev njegove zahteve že na samem začetku ali kadar posameznik, na katerega se nanašajo osebni podatki, teh orodij ni uporabil. Upravljavec ima nato težave s tem, kako dati popoln odgovor, hkrati pa preprečiti poplavo informacij za posameznika, na katerega se nanašajo osebni podatki, ki slednjega ne zanimajo in jih ne more učinkovito obravnavati. To težavo je mogoče rešiti, odvisno od okoliščin in tehničnih možnosti, na primer z zagotavljanjem samopostrežnih orodij v spletnem okolju (glej oddelek 5 o večdelnem pristopu). Če se takšne rešitve ne uporabljajo, lahko upravljavec, kadar obdeluje veliko količino informacij v zvezi s posameznikom, na katerega se nanašajo osebni podatki, pred zagotovitvijo informacij od tega posameznika zahteva, naj podrobno opredeli, na katere informacije ali obdelavo se zahteva nanaša (glej uvodno izjavo 63 splošne uredbe o varstvu podatkov). Primeri tega lahko vključujejo družbo z več področji dejavnosti ali javni organ z različnimi upravnimi enotami, če upravljavec ugotovi, da se v teh podružnicah obdelujejo številni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Poleg tega lahko

[16] Za navodila o ustreznih ukrepih glej oddelek 5, odst. 123–129.
[17] Smernice Evropskega odbora za varstvo podatkov 07/2020 o pojmih upravljavec in obdelovalec iz splošne uredbe o varstvu podatkov, odst. 162f. Obdelovalci morajo upravljavcu pomagati, prav tam, odst. 129.
[18] Za podrobnosti glej oddelek 5.2.3 spodaj o večdelnem pristopu.

veliko količino podatkov obdelujejo upravljavci, ki v daljšem časovnem obdobju zbirajo podatke o pogostih dejavnostih posameznika, na katerega se nanašajo osebni podatki.

**Primer 3:** Več oddelkov javnega organa v različnih kontekstih obdeluje podatke o posamezniku, na katerega se nanašajo osebni podatki. Vodenje in hramba dokumentacije se delno izvajata z neavtomatiziranimi sredstvi, večina podatkov pa se hrani le v papirni obliki. Javni organ v zvezi s splošnim besedilom zahteve dvomi, da je posameznik, na katerega se nanašajo osebni podatki, seznanjen z obsegom zahteve, zlasti z različnimi postopki obdelave, ki bi jih zajemala, količino informacij in številom strani, ki bi jih prejel.

**Primer 4:** Veliki zavarovalnici njena dolgoletna stranka pošlje dopis s splošno zahtevo za dostop. Zavarovalnica v celoti spoštuje roke za izbris, vendar dejansko obdela veliko količino podatkov v zvezi s stranko, saj je obdelava še vedno potrebna za izpolnitev pogodbenih obveznosti, ki izhajajo iz pogodbenega razmerja s stranko (vključno na primer s trajnimi obveznostmi, komunikacijo o spornih vprašanjih s stranko in tretjimi osebami itd.), ali za izpolnjevanje zakonskih obveznosti (arhivirani podatki, ki jih je treba hraniti za davčne namene, itd.). Zavarovalnica lahko dvomi, ali naj bi zelo splošna zahteva, ki je bila predložena, dejansko zajemala vse vrste teh podatkov. To je lahko še posebej problematično, če ima zavarovalnica samo poštni naslov posameznika, na katerega se nanašajo osebni podatki, zato mora vse informacije poslati v papirni obliki. Vendar se enaki dvomi lahko pojavijo tudi pri zagotavljanju informacij na druge načine.

Če se upravljavec v takšnih primerih odloči, da bo od posameznika, na katerega se nanašajo osebni podatki, zahteval, naj podrobneje opredeli zahtevo, da bi lažje izpolnil svojo obveznost glede uresničevanja pravice do dostopa (člen 12(2) splošne uredbe o varstvu podatkov), hkrati zagotovi smiselne informacije o svojih postopkih obdelave, ki bi lahko zadevali posameznika, na katerega se nanašajo osebni podatki, in sicer z obveščanjem o svojih relevantnih vrstah dejavnosti, podatkovnih zbirkah itd.

**Primer 5:** Pri splošni prošnji za dostop v delovnem razmerju ni samo po sebi jasno, ali želi zaposleni prejeti vse prijavne podatke uporabnika, podatke o dostopu do delovnega mesta, podatke o plačilih v menzi, podatke o izplačilih plač itd. Zahteva delodajalca po podrobni opredelitvi bi lahko na primer privedla do pojasnila, da želi zaposleni razumeti ali preveriti, komu se je posredovala njegova ocena uspešnosti. Brez navedene zahteve po podrobnejši opredelitvi bi zaposleni prejel veliko informacij, ki ga večinoma ne bi zanimale. Hkrati bi moral delodajalec zagotoviti informacije o različnih okoliščinah obdelave, ki bi se lahko nanašale na zaposlenega, da bi lahko zaposlenemu omogočil, da zahtevo smiselno podrobneje opredeli.

Pomembno je poudariti, da namen zahteve po podrobni opredelitvi ni omejitev odgovora na zahtevo za dostop in se ne uporablja za prikrivanje informacij o podatkih ali obdelavi v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Če posameznik, na katerega se nanašajo osebni podatki in ki je bil pozvan, naj navede obseg svoje zahteve, potrdi, da bo zahteval vse osebne podatke, ki se nanašajo nanj, jih mora upravljavec seveda zagotoviti v celoti.

Upravljavec bi moral biti v vsakem primeru vedno zmožen dokazati, da je način obravnave zahteve namenjen zagotovitvi najširše uveljavitve pravice do dostopa in da je to v skladu z njegovo obveznostjo, da olajša uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki (člen 12(2) splošne uredbe o varstvu podatkov). Upravljavec lahko ob upoštevanju teh načel počaka na odgovor posameznika, na katerega se nanašajo osebni podatki, preden mu na njegovo željo zagotovi dodatne podatke, če mu je zagotovil jasen pregled vseh postopkov obdelave, ki bi posameznika, na katerega se nanašajo osebni podatki, lahko zadevali, zlasti tistih, ki jih ta posameznik morda ni pričakoval, če mu je

upravljavec omogočil tudi dostop do vseh podatkov, za katere si je posameznik, na katerega se nanašajo osebni podatki, jasno prizadeval, in je skupaj s temi informacijami jasno navedel, kako pridobiti dostop do preostalih delov obdelanih podatkov.

c) Uporabljajo se izjeme ali omejitve pravice do dostopa (glej oddelek 6 v nadaljevanju). V takšnih primerih bi moral upravljavec skrbno preveriti, na katere dele informacij se izjema nanaša, in zagotoviti vse informacije, ki niso izključene z izjemo. Izjema na primer ne sme vplivati na samo potrditev obdelave osebnih podatkov (sestavni del 1). Zato je treba zagotoviti informacije o vseh osebnih podatkih in vse informacije iz člena 15(1) in (2), na katere se izjema ali omejitev ne nanaša.

### 2.3.2 Pravilnost informacij

36. Informacije, vključene v kopijo osebnih podatkov, ki se zagotovijo posamezniku, na katerega se nanašajo osebni podatki, morajo vključevati dejanske informacije ali osebne podatke, ki se hranijo o tem posamezniku. To vključuje obveznost zagotavljanja informacij o netočnih podatkih ali obdelavi podatkov, ki ni ali ni več zakonita. Posameznik, na katerega se nanašajo osebni podatki, lahko na primer uporabi pravico do dostopa, da se seznani z virom netočnih podatkov, ki krožijo med različnimi upravljavci. Če upravljavec popravi netočne podatke, preden o tem obvesti posameznika, na katerega se nanašajo osebni podatki, bi bil ta posameznik prikrajšan za to možnost. Enako velja v primeru nezakonite obdelave. Možnost seznanitve z nezakonito obdelavo v zvezi s posameznikom, na katerega se nanašajo osebni podatki, je eden od glavnih namenov pravice do dostopa. Obveznost obveščanja o nespremenjenem stanju obdelave ne posega v obveznost upravljavca, da ustavi nezakonito obdelavo ali popravi netočne podatke. Odgovori na vprašanja o vrstnem redu izpolnitve teh obveznosti so navedena v nadaljevanju.

### 2.3.3 Referenčna časovna točka ocene

37. Ocena podatkov, ki se obdelujejo, čim bolj odraža obstoječe stanje v trenutku, ko upravljavec prejme zahtevo, odgovor pa bi moral zajemati vse podatke, ki so takrat na voljo. To pomeni, da se mora upravljavec brez nepotrebnega odlašanja poskušati seznaniti z vsemi dejavnostmi obdelave podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Upravljavcem torej ni treba zagotoviti osebnih podatkov, ki so jih obdelovali v preteklosti in jih nimajo več na voljo[19]. Na primer, upravljavec je morda izbrisal osebne podatke v skladu s svojo politiko hrambe podatkov in/ali zakonskimi določbami ter tako morda ne bo več mogel zagotoviti zahtevanih osebnih podatkov. V zvezi s tem je treba opozoriti, da bi bilo treba trajanje hrambe podatkov določiti v skladu s členom 5(1)(e) splošne uredbe o varstvu podatkov, saj mora biti vsaka hramba podatkov objektivno utemeljena.

38. Hkrati upravljavec vnaprej izvede potrebne ukrepe, da olajša uresničevanje pravice do dostopa in takšne zahteve (glej člen 12(3)) obravnava čim prej, preden bo treba podatke izbrisati. Zato bi bilo treba v primeru kratkih obdobij hrambe ukrepe, sprejete za odgovor na zahtevo, prilagoditi ustreznemu obdobju hrambe, da bi se olajšalo uresničevanje pravice do dostopa in preprečila trajna nezmožnost zagotavljanja dostopa do obdelanih podatkov ob predložitvi zahteve[20]. V nekaterih

[19] Glej v tem smislu dodatna pojasnila v oddelku 4 teh smernic in sodbi Sodišča Evropske unije z dne 7. maja 2009 v zadevi C-553/07, College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer, o pravici dostopa do informacij glede prejemnikov ali kategorijah prejemnikov za preteklost.

[20] Da bi se omogočilo takojšnje ukrepanje, bi lahko na primer razmislili o uvedbi samopostrežnega orodja, ki posamezniku, na katerega se nanašajo osebni podatki, omogoča enostaven dostop do zahtevanih osebnih

primerih kljub temu morda ne bo mogoče odgovoriti na zahtevo pred predvidenim izbrisom podatkov. Če na primer upravljavec pri zagotavljanju čim hitrejšega odgovora na zahtevo pridobi osebne podatke, ki naj bi se izbrisali naslednji dan, bo morda potreboval dodaten čas, da preuči, ali je potrebno zakrivanje, da bi zaščitil svoboščine drugih, preden osebi, ki je predložila zahtevo, predloži kopijo osebnih podatkov. Če so bili podatki pridobljeni v predvidenem obdobju hrambe, jih lahko upravljavec še naprej obdeluje, da bi izpolnil svojo obveznost, da odgovori na zahtevo. V takšnih primerih lahko obdelava temelji na členu 6(1)(c) v povezavi s členom 15 splošne uredbe o varstvu podatkov, njeno trajanje pa mora biti v skladu z zahtevami iz člena 12(3) splošne uredbe o varstvu podatkov[21]. Uporaba te pravne podlage je omejena na obdelavo podatkov, za katere je bilo ugotovljeno, da so potrebni za odgovor na konkretno zahtevo, in se ne sme uporabljati kot utemeljitev za splošno podaljšanje obdobij hrambe.

39. Poleg tega se upravljavec ne sme namerno izogniti obveznosti zagotavljanja zahtevanih osebnih podatkov tako, da v odgovor na zahtevo za dostop (glej oddelek 2.3.2) osebne podatke izbriše ali spremeni. Če upravljavec med obdelavo zahteve za dostop odkrije netočne podatke ali nezakonito obdelavo, mora oceniti stanje obdelave in o tem ustrezno obvestiti posameznika, na katerega se nanašajo osebni podatki, preden izpolni svoje druge obveznosti. Upravljavec bi moral v lastnem interesu dodati informacije o naknadnih popravkih ali izbrisih, da ne bi bilo potrebno nadaljnje obveščanje o tem in zaradi skladnosti z načelom preglednosti.

**Primer 6**: Ob odgovoru na zahtevo za dostop upravljavec ugotovi, da je bila prijava posameznika, na katerega se nanašajo osebni podatki, za prosto delovno mesto v podjetju upravljavca hranjena po preteku obdobja hrambe. Upravljavec v tem primeru osebnih podatkov ne more najprej izbrisati in nato posamezniku, na katerega se nanašajo osebni podatki, odgovoriti, da se (v zvezi s prijavo) ne obdelujejo nobeni podatki. Najprej mora omogočiti dostop in nato izbrisati podatke. Da bi preprečil naknadno zahtevo za izbris, bi bilo priporočljivo dodati informacijo o dejanskem izbrisu in času izbrisa.

Zaradi skladnosti z načelom preglednosti bi moralo obvestilo, ki ga upravljavec predloži posamezniku, na katerega se nanašajo osebni podatki, vsebovati točno navedbo časa obdelave, na katerega se nanaša odgovor upravljavca. V nekaterih primerih, na primer v okviru pogostih dejavnosti obveščanja, lahko pride do dodatne obdelave ali sprememb podatkov med to referenčno časovno točko, ko je bila ocenjena obdelava, in odgovorom upravljavca. Če je upravljavec seznanjen s takšnimi spremembami, je priporočljivo, da zagotovi tudi informacije o teh spremembah in dodatni obdelavi, potrebni za odgovor na zahtevo.

### 2.3.4 Skladnost z zahtevami glede varnosti podatkov

40. Ker je sporočanje osebnih podatkov in omogočanje dostopa do njih posamezniku, na katerega se nanašajo osebni podatki, dejanje obdelave, mora upravljavec vedno izvesti ustrezne tehnične in organizacijske ukrepe, da zagotovi primerno raven varnosti glede na tveganje, povezano z obdelavo (glej člen 5(1)(f) ter člena 24 in 32 splošne uredbe o varstvu podatkov). To velja ne glede na način zagotavljanja dostopa. Glede na tveganja, ki jih predstavlja obdelava, lahko v primeru neelektronskega prenosa podatkov posamezniku, na katerega se nanašajo osebni podatki, upravljavec razmisli o uporabi priporočene pošte ali pa posamezniku, na katerega se nanašajo osebni podatki, ponudi

podatkov, in sistema obveščanja, ki upravljavca opozori na zahtevo, ki se nanaša na osebne podatke s kratkim obdobjem hrambe.

[21] To ne posega v naknadno obdelavo podatkov za namene dokazovanja v zvezi z obravnavo zahteve za dostop za ustrezno časovno obdobje.

neobvezujočo možnost, naj dokumente prevzame s podpisom neposredno v eni od njegovih poslovnih enot. Če se v skladu s členom 12(1) in (3) informacije zagotovijo z elektronskimi sredstvi, upravljavec izbere takšna, ki izpolnjujejo zahteve glede varnosti podatkov. Če se kopije podatkov zagotovijo v elektronski obliki, ki je splošno uporabljana (glej člen 15(3)), upravljavec pri izbiri načina za prenos elektronske datoteke posamezniku, na katerega se nanašajo osebni podatki, prav tako upošteva zahteve glede varnosti podatkov. To lahko vključuje šifriranje, zaščito z geslom itd. Za olajšanje dostopa do šifriranih podatkov bi moral upravljavec zagotoviti tudi, da so na voljo ustrezne informacije, ki posamezniku, na katerega se nanašajo osebni podatki, omogočajo dostop do dešifriranih informacij. Če bi bilo zaradi zahtev glede varnosti podatkov potrebno šifriranje elektronske pošte od konca do konca, upravljavec pa bi lahko poslal samo običajno elektronsko pošto, bo moral uporabiti druga sredstva, na primer s (priporočeno) pošto poslati ključ USB posamezniku, na katerega se nanašajo osebni podatki.

# 3 SPLOŠNI PREMISLEKI V ZVEZI S PRESOJO ZAHTEV ZA DOSTOP

## 3.1 Uvod

41. Upravljavec mora vsako zahtevo za dostop do osebnih podatkov presojati posamično ob prejemu. Upravljavec med drugim upošteva naslednja vprašanja, podrobneje opredeljena v odstavkih v nadaljevanju: ali se zahteva nanaša na osebne podatke, povezane z osebo, ki je predložila zahtevo, in kdo je ta oseba. Namen tega oddelka je pojasniti, katere elemente zahteve za dostop bi moral upravljavec upoštevati pri presojanju, ter obravnavati morebitne scenarije take presoje in njenih posledic. Upravljavec pri presoji zahteve za dostop do osebnih podatkov v skladu s členom 12(2) splošne uredbe o varstvu podatkov upošteva tudi obveznost olajšanja uresničevanja pravic posameznika, na katerega se nanašajo osebni podatki, pri čemer je pozoren na ustrezno varnost osebnih podatkov[22].

42. Zato bi morali biti upravljavci proaktivno pripravljeni obravnavati zahteve za dostop do osebnih podatkov. To pomeni, da bi moral biti upravljavec pripravljen, da zahtevo prejme, jo ustrezno presodi (ta presoja se obravnava v tem oddelku smernic) in osebi, ki jo je predložila, brez nepotrebnega odlašanja zagotovi ustrezen odgovor. Upravljavci bi se morali na izvajanje zahtev za dostop pripraviti ustrezno in sorazmerno ter ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov v skladu s členom 24 splošne uredbe o varstvu podatkov. Glede na posamezne okoliščine se lahko od upravljavcev na primer zahteva, da izvedejo ustrezen postopek, s čimer bi se morala zagotoviti varnost podatkov brez oviranja uresničevanja pravic posameznika, na katerega se nanašajo osebni podatki.

[22] Upravljavec zagotovi ustrezno varnost osebnih podatkov v skladu z načelom celovitosti in zaupnosti (člen 5(1)(f) splošne uredbe o varstvu podatkov) z izvajanjem ustreznih tehničnih in organizacijskih ukrepov, kot je navedeno v členu 32 splošne uredbe o varstvu podatkov in podrobneje opredeljeno v členu 24 splošne uredbe o varstvu podatkov. Upravljavec mora biti zmožen dokazati, da zagotavlja ustrezno raven varstva podatkov v skladu z načelom odgovornosti (glej tudi: Mnenje 3/2010 delovne skupine iz člena 29 o načelu odgovornosti, sprejeto 13. julija 2010, 00062/10/EN WP 173, in Smernice Evropskega odbora za varstvo podatkov 07/2020 o pojmih upravljavec in obdelovalec iz splošne uredbe o varstvu podatkov).

### 3.1.1 Analiza vsebine zahteve

43. To vprašanje je mogoče natančneje presoditi z zastavljanjem vprašanj, navedenih v nadaljevanju.

*a) Ali se zahteva nanaša na osebne podatke?*

44. V skladu s splošno uredbo o varstvu podatkov se zahteva nanaša le na osebne podatke[23]. Zato se kakršna koli zahteva po informacijah o drugih vprašanjih, vključno s splošnimi informacijami o upravljavcu, njegovih poslovnih modelih ali dejavnostih obdelave, ki niso povezane z osebnimi podatki, ne šteje za zahtevo, predloženo v skladu s členom 15 splošne uredbe o varstvu podatkov. Poleg tega v obseg pravice do dostopa ne spada zahteva za informacije o anonimnih podatkih ali podatkih, ki se ne nanašajo na osebo, ki je predložila zahtevo, ali osebo, v imenu katere je zahtevo predložila pooblaščena oseba. To vprašanje bo podrobneje analizirano v oddelku 4.

45. V nasprotju z anonimnimi podatki (ki niso osebni podatki) so psevdonimizirani podatki, ki jih je mogoče z uporabo dodatnih informacij pripisati fizični osebi, osebni podatki[24]. Zato je treba v okviru zahteve obravnavati psevdonimizirane podatke, ki jih je mogoče povezati s posameznikom, na katerega se nanašajo osebni podatki, npr. kadar posameznik, na katerega se nanašajo osebni podatki, zagotovi ustrezni identifikator, ki omogoča njegovo identifikacijo, ali kadar lahko upravljavec z lastnimi sredstvi podatke poveže z osebo, ki je predložila zahtevo[25].

*b) Ali se zahteva nanaša na osebo, ki je predložila zahtevo (ali osebo, v imenu katere pooblaščena oseba predloži zahtevo)?*

46. Praviloma se lahko zahteva nanaša le na podatke osebe, ki je zahtevo predložila. Dostop do podatkov drugih oseb se lahko zahteva le na podlagi ustreznega pooblastila[26].

**Primer 7:** Posameznik X, na katerega se nanašajo osebni podatki, dela kot vodja oddelka za podjetje, ki svojim vodjem zagotavlja parkirna mesta na parkirišču podjetja. Čeprav ima posameznik X, na katerega se nanašajo osebni podatki, stalno parkirno mesto, je na tem mestu že parkiran drug avtomobil, ko prispe v pisarno za svojo drugo izmeno. Ker se to ponavlja, posameznik, na katerega se nanašajo osebni podatki, upravljavca videonadzornega sistema, ki pokriva parkirišče podjetja, prosi za dostop do osebnih podatkov voznika, ki nepooblaščeno zaseda parkirno mesto, da bi ugotovil, kdo je. V takšnem primeru zahteva posameznika X, na katerega se nanašajo osebni podatki, ne bo zahteva za dostop do njegovih osebnih podatkov, saj se ne nanaša na podatke osebe, ki je zahtevo predložila, temveč na podatke druge osebe – zato se ne bi smela šteti za zahtevo v skladu s členom 15 splošne uredbe o varstvu podatkov.

*c) Ali se poleg splošne uredbe o varstvu podatkov uporabljajo tudi druge določbe, ki urejajo dostop do določene vrste podatkov?*

[23] Razen če zahteva zajema tudi neosebne podatke, neločljivo povezane z osebnimi podatki posameznika, na katerega se nanašajo osebni podatki. Za dodatna pojasnila glej odstavek 100.

[24] Glej uvodno izjavo 26 splošne uredbe o varstvu podatkov. Dodatna pojasnila o pojmih anonimni in psevdonimizirani podatki so na voljo v Mnenju 4/2007 delovne skupine iz člena 29 o pojmu osebni podatki, str. 18–21.

[25] Delovna skupina iz člena 29, WP 242, rev. 01, 5. april 2017, Smernice o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov), str. 9.

[26] Glej oddelek 3.4 („Zahteve, predložene prek tretjih oseb/pooblaščencev“).

47. Posameznikom, na katere se nanašajo osebni podatki, v zahtevi ni treba navesti pravne podlage. Če pa posamezniki, na katere se nanašajo osebni podatki, pojasnijo, da njihova zahteva temelji na sektorski ali nacionalni zakonodaji, ki ureja posebno vprašanje dostopa do določenih vrst podatkov, in ne na splošno uredbo o varstvu podatkov, upravljavec zahtevo po potrebi preuči v skladu s takšnimi sektorskimi ali nacionalnimi pravili. Odvisno od ustrezne nacionalne zakonodaje se lahko od upravljavcev pogosto zahteva, da predložijo ločene odgovore, od katerih vsak obravnava posebne zahteve, določene v različnih zakonodajnih aktih. To se ne sme zamenjevati z nacionalno zakonodajo ali zakonodajo EU, ki določa omejitve pravice do dostopa in jo je treba upoštevati pri odgovarjanju na zahteve za dostop.

48. Če upravljavec dvomi o tem, katero pravico želi uresničevati posameznik, na katerega se nanašajo osebni podatki, se priporoča, da se od njega zahteva pojasnilo, na kaj se zahteva nanaša. Takšna korespondenca s posameznikom, na katerega se nanašajo osebni podatki, ne vpliva na dolžnost upravljavca, da ukrepa brez nepotrebnega odlašanja[27]. Če v primeru dvoma upravljavec od posameznika, na katerega se nanašajo osebni podatki, zahteva dodatno pojasnilo, vendar ne prejme odgovora, bi si moral ob upoštevanju obveznosti olajšanja uresničevanja pravice do dostopa razložiti informacije iz prve zahteve in ukrepati na tej podlagi. Upravljavec lahko v skladu z načelom odgovornosti določi ustrezen časovni okvir, v katerem lahko posameznik, na katerega se nanašajo osebni podatki, zagotovi dodatno pojasnilo. Upravljavec bi moral tak časovni okvir določiti tako, da je na voljo dovolj časa za izpolnitev zahteve po njenem poteku, zato bi moral preučiti, koliko časa je objektivno potrebno, da se po tem, ko posameznik, na katerega se nanašajo osebni podatki, zagotovi podrobnejšo opredelitev (ali ne), zahtevani podatki pripravijo in zagotovijo.

49. Če zahteva spada na področje uporabe splošne uredbe o varstvu podatkov, obstoj takšne posebne zakonodaje ne prevlada nad splošno uporabo pravice do dostopa, kot je določena v splošni uredbi o varstvu podatkov. Pravo EU ali nacionalno pravo lahko določa omejitve, kadar to dovoljuje člen 23 splošne uredbe o varstvu podatkov (glej oddelek 6.4).

*d) <u>Ali zahteva spada na področje uporabe člena 15?</u>*

50. Opozoriti je treba, da splošna uredba o varstvu podatkov ne uvaja nobenih formalnih zahtev za osebe, ki zahtevajo dostop do podatkov. Za predložitev zahteve za dostop zadostuje, da osebe, ki zahtevajo dostop, navedejo, da želijo vedeti, katere osebne podatke v zvezi z njimi obdeluje upravljavec. Zato upravljavec ne more zavrniti zagotovitve podatkov z utemeljitvijo, da ni navedena pravna podlaga zahteve, zlasti posebno sklicevanje na pravico do dostopa ali splošno uredbo o varstvu podatkov.

Za predložitev zahteve bi na primer zadostovalo, da oseba, ki jo predloži, navede, da:

- želi pridobiti dostop do osebnih podatkov, ki se nanašajo nanjo;
- uveljavlja svojo pravico do dostopa; ali
- želi vedeti, katere informacije v zvezi z njo upravljavec obdeluje.

Upoštevati je treba, da prosilci morda niso seznanjeni s podrobnostmi splošne uredbe o varstvu podatkov in da je priporočljivo biti prizanesljiv do oseb, ki uveljavljajo svojo pravico do dostopa, zlasti kadar so to mladoletniki. Kot je navedeno zgoraj, se v primeru kakršnih koli dvomov priporoča, da upravljavec od posameznika, na katerega se nanašajo osebni podatki in ki je predložil zahtevo, zahteva, naj navede, na kaj se zahteva nanaša.

[27] Glej dodatne smernice o časovnem okviru v oddelku 5.3.

*e) Ali želijo posamezniki, na katere se nanašajo osebni podatki, dostopati do vseh informacij, ki se obdelujejo o njih, ali do njihovih delov?*

51. Upravljavec mora tudi oceniti, ali se zahteve oseb, ki so predložile zahtevo, nanašajo na vse informacije, ki se obdelujejo o njih, ali njihove dele. Vsaka omejitev področja uporabe zahteve, ki jo vložijo posamezniki, na katere se nanašajo osebni podatki, na posebno določbo člena 15 splošne uredbe o varstvu podatkov mora biti jasna in nedvoumna. Če na primer posamezniki, na katere se nanašajo osebni podatki, zahtevajo dobesedne „informacije o podatkih, ki se obdelujejo v zvezi z njimi“, bi moral upravljavec domnevati, da nameravajo uveljavljati svojo polno pravico iz člena 15(1) in (2) splošne uredbe o varstvu podatkov. Takšne zahteve se ne bi smelo razlagati, kot da želijo posamezniki, na katere se nanašajo osebni podatki, prejeti samo informacije o vrsti osebnih podatkov, ki se obdelujejo, in se odpovedati pravici do prejema informacij iz člena 15(1)(a) do (h). Drugače bi bilo, na primer, če bi posamezniki, na katere se nanašajo osebni podatki, v zvezi s podatki, ki jih navedejo, želeli dostop do informacij o viru ali izvoru osebnih podatkov ali določenem obdobju hrambe. V takšnem primeru lahko upravljavec svoj odgovor omeji na zadevne zahtevane informacije.

### 3.1.2 Oblika zahteve

52. Kot je bilo že navedeno, splošna uredba o varstvu podatkov posameznikom, na katere se nanašajo osebni podatki, ne nalaga nobenih zahtev glede oblike zahteve za dostop do osebnih podatkov. Zato v skladu s splošno uredbo o varstvu podatkov načeloma ni zahtev, ki bi jih morali posamezniki, na katere se nanašajo osebni podatki, upoštevati pri izbiri komunikacijskega kanala, prek katerega stopijo v stik z upravljavcem.

53. Evropski odbor za varstvo podatkov spodbuja upravljavce, naj zagotovijo najustreznejše in uporabnikom prijazne komunikacijske kanale v skladu s členom 12(2) in členom 25 splošne uredbe o varstvu podatkov, da se posamezniku, na katerega se nanašajo osebni podatki, omogoči predložitev veljavne zahteve. Če posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži prek komunikacijskega kanala, ki ga zagotovi upravljavec[28] in se razlikuje od tistega, ki je bil naveden kot zaželen, se takšna zahteva kljub temu na splošno šteje za veljavno in upravljavec bi jo moral ustrezno obravnavati (glej primere v nadaljevanju). Upravljavci bi si morali razumno prizadevati, da se olajša uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki (če na primer posameznik, na katerega se nanašajo osebni podatki, pošlje zahtevo za dostop zaposlenemu, ki je na dopustu, bi razumno prizadevanje lahko predstavljalo samodejno sporočilo, s katerim se posameznika, na katerega se nanašajo osebni podatki, obvesti o drugem komunikacijskem kanalu za njegovo zahtevo).

54. Opozoriti je treba, da upravljavcu ni treba ukrepati v zvezi z zahtevo, poslano na naključni ali nepravilni elektronski (ali poštni) naslov, ki ga upravljavec ni sporočil neposredno, ali na kateri koli komunikacijski kanal, ki očitno ni namenjen prejemanju zahtev v zvezi s pravicami posameznika, na katerega se nanašajo osebni podatki, če je upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotovil ustrezen komunikacijski kanal.

55. Upravljavcu tudi ni treba ukrepati v zvezi z zahtevo, poslano na elektronski naslov njegovega zaposlenega, ki morda ne sodeluje pri obdelavi zahtev v zvezi s pravicami posameznikov, na katere se nanašajo osebni podatki (npr. vozniki, čistilno osebje itd.). Takšne zahteve se ne štejejo za veljavne, če

[28] To lahko na primer vključuje komunikacijske podatke upravljavca, navedene v njegovih sporočilih, naslovljenih neposredno na posameznike, na katere se nanašajo osebni podatki, ali kontaktne podatke, ki jih objavi upravljavec, na primer v svoji politiki zasebnosti ali drugih obveznih pravnih obvestilih (npr. kontaktni podatki o lastniku ali podjetju na spletnem mestu).

je upravljavec posamezniku, na katerega se nanašajo osebni podatki, jasno zagotovil ustrezen komunikacijski kanal. Če pa posameznik, na katerega se nanašajo osebni podatki, pošlje zahtevo zaposlenemu pri upravljavcu, ki mu je bil dodeljen kot redna kontaktna oseba (npr. skrbnik osebnega računa v banki ali stalni svetovalec pri operaterju mobilne telefonije), se tak stik ne bi smel šteti za naključnega, upravljavec pa bi si moral po najboljših močeh prizadevati za obravnavo takšne zahteve, tako da jo je mogoče preusmeriti na kontaktno točko in nanjo odgovoriti v rokih, določenih v splošni uredbi o varstvu podatkov.

56. Evropski odbor za varstvo podatkov kljub temu kot dobro prakso priporoča, naj upravljavci uvedejo ustrezne mehanizme za lažje uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, vključno s sistemi za samodejni odgovor za obveščanje o odsotnosti osebja in ustreznih nadomestnih osebah za stik ter, kjer je mogoče, mehanizme za izboljšanje notranje komunikacije med zaposlenimi v zvezi z zahtevami, ki jih prejmejo tisti, ki morda niso pristojni za njihovo obravnavo.

**Primer 8**: Upravljavec X ima na svojem spletnem mestu in v izjavi o varstvu osebnih podatkov navedena dva elektronska naslova – splošni elektronski naslov upravljavca: KONTAKT@X.COM in elektronski naslov kontaktne točke upravljavca za varstvo podatkov: VPRAŠANJA@X.COM. Poleg tega upravljavec X na svojem spletnem mestu navaja, da bi se morali posamezniki za vložitev poizvedb ali zahtev v zvezi z obdelavo osebnih podatkov obrniti na kontaktno točko za varstvo podatkov prek navedenega elektronskega naslova. Vendar posameznik, na katerega se nanašajo osebni podatki, pošlje zahtevo na splošni elektronski naslov upravljavca: KONTAKT@X.COM.

V takem primeru bi si moral upravljavec razumno prizadevati, da bi bile njegove službe seznanjene z zahtevo, predloženo prek splošne elektronske pošte, da bi jo bilo mogoče preusmeriti na kontaktno točko za varstvo podatkov in nanjo odgovoriti v rokih, določenih v splošni uredbi o varstvu podatkov. Poleg tega upravljavec ne more podaljšati roka za odgovor na zahtevo zgolj zato, ker je posameznik, na katerega se nanašajo osebni podatki, poslal zahtevo na njegov splošni elektronski naslov in ne na elektronski naslov njegove kontaktne točke za varstvo podatkov.

**Primer 9**: Upravljavec Y vodi mrežo fitnes klubov. Na svojem spletnem mestu in v izjavi o varstvu osebnih podatkov za stranke fitnes kluba navaja, da bi morali posamezniki za predložitev poizvedb ali zahteve v zvezi z obdelavo osebnih podatkov z njim stopiti v stik prek elektronskega naslova: VPRAŠANJA@Y.COM. Kljub temu posameznik, na katerega se nanašajo osebni podatki, zahtevek pošlje na elektronski naslov, ki ga je našel v obvestilu v garderobi, ki se glasi: „Če niste zadovoljni s čistočo dvorane, nam pišite na naslov: ČISTILCI@Y.COM“, ki je elektronski naslov čistilnega osebja, zaposlenega pri Y. Čistilno osebje seveda ne sodeluje pri obravnavi zadev v zvezi z uresničevanjem pravic posameznikov, na katere se nanašajo osebni podatki – strank fitnes kluba. Čeprav je bil elektronski naslov na voljo v prostorih fitnes kluba, posameznik, na katerega se nanašajo osebni podatki, ni mogel razumno pričakovati, da je bil to ustrezen kontaktni naslov za takšne zahteve, saj je na spletnem mestu in izjavi o varstvu osebnih podatkov jasno naveden komunikacijski kanal, ki se uporablja za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki.

57. Na dan, ko upravljavec prejme zahtevo, praviloma začne teči enomesečni rok, v katerem mora upravljavec zagotoviti informacije o ukrepih, sprejetih v zvezi z zahtevo, v skladu s členom 12(3) splošne uredbe o varstvu podatkov (nadaljnje smernice o časovnem okviru so navedene v oddelku 5.3). Evropski odbor za varstvo podatkov meni, da je dobra praksa za upravljavce, da pisno potrdijo prejem zahtev, na primer tako, da osebam, ki so zahtevo predložile, pošljejo elektronsko pošto (ali informacije

po pošti, če je ustrezno), ki potrjuje, da je bila zahteva prejeta in da enomesečno obdobje traja od dneva X do dneva Y.

## 3.2 Identifikacija in avtentifikacija

58. Za zagotovitev varnosti obdelave in zmanjšanje tveganja nepooblaščenega razkritja osebnih podatkov mora biti upravljavec zmožen ugotoviti, kateri podatki zadevajo posameznika, na katerega se nanašajo osebni podatki (identifikacija), in potrditi identiteto te osebe (avtentifikacija).

59. Opozoriti velja, da če identifikacija posameznika, na katerega se nanašajo osebni podatki, ni potrebna ali ni več potrebna za namen, za katerega se obdelujejo osebni podatki, upravljavcu ni treba izvajati identifikacije samo zaradi zagotavljanja skladnosti s pravicami posameznikov, na katere se nanašajo osebni podatki, upoštevajoč tudi načelo najmanjšega obsega podatkov. Ti primeri so obravnavani v členu 11(1) splošne uredbe o varstvu podatkov.

60. Člen 12(2) splošne uredbe o varstvu podatkov določa, da upravljavec ne zavrne ukrepanja na zahtevo posameznika, na katerega se nanašajo osebni podatki, za uresničevanje njegovih pravic, razen če upravljavec obdeluje osebne podatke za namen, za katerega identifikacije posameznika, na katerega se nanašajo osebni podatki, ni potrebna, in dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki. V takšnih okoliščinah se lahko posameznik, na katerega se nanašajo osebni podatki, odloči, da bo zagotovil dodatne informacije, s katerimi ga je mogoče identificirati (člen 11(2) splošne uredbe o varstvu podatkov)[29].

61. Upravljavec ni dolžan pridobiti takšnih dodatnih informacij, da bi identificiral posameznika, na katerega se nanašajo osebni podatki, zgolj zaradi skladnosti z zahtevo tega posameznika, upoštevajoč tudi načelo najmanjšega obsega podatkov. Vendar pa upravljavec ne bi smel zavrniti takšnih dodatnih informacij, ki jih posameznik, na katerega se nanašajo osebni podatki, predloži v pomoč pri uresničevanju svojih pravic (uvodna izjava 57 splošne uredbe o varstvu podatkov).

**Primer 10**: X je upravljavec podatkov, obdelanih v zvezi z videonadzorom stavbe. V skladu s členom 11(1) splošne uredbe o varstvu podatkov upravljavec ni dolžan identificirati vseh oseb, posnetih z varnostno kamero v okviru spremljanja (namen, ki ne zahteva identifikacije). Upravljavec prejme zahtevo za dostop do osebnih podatkov od osebe, ki trdi, da je bila posneta z videonadzorno kamero upravljavca. Ukrepi upravljavca bodo odvisni od dodatnih predloženih informacij. Če oseba, ki predloži zahtevo, navede točen dan in uro, ko naj bi kamere posnele zadevni dogodek, bo upravljavec verjetno lahko zagotovil te podatke (člen 11(2) splošne uredbe o varstvu podatkov). Če pa upravljavec ne more identificirati posameznika, na katerega se nanašajo osebni podatki (npr. ne more biti prepričan, da je oseba, ki zahteva podatke, dejansko posameznik, na katerega se nanašajo osebni podatki, ali če se na primer zahteva nanaša na dolg posnetek in upravljavec ne more obdelati tako velike količine podatkov), lahko upravljavec zavrne ukrepanje, če dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki (člen 12(2) splošne uredbe o varstvu podatkov).

**Primer 11:** Upravljavec C obdeluje osebne podatke za namene vedenjskega ciljanja na svoje spletne uporabnike. Osebni podatki se za vedenjsko ciljanje običajno zbirajo s piškotki in so povezani z naključnimi psevdonimnimi identifikatorji. Gospod X, na katerega se nanašajo osebni podatki, uresničuje svojo pravico do dostopa pri C prek spletnega mesta C. C lahko natančno identificira

[29] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 13.

gospoda X za prikaz vedenjskega ciljanja na posameznika, na katerega se nanašajo osebni podatki, tako da terminalsko opremo gospoda X poveže z njegovim oglaševalskim profilom s piškotki, shranjenimi na terminalu. C bi moral biti zmožen tudi natančno identificirati gospoda X, da mu omogoči dostop do njegovih osebnih podatkov, saj je mogoče najti povezavo med obdelanimi podatki in posameznikom, na katerega se nanašajo osebni podatki. Zato ob upoštevanju načel splošne uredbe o varstvu podatkov zgornji primer ne bi spadal na področje uporabe člena 11 navedene uredbe. Natančneje, v zgornjem primeru namen C zahteva identifikacijo posameznikov, na katere se nanašajo osebni podatki, medtem ko člen 11 splošne uredbe o varstvu podatkov obravnava primer obdelave, ki ne zahteva identifikacije, pri čemer upravljavec ni zavezan obdelovati dodatnih podatkov v smislu člena 11(1) splošne uredbe o varstvu podatkov zgolj zaradi zmožnosti zagotavljanja skladnosti s splošno uredbo o varstvu podatkov. Posledično se v nekaterih primerih ne bi smeli zahtevati nobeni dodatni podatki za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki.

Če pa gospod X poskuša uresničevati svojo pravico do dostopa po elektronski ali navadni pošti, C v tem okviru ne bo imel druge izbire, kot da od njega zahteva „dodatne informacije“ (člen 12(6) splošne uredbe o varstvu podatkov), da bi lahko prepoznal oglaševalski profil, povezan z gospodom X. V tem primeru bo dodatna informacija identifikator piškotkov, shranjen v terminalski opremi gospoda X.

62. Kadar upravljavec dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki (člen 11 splošne uredbe o varstvu podatkov), mora slednjega, ustrezno obvestiti, če je to mogoče, saj mora upravljavec na zahteve posameznika, na katerega se nanašajo osebni podatki, odgovoriti brez nepotrebnega odlašanja in kadar ne namerava izpolniti takih zahtev, mora to utemeljiti. Te informacije je treba zagotoviti le „če je to mogoče“, saj upravljavec posameznikov, na katere se nanašajo osebni podatki, morda ne more obvestiti, če jih ne more identificirati.

63. Kadar ima upravljavec upravičen dvom v zvezi z identiteto posameznika, ki predloži zahtevo, lahko zahteva zagotovitev dodatnih informacij, ki so potrebne za potrditev identitete posameznika, na katerega se nanašajo osebni podatki, ne glede na to, ali obdelava zahteva identifikacijo ali ne (člen 12(6) splošne uredbe o varstvu podatkov).

64. v splošni uredbi o varstvu podatkov ni zahtev glede avtentikacije posameznika, na katerega se nanašajo osebni podatki. Vendar člena 11 in 12 splošne uredbe o varstvu podatkov opredeljujeta pogoje za uresničevanje vseh pravic posameznika, na katerega se nanašajo osebni podatki, vključno s pravico do dostopa do osebnih podatkov.

65. Opozoriti je treba, da upravljavec praviloma ne more zahtevati več osebnih podatkov, kot jih potrebuje za avtentikacijo, in da bi morala biti uporaba takšnih informacij strogo omejena na izpolnitev zahteve posameznikov, na katere se nanašajo osebni podatki.

66. Med posamezniki, na katere se nanašajo osebni podatki, in upravljavci so pogosto že vzpostavljeni postopki avtentikacije. Upravljavci lahko te postopke avtentikacije uporabijo za preverjanje identitete posameznikov, na katere se nanašajo osebni podatki, ki zahtevajo svoje osebne podatke ali uresničujejo pravice s splošno uredbo o varstvu podatkov[30]. V nasprotnem primeru bi morali upravljavci v ta namen izvesti postopek avtentikacije[31].

67. Upravljavec vsakič, ko zahteva dodatne informacije, potrebne za potrditev identitete posameznika, na katerega se nanašajo osebni podatki, ali ko mu ta posameznik takšne informacije zagotovi, oceni,

[30] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 14.

[31] Glej dodatne smernice o avtentikaciji v oddelku 3.3.

katere informacije mu bodo omogočile, da potrdi identiteto posameznika, na katerega se nanašajo osebni podatki, in osebi, ki predloži zahtevo, morda postavi dodatna vprašanja ali od posameznika, na katerega se nanašajo osebni podatki, zahteva, naj predloži nekatere dodatne identifikacijske elemente, če je to sorazmerno (glej oddelek 3.3).

68. Da bi lahko posameznik, na katerega se nanašajo osebni podatki, zagotovil dodatne informacije, potrebne za identifikacijo njegovih podatkov, bi mu moral upravljavec sporočiti naravo dodatnih informacij, potrebnih za identifikacijo. Takšne dodatne informacije ne bi smele presegati informacij, ki so bile prvotno potrebne za avtentikacijo posameznika, na katerega se nanašajo osebni podatki. Dejstvo, da lahko upravljavec zahteva dodatne informacije za oceno identitete posameznika, na katerega se nanašajo osebni podatki, na splošno ne more voditi do čezmernih zahtev in zbiranja osebnih podatkov, ki niso relevantni ali potrebni za krepitev povezave med posameznikom in zahtevanimi osebnimi podatki[32].

69. Zato lahko upravljavec, kadar so informacije, zbrane prek spleta, povezane s psevdonimi ali drugimi edinstvenimi identifikatorji, izvede ustrezne postopke, ki posamezniku omogočajo, da predloži zahtevo za dostop do podatkov in prejme podatke v zvezi z njim[33].

**Primer 12:** Gospa X, na katero se nanašajo osebni podatki, v telefonskem pogovoru s svetovalcem za pomoč strankam elektroenergetskega podjetja, s katerim je sklenila pogodbo, zaprosi za dostop do svojih podatkov. Svetovalec dvomi o identiteti osebe, ki je predložila zahtevo, zato v sistemu podjetja ustvari enkratno edinstveno kodo, ki se pošlje na uporabnikovo mobilno številko, navedeno v okviru sistema za dvojno preverjanje ob odprtju računa, kar bi bilo treba v tem primeru šteti za sorazmerno dejanje.

## 3.3 Ocena sorazmernosti v zvezi z avtentikacijo osebe, ki je predložila zahtevo

70. Kot je navedeno zgoraj, lahko upravljavec, če ima utemeljene razloge za dvom o identiteti osebe, ki je predložila zahtevo, zahteva dodatne informacije za potrditev identitete posameznika, na katerega se nanašajo osebni podatki. Vendar mora upravljavec hkrati zagotoviti, da ne zbere več osebnih podatkov, kot je potrebno za avtentikacijo osebe, ki je predložila zahtevo. Zato upravljavec izvede oceno sorazmernosti, ki mora upoštevati vrsto osebnih podatkov, ki se obdelujejo (npr. posebne vrste podatkov ali ne), naravo zahteve, okoliščine, v katerih se zahteva predloži, in vso škodo, ki bi lahko nastala zaradi nepravilnega razkritja. Velja opozoriti, da se je treba pri ocenjevanju sorazmernosti izogibati pretiranemu zbiranju podatkov in hkrati zagotoviti ustrezno raven varnosti obdelave.

71. Upravljavec bi moral izvesti postopek avtentikacije, da bi se prepričal o identiteti oseb, ki zahtevajo dostop do svojih podatkov[34], in zagotavljati varnost obdelave med celotnim postopkom obravnave zahtev za dostop v skladu s členom 32 splošne uredbe o varstvu podatkov, vključno na primer z varnim kanalom, prek katerega lahko posamezniki, na katere se nanašajo osebni podatki, zagotovijo dodatne informacije. Metoda, ki se uporablja za avtentikacijo, bi morala biti ustrezna, primerna, sorazmerna in v skladu z načelom najmanjšega obsega podatkov. Če upravljavec uvede obremenjujoče ukrepe za avtentikacijo posameznika, na katerega se nanašajo osebni podatki, mora to ustrezno utemeljiti in

[32] Prav tam, str. 14.
[33] Prav tam, str. 13 in 14.
[34] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 14.

zagotoviti skladnost z vsemi temeljnimi načeli, vključno z načelom najmanjšega obsega podatkov in obveznostjo olajšanja uresničevanja pravic posameznikov, na katere se nanašajo osebni podatki (člen 12(2) splošne uredbe o varstvu podatkov).

72. V spletnem okolju lahko mehanizem avtentikacije vključuje isto poverilnico, ki jo posameznik, na katerega se nanašajo osebni podatki, uporablja za prijavo na spletno storitev, ki jo ponuja upravljavec (uvodna izjava 57 splošne uredbe o varstvu podatkov)[35].

73. V praksi pogosto obstajajo postopki avtentikacije in upravljavcem ni treba uvesti dodatnih zaščitnih ukrepov za preprečevanje nepooblaščenega dostopa do storitev. Upravljavci za dostop posameznikov do podatkov v njihovih računih (kot so e-poštni račun, račun na družbenih omrežjih ali v spletni trgovini) najverjetneje zahtevajo prijavo z uporabniškim imenom in geslom, kar bi moralo v takih primerih zadostovati za avtentikacijo posameznika, na katerega se nanašajo osebni podatki[36]. Poleg tega upravljavec avtentikacijo posameznikov, na katere se nanašajo osebni podatki, pogosto izvede, že preden z njimi sklene pogodbo ali pridobi njihovo privolitev v obdelavo, zato se osebni podatki, ki se uporabijo za registracijo posameznika, na katerega se nanaša obdelava, lahko uporabijo tudi kot dokaz za avtentikacijo posameznika, na katerega se nanašajo osebni podatki, za namene prenosljivosti[37]. Zato je nesorazmerno zahtevati kopijo osebnega dokumenta, če je upravljavec že avtenticiral posameznika, na katerega se nanašajo osebni podatki in ki je predložil zahtevo.

74. Poudariti je treba, da lahko uporaba kopije osebnega dokumenta v okviru postopka avtentikacije povzroči tveganje za varnost osebnih podatkov in privede do nepooblaščene ali nezakonite obdelave, zato bi jo bilo treba šteti za neustrezno, razen če je potrebna, ustrezna in v skladu z nacionalnim pravom. V takšnih primerih bi morali imeti upravljavci vzpostavljene sisteme, ki pri prejemu takšnih podatkov zagotavljajo ustrezno raven varnosti za ublažitev večjih tveganj za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki. Pomembno je tudi opozoriti, da avtentikacija z osebno izkaznico ni nujno v pomoč v spletnem okolju (npr. z uporabo psevdonimov), če zadevna oseba ne more predložiti nobenega drugega dokaza, npr. dodatnih značilnosti, ki se ujemajo z uporabniškim računom.

75. Čeprav številne organizacije (npr. hoteli, banke, družbe, ki ponujajo izposojo vozil) od svojih strank zahtevajo kopijo osebne izkaznice, se to na splošno ne bi smelo šteti za ustrezen način avtentikacije. Namesto tega lahko upravljavec izvede hiter in učinkovit varnostni ukrep za identifikacijo posameznika, na katerega se nanašajo osebni podatki, na podlagi predhodne avtentikacije, npr. prek elektronske pošte ali besedilnega sporočila, ki vsebuje potrditvene povezave, varnostna vprašanja ali potrditvene kode[38].

76. Informacije na osebnem dokumentu, ki na podlagi presoje posameznega primera niso potrebne za potrditev identitete posameznika, na katerega se nanašajo osebni podatki, kot so številka za dostop in

---

[35] Glej dodatne smernice o metodah avtentikacije v Smernicah Evropskega odbora za varstvo podatkov 01/2021 o primerih v zvezi z uradnim obveščanjem o kršitvah varstva podatkov, sprejetih 14. januarja 2021, str. 30–31, in v Smernicah Evropskega odbora za varstvo podatkov 02/2021 o virtualnih glasovnih pomočnikih, različica 2.0, sprejetih 7. julija 2021, oddelek 3.7.

[36] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 14.

[37] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 14.

[38] Glej tudi Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES, ki je uvedla različne storitve za varno identifikacijo na daljavo.

serijska številka, državljanstvo, velikost, barva oči, fotografija in strojno berljivi del, lahko posameznik, na katerega se nanašajo osebni podatki, prekrije ali zakrije, preden jih predloži upravljavcu, razen če nacionalna zakonodaja zahteva popolno neredigirano kopijo osebne izkaznice (glej odstavek 78 v nadaljevanju). Datum izdaje ali poteka veljavnosti, izdajatelj in polno ime, ki se ujema s spletnim računom, na splošno zadostujejo, da upravljavec preveri identiteto, pri čemer morata biti vedno zagotovljena avtentičnost kopije in razmerje do osebe, ki je predložila zahtevo. Dodatne informacije, kot je rojstni datum posameznika, na katerega se nanašajo osebni podatki, se lahko zahtevajo le, če še vedno obstaja tveganje napačne identitete in če jih upravljavec lahko primerja z informacijami, ki jih že obdeluje.

77. Upravljavec bi moral zaradi skladnosti z načelom najmanjšega obsega podatkov posameznika, na katerega se nanašajo osebni podatki, obvestiti o informacijah, ki niso potrebne, in o možnosti, da se ti deli osebnega dokumenta prekrijejo ali zakrijejo. Če posameznik, na katerega se nanašajo osebni podatki, v takšnem primeru ne ve, kako zakriti takšne informacije ali tega ne more storiti, je dobra praksa, da upravljavec te informacije prekrije ob prejemu dokumenta, če je to mogoče glede na sredstva, ki so mu na voljo v danih okoliščinah.

**Primer 13:** Uporabnica, oseba Y, je v spletni trgovini ustvarila račun, zaščiten z geslom, pri čemer je navedla svoj e-naslov in/ali uporabniško ime. Lastnica računa upravljavca nato zaprosi za informacije o tem, ali obdeluje njene osebne podatke, in če jih, prosi za dostop do njih v okviru iz člena 15. Upravljavec zahteva osebni dokument osebe, ki predloži zahtevo, da potrdi njeno identiteto. Ukrep upravljavca je v tem primeru nesorazmeren in vodi v nepotrebno zbiranje podatkov.

Da bi potrdil identiteto osebe, ki zahteva podatke, in hkrati preprečil nepotrebno zbiranje podatkov, bi upravljavec lahko zahteval, da se oseba avtenticira prek prijave na račun, ali ji postavil (nevsiljiva) varnostna vprašanja, na katera bi znal odgovoriti le posameznik, na katerega se nanašajo osebni podatki, ali pa uporabil večfaktorsko avtentikacijo, konfigurirano, ko je posameznik, na katerega se nanašajo osebni podatki, registriral svoj račun, ali druga obstoječa komunikacijska sredstva za pošiljanje gesla za dostop, za katera je znano, da pripadajo posamezniku, na katerega se nanašajo osebni podatki, kot sta elektronski naslov ali telefonska številka.

**Primer 14:** Stranka banke, gospod Y, namerava pridobiti potrošniški kredit. S tem namenom gospod Y obišče bančno poslovalnico, da bi pridobil informacije, vključno s svojimi osebnimi podatki, ki so potrebne za oceno njegove kreditne sposobnosti. Da bi preveril identiteto posameznika, na katerega se nanašajo osebni podatki, svetovalec prosi za notarsko overitev identitete, da mu lahko zagotovi zahtevane informacije.

Upravljavec ne bi smel zahtevati notarske overitve identitete, razen če je to potrebno, ustrezno in v skladu z nacionalnim pravom (na primer, kadar oseba začasno nima nobenega osebnega dokumenta in nacionalno pravo za izvedbo pravnega dejanja zahteva dokazilo o identiteti posameznika, na katerega se nanašajo osebni podatki). Zaradi takšne prakse so osebe, ki predložijo zahtevo, izpostavljene dodatnim stroškom, posameznikom, na katere se nanašajo osebni podatki, pa je naloženo preveliko breme, kar ovira uresničevanje njihove pravice do dostopa.

78. Brez poseganja v zgoraj navedena splošna načela je lahko avtentikacija na podlagi osebnega dokumenta v določenih okoliščinah upravičen in sorazmeren ukrep, zlasti če se obdelujejo posebne vrste osebnih podatkov ali če obdelava podatkov lahko pomeni tveganje za posameznika, na katerega se nanašajo osebni podatki (npr. zdravstvene informacije). Vendar je treba hkrati upoštevati, da nekatere nacionalne določbe predpisujejo omejitve obdelave podatkov, ki jih vsebujejo javne listine,

vključno z dokumenti, ki potrjujejo identiteto osebe (tudi na podlagi člena 87 splošne uredbe o varstvu podatkov). Omejitve obdelave podatkov iz teh dokumentov se lahko nanašajo zlasti na optično branje ali fotokopiranje osebnih izkaznic ali obdelavo uradnih osebnih identifikacijskih številk[39].

79. Ob upoštevanju navedenega mora upravljavec, kadar se zahteva osebni dokument (kar je v skladu z nacionalnim pravom ter upravičeno in sorazmerno na podlagi splošne uredbe o varstvu podatkov), uvesti zaščitne ukrepe za preprečevanje nezakonite obdelave osebnega dokumenta. Ne glede na morebitne veljavne nacionalne določbe o avtentikaciji identitete, lahko to vključuje opustitev izdelave kopije ali brisanje kopije osebnega dokumenta takoj po uspešni avtentikaciji identitete posameznika, na katerega se nanašajo osebni podatki. Razlog za to je, da bi nadaljnja hramba kopije osebnega dokumenta verjetno pomenila kršitev načel omejitve namena in omejitve hrambe (člen 5(1)(b) in (e) splošne uredbe o varstvu podatkov) ter tudi nacionalne zakonodaje o obdelavi nacionalne identifikacijske številke (člen 87 splošne uredbe o varstvu podatkov). Evropski odbor za varstvo podatkov kot dobro prakso priporoča, naj si upravljavec po preverjanju osebne izkaznice to zabeleži, npr. „osebna izkaznica je bila preverjena“, da prepreči nepotrebno kopiranje ali shranjevanje kopij osebnih izkaznic.

### 3.4 Zahteve, vložene prek tretjih oseb/pooblaščencev

80. Čeprav pravico do dostopa običajno uveljavljajo posamezniki, na katere se nanašajo osebni podatki, lahko zahtevo v imenu posameznika, na katerega se nanašajo osebni podatki, predloži tudi tretja oseba. To lahko med drugim velja za zahteve, ki se v imenu mladoletnikov predložijo prek pooblaščenca ali zakonitih skrbnikov, pa tudi drugih subjektov prek spletnih portalov. V nekaterih okoliščinah je lahko potrebno preverjanje identitete osebe, pooblaščene za uresničevanje pravice do dostopa, in pooblastila za delovanje v imenu posameznika, na katerega se nanašajo osebni podatki, če je to ustrezno in sorazmerno (glej oddelek 3.3 zgoraj)[40]. Opozoriti je treba, da lahko predložitev osebnih podatkov osebi, ki nima pravice dostopa do njih, pomeni kršitev varstva osebnih podatkov[41].

81. Pri tem bi bilo treba upoštevati nacionalne zakone, ki urejajo pravno zastopanje (npr. pooblastila), v katerih so lahko določene posebne zahteve za dokazovanje pooblastila za predložitev zahteve v imenu posameznika, na katerega se nanašajo osebni podatki, saj splošna uredba o varstvu podatkov tega vprašanja ne ureja. V skladu z načelom odgovornosti in drugimi načeli varstva podatkov morajo biti upravljavci zmožni dokazati obstoj ustreznega pooblastila za predložitev zahteve v imenu posameznika, na katerega se nanašajo osebni podatki, in za prejem zahtevanih informacij, razen če nacionalno pravo določa drugače (npr. nacionalno pravo vsebuje posebna pravila o verodostojnosti odvetnikov), pri čemer upravljavec preveri identiteto pooblaščenca (npr. če je to odvetnik, upravljavec preveri vpis v imenik odvetnikov). Zato se priporoča, da se v tem smislu zbere ustrezna dokumentacija v zvezi s predhodno navedenimi splošnimi pravili glede potrditve identitete fizične osebe, ki predloži zahtevo, in če upravljavec upravičeno dvomi o identiteti osebe, ki deluje v imenu posameznika, na katerega se nanašajo osebni podatki, zahteva dodatne informacije, da potrdi identiteto te osebe.

82. Uresničevanje pravice dostopa do osebnih podatkov umrlih oseb je še en primer dostopa tretje osebe, ki ni posameznik, na katerega se nanašajo osebni podatki, vendar je v uvodni izjavi 27 splošne uredbe o varstvu podatkov navedeno, da se navedena uredba ne uporablja za osebne podatke umrlih oseb.

---

[39] Več držav članic je v zvezi s tem v svoje nacionalne določbe vključilo takšno omejitev, pri čemer so na primer navedle, da je kopiranje osebnih izkaznic zakonito le, če izhaja neposredno iz določb pravnega akta.
[40] Glede rokov za uveljavljanje pravice do dostopa, kadar mora upravljavec pridobiti dodatne informacije, glej odstavek 157.
[41] Člen 4(12) splošne uredbe o varstvu podatkov.

Zadeva je torej obravnavana v nacionalnem pravu, države članice pa lahko določijo pravila o obdelavi osebnih podatkov umrlih oseb. Vendar je treba upoštevati, da se lahko podatki nanašajo tudi na žive tretje osebe, na primer v okviru zahtevanega dostopa do korespondence pokojne osebe. Zaupnost takih podatkov je treba še vedno zaščititi.

### 3.4.1 Uresničevanje pravice do dostopa v imenu otrok

83. Otroci si zaslužijo posebno varstvo v zvezi s svojimi osebnimi podatki, saj se morda manj zavedajo zadevnih tveganj, posledic in zaščitnih ukrepov ter svojih pravic v zvezi z obdelavo osebnih podatkov[42]. Vse informacije in komunikacija, pri katerih se obdelava nanaša na osebne podatke otroka, bi morale biti v jasnem in preprostem jeziku, da ga lahko otrok zlahka razume[43].

84. Otroci so tudi sami posamezniki, na katere se nanašajo osebni podatki, zato jim pripada pravica do dostopa. Tretja oseba, ki deluje v imenu otroka, npr. nosilec starševske odgovornosti, je lahko potrebna glede na zrelost in zmožnost otroka.

85. Pri vseh odločitvah v zvezi z uresničevanjem pravice otroka do dostopa bi bilo treba upoštevati predvsem njegov interes, zlasti kadar to pravico v imenu otroka uresničuje na primer nosilec starševske odgovornosti.

86. Zaradi posebnega varstva osebnih podatkov otrok na podlagi splošne uredbe o varstvu podatkov upravljavec sprejme ustrezne ukrepe, da prepreči kakršno koli razkritje osebnih podatkov mladoletnika nepooblaščeni osebi (v zvezi s tem glej tudi oddelek 3.4 zgoraj).

87. Nazadnje, pravice nosilca starševske odgovornosti, da deluje v imenu otroka, ne bi smeli zamenjevati s primeri zunaj prava o varstvu podatkov, kadar lahko nacionalna zakonodaja nosilcu starševske odgovornosti dodeljuje pravico, da zahteva in prejme informacije o otroku (npr. uspeh otroka v šoli).

### 3.4.2 Uresničevanje pravice do dostopa prek portalov/kanalov, ki jih zagotavlja tretja oseba

88. Nekatera podjetja zagotavljajo storitve, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo, da predložijo zahteve za dostop prek portala. Posameznik, na katerega se nanašajo osebni podatki, se prijavi in dobi dostop do portala, prek katerega lahko na primer predloži zahtevo za dostop ali zahteva popravek ali izbris podatkov od različnih upravljavcev. Zaradi uporabe portalov, ki jih zagotavlja tretja oseba, se pojavljajo različna vprašanja.

89. Prvo vprašanje, ki ga morajo upravljavci obravnavati v teh okoliščinah, je zagotavljanje, da tretja oseba zakonito deluje v imenu posameznika, na katerega se nanašajo osebni podatki, saj je treba zagotoviti, da se podatki ne razkrijejo nepooblaščenim osebam.

90. Poleg tega mora upravljavec zahtevo, katero prejme prek takšnega portala, vedno pravočasno obravnavati[44]. Vendar v skladu s členom 15 splošne uredbe o varstvu podatkov upravljavec podatkov ni dolžan zagotoviti neposredno portalu, če na primer ugotovi, da varnostni ukrepi niso zadostni ali če

---

[42] Uvodna izjava 38 splošne uredbe o varstvu podatkov. Kot je navedeno v delovnem programu Evropskega odbora za varstvo podatkov, je njegov namen zagotoviti smernice o podatkih otrok. Tak dokument naj bi zagotovil več smernic o pogojih, pod katerimi lahko otrok uresničuje svojo pravico do dostopa, nosilec starševske odgovornosti pa lahko uveljavlja pravico do dostopa v njegovem imenu.

[43] Uvodna izjava 58 splošne uredbe o varstvu podatkov. Smernice Evropskega odbora za varstvo podatkov 05/2020 o privolitvi na podlagi Uredbe 2016/679, oddelek 7.

[44] Glede rokov za uresničevanje pravice do dostopa, kadar mora upravljavec pridobiti dodatne informacije, glej odstavek 157.

meni, da bi bilo posamezniku, na katerega se nanašajo osebni podatki, podatke primerno razkriti na drug način. V takšnih okoliščinah, ko ima upravljavec vzpostavljene druge postopke za učinkovito in varno obravnavo zahtev za dostop, lahko zahtevane informacije zagotovi s temi postopki.

# 4 OBSEG PRAVICE DO DOSTOPA TER OSEBNIH PODATKOV IN INFORMACIJ, NA KATERE SE NANAŠA

91. Namen tega oddelka je pojasniti opredelitev osebnih podatkov (4.1) ter obseg informacij, ki jih zajema pravica do dostopa na splošno (4.2 in 4.3). Opozoriti je treba, da je obseg pojma osebni podatki in s tem razlikovanje med osebnimi in drugimi podatki sestavni del ocene, ki jo opravi upravljavec za opredelitev obsega podatkov, do katerih ima posameznik, na katerega se nanašajo osebni podatki, pravico pridobiti dostop[45].

92. Najprej je treba upoštevati, da se pravica do dostopa lahko uresničuje le v zvezi z obdelavo osebnih podatkov, ki spadajo na stvarno in ozemeljsko področje uporabe splošne uredbe o varstvu podatkov. Zato pravica do dostopa ne velja za osebne podatke, ki se ne obdelujejo z avtomatiziranimi sredstvi ali niso del zbirke ali niso namenjeni temu, da bi postali del zbirke iz člena 2(1) splošne uredbe o varstvu podatkov, ali osebne podatke, ki jih obdeluje fizična oseba v okviru popolnoma osebne ali domače dejavnosti v skladu s členom 2(2) splošne uredbe o varstvu podatkov.

## 4.1 Opredelitev pojma osebni podatki

93. Člen 15(1) in (3) splošne uredbe o varstvu podatkov se nanaša na „osebne podatke“ in „osebne podatke, ki se obdelujejo“. Zato je področje uporabe pravice do dostopa določeno predvsem s področjem uporabe pojma osebni podatki, opredeljenega v členu 4(1) splošne uredbe o varstvu podatkov[46]. Pojem osebni podatki je že bil obravnavan v več dokumentih[47] delovne skupine iz člena 29[48] ter ga je razložilo Sodišče Evropske unije, tudi v okviru pravice do dostopa iz člena 12 Direktive 95/46/ES.

94. Delovna skupina iz člena 29 je menila, da je iz opredelitve osebnih podatkov v Direktivi 95/46/ES „razvidno, da je evropski zakonodajalec želel oblikovati širok pojem ‚osebnih podatkov‘“[49]. V skladu s

---

[45] V skladu z načelom vgrajene zasebnosti je takšna analiza del ocene ustreznih zaščitnih ukrepov in drugih ukrepov za zaščito načel varstva podatkov in pravic posameznikov, na katere se nanašajo osebni podatki, ki se izvede „v času določanja sredstev obdelave kot tudi v času same obdelave“, npr. skrajšanje odzivnega časa, ko posamezniki, na katere se nanašajo osebni podatki, uresničujejo svoje pravice, je lahko eno od meril. Za dodatna pojasnila glej Smernice št. 4/2019 o členu 25, Vgrajeno in privzeto varstvo podatkov.

[46] V skladu s členom 4(1) splošne uredbe o varstvu podatkov „‚osebni podatki‘ pomenijo katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;“.

[47] Npr. Smernice WP 251, rev. 01, o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov za namene Uredbe 2016/679, in sicer str. 19; Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 9.

[48] Delovna skupina iz člena 29 je neodvisna evropska delovna skupina, ki je bila do 25. maja 2018 (začetek uporabe splošne uredbe o varstvu podatkov) pristojna za obravnavo vprašanj v zvezi z varstvom zasebnosti in osebnih podatkov ter je predhodnica Evropskega odbora za varstvo podatkov.

[49] Mnenje 4/2007 delovne skupine iz člena 29 o pojmu osebnih podatkov, str. 4.

splošno uredbo o varstvu podatkov se opredelitev še vedno nanaša na „katero koli informacijo v zvezi z določenim ali določljivim posameznikom“. Poleg osnovnih osebnih podatkov, kot so ime in naslov, telefonska številka itd., lahko v to opredelitev spadajo različni podatki, vključno z zdravniškimi ugotovitvami, zgodovino nakupov, kazalniki kreditne sposobnosti, vsebino sporočil itd. Glede na širok obseg opredelitve osebnih podatkov bi omejevalna ocena te opredelitve s strani upravljavca privedla do napačne razvrstitve osebnih podatkov[50] in nazadnje do kršitve pravice do dostopa.

95. Sodišče je v združenih zadevah C-141/12 in C-372/12[51] razsodilo, da pravica do dostopa zajema osebne podatke, vsebovane v poročilu, kot so „ime in priimek, datum rojstva, državljanstvo, spol, narodnost, veroizpoved in jezik“ prosilca in „morebitni taki podatki, ki jih vsebuje pravna analiza, vsebovana v poročilu“, ne pa tudi same pravne analize[52]. V tem okviru analiza kot taka ne more biti predmet preverjanja točnosti s strani posameznika, na katerega se nanašajo osebni podatki, niti popravka. Poleg tega zagotavljanje dostopa do pravne analize ne izpolnjuje namena zagotavljanja zasebnosti, temveč dostopa do upravnih dokumentov.

96. V zadevi Nowak[53] je Sodišče Evropske unije opravilo širšo analizo in ugotovilo, da so pisni odgovori, ki jih je na poklicnem izpitu dal kandidat, in morebitni komentarji popravljavca glede teh odgovorov osebni podatki, ki se nanašajo na kandidata za izpit. Natančneje, takšne subjektivne informacije so osebni podatki „v obliki mnenj ali presoj, če se te ‚nanašajo‘ na zadevno osebo“[54], v nasprotju z izpitnimi vprašanji, ki se ne štejejo za osebne podatke[55]. Tako bi bilo treba s presojo glede na dane okoliščine pojasniti učinek ali rezultat, ki bi ga informacije lahko imele za posameznika in s tem obseg pravice do dostopa.

**Primer 15:** Posameznik ima razgovor za zaposlitev v podjetju. V zvezi s tem kandidat za delovno mesto izroči življenjepis in prijavo. Med razgovorom kadrovik v računalnik dela zapiske za dokumentiranje razgovora. Nato prosilec za delovno mesto kot posameznik, na katerega se nanašajo osebni podatki, zahteva dostop do osebnih podatkov, ki jih je podjetje kot upravljavec podatkov zbralo med postopkom zaposlovanja.

Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke, ki jih je slednji dejavno sporočil v življenjepisu in prijavnici. Poleg tega mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotoviti povzetek razgovora, vključno s subjektivnimi pripombami o njegovem vedenju, ki ga je kadrovik pisal med razgovorom za delovno mesto, ob upoštevanju morebitnih izjem na podlagi nacionalnega prava in v skladu s členom 23 splošne uredbe o varstvu podatkov.

97. Zato morajo upravljavci pri presoji posamezne zahteve za dostop brez poseganja v člen 15(4) splošne uredbe o varstvu podatkov ob upoštevanju posebnih dejstev primera med drugim zagotoviti naslednje vrste podatkov:

— posebne vrste osebnih podatkov v skladu s členom 9 splošne uredbe o varstvu podatkov;

[50] Kot informacij, ki se ne nanašajo na določeno ali določljivo fizično osebo.
[51] Sodišče Evropske unije, združeni zadevi C-141/12 in C-372/12, YS/Minister voor Immigratie, Integratie en Asiel, in Minister voor Immigratie, Integratie en Asiel/M in S, 17. julij 2014.
[52] Sodišče Evropske unije, združeni zadevi C-141/12 in C-372/12, YS in drugi, točki 38 in 48.
[53] Sodba Sodišča v zadevi C-434/16, Peter Nowak/Data Protection Commissioner, 20. december 2017.
[54] Sodišče Evropske unije, C-434/16, Nowak, točki 34 in 35.
[55] Sodišče Evropske unije, C-434/16, Nowak, točka 58.

— osebne podatke v zvezi s kazenskimi obsodbami in prekrški v skladu s členom 10 splošne uredbe o varstvu podatkov;
— podatke, ki jih posameznik, na katerega se nanašajo osebni podatki, zavestno in dejavno zagotovi (npr. podatki o računih, predloženi prek obrazcev, odgovori na vprašalnik)[56];
— opazovane podatke ali neobdelane podatke, ki jih posameznik, na katerega se nanašajo osebni podatki, zagotovi z uporabo storitve ali naprave (npr. podatki, ki jih obdelujejo povezani predmeti, zgodovina transakcij, dnevniki dejavnosti, kot so dnevniki dostopa, zgodovina uporabe spletnega mesta, dejavnosti iskanja, podatki o lokaciji, dejavnost klikanja, edinstveni vidiki vedenja osebe, kot so pisava, pritiski na tipko, poseben način hoje ali govora)[57];
— podatke, ki jih ni neposredno zagotovil posameznik, na katerega se nanašajo osebni podatki, temveč so pridobljeni iz drugih podatkov (npr. kreditno razmerje, razvrstitev na podlagi skupnih lastnosti posameznikov, na katere se nanašajo osebni podatki, država prebivališča, ugotovljena na podlagi poštne številke)[58];
— podatke, ki izhajajo iz drugih podatkov in jih ne zagotovi neposredno posameznik, na katerega se nanašajo osebni podatki (npr. podatki za dodelitev kreditne ocene ali skladnost s pravili o preprečevanju pranja denarja, algoritemski rezultati, zdravstveni izvidi ali postopek personalizacije ali priporočil)[59];
— psevdonimizirane podatke v nasprotju z anonimiziranimi podatki (glej tudi oddelek 3 teh smernic).

**Primer 16**: Elementi, uporabljeni za sprejetje odločitve o npr. napredovanju zaposlenega, zvišanju plače ali novem delovnem mestu (npr. letni pregledi uspešnosti, zahtevki za usposabljanje, zapisniki disciplinskih postopkov, razvrstitev, poklicne možnosti), so osebni podatki v zvezi s tem zaposlenim. Zato lahko posameznik, na katerega se nanašajo osebni podatki, dostopa do takšnih elementov na zahtevo in v skladu s členom 15(4) splošne uredbe o varstvu podatkov, če se ti na primer nanašajo tudi na drugega posameznika (npr. za identiteto ali elemente, ki razkrivajo identiteto drugega zaposlenega, katerega pričevanje o poklicni uspešnosti je vključeno v letni pregled uspešnosti, lahko veljajo omejitve iz člena 15(4) splošne uredbe o varstvu podatkov, zato jih morda ni mogoče sporočiti posamezniku, na katerega se nanašajo osebni podatki, da bi se zaščitile pravice in svoboščine navedenega zaposlenega). Kljub temu se lahko uporabljajo določbe nacionalnega delovnega prava, na primer v zvezi z dostopom zaposlenih do kadrovske evidence, ali druge nacionalne določbe, kot so določbe o poslovni skrivnosti. Takšne omejitve uresničevanja pravice posameznika, na katerega se nanašajo osebni podatki, do dostopa (ali drugih pravic), določene v nacionalni zakonodaji, morajo spoštovati pogoje iz člena 23 splošne uredbe o varstvu podatkov (glej oddelek 6.4).

[56] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 9.
[57] Mnenje 4/2007 delovne skupine iz člena 29 o pojmu osebni podatki, str. 8.
[58] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 10–11.
[59] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 10–11; Delovna skupina iz člena 29, WP 251, rev. 01, 6. februar 2018, Smernice o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov za namene Uredbe 2016/679, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: Smernice delovne skupine iz člena 29 o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov, ki jih je potrdil Evropski odbor za varstvo podatkov), str. 9–10.

98. Iz zgoraj navedenega neizčrpnega seznama osebnih podatkov, ki se lahko v okviru zahteve za dostop zagotovijo posamezniku, na katerega se nanašajo osebni podatki, lahko izhaja več premislekov. Iz navedenega izhaja, da upravljavec pri omogočanju dostopa do osebnih podatkov ne sme razlikovati med podatki, ki jih vsebujejo dokumenti v papirni obliki, in tistimi, ki se hranijo elektronsko, če spadajo na področje uporabe splošne uredbe o varstvu podatkov. Z drugimi besedami, za osebne podatke, ki jih vsebujejo dokumenti v papirni obliki, ki so ali naj bi bili del zbirke, enako velja pravica do dostopa kot za osebne podatke, shranjene v računalniškem pomnilniku, na primer z binarno kodo, ali na videotraku.

99. Tako kot večina pravic posameznikov, na katere se nanašajo osebni podatki, tudi pravica do dostopa vključuje povzete in izpeljane podatke, vključno z osebnimi podatki, ki jih ustvari ponudnik storitev, medtem ko pravica do prenosljivosti podatkov vključuje le podatke, ki jih zagotovi posameznik, na katerega se nanašajo osebni podatki[60]. Zato bi bilo treba v primeru zahteve za dostop in v nasprotju z zahtevo za prenosljivost podatkov posamezniku, na katerega se nanašajo osebni podatki, zagotoviti ne le osebne podatke, predložene upravljavcu za naknadno analizo ali oceno teh podatkov, temveč tudi rezultat vsake takšne naknadne analize ali ocene.

100. Opozoriti je treba tudi, da obstajajo informacije, kot so anonimni podatki[61], tj. podatki, ki se ne nanašajo neposredno ali posredno na določljivo osebo in so zato izključeni iz področja uporabe splošne uredbe o varstvu podatkov. Na primer, lokacija strežnika, na katerem se obdelujejo osebni podatki posameznika, na katerega se nanašajo osebni podatki, ni osebni podatek. Razlikovanje je lahko zahtevno, upravljavci pa se lahko sprašujejo, kako jasno razločiti med osebnimi in neosebnimi podatki, zlasti v primeru mešanih podatkovnih nizov. V takem primeru bi lahko bilo koristno razlikovati med mešanimi podatkovnimi nizi, ki vsebujejo neločljivo povezane osebne in neosebne podatke, in tistimi, ki jih ne. Osebni in neosebni podatki so lahko neločljivo povezani v mešanih podatkovnih nizih in v celoti spadajo v obseg pravice do dostopa posameznika, na katerega se nanašajo osebni podatki[62]. V drugih primerih osebni in neosebni podatki v mešanih podatkovnih nizih morda niso neločljivo povezani, zaradi česar bi bili posamezniku, na katerega se nanašajo osebni podatki, dostopni samo osebni podatki iz nabora. Na primer, podjetje bo morda moralo posamezniku, na katerega se nanašajo osebni podatki, predložiti posamezna poročila o nastalih incidentih v zvezi z IT, ne pa tudi podatkovne zbirke znanja podjetja o težavah v zvezi z IT. Dejstvo, katere varnostne ukrepe je sprejel upravljavec, se na splošno naj ne bi štelo za osebne podatke, če niso neločljivo povezani z osebnimi podatki, in zato zanje ne velja pravica do dostopa.

101. Evropski odbor za varstvo podatkov pred zaključkom oddelka v zvezi s tem opozarja, da varstvo posameznikov pri obdelavi osebnih podatkov zajema vse zgoraj navedene vrste osebnih podatkov in da je ozka razlaga opredelitve v nasprotju z določbami splošne uredbe o varstvu podatkov in navsezadnje krši člen 8 Listine o temeljnih pravicah. Uporaba drugačne ureditve za uresničevanje pravice v zvezi z nekaterimi vrstami osebnih podatkov, ki ni predvidena v splošni uredbi o varstvu podatkov, se lahko uvede izključno s pravom v skladu s členom 23 splošne uredbe o varstvu podatkov

---

[60] Kot je že navedeno na strani 10 Smernic delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, in ponovljeno na strani 17 Smernic delovne skupine iz člena 29 o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov, ki jih je potrdil Evropski odbor za varstvo podatkov.

[61] Dodatna pojasnila o pojmu anonimizacije so na voljo v Mnenju 5/2014 delovne skupine iz člena 29 o anonimizacijskih tehnikah, WP 216, 10. april 2014, str. 5–19.

[62] Sporočilo Komisije Evropskemu parlamentu in Svetu, Smernice k uredbi o okviru za prosti pretok neosebnih podatkov v Evropski uniji, 29. maj 2019, COM(2019) 250 final.

(kot je podrobneje pojasnjeno v oddelku 6.4). Upravljavci torej ne morejo omejiti uresničevanja pravice do dostopa z neupravičenim omejevanjem obsega osebnih podatkov.

## 4.2 Osebni podatki, na katere se nanaša pravica do dostopa

102. V skladu s členom 15(1) splošne uredbe o varstvu podatkov ima „[p]osameznik, na katerega se nanašajo osebni podatki, [...] pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije“ (poudarek dodan).

103. Iz odstavka 1 člena 15 splošne uredbe o varstvu podatkov izhaja več elementov. Odstavek izrecno navaja osebne podatke, ki se „v zvezi z njim“ (4.2.1), „obdelujejo“ s strani upravljavca (4.2.2):

### 4.2.1 Osebni podatki „v zvezi s posameznikom“

104. Pravica do dostopa se lahko uresničuje izključno v zvezi z osebnimi podatki posameznika, na katerega se nanašajo osebni podatki in ki zahteva dostop, ali pa jo lahko po potrebi uveljavlja pooblaščena oseba ali pooblaščenec (glej oddelek 3.4). Obstajajo tudi primeri, v katerih podatki niso povezani z osebo, ki uveljavlja pravico do dostopa, temveč z drugim posameznikom. Vendar je posameznik, na katerega se nanašajo osebni podatki, upravičen le do osebnih podatkov, ki se nanašajo nanj, brez podatkov, ki se nanašajo izključno na nekoga drugega[63].

105. Vendar opredelitev podatkov kot osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ni odvisna od dejstva, da se ti osebni podatki nanašajo tudi na nekoga drugega[64]. Torej se lahko osebni podatki nanašajo na več kot enega posameznika hkrati. To ne pomeni samodejno, da bi bilo treba odobriti dostop do osebnih podatkov, ki se nanašajo tudi na nekoga drugega, saj mora upravljavec ravnati v skladu s členom 15(4) splošne uredbe o varstvu podatkov.

106. Upravljavci besedne zveze „osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki“ ne bi smeli razlagati „preveč omejevalno“, kot je delovna skupina iz člena 29 že navedla v zvezi s pravico do prenosljivosti podatkov[65]. Evropski odbor za varstvo podatkov v zvezi s pravico do

---

[63] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 9: „Na področje zahteve za prenosljivost podatkov spadajo le osebni podatki. Zato anonimni podatki in podatki, ki niso povezani s posameznikom, na katerega se nanašajo osebni podatki, ne bodo spadali na to področje. Vendar pa nanj spadajo psevdonimni podatki, ki jih je mogoče jasno povezati s posameznikom, na katerega se nanašajo osebni podatki (npr. tako, da posameznik zagotovi ustrezen identifikator, glej člen 11(2)).“

[64] Sodba Sodišča v zadevi C-434/16, Peter Nowak/Data Protection Commissioner, 2017, točka 44.

[65] Smernice delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 9: „V številnih okoliščinah bodo upravljavci podatkov obdelali informacije, ki vsebujejo osebne podatke več posameznikov, na katere se nanašajo osebni podatki. V tem primeru upravljavci podatkov ne bi smeli preveč omejevalno razlagati besedne zveze ‚osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki‘. Primer so evidence telefonskih pogovorov, medosebnega pošiljanja sporočil ali govora po IP, ki lahko vključujejo (v zgodovini računa naročnika) podrobnosti o tretjih osebah, udeleženih pri vhodnih in izhodnih klicih. Čeprav bodo evidence torej vsebovale osebne podatke v zvezi z več osebami, bi bilo treba naročnikom omogočiti, da se jim v odgovoru na zahteve za prenosljivost podatkov te evidence zagotovijo, saj so povezane (tudi) s posameznikom, na katerega se nanašajo osebni podatki. Če pa se takšne evidence nato

dostopa na primer meni, da lahko pravica do dostopa zajema posnetke telefonskih pogovorov (in njihov prepis) med posameznikom, na katerega se nanašajo osebni podatki in ki zahteva dostop, ter upravljavcem, če ti posnetki vsebujejo osebne podatke[66]. Če se uporablja splošna uredba o varstvu podatkov in če obdelava ni zajeta v izjemi glede domače dejavnosti v skladu s členom 2(2)(c) splošne uredbe o varstvu podatkov, bo posameznik, na katerega se nanašajo osebni podatki in ki pridobljeni posnetek z osebnimi podatki sogovornika uporabi za druge namene, na primer z objavo posnetka, postal upravljavec v smislu obdelave osebnih podatkov v zvezi z drugo osebo, katere glas je bil posnet. Čeprav upravljavec v tem primeru ne bo oproščen obveznosti, da v smislu varstva podatkov opravi ustrezno analizo, ali se lahko zagotovi dostop do celotnega posnetka, se ga spodbuja, naj posameznika, na katerega se nanašajo osebni podatki, obvesti o dejstvu, da lahko v takem primeru postane upravljavec. To ne posega v kakršno koli nadaljnjo oceno v skladu s členom 15(4) splošne uredbe o varstvu podatkov, podrobno opisano v oddelku 6. Podobno lahko pravica do dostopa velja za sporočila, ki so jih posamezniki, na katere se nanašajo osebni podatki, poslali drugim v obliki medosebnih sporočil in jih izbrisali s svoje naprave, ponudniku storitev pa so še vedno na voljo.

107. Obstajajo pa tudi primeri, v katerih se upravljavcu lahko zdi povezava med podatki in več posamezniki nejasna, na primer v primeru kraje identitete. V primeru kraje identitete oseba goljufivo ravna v imenu druge osebe. V zvezi s tem je treba opozoriti, da bi bilo treba žrtvi zagotoviti informacije o vseh osebnih podatkih, ki jih upravljavec hrani v zvezi z njeno identiteto, vključno s tistimi, ki so bili zbrani na podlagi dejanj goljufa. Z drugimi besedami, osebni podatki, ki so povezani z identiteto žrtve ali se nanjo nanašajo, štejejo za osebne podatke posameznika, na katerega se nanašajo osebni podatki, tudi po tem, ko je upravljavec izvedel za krajo identitete.

**Primer 17:** Posameznik za igranje pokra na spletu goljufivo uporablja identiteto nekoga drugega. Storilec plača spletni igralnici s kreditno kartico, ki jo je ukradel žrtvi. Ko žrtev odkrije krajo identitete, od ponudnika spletne igralnice zahteva, naj ji zagotovi dostop do njenih osebnih podatkov, natančneje do spletnih iger in informacij o kreditni kartici, ki jo je uporabil storilec.

Obstaja povezava med zbranimi podatki in žrtvijo, saj je bila uporabljena njena identiteta. Po odkritju goljufije so zgoraj navedeni osebni podatki še vedno povezani zaradi svoje vsebine (kreditna kartica se očitno nanaša na žrtev), namena in učinka (informacije o spletnih igrah, ki jih je igral storilec, se lahko na primer uporabijo za izdajanje računov žrtvi). Zato spletna igralnica žrtvi omogoči dostop do navedenih osebnih podatkov.

108. Po potrebi se lahko interni dnevniki povezav uporabijo za evidenco o dostopih do datotek in za sledenje dejanj, izvedenih v zvezi z dostopom do evidence, kot so tiskanje, kopiranje ali brisanje osebnih podatkov. Ti dnevniki lahko vključujejo čas beleženja, razlog za dostop do datoteke in podatke o identiteti osebe, ki je imela dostop. Vprašanja v zvezi s to temo se obravnavajo v zadevi, ki je trenutno pred Sodiščem Evropske unije (C-579/21). Vzpostavitev, nadzor in revizija dnevnikov povezav so v pristojnosti upravljavca in jih lahko preverijo nadzorni organi. Upravljavec bi zato moral zagotoviti, da osebe, ki delujejo pod njegovim vodstvom in imajo dostop do osebnih podatkov, teh podatkov ne obdelujejo brez navodil upravljavca, kot je določeno v členu 29 splošne uredbe o varstvu podatkov. Če oseba kljub temu obdeluje osebne podatke za druge namene, ki niso izpolnjevanje navodil upravljavca, lahko postane upravljavec za to obdelavo in zanjo veljajo disciplinski ali kazenski postopki ali upravne

posredujejo novemu upravljavcu podatkov, jih ta novi upravljavec podatkov ne bi smel obdelati za namene, ki bi negativno vplivali na pravice in svoboščine tretjih oseb (glej tretji pogoj spodaj)."

[66] Glej primer 34 v oddelku 6.2.

sankcije, ki jih izrečejo nadzorni organi. Evropski odbor za varstvo podatkov ugotavlja, da je del odgovornosti delodajalca v skladu s členom 24 splošne uredbe o varstvu podatkov, da uporabi ustrezne ukrepe, ki zajemajo vse od izobraževanja do disciplinskih postopkov, da zagotovi skladnost obdelave s splošno uredbo o varstvu podatkov in prepreči kršitev.

### 4.2.2 Osebni podatki, ki se „obdelujejo“

109. Odstavek 1 člena 15 splošne uredbe o varstvu podatkov se nanaša tudi na osebne podatke, ki se „obdelujejo“. Referenčna časovna točka za določitev obsega osebnih podatkov, ki jih zajema zahteva za dostop, je že opredeljena v oddelku 2.3.3. Besedilo pa kaže tudi, da pravica do dostopa ne razlikuje med nameni dejanj obdelave.

> **Primer 18**: Podjetje je obdelalo osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, da bi obdelalo naročilnico in uredilo odpremo na domači naslov posameznika, na katerega se nanašajo osebni podatki. Ko prvotni nameni, za katere so bili osebni podatki zbrani, prenehajo, upravljavec hrani nekatere osebne podatke izključno zaradi izpolnjevanja svojih pravnih obveznosti v zvezi z vodenjem evidenc.
>
> Posameznik, na katerega se nanašajo osebni podatki, zahteva dostop do osebnih podatkov, ki se nanašajo nanj. Da bi upravljavec izpolnil svojo obveznost iz člena 15(1) splošne uredbe o varstvu podatkov, mora posamezniku, na katerega se nanašajo osebni podatki, zagotoviti zahtevane osebne podatke, ki jih hrani zaradi izpolnjevanja svojih pravnih obveznosti.

110. Arhivirane osebne podatke je treba razlikovati od varnostnih kopij podatkov, tj. osebnih podatkov, shranjenih izključno za namene obnovitve podatkov v primeru izgube podatkov. Poudariti je treba, da so ob upoštevanju načel vgrajenega varstva podatkov in najmanjšega obsega podatkov varnostne kopije podatkov načeloma podobne podatkom v sistemu v živo. Kadar so med osebnimi podatki v varnostnem in aktivnem produkcijskem sistemu manjše razlike, so običajno povezane z zbiranjem dodatnih podatkov od zadnje varnostne kopije. V primeru zmanjšanja obsega podatkov v sistemu v živo (npr. izbris po koncu obdobja hrambe nekaterih podatkov ali po zahtevi za izbris) se bodo ti podatki v varnostnih kopijah v nekaterih primerih prepisali šele z naslednjo varnostno kopijo. Če je ob predložitvi zahteve za dostop v varnostnem sistemu v zvezi s posameznikom, na katerega se nanašajo osebni podatki, več osebnih podatkov kot v sistemu v živo ali drugačnih osebnih podatkov (kar je razvidno iz dnevnika izbrisov v aktivnem produkcijskem sistemu, ki se izvajajo popolnoma v skladu z načelom najmanjšega obsega podatkov), mora upravljavec zagotoviti preglednost tega stanja in, kadar je to tehnično izvedljivo, zagotoviti dostop, ki ga zahteva posameznik, na katerega se nanašajo osebni podatki, vključno z osebnimi podatki, shranjenimi v varnostni kopiji. V dnevniku izbrisov v aktivnem produkcijskem sistemu, namenjenem preglednosti za posameznike, na katere se nanašajo osebni podatki in ki uresničujejo svojo pravico, lahko upravljavec vidi, da v varnostni kopiji obstajajo podatki, ki niso več v sistemu v živo, saj so bili nedavno izbrisani in v varnostni kopiji še niso bili prepisani.

### 4.2.3 Obseg nove zahteve za dostop

111. Posamezniki, na katere se nanašajo osebni podatki, imajo torej pravico do dostopa do vseh podatkov, ki se obdelujejo v zvezi z njimi, ali do delov podatkov, odvisno od obsega zahteve (glej tudi 2.3.1 o popolnosti informacij in 3.1.1 o analizi vsebine zahteve). Zato upravljavec ne more zožiti obsega nove zahteve, če je v preteklosti že izpolnil zahtevo za dostop in zahteva ni pretirana. To pomeni, da v zvezi s katero koli nadaljnjo zahtevo za dostop posameznika, na katerega se nanašajo osebni podatki, upravljavec le-tega ne bi smel obvestiti samo o spremembah osebnih podatkov, ki se obdelujejo, ali o sami obdelavi od zadnje zahteve, razen če se posameznik, na katerega se nanašajo osebni podatki, s

tem izrecno strinja. V nasprotnem primeru bi morali posamezniki, na katere se nanašajo osebni podatki, zbrati svoje osebne podatke, da bi pridobili popoln sklop osebnih podatkov v zvezi z njihovimi informacijami o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki.

## 4.3 Informacije o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki

112. Upravljavec mora poleg dostopa do osebnih podatkov zagotoviti tudi informacije o obdelavi in pravicah posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 15(1)(a) do (h) in členom 15(2) splošne uredbe o varstvu podatkov. Večina informacij o teh posebnih točkah je že zbranih, vsaj v splošni obliki, v evidenci dejavnosti obdelave upravljavca iz člena 30 splošne uredbe o varstvu podatkov in/ali v izjavi o varstvu osebnih podatkov, pripravljeni v skladu s členi 12 do 14 splošne uredbe o varstvu podatkov. Zato bi bilo koristno najprej prebrati „Smernice o preglednosti na podlagi Uredbe 2016/679“[67] delovne skupine iz člena 29 o vsebini informacij, ki jih je treba zagotoviti v skladu s členoma 13 in 14 splošne uredbe o varstvu podatkov.

113. Zaradi skladnosti s členom 15(1)(a) do (h) in členom 15(2) lahko upravljavci skrbno uporabljajo module besedila svoje izjave o varstvu osebnih podatkov, če zagotovijo, da so posodobljeni in natančni v zvezi z zahtevo posameznika, na katerega se nanašajo osebni podatki. Nekatere informacije, kot so identifikacija določenih uporabnikov ali trajanje določene obdelave podatkov, pred obdelavo podatkov ali ob njenem začetku pogosto še niso na voljo. Nekatere informacije, kot je na primer pravica do vložitve pritožbe pri nadzornem organu (glej člen 15(1)(f)), ostanejo enake, ne glede na osebo, ki predloži zahtevo za dostop. Zato se lahko sporočijo v splošni obliki, kot je to storjeno tudi v izjavi o varstvu osebnih podatkov. Druge vrste informacij, kot so informacije o uporabnikih, vrstah in viru podatkov, se lahko razlikujejo glede na to, kdo predloži zahtevo in kakšen je njen obseg. V okviru zahteve za dostop v skladu s členom 15 je zato treba vse informacije o obdelavi, ki so na voljo upravljavcu, posodobiti in prilagoditi postopkom obdelave, ki se dejansko izvajajo v zvezi s posameznikom, na katerega se nanašajo osebni podatki in ki je predložil zahtevo. Zato sklicevanje na besedilo politike zasebnosti ne bi zadostovalo, da bi upravljavec zagotovil informacije, zahtevane v členu 15(1)(a) do (h) in členu 15(2), razen če so „prilagojene in posodobljene“ informacije enake informacijam, zagotovljenim na začetku obdelave. Pri razlagi, katere informacije se nanašajo na osebo, ki je predložila zahtevo, bi se upravljavec po potrebi lahko skliceval na nekatere dejavnosti (kot so „če ste uporabili to storitev …“, „če ste plačali na podlagi računa“), če je posameznikom, na katere se nanašajo osebni podatki, jasno, ali to velja zanje. V nadaljevanju je pojasnjena zahtevana stopnja podrobne opredelitve v zvezi s posameznimi vrstami informacij.

114. Informacije o namenih v skladu s členom 15(1)(a) morajo biti natančne glede točnega(-ih) namena(-ov) v dejanskem primeru posameznika, na katerega se nanašajo osebni podatki in ki zahteva podatke. Navedba splošnih namenov upravljavca brez pojasnila, katere namene si upravljavec prizadeva doseči v zadevnem primeru posameznika, na katerega se nanašajo osebni podatki in ki je zahteval podatke, ne bi zadostovala. Če se obdelava izvaja za več namenov, mora upravljavec pojasniti, kateri podatki ali katere vrste podatkov se obdelujejo za katere namene. V nasprotju s členom 13(1)(c) in členom 14(1)(c) splošne uredbe o varstvu podatkov informacije o obdelavi iz člena 15(1)(a) ne vsebujejo informacij o pravni podlagi za obdelavo. Ker pa so nekatere pravice posameznikov, na katere se nanašajo osebni podatki, odvisne od veljavne pravne podlage, so te informacije pomembne, da

[67] Delovna skupina iz člena 29, WP 260 rev. 01, 11. april 2018, Smernice o preglednosti na podlagi Uredbe 2016/679, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov).

posamezniki, na katere se nanašajo osebni podatki, preverijo zakonitost obdelave podatkov in ugotovijo, katere pravice posameznika, na katerega se nanašajo osebni podatki, veljajo v danih okoliščinah. Da bi se v skladu s členom 12(2) splošne uredbe o varstvu podatkov olajšalo uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, se upravljavcu priporoča, da posameznika, na katerega se nanašajo osebni podatki, obvesti tudi o veljavni pravni podlagi za vsako dejanje obdelave ali navede, kje lahko te informacije najde. V vsakem primeru načelo pregledne obdelave zahteva, da so informacije o pravnih podlagah za obdelavo na voljo posamezniku, na katerega se nanašajo osebni podatki, na dostopen način (npr. v izjavi o varstvu osebnih podatkov).

115. Informacije o vrstah podatkov (člen 15(1)(b)) je morda treba prilagoditi tudi razmeram posameznika, na katerega se nanašajo osebni podatki, tako da bi bilo treba izločiti vrste, za katere se je izkazalo, da niso relevantne za osebo, ki je predložila zahtevo.

**Primer 19**: Hotel v zvezi z informacijami iz člena 13 oziroma 14 splošne uredbe o varstvu podatkov navaja, da obdeluje več vrst podatkov o strankah (identifikacijski podatki, kontaktni podatki, bančni podatki, številka kreditne kartice itd.). Če se zahteva za dostop predloži na podlagi člena 15, mora biti posameznik, na katerega se nanašajo osebni podatki in ki zahtevo predloži, obveščen o dostopu do dejanskih podatkov, ki se obdelujejo (sestavni del 2), in v skladu s členom 15(1)(b) tudi o posebnih vrstah podatkov, ki se obdelujejo v posameznem primeru (npr. v primeru plačila v gotovini obdelava ne vključuje bančnih podatkov ali podatkov o kreditni kartici).

116. Informacije o „uporabnikih ali kategorijah uporabnikov“ (člen 15(1)(c)) morajo najprej upoštevati opredelitev uporabnikov iz člena 4(9) splošne uredbe o varstvu podatkov. Opredelitev uporabnikov temelji na razkritju osebnih podatkov fizični ali pravni osebi, javnemu organu, agenciji ali drugemu organu[68]. Iz člena 4(9) splošne uredbe o varstvu podatkov izhaja, da se javni organi, ki delujejo v okviru posamezne poizvedbe, za katero veljajo posebne nacionalne določbe, ne štejejo za uporabnike.

117. V zvezi z vprašanjem, ali lahko upravljavec prosto izbira med informacijami o uporabnikih ali o kategorijah uporabnikov, je treba opozoriti, da „drugače kot člena 13 in 14 splošne uredbe o varstvu podatkov, ki določata obveznost upravljavca […], člen 15 splošne uredbe o varstvu podatkov določa dejansko pravico dostopa v korist posameznika, na katerega se nanašajo osebni podatki, tako da mora imeti ta na voljo, da izbere bodisi prejem informacij o konkretnih uporabnikih, ki so jim bili ali jim bodo razkriti navedeni podatki, kadar je to mogoče, bodisi informacij o kategorijah uporabnikov.“[69] Opozoriti je treba tudi, da bi morale biti, kot je navedeno v zgoraj navedenih smernicah o preglednosti[70], že v skladu s členoma 13 in 14 splošne uredbe o varstvu podatkov informacije o uporabnikih ali kategorijah uporabnikov čim bolj podrobne ob upoštevanju načel preglednosti in pravičnosti. Če se posameznik, na katerega se nanašajo osebni podatki, ni odločil drugače, mora upravljavec v skladu s členom 15 imenovati dejanske uporabnike, razen če identifikacija teh uporabnikov ni mogoča ali če navedeni upravljavec dokaže, da so zahteve za dostop posameznika, na katerega se nanašajo osebni podatki,

[68] Poleg tega je treba opozoriti, da lahko v istem podjetju obstajajo različni upravljavci, kot so opredeljeni v členu 4(7) splošne uredbe o varstvu podatkov. V takem položaju je mogoče, da uporabnik razkrije podatke drugemu uporabniku znotraj istega podjetja.

[69] Sodišče Evropske unije, C-154/21 (Österreichische Post AG), točka 36.

[70] Delovna skupina iz člena 29, WP 260 rev. 01, 11. april 2018, Smernice o preglednosti na podlagi Uredbe 2016/679, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov), str. 37 (Priloga).

očitno neutemeljene ali pretirane v smislu člena 12(5) splošne uredbe o varstvu podatkov[71] [72]. Evropski odbor za varstvo podatkov v zvezi s tem opozarja, da je hramba informacij v zvezi z dejanskimi uporabniki med drugim potrebna za izpolnjevanje obveznosti upravljavca iz člena 5(2) in člena 19 splošne uredbe o varstvu podatkov.

**Primer 20**: Delodajalec v skladu s členom 13(1)(e) in členom 14(1)(e) splošne uredbe o varstvu podatkov v izjavi o varstvu osebnih podatkov navede informacije o tem, katere vrste podatkov se posredujejo „potovalnim agencijam“ ali „hotelom“ v primeru poslovnih potovanj. Če zaposleni vloži zahtevo za dostop do osebnih podatkov po poslovnih potovanjih, bi moral delodajalec v skladu s členom 15(1)(c) v zvezi z uporabniki osebnih podatkov v svojem odgovoru navesti potovalne agencije in hotele, ki so prejeli podatke. Čeprav je delodajalec v svoji izjavi o varstvu osebnih podatkov v skladu s členoma 13 in 14 upravičeno navedel kategorije uporabnikov, ker uporabnikov na tej stopnji še ni bilo mogoče imenovati, bi moral zaposlenemu na podlagi predložene zahteve za dostop zagotoviti informacije o konkretnih uporabnikih (ime potovalnih agencij, hotelov itd.), razen če se zaposleni odloči drugače.

Kadar lahko upravljavec ob upoštevanju zgoraj navedenih pogojev zagotovi le kategorije uporabnikov, bi morale biti informacije čim bolj podrobne, pri čemer bi bilo treba navesti vrsto uporabnika (tj. s sklicevanjem na dejavnosti, ki jih opravlja), panogo, sektor in podsektor ter lokacijo uporabnikov[73].

118. V skladu s členom 15(1)(d) je treba zagotoviti informacije o predvidenem obdobju hrambe osebnih podatkov, kadar je to mogoče. V nasprotnem primeru je treba navesti merila, ki se uporabijo za določitev tega obdobja. Informacije, ki jih zagotovi upravljavec, morajo biti dovolj natančne, da posameznik, na katerega se nanašajo osebni podatki, ve, kako dolgo se bodo podatki v zvezi njim hranili. Če časa izbrisa ni mogoče določiti, se navede trajanje obdobja hrambe in začetek tega obdobja ali sprožilni dogodek (npr. prekinitev pogodbe, potek garancijskega roka itd.). Zgolj sklicevanje na primer na „izbris po izteku predpisanih obdobij hrambe“, ni dovolj. Navedbe v zvezi z obdobji hrambe podatkov bodo morale biti osredotočene na posebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Če za osebne podatke posameznika, na katerega se nanašajo osebni podatki, veljajo različna obdobja za izbris (npr. ker zakonske obveznosti hrambe ne veljajo za vse podatke), se obdobja izbrisa navedejo v zvezi z zadevnimi dejanji obdelave in vrstami podatkov.

119. Medtem ko informacije o pravici do vložitve pritožbe pri nadzornem organu (člen 15(1)(f)) niso odvisne od konkretnih okoliščin, se pravice posameznikov, na katere se nanašajo osebni podatki, iz člena 15(1)(e) razlikujejo glede na pravno podlago, na kateri temelji obdelava. Kar zadeva obveznost upravljavca, da olajša uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 12(2) splošne uredbe o varstvu podatkov, je odziv upravljavca na te pravice prilagojen primeru posameznika, na katerega se nanašajo osebni podatki, in povezan z zadevnimi dejanji obdelave. Izogibati bi se bilo treba informacijam o pravicah, ki v posebnih okoliščinah ne veljajo za posameznika, na katerega se nanašajo osebni podatki.

[71] Sodišče Evropske unije, C-154/21 (Österreichische Post AG).

[72] Zgolj dejstvo, da so bili podatki razkriti velikemu številu uporabnikov, samo po sebi ne pomeni, da je zahteva pretirana (glej odstavek 188 oddelka 6).

[73] Smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 37 (Priloga).

120. V skladu s členom 15(1)(g) je treba zagotoviti „vse razpoložljive informacije“ v zvezi z njihovim virom, kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo. Stopnja razpoložljivih informacij se lahko sčasoma spremeni.

**Primer 21**: Veliko podjetje v svoji politiki zasebnosti navaja:

„Kreditna preverjanja nam pomagajo preprečevati težave pri plačilnih transakcijah. Zagotavljajo zaščito našega podjetja pred finančnimi tveganji, ki lahko srednje- in dolgoročno vplivajo tudi na prodajne cene. Kreditno preverjanje je potrebno, kadar bomo odpremili blago, ne da bi prejeli ustrezno kupnino, npr. v primeru nakupa na kredit. Brez kreditnega preverjanja je mogoče le predplačilo (takojšnje bančno nakazilo, plačilo prek spleta kreditna kartica).

Za namene kreditnega preverjanja bomo vaše ime in priimek, naslov in datum rojstva poslali naslednjim ponudnikom storitev, na primer: (1) agenciji za finančne storitve X, (2) ponudniku poslovnih informacij Y, (3) agenciji za ocenjevanje kreditne sposobnosti podjetij Z.

Podatki se posredujejo zgoraj navedenim kreditnim institucijam samo v zakonsko dovoljenem okviru in samo za namene analize vaše pretekle plačilne discipline ter za oceno tveganja neplačila na podlagi matematično-statističnih postopkov, pri katerih se uporabljajo podatki o naslovih, ter za preverjanje vašega naslova (preverjanje dostave). Odvisno od rezultata kreditnega preverjanja vam morda ne bomo več mogli ponuditi posameznih načinov plačila, kot je financiranje računov.“

Izjava o varstvu osebnih podatkov torej vsebuje splošne informacije o možnosti pridobitve informacij od navedenih uradov za ekonomske informacije v skladu s členoma 13 in 14 splošne uredbe o varstvu podatkov. Če predhodno ni jasno, katera podjetja bodo vključena v obdelavo, zadostuje navedba imen upravičenih podjetij v politiki zasebnosti. V okviru zahteve na podlagi člena 15 bi bilo treba poleg obvestila o pridobitvi informacij o kreditni sposobnosti, (naknadno) razkriti, točno katero od navedenih podjetij je bilo vključeno. Člen 15(1)(g) jasno določa, da informacije o obdelavi podatkov vključujejo „vse razpoložljive informacije v zvezi z njihovim virom“, kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo.

121. Člen 15(1)(h) določa, da bi moral imeti vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da je smiselno obveščen med drugim o obstoju avtomatiziranega sprejemanja odločitev in razlogih zanj, vključno z oblikovanjem profilov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ter o pomenu in predvidenih posledicah take obdelave[74]. Če je mogoče, morajo biti informacije iz člena 15(1)(h) natančnejše v zvezi z razlogi za posebne odločitve glede posameznika, na katerega se nanašajo osebni podatki in ki je zahteval dostop.

122. Informacije o nameravanih prenosih podatkov v tretjo državo ali mednarodno organizacijo, vključno z obstojem sklepa Komisije o ustreznosti ali ustreznih zaščitnih ukrepih, je treba zagotoviti v skladu s členom 13(1)(f) in členom 14(1)(f) splošne uredbe o varstvu podatkov. V okviru zahteve za dostop v skladu s členom 15 zahteva člen 15(2) informacije o ustreznih zaščitnih ukrepih v skladu s členom 46 splošne uredbe o varstvu podatkov le v primerih, ko se prenos v tretjo državo ali mednarodno organizacijo dejansko izvede.

[74] V zvezi s tem glej Smernice o preglednosti na podlagi Uredbe 2016/679 (WP 260), odstavek 41, s sklicevanjem na Smernice o avtomatiziranem posameznem sprejemanju odločitev in oblikovanju profilov za namene Uredbe 2016/679 (WP 251).

# 5 KAKO LAHKO UPRAVLJAVEC ZAGOTOVI DOSTOP?

123. Splošna uredba o varstvu podatkov ni zelo predpisujoča glede tega, kako mora upravljavec zagotoviti dostop. Pravica do dostopa se lahko v nekaterih primerih enostavno in preprosto uporabi, na primer kadar ima majhna organizacija omejene informacije o posamezniku, na katerega se nanašajo osebni podatki. V drugih primerih je pravica do dostopa bolj zapletena, ker je bolj zapletena obdelava podatkov; glede na število posameznikov, na katere se nanašajo osebni podatki, vrste podatkov, ki se obdelujejo, ter pretok podatkov znotraj različnih organizacij in med njimi. Glede na razlike v obdelavi osebnih podatkov se lahko ustrezen način zagotavljanja dostopa temu primerno razlikuje.

124. Namen tega oddelka je podati nekaj smernic in praktičnih primerov o različnih načinih, na katere upravljavci izpolnjujejo zahtevo za dostop, in o pomenu člena 12(1) splošne uredbe o varstvu podatkov v zvezi s pravico do dostopa. Ta oddelek bo zagotovil tudi nekaj smernic o tem, kaj se šteje za elektronsko obliko, ki je splošno uporabljana, in o časovnem okviru za zagotovitev dostopa v skladu s členom 12(3) splošne uredbe o varstvu podatkov.

## 5.1 Kako lahko upravljavec pridobi zahtevane podatke?

125. Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti dostop do vseh informacij, ki jih upravljavec obdeluje v zvezi z njimi. To na primer pomeni, da mora upravljavec iskati osebne podatke v vseh svojih informacijskih sistemih in zbirkah, ki ne temeljijo na informacijski tehnologiji. Upravljavec bi moral pri takem iskanju uporabiti razpoložljive informacije v organizaciji v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ki bodo verjetno privedle do ujemanj v sistemih, odvisno od tega, kako so informacije strukturirane[75]. Če so na primer informacije razvrščene v datoteke glede na ime ali referenčno številko, se iskanje lahko omeji na ta dejavnika. Če pa je sestava podatkov odvisna od drugih dejavnikov, kot so družinska razmerja ali poklicni nazivi ali kakršni koli neposredni ali posredni identifikatorji (npr. številka stranke, uporabniško ime ali naslovi IP), je treba iskanje razširiti tako, da vključuje te dejavnike, če ima upravljavec tudi te informacije v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali če mu te informacije zagotovi tak posameznik. Enako velja, kadar je verjetno, da evidence, povezane s tretjimi osebami, vsebujejo osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Vendar upravljavec od posameznika, na katerega se nanašajo osebni podatki, ne sme zahtevati, naj zagotovi več informacij, kot je potrebno za identifikacijo navedenega posameznika. Če upravljavec uporablja obdelovalca za svoje dejavnosti obdelave podatkov, je treba iskanje razširiti tudi na osebne podatke, ki jih obdeluje obdelovalec.

126. V skladu s členom 25 splošne uredbe o varstvu podatkov o vgrajenem in privzetem varstvu podatkov bi moral upravljavec (in vsi obdelovalci, ki jih uporablja) izvajati tudi že funkcije, ki omogočajo skladnost s pravicami posameznikov, na katere se nanašajo osebni podatki. V tem okviru to pomeni, da bi morali pri obravnavi zahtevka obstajati ustrezni načini za iskanje in pridobivanje informacij o posamezniku, na katerega se nanašajo osebni podatki. Vendar je treba opozoriti, da bi lahko preširoka razlaga v zvezi s tem privedla do funkcij iskanja in pridobivanja informacij, ki same po sebi ogrožajo zasebnost posameznikov, na katere se nanašajo osebni podatki. Zato se je treba zavedati, da bi moral biti tudi postopek pridobivanja podatkov zasnovan na način, prijazen varstvu podatkov, tako da ne ogroža zasebnosti drugih, na primer zaposlenih pri upravljavcu.

[75] Takšno iskanje bi seveda moralo vključevati tudi informacije, ki jih ima obdelovalec, glej člen 28(3)(e) splošne uredbe o varstvu podatkov.

## 5.2 Ustrezni ukrepi za zagotavljanje dostopa

### 5.2.1 Sprejetje „ustreznih ukrepov“

127. Člen 12 splošne uredbe o varstvu podatkov določa zahteve za zagotavljanje dostopa, tj. za zagotovitev potrditve, osebnih podatkov in dopolnilnih informacij v skladu s členom 15, ter določa tudi obliko, način in rok v zvezi s pravico do dostopa. Smernice delovne skupine iz člena 29 o preglednosti na podlagi Uredbe 2016/679[76] zagotavljajo dodatna navodila glede člena 12, večinoma v zvezi s členoma 13 in 14 splošne uredbe o varstvu podatkov, pa tudi v zvezi s členom 15 in preglednostjo na splošno. Kar je opredeljeno v teh smernicah, se lahko zato pogosto uporablja tudi v zvezi z zagotavljanjem dostopa v skladu s členom 15.

128. Člen 12(1) splošne uredbe o varstvu podatkov določa, da upravljavec sprejme ustrezne ukrepe, s katerimi posamezniku, na katerega se nanašajo osebni podatki, zagotovi vsa sporočila iz člena 15, povezana z obdelavo, v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku. Člen 12(2) določa, da upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajša uresničevanje njegove pravice do dostopa. Natančnejše zahteve v zvezi s tem bo treba oceniti za vsak primer posebej. Upravljavci morajo pri odločanju, kateri ukrepi so ustrezni, upoštevati vse ustrezne okoliščine, med drugim tudi količino podatkov, ki se obdelujejo, kompleksnost obdelave podatkov in znanje, ki ga imajo o posameznikih, na katere se nanašajo osebni podatki, katerih podatke obdelujejo, na primer, če je večina posameznikov, na katere se nanašajo osebni podatki, otrok, starejših ali invalidov. Poleg tega mora upravljavec v primerih, ko je seznanjen s posebnimi potrebami posameznika, na primer prek dodatnih informacij v zahtevi, ki jo je predložil posameznik, na katerega se nanašajo osebni podatki, te okoliščine upoštevati. Zato se bodo ustrezni ukrepi razlikovali.

129. Pri oceni je treba upoštevati, da izraza „ustrezen“ nikoli ne bi smeli razumeti kot način za omejevanje obsega podatkov, za katere velja pravica do dostopa. Izraz „ustrezen“ ne pomeni, da je mogoče prizadevanja za zagotavljanje informacij uravnotežiti, na primer z morebitnim interesom posameznika, na katerega se nanašajo osebni podatki, za pridobitev osebnih podatkov. Namesto tega bi moral biti cilj ocene izbrati najustreznejšo metodo za zagotavljanje vseh informacij, ki jih zajema ta pravica, glede na posebne okoliščine posameznega primera. Zato mora biti upravljavec, ki izvaja obsežno obdelavo velike količine podatkov, pripravljen vložiti veliko truda za zagotovitev pravice do dostopa posameznikom, na katere se nanašajo osebni podatki, v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku.

130. V odgovor na zahtevo za dostop do podatkov se je treba izogibati usmerjanju posameznika, na katerega se nanašajo osebni podatki, k različnim virom. Kot je bilo že navedeno v smernicah delovne skupine iz člena 29 o preglednosti (v zvezi s pojmom „zagotovi“ v členih 13 in 14 splošne uredbe o varstvu podatkov), pojem „zagotovi“ pomeni, da se „[o]d posameznika, na katerega se nanašajo osebni podatki, […] ne sme zahtevati, naj dejavno išče informacije, zajete s tema členoma, med drugimi informacijami, kot so pogoji uporabe spletnega mesta ali aplikacije“[77]. Zato in glede na načelo preglednosti morajo posamezniki, na katere se nanašajo osebni podatki, od upravljavca pridobiti informacije in osebne podatke, zahtevane v členu 15(1), (2) in (3), na način, ki omogoča popoln dostop

[76] Delovna skupina iz člena 29, WP 260 rev. 01, 11. april 2018, Smernice o preglednosti na podlagi Uredbe 2016/679, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljnjem besedilu: smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov).
[77] Smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, odstavek 33.

do zahtevanih informacij. V posebnih okoliščinah bi bilo neprimerno ali celo nezakonito deliti informacije znotraj upravljavca, na primer zaradi njihove občutljive narave (kot so informacije v zvezi z žvižgaštvom). V teh primerih bi se zdelo primerno, da se informacije v odziv na zahtevo za dostop posameznikov, na katere se nanašajo osebni podatki, razdelijo na več odgovorov. Metoda, ki jo izbere upravljavec, mora posamezniku, na katerega se nanašajo osebni podatki, dejansko zagotoviti zahtevane podatke in informacije, zato ne bi bilo primerno posameznika, na katerega se nanašajo osebni podatki, zgolj napotiti, naj preveri zahtevane podatke, shranjene na svoji napravi, vključno na primer s preverjanjem zgodovine poteka klikanja in naslovov IP na njegovem mobilnem telefonu.

131. V skladu z načelom odgovornosti mora upravljavec dokumentirati svoj pristop, da lahko dokaže, da so sredstva, izbrana za zagotavljanje potrebnih informacij v skladu s členom 15, v danih okoliščinah ustrezna.

### 5.2.2 Različni načini zagotavljanja dostopa

132. Kot je že pojasnjeno v oddelku 2.2.2 zgoraj, so posamezniki, na katere se nanašajo osebni podatki, pri predložitvi zahteve za dostop upravičeni do prejema kopije svojih podatkov, ki se obdelujejo v skladu s členom 15(3), skupaj z dopolnilnimi informacijami, ki se štejejo za glavni način zagotavljanja dostopa do osebnih podatkov.

133. Vendar bi lahko bilo v nekaterih okoliščinah primerno, da upravljavec zagotovi dostop na druge načine kot s predložitvijo kopije. Takšni nestalni načini dostopa do podatkov bi lahko bili na primer: ustne informacije, pregled datotek, dostop na kraju samem ali na daljavo brez možnosti prenosa. Ti načini so lahko ustrezni načini odobritve dostopa, na primer v primerih, ko je to v interesu posameznika, na katerega se nanašajo osebni podatki, ali če posameznik, na katerega se nanašajo osebni podatki, to zahteva. Dostop na kraju samem bi lahko bil ustrezen začetni ukrep tudi, kadar upravljavec obdeluje veliko količino nedigitaliziranih podatkov, da bi se lahko posameznik, na katerega se nanašajo osebni podatki, seznanil s tem, kateri osebni podatki se obdelujejo, in sprejel informirano odločitev o tem, katere osebne podatke želi pridobiti prek kopije. Nestalni načini dostopa so lahko v nekaterih primerih zadostni in ustrezni; lahko na primer zadovoljijo potrebo posameznikov, na katere se nanašajo osebni podatki, da preverijo, ali so podatki, ki jih obdeluje upravljavec, pravilni, tako da jim omogočijo vpogled v prvotne podatke. Upravljavec ni dolžan zagotoviti informacij na druge načine kot s predložitvijo kopije, vendar bi moral pri obravnavi take zahteve uporabiti razumen pristop. Omogočanje dostopa na druge načine kot s predložitvijo kopije posameznikom, na katere se nanašajo osebni podatki, ne preprečuje, da bi imeli tudi kopijo, razen če se odločijo nasprotno.

134. Upravljavec se lahko glede na okoliščine odloči, da bo kopijo podatkov, ki se obdelujejo, skupaj z dopolnilnimi informacijami zagotovil na različne načine, npr. po elektronski pošti, fizični pošti ali z uporabo samopostrežnega orodja. Če posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi in če ne zahteva drugače, se informacije zagotovijo v elektronski obliki, ki je splošno uporabljana, kot je navedeno v členu 15(3). Upravljavec mora pri zagotavljanju informacij prek elektronske pošte ali spletnih samopostrežnih orodij v vsakem primeru upoštevati ustrezne tehnične in organizacijske ukrepe, vključno z ustreznim šifriranjem.

135. Kadar upravljavec le v majhnem obsegu obdeluje osebne podatke v zvezi z osebo, ki predloži zahtevo, se kopija osebnih podatkov in dopolnilne informacije lahko zagotovijo in bi se morale zagotoviti s preprostim postopkom.

**Primer 22:** Lokalna knjigarna vodi evidenco imen in naslovov svojih strank, ki so naročile dostavo na dom. Stranka obišče knjigarno in predloži zahtevo za dostop. V tem primeru bi zadostovalo, da se

osebni podatki o stranki natisnejo neposredno iz poslovnega sistema, hkrati pa se zagotovijo dopolnilne informacije iz člena 15(1) in (2).

**Primer 23:** Mesečni donator dobrodelne organizacije predloži zahtevo za dostop po elektronski pošti. Dobrodelna organizacija hrani informacije o donacijah v zadnjih dvanajstih mesecih ter imena in elektronske naslove donatorjev. Upravljavec bi lahko zagotovil kopijo osebnih podatkov in dopolnilne informacije v odgovoru na elektronsko sporočilo, pod pogojem, da uporabi vse potrebne zaščitne ukrepe, na primer ob upoštevanju narave podatkov.

136. Celo upravljavci, ki obdelujejo veliko količino podatkov, lahko za obravnavo zahtev za dostop uporabijo ročne postopke. Če upravljavec obdeluje podatke v več različnih oddelkih, mora zbrati osebne podatke od vsakega oddelka, da se lahko odzove na zahtevo posameznika, na katerega se nanašajo osebni podatki.

**Primer 24:** Upravljavec imenuje administratorja, ki obravnava praktična vprašanja v zvezi z zahtevami za dostop. Ko prejme zahtevek, administrator pošlje poizvedbo po elektronski pošti različnim oddelkom organizacije in jih prosi, naj zberejo osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki. Predstavniki vsakega oddelka administratorju posredujejo osebne podatke, ki jih obdeluje njihov oddelek. Administrator nato pošlje vse osebne podatke posamezniku, na katerega se nanašajo osebni podatki, skupaj s potrebnimi dopolnilnimi informacijami, na primer po elektronski pošti, kadar je to potrebno.

137. Čeprav bi se lahko ročni postopki za obravnavo zahtev za dostop šteli za ustrezne, bi nekateri upravljavci lahko imeli korist od uporabe avtomatiziranih postopkov za obravnavo zahtev posameznikov, na katere se nanašajo osebni podatki. To bi lahko na primer veljalo za upravljavce, ki prejmejo veliko zahtev. Eden od načinov za zagotavljanje informacij v skladu s členom 15 je zagotovitev samopostrežnih orodij posamezniku, na katerega se nanašajo osebni podatki. To bi lahko olajšalo učinkovito in pravočasno obravnavo zahtev za dostop posameznikov, na katere se nanašajo osebni podatki, ter upravljavcu omogočilo, da mehanizem preverjanja vključi v samopostrežno orodje.

**Primer 25:** Storitev družbenih medijev ima vzpostavljen avtomatiziran postopek za obravnavo zahtev za dostop, ki posamezniku, na katerega se nanašajo osebni podatki, omogoča dostop do njegovih osebnih podatkov iz njegovega uporabniškega računa. Za pridobitev osebnih podatkov lahko uporabniki družbenih medijev ob prijavi v svoj uporabniški račun izberejo možnost „prenos vaših osebnih podatkov“. Ta samopostrežna možnost uporabnikom omogoča, da datoteko, ki vsebuje njihove osebne podatke, prenesejo neposredno z uporabniškega računa na svoj računalnik.

138. Uporaba samopostrežnih orodij ne bi smela nikoli omejevati obsega prejetih osebnih podatkov. Če vseh informacij iz člena 15 ni mogoče posredovati prek samopostrežnega orodja, je treba preostale informacije zagotoviti na drugačen način. Upravljavec lahko posameznika, na katerega se nanašajo osebni podatki, dejansko spodbudi k uporabi samopostrežnega orodja, ki ga je upravljavec vzpostavil za obravnavo zahtev za dostop. Vendar je treba opozoriti, da mora upravljavec obravnavati tudi zahteve za dostop, ki se ne pošljejo prek uveljavljenega komunikacijskega kanala[78].

[78] Glej oddelek 3.1.2.

### 5.2.3 Zagotavljanje dostopa v „jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku“

139. V skladu s členom 12(1) splošne uredbe o varstvu podatkov upravljavec sprejme ustrezne ukrepe za zagotovitev dostopa v skladu s členom 15 v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku.

140. Zahteva, da je treba dostop posamezniku, na katerega se nanašajo osebni podatki, zagotoviti v jedrnati in pregledni obliki, pomeni, da bi morali upravljavci informacije predstaviti učinkovito in strnjeno, da bi jih posameznik, na katerega se nanašajo osebni podatki, zlahka razumel, zlasti če je otrok. Upravljavec mora pri izbiri sredstev za zagotavljanje dostopa v skladu s členom 15 upoštevati količino in kompleksnost podatkov.

**Primer 26:** Ponudnik družbenih medijev obdeluje veliko količino informacij o posamezniku, na katerega se nanašajo osebni podatki. Velik del teh osebnih podatkov so informacije na več sto straneh dnevniških datotek, v katerih so evidentirane dejavnosti posameznika, na katerega se nanašajo osebni podatki, na spletnem mestu. Če posamezniki, na katere se nanašajo osebni podatki, zahtevajo dostop do svojih osebnih podatkov, za osebne podatke v teh dnevniških datotekah dejansko velja pravica do dostopa. Pravica do dostopa se torej lahko formalno izpolni, če bi se posamezniku, na katerega se nanašajo osebni podatki, zagotovile te stotine strani dnevniških datotek. Vendar brez ukrepov, sprejetih za lažje razumevanje informacij v dnevniških datotekah, pravica posameznika, na katerega se nanašajo osebni podatki, do dostopa v praksi morda ne bo izpolnjena, saj se iz dnevniških datotek ni mogoče zlahka razbrati informacij, zato ni izpolnjena zahteva iz člena 12(1) splošne uredbe o varstvu podatkov. Zato mora upravljavec skrbno in natančno izbrati način predstavitve informacij in osebnih podatkov posamezniku, na katerega se nanašajo osebni podatki.

141. V okoliščinah iz zgornjega primera bi lahko bila uporaba večdelnega pristopa, podobnega tistemu, ki se priporoča v smernicah o preglednosti v zvezi z izjavo o varstvu osebnih podatkov[79], ustrezen ukrep za izpolnitev zahtev iz člena 15 in člena 12(1) splošne uredbe o varstvu podatkov. To bo podrobneje opredeljeno v oddelku 5.2.4 v nadaljevanju. Zahteva, da je treba informacije zagotoviti v „razumljivi“ obliki, pomeni, da bi morale biti razumljive ciljni skupini[80], pri čemer je treba upoštevati morebitne posebne potrebe posameznika, na katerega se nanašajo osebni podatki, s katerimi je upravljavec seznanjen[81]. Ker pravica do dostopa pogosto omogoča uresničevanje drugih pravic posameznikov, na katere se nanašajo osebni podatki, je bistveno, da so zagotovljene informacije razumljive in jasne. Razlog za to je, da se bodo lahko posamezniki, na katere se nanašajo osebni podatki, odločili, ali bodo uveljavljali svojo pravico, na primer do popravka v skladu s členom 16 splošne uredbe o varstvu podatkov šele, ko bodo vedeli, kateri osebni podatki se obdelujejo, za katere namene itd. Zato bo upravljavec posamezniku, na katerega se nanašajo osebni podatki, morda moral zagotoviti dodatne informacije, ki pojasnjujejo predložene podatke. Poudariti je treba, da mora upravljavec zaradi kompleksnosti obdelave podatkov zagotoviti sredstva za razumljivost podatkov in da s kompleksnostjo

[79] Smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, odstavek 35.

[80] Razumljivost je tesno povezana z zahtevo po uporabi jasnega in preprostega jezika (smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, odstavek 9). Kar je v odstavkih 12 do 16 navedeno o preprostem in jasnem jeziku v zvezi z informacijami iz členov 13 in 14 splošne uredbe o varstvu podatkov, velja tudi za komuniciranje v skladu s členom 15.

[81] Glej odstavek 128.

ni mogoče utemeljevati omejitve dostopa do vseh podatkov. Prav tako obveznosti upravljavca, da zagotovi jedrnate podatke, ni mogoče uporabiti kot utemeljitve za omejitev dostopa do vseh podatkov.

**Primer 27:** Na spletnem mestu e-trgovine se za namene trženja zbirajo podatki o ogledanih ali kupljenih predmetih. Del teh podatkov bo zajemal podatke v neobdelani obliki[82], ki niso bili analizirani in morda niso neposredno pomembni za bralca (kode, zgodovina dejavnosti itd.). Za takšne podatke, povezane z dejavnostmi posameznikov, na katere se nanašajo osebni podatki, prav tako velja pravica do dostopa in bi jih bilo zato treba posamezniku, na katerega se nanašajo osebni podatki, zagotoviti v odgovor na zahtevo za dostop. Pri zagotavljanju podatkov v neobdelani obliki je pomembno, da upravljavec sprejme ukrepe, potrebne za zagotovitev, da posameznik, na katerega se nanašajo osebni podatki, razume podatke, na primer s predložitvijo obrazložitvenega dokumenta, s katerim se podatki v neobdelani obliki pretvorijo v uporabniku prijazno obliko. Takšen dokument bi lahko tudi vseboval pojasnilo, da okrajšave in druge kratice, na primer „A“, pomenijo, da je bil nakup prekinjen, „B“ pa, da je bil nakup opravljen.

142. Element „lahko dostopen“ pomeni, da bi morale biti informacije iz člena 15 predložene na način, ki je posamezniku, na katerega se nanašajo osebni podatki, lahko dostopen. To velja na primer za razporeditev, ustrezne naslove in delitev na odstavke. Informacije bi bilo treba vedno zagotoviti v preprostem in jasnem jeziku. Upravljavec, ki ponuja storitev v državi, bi moral zagotoviti tudi odgovore v jeziku, ki ga razumejo posamezniki v tej državi, na katere se nanašajo osebni podatki. Spodbuja se tudi uporaba standardiziranih ikon, kadar olajšuje razumljivost in dostopnost informacij. Kadar se zahteva po informacijah nanaša na slepe in slabovidne posameznike, na katere se nanašajo osebni podatki, ali druge posameznike, na katere se nanašajo osebni podatki, ki imajo lahko težave z dostopom ali razumevanjem informacij, se od upravljavca pričakuje, da bo sprejel ukrepe za lažje razumevanje zagotovljenih informacij, vključno z ustnimi informacijami, kadar je to ustrezno[83]. Upravljavec bi moral posebno pozornost nameniti zagotavljanju, da lahko starejši, otroci, slepe in slabovidne osebe ali osebe s kognitivnimi ali drugimi motnjami uresničujejo svoje pravice, na primer s proaktivnim zagotavljanjem lahko dostopnih elementov za lažje uresničevanje teh pravic.

### 5.2.4 Za veliko količino informacij so potrebne posebne zahteve glede načina zagotavljanja informacij

143. Ne glede na sredstva, s katerimi se zagotavlja dostop, lahko obstaja nasprotje med količino informacij, ki jih mora upravljavec zagotoviti posameznikom, na katere se nanašajo osebni podatki, in zahtevo po jedrnatosti. Eden od načinov, da se doseže oboje, in primer ustreznega ukrepa za nekatere upravljavce, ko je treba zagotoviti veliko podatkov, je uporaba večdelnega pristopa. Ta pristop lahko posameznikom, na katere se nanašajo osebni podatki, olajša razumevanje podatkov. Kljub temu je treba poudariti, da je ta pristop mogoče uporabiti le v določenih okoliščinah in da ga je treba izvajati na način, ki ne omejuje pravice do dostopa, kot je pojasnjeno v nadaljevanju. Poleg tega uporaba večdelnega pristopa ne bi smela povzročiti dodatnega bremena za posameznika, na katerega se nanašajo osebni podatki. Zato bi bil tak najprimernejši v spletnem okolju. Večdelni pristop je zgolj način predstavitve informacij iz člena 15 na način, ki je skladen tudi z zahtevami iz člena 12(1) splošne uredbe

[82] Neobdelano obliko iz primera je treba razumeti kot neanalizirane podatke, na katerih temelji obdelava, in ne kot neobdelane podatke najnižje ravni, ki so lahko samo strojno berljivi (kot so biti).
[83] Glej smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, odstavek 21.

o varstvu podatkov, in se ne bi smel zamenjevati z možnostjo upravljavcev, da od posameznika, na katerega se nanašajo osebni podatki, zahtevajo, naj podrobno opredeli, na katere informacije ali dejavnosti obdelave se zahteva nanaša, kot je določeno v uvodni izjavi 63 splošne uredbe o varstvu podatkov[84].

144. Večdelni pristop v zvezi s pravico do dostopa pomeni, da lahko upravljavec v določenih okoliščinah osebne podatke in dopolnilne informacije, ki se zahtevajo v skladu s členom 15, zagotovi v različnih delih. Prvi del bi moral vključevati informacije o obdelavi in pravicah posameznika, na katerega se nanašajo osebni podatki, v skladu s členom 15(1)(a) do (h) in členom 15(2) ter prvi del obdelanih osebnih podatkov. V drugem delu bi bilo treba zagotoviti več osebnih podatkov.

145. Pri odločanju o tem, katere informacije bi bilo treba predložiti v različnih delih, bi moral upravljavec upoštevati, katere informacije bi posameznik, na katerega se nanašajo osebni podatki, na splošno štel za najpomembnejše. V skladu z načelom pravičnosti bi moral prvi del vsebovati tudi informacije o obdelavi, ki najbolj vpliva na posameznika, na katerega se nanašajo osebni podatki[85]. Upravljavci morajo biti zmožni dokazati odgovornost za utemeljitev zgoraj navedenega.

**Primer 28:** Upravljavec analizira velike podatkovne nize, da bi stranke razvrstil v različne segmente glede na njihovo vedenje na spletu. V tem primeru je mogoče domnevati, da so informacije, za katere je najpomembneje, da jih posamezniki, na katere se nanašajo osebni podatki, pridobijo, informacije o tem, v kateri segment so bili vključeni. Zato je treba te informacije vključiti v prvi del. Tudi podatki v neobdelani obliki[86], ki še niso bili analizirani ali nadalje obdelani, kot na primer dejavnost uporabnika na spletnem mestu, so osebni podatki, za katere velja pravica do dostopa, vendar bi v nekaterih primerih lahko zadostovalo, da se te informacije zagotovijo v drugem delu.

146. Da bi se uporaba večdelnega pristopa štela za ustrezen ukrep, je treba posameznika, na katerega se nanašajo osebni podatki, že na začetku obvestiti, da so informacije iz člena 15 strukturirane v različne dele, in jim zagotoviti opis, katere osebne podatke in informacije bodo vsebovali različni deli. To bo posamezniku, na katerega se nanašajo osebni podatki, olajšalo odločitev o tem, do katerih delov želi dostopati. Opis bi moral objektivno odražati vse vrste osebnih podatkov, ki jih upravljavec dejansko obdeluje. Prav tako mora biti jasno, kako lahko posameznik, na katerega se nanašajo osebni podatki, pridobi dostop do različnih delov. Za dostop do različnih delov ne sme biti potreben nesorazmeren trud posameznika, na katerega se nanašajo osebni podatki, in ni pogojen s pripravo nove zahteve posameznika, na katerega se nanašajo osebni podatki. To pomeni, da morajo imeti posamezniki, na katere se nanašajo osebni podatki, možnost izbire, ali bodo dostopali do vseh delov naenkrat ali do enega ali dveh, če so s tem zadovoljni.

**Primer 29:** Posameznik, na katerega se nanašajo osebni podatki, vloži zahtevo za dostop do storitve pretakanja video vsebin. Zahteva se predloži z izbiro možnosti, ki je na voljo, ko se posamezniki, na katere se nanašajo osebni podatki, prijavijo v svoj račun. Posameznik, na katerega se nanašajo osebni podatki, ima dve možnosti, ki sta na spletni strani prikazani kot gumba. Prva možnost je prenos 1. dela osebnih podatkov in dopolnilnih informacij. To na primer vsebuje nedavno zgodovino pretakanja, informacije o računu in plačilih. Druga možnost je prenos 2. dela osebnih podatkov, ki vsebuje tehnične dnevniške datoteke o dejavnostih posameznikov, na katere se nanašajo osebni podatki, in pretekle

[84] Glej tudi oddelek 2.3.1.

[85] Glej smernice delovne skupine iz člena 29 o preglednosti, ki jih je potrdil Evropski odbor za varstvo podatkov, odstavek 36.

[86] Glej opombo 82.

informacije o računu. V tem primeru je upravljavec posameznikom, na katere se nanašajo osebni podatki, omogočil, da uresničujejo svojo pravico na način, ki jim ne povzroča dodatnega bremena.

**Različica 1:** Kadar posameznik, na katerega se nanašajo osebni podatki, izbere samo gumb za prenos 1. dela osebnih podatkov, mora upravljavec zagotoviti le 1. del podatkov.

**Različica 2**: Kadar posameznik, na katerega se nanašajo osebni podatki, izbere gumba za 1. in 2. del podatkov, upravljavec ne more sporočiti le 1. dela podatkov in zahtevati nove potrditve, preden predloži 2. del podatkov. Namesto tega je treba posamezniku, na katerega se nanašajo osebni podatki, zagotoviti oba dela podatkov, kot izhaja iz zahteve.

147. Uporaba večdelnega pristopa se ne bo štela za primerno za vse upravljavce ali v vseh primerih. Uporabiti bi jo bilo treba le, kadar bi posameznik, na katerega se nanašajo osebni podatki, težko razumel informacije, če bi bile navedene v celoti. Z drugimi besedami, upravljavec mora biti zmožen dokazati, da uporaba večdelnega pristopa posamezniku, na katerega se nanašajo osebni podatki, prinaša dodano vrednost, saj mu pomaga razumeti zagotovljene informacije. Večdelni pristop bi se zato štel za primernega le, kadar upravljavec obdela veliko osebnih podatkov o posamezniku, na katerega se nanašajo osebni podatki in ki vloži zahtevo, in kadar bi posameznik, na katerega se nanašajo osebni podatki, imel očitne težave pri dojemanju ali razumevanju informacij, če bi bilo treba zagotoviti vse naenkrat. Dejstvo, da bi bilo za zagotovitev informacij v skladu s členom 15 potrebno veliko truda in virov upravljavca, samo po sebi ni razlog za uporabo večdelnega pristopa.

### 5.2.5 Oblika

148. V skladu s členom 12(1) splošne uredbe o varstvu podatkov se informacije iz člena 15 zagotovijo v pisni obliki ali z drugimi sredstvi, vključno z elektronskimi sredstvi, kjer je ustrezno. Kar zadeva dostop do osebnih podatkov, ki se obdelujejo, člen 15(3) določa, da kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, in če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače, se informacije zagotovijo v elektronski obliki, ki je splošno uporabljana. Splošna uredba o varstvu podatkov ne opredeljuje, kaj je elektronska oblika, ki je splošno uporabljana. Zato obstaja več oblik, ki jih je mogoče uporabiti. Prav tako se bo sčasoma spreminjalo to, kar šteje za elektronsko obliko, ki je splošno uporabljana.

149. Kar bi se lahko štelo za elektronsko obliko, ki je splošno uporabljana, bi moralo temeljiti na objektivni oceni in ne na obliki, ki jo upravljavec uporablja pri svojem vsakodnevnem delovanju. Da bi ugotovil, katero obliko je treba v zadevnem primeru šteti za splošno uporabljano, bo moral upravljavec oceniti, ali obstajajo posebne oblike, ki se na splošno uporabljajo na njegovem področju delovanja ali v danem okviru. Kadar takih oblik, ki so splošno uporabljane, ni, bi bilo treba na splošno kot takšne šteti odprte formate, določene v mednarodnem standardu, kot je ISO. Vendar Evropski odbor za varstvo podatkov ne izključuje možnosti, da se lahko tudi za druge oblike šteje, da so splošno uporabljane v smislu člena 15(3). Evropski odbor za varstvo podatkov meni, da je pri ocenjevanju, ali je oblika elektronska oblika, ki je splošno uporabljana, pomembno, kako enostavno lahko posameznik dostopa do informacij, zagotovljenih v obstoječi obliki. V zvezi s tem je treba upoštevati, katere informacije je upravljavec zagotovil posamezniku, na katerega se nanašajo osebni podatki, o tem, kako dostopati do datoteke, zagotovljene v posebni obliki, na primer, katere programe ali programsko opremo lahko uporabi, da bi bila oblika posamezniku, na katerega se nanašajo osebni podatki, dostopnejša. Vendar posameznik, na katerega se nanašajo osebni podatki, ne bi smel biti zavezan k nakupu programske opreme, da bi pridobil dostop do informacij.

150. Pri odločanju o obliki, v kateri bi bilo treba zagotoviti kopijo osebnih podatkov in informacije v skladu s členom 15, mora upravljavec upoštevati, da mora oblika omogočati predstavitev informacij na

razumljiv in lahko dostopen način. Pomembno je, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovijo informacije v oprijemljivi, trajni obliki (besedilo, elektronsko). Ker bi se morale informacije ohraniti dlje časa, so informacije v pisni obliki, vključno z elektronskimi sredstvi, načeloma primernejše od drugih oblik. Kopija osebnih podatkov se lahko po potrebi shrani na elektronski pomnilniški napravi, kot sta zgoščenka ali USB.

151. Opozoriti je treba, da zagotovitev dostopa do osebnih podatkov posameznikom, na katere se nanašajo osebni podatki, ne zadostuje, da bi upravljavec lahko štel, da so prejeli kopijo osebnih podatkov. Da bi bila izpolnjena zahteva po zagotovitvi kopije osebnih podatkov in če se podatki zagotovijo elektronsko/digitalno, morajo imeti posamezniki, na katere se nanašajo osebni podatki, možnost, da svoje podatke prenesejo v elektronski obliki, ki je splošno uporabljana.

152. Upravljavec je odgovoren za odločitev o ustrezni obliki, v kateri bodo zagotovljeni osebni podatki. Upravljavec lahko dokumente, ki vsebujejo osebne podatke o posameznikih, na katere se nanašajo osebni podatki, ki so predložili zahtevo, predloži v izvirni obliki, vendar k temu ni nujno zavezan. Upravljavec bi lahko na primer za vsak primer posebej zagotovil dostop do kopije nosilca podatkov glede na potrebo po preglednosti (na primer, da se preveri točnost podatkov, ki jih upravljavec hrani v primeru zahteve za dostop do zdravstvene kartoteke, ali zvočnega posnetka, katerega prepis je sporen). Vendar je Sodišče Evropske unije v svoji razlagi pravice do dostopa na podlagi Direktive 95/46/ES navedlo, da „za uresničitev te pravice zadostuje, da ta prosilec prejme popoln pregled vseh teh podatkov v razumljivi obliki, to je obliki, ki temu prosilcu omogoča, da se z njimi seznani in preveri, ali so točni in ali se obdelujejo v skladu s to direktivo, da bi lahko po potrebi izvrševal pravice, ki mu jih daje“[87]. Splošna uredba o varstvu podatkov v nasprotju z navedeno direktivo izrecno določa obveznost, da se posamezniku, na katerega se nanašajo osebni podatki, zagotovi kopija osebnih podatkov, ki se obdelujejo. Vendar to ne pomeni, da ima posameznik, na katerega se nanašajo osebni podatki, vedno pravico pridobiti kopijo dokumentov, ki vsebujejo osebne podatke, ampak nespremenjeno kopijo osebnih podatkov, ki se obdelujejo, v teh dokumentih.[88] Takšna kopija osebnih podatkov bi se lahko zagotovila z zbirko, ki vsebuje vse osebne podatke, za katere velja pravica do dostopa, če zbirka omogoča, da se posameznik, na katerega se nanašajo osebni podatki, seznani z obdelavo in preveri njeno zakonitost. Zato ni protislovja med besedilom splošne uredbe o varstvu podatkov in sodbo Sodišča Evropske unije v zvezi s tem. Beseda „pregled“ v sodbi se ne sme napačno razlagati v smislu, da zbirka ne bi zajemala vseh podatkov, za katere velja pravica do dostopa, temveč je le način za predstavitev vseh teh podatkov, ne da bi se omogočil dostop do osnovnih dokumentov, ki vsebujejo osebne podatke. Ker mora zbirka vsebovati kopijo osebnih podatkov, je treba poudariti, da se je ne sme narediti tako, da se na nek način spremeni vsebina informacij.

**Primer 30:** Posameznik, na katerega se nanašajo osebni podatki, je že več let zavarovan pri zavarovalnici. Prišlo je do več zavarovanih dogodkov. V vsakem primeru sta si posameznik, na katerega se nanašajo osebni podatki, in zavarovalnica izmenjala pisno korespondenco po elektronski pošti. Ker je moral posameznik, na katerega se nanašajo osebni podatki, zagotoviti informacije o posebnih okoliščinah vsakega dogodka, korespondenca vključuje veliko osebnih informacij o njem (hobijih, sostanovalcih, vsakdanjih navadah itd.). V nekaterih primerih je prišlo do nesoglasja glede obveznosti zavarovalnice, da posamezniku, na katerega se nanašajo osebni podatki, izplača odškodnino, kar je povzročilo izmenjavo obsežne komunikacije. Zavarovalnica vso to korespondenco hrani. Posameznik, na katerega se nanašajo osebni podatki, predloži zahtevo za dostop. V tem primeru upravljavcu ni treba

[87] Sodišče Evropske unije, združeni zadevi C-141/12 in 372/12, YS in drugi, točka 60.
[88] Vprašanja v zvezi s to temo se obravnavajo v zadevah, ki sta trenutno pred Sodiščem Evropske unije (C-487/21 in C-307/21).

nujno zagotoviti izvirnih elektronskih sporočil tako, da jih posreduje posamezniku, na katerega se nanašajo osebni podatki. Namesto tega bi se upravljavec lahko odločil, da korespondenco po elektronski pošti, ki vsebuje osebne podatke posameznika, na katerega se nanašajo osebni podatki, zbere v datoteki, ki se zagotovi posamezniku, na katerega se nanašajo osebni podatki.

153. Ne glede na obliko, v kateri upravljavec zagotovi osebne podatke, npr. s predložitvijo dejanskih dokumentov, ki vsebujejo osebne podatke, ali zbirke osebnih podatkov, informacije izpolnjujejo zahteve glede preglednosti iz člena 12 splošne uredbe o varstvu podatkov. V nekaterih primerih bi bilo mogoče te zahteve izpolniti tako, da bi se izdelala zbirka in/ali pridobili podatki na način, ki omogoča, da so informacije lahko razumljive. V drugih primerih se informacije bolje razumejo, če se zagotovi kopija dejanskega dokumenta, ki vsebuje osebne podatke. Zato je treba najprimernejšo obliko določiti za vsak primer posebej.

154. V zvezi s tem si je treba zapomniti, da obstaja razlika med pravico do dostopa v skladu s členom 15 splošne uredbe o varstvu podatkov in pravico do prejema kopije upravnih dokumentov, ki jo ureja nacionalno pravo, pri čemer je slednja pravica do prejema kopije dejanskega dokumenta. To ne pomeni, da pravica do dostopa iz člena 15 splošne uredbe o varstvu podatkov izključuje možnost prejema kopije dokumenta/medija, na katerem so osebni podatki.

155. V nekaterih primerih je oblika, v kateri bi bilo treba osebne podatke zagotoviti, odvisna od samih osebnih podatkov. Na primer, kadar so osebni podatki ročno izpisane informacije posameznika, na katerega se nanašajo osebni podatki, bo le-temu morda treba zagotoviti fotokopijo teh ročno izpisanih informacij, saj je to ročno napisano besedilo osebni podatek. To bi se lahko zgodilo zlasti, kadar je ročno napisano besedilo pomembno za obdelavo, npr. analizo pisave. Enako na splošno velja za zvočne posnetke, saj je glas posameznika, na katerega se nanašajo osebni podatki, sam po sebi osebni podatek. V nekaterih primerih pa se dostop lahko omogoči tako, da se na primer zagotovi prepis pogovora, če se posameznik, na katerega se nanašajo osebni podatki, in upravljavec tako dogovorita.

156. Opozoriti je treba, da se določbe o zahtevah glede oblike razlikujejo z vidika pravice do dostopa in pravice do prenosljivosti podatkov. Medtem ko pravica do prenosljivosti podatkov v skladu s členom 20 splošne uredbe o varstvu podatkov zahteva, da se informacije zagotovijo v strojno berljivi obliki, pravica do informacij iz člena 15 tega ne zahteva. To pomeni, da bi lahko bile oblike, ki ne veljajo za primerne za izpolnjevanje zahteve za prenosljivost podatkov, na primer datoteke pdf, vseeno primerne za izpolnitev zahteve za dostop.

## 5.3 Časovni okvir za zagotovitev dostopa

157. Člen 12(3) splošne uredbe o varstvu podatkov določa, da upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotovi informacije o ukrepih, sprejetih na zahtevo v skladu s členom 15, brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev, pod pogojem, da je bil posameznik, na katerega se nanašajo osebni podatki, o takem podaljšanju obveščen v enem mesecu po prejemu zahteve. Ta obveznost obveščanja posameznika, na katerega se nanašajo osebni podatki, o podaljšanju in razlogih zanj se ne bi smela zamenjevati z informacijami, ki jih je treba zagotoviti nemudoma in najpozneje v enem mesecu, če upravljavec ne ukrepa na zahtevo, kot je določeno v členu 12(4) splošne uredbe o varstvu podatkov.

158. Upravljavec se odzove in praviloma zagotovi informacije iz člena 15 brez nepotrebnega odlašanja, kar pomeni, da bi bilo treba informacije zagotoviti čim prej. To pomeni, da če je mogoče zahtevane informacije zagotoviti v manj kot enem mesecu, bi moral upravljavec to storiti. Evropski odbor za

varstvo podatkov meni tudi, da je treba v nekaterih primerih rok za odgovor na zahtevo prilagoditi obdobju hrambe, da se lahko zagotovi dostop[89].

159. Rok začne teči, ko upravljavec prejme zahtevo iz člena 15, kar pomeni, da jo prejme prek enega od svojih uradnih kanalov[90]. Ni nujno, da je upravljavec dejansko seznanjen z zahtevo. Kadar pa mora upravljavec zaradi negotovosti glede identitete osebe, ki predloži zahtevo, komunicirati s posameznikom, na katerega se nanašajo osebni podatki, lahko rok začasno preneha teči, dokler upravljavec od posameznika, na katerega se nanašajo osebni podatki, ne pridobi potrebnih informacij, pod pogojem, da upravljavec dodatne informacije zahteva brez nepotrebnega odlašanja. Enako velja, kadar upravljavec od posameznika, na katerega se nanašajo osebni podatki, zahteva, naj navede dejanja obdelave, na katera se zahteva nanaša, če so izpolnjeni pogoji iz uvodne izjave 63[91].

**Primer 31**: Po prejemu zahteve se upravljavec takoj odzove in zaprosi za informacije, ki jih potrebuje za potrditev identitete osebe, ki je predložila zahtevo. Ta oseba odgovori šele nekaj dni pozneje, informacije, ki jih posameznik, na katerega se nanašajo osebni podatki, pošlje za preverjanje identitete, pa se ne zdijo zadostne, zato mora upravljavec zahtevati pojasnila. V tem primeru bo rok začasno prenehal teči, dokler upravljavec ne pridobi dovolj informacij, da preveri identiteto posameznika, na katerega se nanašajo osebni podatki.

160. Rok za odgovor na zahtevo za dostop je treba izračunati v skladu z Uredbo št. 1182/71[92].

**Primer 32:** Organizacija prejme zahtevo 5. marca. Rok začne teči isti dan. Organizacija ima torej čas, da najpozneje do vključno 5. aprila izpolni zahtevo.

**Primer 33:** Če organizacija prejme zahtevek 31. avgusta in ker je naslednji mesec krajši, ni istega datuma, je rok za odgovor najpozneje zadnji dan naslednjega meseca, torej 30. september.

161. Če je zadnji dan tega roka konec tedna ali državni praznik, mora upravljavec odgovoriti do naslednjega delovnega dne.

162. Upravljavec lahko v nekaterih okoliščinah podaljša rok za odgovor na zahtevo za dostop za dodatna dva meseca, če je to potrebno, pri čemer upošteva kompleksnost in število zahtev. Poudariti je treba, da je ta možnost izjema od splošnega pravila in je ne bi smeli pretirano uporabljati. Če so upravljavci pogosto prisiljeni podaljšati rok, bi to lahko pomenilo, da morajo nadalje razviti svoje splošne postopke za obravnavo zahtev.

163. Kaj pomeni kompleksna zahteva, se razlikuje glede na posebne okoliščine posameznega primera. Nekateri dejavniki, ki bi se lahko šteli za pomembne, so na primer:

- količina podatkov, ki jih obdeluje upravljavec,
- kako se hranijo informacije, zlasti kadar jih je težko pridobiti, na primer kadar podatke obdelujejo različne enote organizacije,

[89] Glej oddelek 2.3.3.
[90] V nekaterih državah članicah nacionalna zakonodaja določa, kdaj se sporočilo šteje za prejeto, ob upoštevanju koncev tedna in državnih praznikov.
[91] Glej tudi oddelek 2.3.1.
[92] Uredba Sveta (EGS, Euratom) št. 1182/71 z dne 3. junija 1971 o določitvi pravil glede rokov, datumov in iztekov rokov.

- potreba po zakrivanju informacij, kadar se uporablja izjema, na primer informacij o drugih posameznikih, na katere se nanašajo osebni podatki, ali informacij, ki so poslovna skrivnost, in
- kadar je za razumljivost informacij potrebno nadaljnje delo.

164. Zgolj dejstvo, da bi bilo za izpolnitev zahteve potrebno veliko truda, ne pomeni, da je zahteva kompleksna. Prav tako se podaljšanje roka ne sproži zaradi tega, ker veliko podjetje prejme veliko zahtev. Kadar pa upravljavec začasno prejema veliko zahtev, na primer zaradi izrednega obveščanja javnosti o svojih dejavnostih, bi se to lahko štelo za utemeljen razlog za podaljšanje roka za odgovor. Kljub temu bi moral imeti upravljavec, zlasti tisti, ki ravna z veliko količino podatkov, vzpostavljene postopke in mehanizme, da bi lahko v običajnih okoliščinah zahteve obravnaval v roku.

# 6 OMEJITVE PRAVICE DO DOSTOPA

## 6.1 Splošne opombe

165. Za pravico do dostopa veljajo omejitve, ki izhajajo iz člena 15(4) splošne uredbe o varstvu podatkov (pravice in svoboščine drugih) in člena 12(5) splošne uredbe o varstvu podatkov (očitno neutemeljene ali pretirane zahteve). Poleg tega lahko pravo Unije ali držav članic omeji pravico do dostopa v skladu s členom 23 splošne uredbe o varstvu podatkov. Odstopanja v zvezi z obdelavo osebnih podatkov v znanstvene, zgodovinskoraziskovalne ali statistične namene ali namene arhiviranja v javnem interesu lahko temeljijo na členu 89(2) oziroma (3) splošne uredbe o varstvu podatkov, odstopanja v zvezi z obdelavo v novinarske namene ali zaradi akademskega, umetniškega ali književnega izražanja pa lahko temeljijo na členu 85(2) splošne uredbe o varstvu podatkov.

166. Opozoriti je treba, da splošna uredba o varstvu podatkov poleg zgoraj navedenih omejitev, odstopanj in morebitnih omejitev ne dovoljuje nobenih nadaljnjih izjem ali odstopanj od pravice do dostopa. To med drugim pomeni, da je pravica do dostopa brez vsakega splošnega pridržka glede sorazmernosti v zvezi s prizadevanji, ki jih mora upravljavec vložiti v izpolnitev zahteve posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 15 splošne uredbe o varstvu podatkov[93]. Pravica do dostopa se prav tako ne sme omejiti s pogodbo med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki.

167. V skladu z uvodno izjavo 63 se pravica do dostopa dodeli posameznikom, na katere se nanašajo osebni podatki, da bi se seznanili z obdelavo in preverili njeno zakonitost. Pravica do dostopa posamezniku, na katerega se nanašajo osebni podatki, med drugim omogoča, da glede na okoliščine doseže, da se osebne podatke popravi, izbriše ali blokira[94]. Vendar posameznikom, na katere se nanašajo osebni podatki, ni treba navesti razlogov ali utemeljiti svoje zahteve. Če so izpolnjene zahteve iz člena 15 splošne uredbe o varstvu podatkov, bi bilo treba namene, na katerih temelji zahteva, šteti za brezpredmetne[95].

---

[93] Kadar upravljavec obdeluje veliko količino informacij v zvezi s posameznikom, na katerega se nanašajo osebni podatki, kot je navedeno v uvodni izjavi 63 splošne uredbe o varstvu podatkov, lahko od tega posameznika zahteva, naj podrobno opredeli, na katere informacije ali dejavnosti obdelave se zahteva nanaša. Glej tudi oddelek 2.3.1.

[94] Sodišče Evropske unije, združeni zadevi C-141/12 in C-372/12, YS in drugi.

[95] To ne posega v katero koli veljavno nacionalno pravo, ki je v skladu z zahtevami iz člena 23 splošne uredbe o varstvu podatkov, glej poglavje 6.4.

## 6.2 Člen 15(4) splošne uredbe o varstvu podatkov

168. V skladu s členom 15(4) splošne uredbe o varstvu podatkov pravica do pridobitve kopije ne vpliva negativno na pravice in svoboščine drugih. Pojasnila o tej omejitvi so navedena v petem in šestem stavku uvodne izjave 63. Ta pravica ne bi smela negativno vplivati na pravice ali svoboščine drugih, vključno s poslovnimi skrivnostmi ali intelektualno lastnino, ter predvsem na avtorske pravice, ki ščitijo programsko opremo.
To pa ne bi smelo povzročiti, da se posamezniku, na katerega se nanašajo osebni podatki, zavrne dostop do vseh informacij. Pri razlagi člena 15(4) splošne uredbe o varstvu podatkov je potrebna posebna pozornost, da se ne bi neupravičeno razširile omejitve iz člena 23 splošne uredbe o varstvu podatkov, ki so dovoljene le pod strogimi pogoji.

169. Člen 15(4) splošne uredbe o varstvu podatkov se uporablja za pravico do pridobitve kopije podatkov, ki je glavni način zagotavljanja dostopa do obdelanih podatkov (drugi sestavni del pravice do dostopa). Uporablja se tudi, če se dostop do osebnih podatkov izjemoma odobri na drug način kot s kopijo, pri čemer se upoštevajo pravice in svoboščine drugih. Na primer, ni utemeljene razlike glede na to, ali na poslovne skrivnosti vpliva predložitev kopije ali odobritev dostopa posamezniku, na katerega se nanašajo osebni podatki, na kraju samem. Člen 15(4) splošne uredbe o varstvu podatkov se ne uporablja za dodatne informacije o obdelavi, kot je navedeno v členu 15(1)(a) do (h) splošne uredbe o varstvu podatkov.

170. V skladu z uvodno izjavo 63 nasprotujoče si pravice in svoboščine vključujejo poslovne skrivnosti ali intelektualno lastnino ter zlasti avtorske pravice, ki ščitijo programsko opremo. Te izrecno navedene pravice in svoboščine bi bilo treba obravnavati zgolj kot primere, saj se za vsako pravico ali svoboščino, ki temelji na pravu Unije ali pravu države članice, načeloma lahko šteje, da se sklicuje na omejitev iz člena 15(4) splošne uredbe o varstvu podatkov[96]. Zato se lahko pravica do varstva osebnih podatkov (člen 8 Listine Evropske unije o temeljnih pravicah) prav tako šteje za zadevno pravico v smislu člena 15(4) splošne uredbe o varstvu podatkov. Kar zadeva pravico do pridobitve kopije, je pravica drugih do varstva podatkov značilen primer, v katerem je treba oceniti omejitev. Poleg tega je treba upoštevati pravico do zaupnosti korespondence, na primer v zvezi z zasebno korespondenco po elektronski pošti v okviru zaposlitve[97]. Pomembno je opozoriti, da vsak interes ne pomeni „pravice in svoboščine“ v skladu s členom 15(4) splošne uredbe o varstvu podatkov. Na primer, gospodarski interesi družbe, da ne razkrije osebnih podatkov, ne dosegajo praga za uporabo izjeme iz člena 15(4), če razkritje ne vpliva na poslovne skrivnosti, pravice intelektualne lastnine ali druge zaščitene pravice.

171. „Drugi[h]“ pomeni vsako drugo osebo ali subjekt, razen posameznika, na katerega se nanašajo osebni podatki in ki uveljavlja svojo pravico do dostopa. Zato se lahko upoštevajo pravice in svoboščine upravljavca ali obdelovalca (na primer pri ohranjanju zaupnosti poslovnih skrivnosti in intelektualne lastnine). Če bi zakonodajalec EU želel izključiti pravice in svoboščine upravljavcev ali obdelovalcev, bi uporabil izraz „tretja oseba“, ki je opredeljen v členu 4(10) splošne uredbe o varstvu podatkov.

172. Splošni pomislek, da bi izpolnitev zahteve za dostop lahko vplivala na pravice in svoboščine drugih, ne zadostuje za sklicevanje na člen 15(4) splošne uredbe o varstvu podatkov. Upravljavec mora biti zmožen dokazati, da bi bile v konkretnem primeru pravice ali svoboščine drugih dejansko prizadete.

---

[96] Teža ali prednost nasprotujočih si pravic in svoboščin ni vprašanje opredelitve pojmov „pravice in svoboščine“. Vendar je uravnoteženje takšnih interesov del drugega koraka ocene, ali se uporablja člen 15(4). Glej odstavek 173 spodaj.

[97] ESČP, Bărbulescu proti Romuniji, št. 61496/08, točka 80, 5. september 2017.

**Primer 34:** Zdaj odrasla oseba je bila v preteklosti več let v oskrbi urada za mladino. Zadevne datoteke lahko vsebujejo občutljive informacije o drugih osebah (starši, socialni delavci, drugi mladoletniki). Vendar zahteve po informacijah posameznika, na katerega se nanašajo osebni podatki, na podlagi tega razloga na splošno ni mogoče zavrniti s sklicevanjem na člen 15(4) splošne uredbe o varstvu podatkov. Namesto tega mora urad za mladino kot upravljavec podrobno preučiti pravice in svoboščine drugih ter jih izkazati. Glede na zadevne interese in njihovo relativno težo se lahko zagotovitev takšnih posebnih informacij zavrne (npr. z zakritjem imen).

173. Kar zadeva uvodno izjavo 4 splošne uredbe o varstvu podatkov in utemeljitev člena 52(1) Listine Evropske unije o temeljnih pravicah, pravica do varstva osebnih podatkov ni absolutna pravica[98]. Zato je tudi treba uresničevanje pravice do dostopa uravnotežiti z drugimi temeljnimi pravicami v skladu z načelom sorazmernosti. Kadar ima glede na oceno iz člena 15(4) splošne uredbe o varstvu podatkov izpolnitev zahteve škodljive (negativne) učinke na pravice in svoboščine drugih udeležencev (prvi korak), je treba pretehtati interese vseh udeležencev ob upoštevanju posebnih okoliščin primera ter zlasti verjetnosti in resnosti tveganj, ki jih predstavlja sporočanje podatkov. Upravljavec bi si moral prizadevati za uskladitev nasprotujočih si pravic (drugi korak), na primer z izvajanjem ustreznih ukrepov za zmanjšanje tveganja za pravice in svoboščine drugih. Kot je poudarjeno v uvodni izjavi 63, varstvo pravic in svoboščin drugih na podlagi člena 15(4) splošne uredbe o varstvu podatkov ne bi smelo povzročiti, da se posamezniku, na katerega se nanašajo osebni podatki, zavrne dostop do vseh informacij. To na primer pomeni, da če velja omejitev, je treba informacije o drugih narediti čim bolj nečitljive, namesto da se zavrne zagotovitev kopije osebnih podatkov. Če pa ni mogoče najti rešitve za uskladitev zadevnih pravic, se mora upravljavec v naslednjem koraku odločiti, katera od nasprotujočih si pravic in svoboščin prevlada (tretji korak).

**Primer 35**: Trgovec na drobno svojim strankam ponuja možnost, da naročijo proizvode prek telefonske linije, ki jo upravlja njegova služba za stranke. Trgovec na drobno hrani posnetek klicev za namene dokazovanja trgovinskega poslovanja v skladu s strogimi zahtevami veljavne zakonodaje. Stranka želi prejeti kopijo posnetka svojega pogovora z zastopnikom službe za stranke. V prvem koraku trgovec na drobno analizira zahtevo in ugotovi, da evidenca vsebuje osebne podatke, ki se nanašajo tudi na nekoga drugega, in sicer na zastopnika službe za stranke. V drugem koraku mora trgovec na drobno uravnotežiti nasprotujoče si interese, da oceni, ali bi zagotovitev kopije vplivala na pravice in svoboščine drugih, pri čemer upošteva zlasti verjetnost in resnost morebitnih tveganj za pravice in svoboščine zastopnika službe za stranke pri posredovanju evidence stranki. Trgovec na drobno ugotovi, da je v evidenci zelo malo osebnih podatkov o zastopniku službe za stranke, in sicer samo njegov glas. Trgovec na drobno/upravljavec ugotovi, da zastopnika ni mogoče zlahka identificirati. Poleg tega je vsebina pogovora strokovne narave, sogovornik pa je bil posameznik, na katerega se nanašajo osebni podatki. Upravljavec na podlagi zgoraj navedenih okoliščin objektivno sklepa, da pravica do dostopa ne vpliva negativno na pravice in svoboščine zastopnika službe za stranke, zato lahko posamezniku, na katerega se nanašajo osebni podatki, zagotovi popolno evidenco, vključno z deli zvočnega posnetka, ki se nanašajo na zastopnika službe storitve za stranke.

**Primer 36:** Stranka trgovine z medicinskimi pripomočki želi dostop do rezultatov meritev v zvezi z njenimi nogami na podlagi člena 15 splošne uredbe o varstvu podatkov. Trgovina z medicinskimi pripomočki je izmerila noge posameznika, na katerega se nanašajo osebni podatki, da bi zanj izdelala medicinske kompresijske nogavice. Zdi se, da je imela trgovina z medicinskimi pripomočki

[98] Glej na primer tudi sodbo Sodišča Evropske unije, združeni zadevi C-92/09 in C-93/09, Volker und Markus Schecke GbR in Hartmut Eifert/Land Hessen [VS], 9. november 2010, točka 48.

veliko izkušenj in je vzpostavila poseben način za natančno merjenje. Po merjenju v trgovini z medicinskimi pripomočki želi stranka uporabiti rezultate meritev za nakup cenejših nogavic drugje (želi jih naročiti v spletni trgovini). Trgovina z medicinskimi pripomočki delno zavrne dostop do podatkov na podlagi člena 15(4) splošne uredbe o varstvu podatkov, pri čemer trdi, da so bili rezultati zaradi posebnih in natančnih merilnih tehnik zaščiteni kot poslovna skrivnost. Če lahko upravljavec dokaže, da:

- posamezniku, na katerega se nanašajo osebni podatki, ni mogoče zagotoviti informacij o rezultatih meritev, ne da bi se razkrilo, kako so bile meritve opravljene, in
- da so informacije o tem, kako so bile opravljene meritve, po potrebi vključno z natančno določitvijo merilnih točk, poslovna skrivnost,

lahko uporabi člen 15(4) splošne uredbe o varstvu podatkov.

Upravljavec bi moral vseeno zagotoviti toliko informacij o rezultatih merjenja, kot je mogoče, ne da bi razkril svojo poslovno skrivnost, tudi če bi moral za to rezultate revidirati in urediti.

**Primer 37:** IGRALEC X je registriran kot uporabnik na igralni platformi PLATFORMA Y. Nekega dne prejme obvestilo, da je bil njegov spletni račun omejen. Ker se IGRALEC X ne more več prijaviti, prosi upravljavca za dostop do vseh osebnih podatkov, ki se nanašajo nanj. Poleg tega IGRALEC X zahteva dostop do informacij o razlogih za omejitev računa. PLATFORMA Y, upravljavec platforme za spletne igre, ki mu je bila predložena zahteva, uporabnike v splošnih pogojih poslovanja, ki so na voljo na njegovem spletnem mestu, obvešča, da bo vsaka vrsta goljufanja (predvsem z uporabo programske opreme tretjih oseb) povzročila začasno ali trajno prepoved dostopa do njegove platforme. PLATFORMA Y uporabnike v svoji politiki zasebnosti obvešča tudi o obdelavi osebnih podatkov za namen odkrivanja goljufij pri igrah na srečo v skladu z zahtevami iz člena 13 splošne uredbe o varstvu podatkov.

Ko PLATFORMA Y prejme zahtevo IGRALCA X za dostop, bi mu morala predložiti kopijo obdelanih osebnih podatkov v zvezi z njim. Glede na razlog za omejitev računa bi morala PLATFORMA Y IGRALCU X potrditi, da se je odločila omejiti njegov dostop do spletnih iger zaradi ene goljufije ali več goljufij pri igrah na srečo, ki so v nasprotju s splošnimi pogoji uporabe. PLATFORMA Y bi morala poleg informacij o obdelavi za odkrivanje goljufij pri igrah na srečo IGRALCU X odobriti dostop do informacij, ki jih je shranila o goljufijah IGRALCA X pri igrah na srečo, ki so vodile do omejitve. PLATFORMA Y bi morala IGRALCU X zagotoviti zlasti informacije, ki so privedle do omejitve računa (npr. pregled dnevnikov, datum in čas goljufanja, odkritje programske opreme tretje osebe ...), da lahko posameznik, na katerega se nanašajo osebni podatki (tj. IGRALEC X), preveri, ali je bila obdelava podatkov točna.

Vendar v skladu s členom 15(4) in uvodno izjavo 63 splošne uredbe o varstvu podatkov PLATFORMA Y ni dolžna razkriti nobenega dela tehničnega delovanja programske opreme za zaščito pred goljufijami, tudi če se te informacije nanašajo na IGRALCA X, če se to lahko šteje za poslovno skrivnost. Potrebno uravnoteženje interesov v skladu s členom 15(4) splošne uredbe o varstvu podatkov bo povzročilo, da poslovne skrivnosti PLATFORME Y preprečijo razkritje teh osebnih

podatkov, saj bi poznavanje tehničnega delovanja programske opreme za zaščito pred goljufijami uporabniku lahko omogočilo tudi, da se v prihodnosti izogne odkrivanju goljufij ali prevar[99].

174. Če upravljavci v celoti ali delno zavrnejo ukrepanje v zvezi z zahtevo za pravico do dostopa v skladu s členom 15(4) splošne uredbe o varstvu podatkov, morajo posameznika, na katerega se nanašajo osebni podatki, brez odlašanja, najpozneje pa v enem mesecu obvestiti o razlogih (člen 12(4) splošne uredbe o varstvu podatkov). Obrazložitev se mora nanašati na konkretne okoliščine, da lahko posamezniki, na katere se nanašajo osebni podatki, ocenijo, ali želijo ukrepati proti zavrnitvi. Vključevati mora informacije o možnosti vložitve pritožbe pri nadzornem organu (člen 77 splošne uredbe o varstvu podatkov) in uveljavljanja pravnega sredstva (člen 79 splošne uredbe o varstvu podatkov).

## 6.3 Člen 12(5) splošne uredbe o varstvu podatkov

175. Člen 12(5) splošne uredbe o varstvu podatkov upravljavcem omogoča, da razveljavijo zahteve za pravico do dostopa, ki so očitno neutemeljene ali pretirane. Ta pojma je treba razlagati ozko, saj se ne sme ogroziti načel preglednosti in brezplačnih pravic posameznikov, na katere se nanašajo osebni podatki.

176. Upravljavci morajo biti zmožni posamezniku dokazati, zakaj menijo, da je zahteva očitno neutemeljena ali pretirana, in pristojnemu nadzornemu organu na njegovo zahtevo pojasniti razloge za to. Vsako zahtevo bi bilo treba obravnavati posamično v okviru, v katerem je bila predložena, da se odloči, ali je očitno neutemeljena ali pretirana.

### 6.3.1 Kaj pomeni očitno neutemeljena?

177. Zahteva za pravico do dostopa je očitno neutemeljena, če zahteve iz člena 15 splošne uredbe o varstvu podatkov pri uporabi objektivnega pristopa nedvomno in očitno niso izpolnjene. Toda kot je pojasnjeno zlasti v oddelku 3 zgoraj, je zelo malo predpogojev za zahteve za pravico do dostopa. Zato Evropski odbor za varstvo podatkov poudarja, da je možnost sklicevanja na to, da je zahteva za pravico do dostopa v skladu s členom 12(5) splošne uredbe o varstvu podatkov „očitno neutemeljena, zelo omejena.

178. Poleg tega je treba opozoriti, da morajo upravljavci, preden se sklicujejo na omejitev, skrbno analizirati vsebino in obseg zahteve. Zahteva se na primer ne bi smela šteti za očitno neutemeljeno, če se nanaša na obdelavo osebnih podatkov, za katere se splošna uredba o varstvu podatkov ne uporablja (v tem primeru se zahteva sploh ne bi smela obravnavati kot zahteva iz člena 15).

179. Drugi primeri, v katerih je uporaba člena 12(5) splošne uredbe o varstvu podatkov vprašljiva, so zahteve v zvezi z dejavnostmi obveščanja ali obdelave, ki nedvomno in očitno niso predmet dejavnosti obdelave upravljavca.

**Primer 38**: Posameznik, na katerega se nanašajo osebni podatki, na občinski organ naslovi zahtevo v zvezi s podatki, ki jih obdeluje državni organ. Namesto trditve, da je zahteva očitno neutemeljena, bi

[99] Obseg informacij, zagotovljenih posameznikom, bo zelo odvisen od okoliščin, ob upoštevanju narave upravljavca in narave kršitve pogojev uporabe. V nekaterih primerih lahko upravljavec v odgovor na zahtevo za dostop, za katero se uporablja člen 15(4), zagotovi le osnovne informacije.

bilo primernejše in lažje, če bi naslovni organ potrdil, da teh podatkov ne obdeluje (prvi sestavni del člena 15 splošne uredbe o varstvu podatkov: „ali“ se osebni podatki obdelujejo)[100].

180. Upravljavec ne bi smel domnevati, da je zahteva očitno neutemeljena, ker je posameznik, na katerega se nanašajo osebni podatki, predhodno predložil zahteve, ki so bile očitno neutemeljene ali pretirane, ali če vsebuje neobjektiven ali neprimeren jezik.

### 6.3.2 Kaj pomeni pretirano?

181. Splošna uredba o varstvu podatkov ne opredeljuje pojma „pretirano“. Po eni strani je mogoče glede na besedilo „zlasti ker se ponavljajo“ v členu 12(5) splošne uredbe o varstvu podatkov sklepati, da je glavni scenarij za uporabo tega dela v zvezi s členom 15 splošne uredbe o varstvu podatkov povezan s številom zahtev posameznika, na katerega se nanašajo osebni podatki, za pravico do dostopa. Po drugi strani navedeno besedilo kaže, da drugi razlogi, ki bi lahko povzročili pretiranost, niso vnaprej izključeni.

182. V skladu s členom 15(3) splošne uredbe o varstvu podatkov v zvezi s pravico do pridobitve kopije lahko posameznik, na katerega se nanašajo osebni podatki, upravljavcu predloži več kot eno zahtevo[101]. V primeru zahtev, ki bi se lahko štele za pretirane, je ocena „prekomernosti“ odvisna od analize, ki jo opravi upravljavec, in posebnosti sektorja, v katerem deluje.

183. V primeru naknadnih zahtev je treba presoditi, ali je bil prag razumnih časovnih presledkov (glej uvodno izjavo 63) presežen ali ne. Upravljavci morajo skrbno upoštevati posebne okoliščine vsakega primera.

184. Na primer, v primeru družbenih omrežij se pričakuje, da se nabor podatkov spreminja v krajših časovnih presledkih kot v primeru zemljiških knjig ali centralnih registrov gospodarskih družb. V primeru poslovnih partnerjev je treba upoštevati pogostost stikov s stranko. V skladu s tem se razlikujejo tudi „razumni časovni presledki“, v katerih lahko posamezniki, na katere se nanašajo osebni podatki, ponovno uresničujejo svojo pravico do dostopa. Čim pogosteje se spreminja podatkovna zbirka upravljavca, tem pogosteje se lahko posameznikom, na katere se nanašajo osebni podatki, dovoli, da zahtevajo dostop do svojih osebnih podatkov, ne da bi bilo to pretirano. Po drugi strani bi se lahko v nekaterih okoliščinah štelo, da se zahteva posameznika, na katerega se nanašajo osebni podatki, ponavlja, če jo predloži drugič.

185. Upravljavci bi morali pri odločanju, ali je pretekel razumen časovni presledek, glede na razumna pričakovanja posameznika, na katerega se nanašajo osebni podatki, upoštevati naslednje:

- kako pogosto se podatki spreminjajo – ali je malo verjetno, da bi se informacije med zahtevami spremenile? Če je jasno, da se zbirka podatkov obdeluje samo za shranjevanje in je posameznik, na katerega se nanašajo osebni podatki, s tem seznanjen, npr. zaradi predhodne zahteve za pravico do dostopa, bi to lahko kazalo, da je zahteva pretirana;
- naravo podatkov – na primer, ali so posebej občutljivi;

[100] Ali je organ, na katerega je bila naslovljena zahteva za dostop, upravičen, da zahtevo posreduje pristojnemu državnemu organu, pa je drugo vprašanje.
[101] V skladu z drugim stavkom člena 15(3) lahko upravljavec zaračuna razumno pristojbino za zahtevane nadaljnje kopije.

- namene obdelave – na primer, ali je verjetno, da bo obdelava osebi, ki je predložila zahtevo, povzročila škodo, če se razkrije;
- ali se naknadne zahteve nanašajo na isto vrsto informacij ali dejavnosti obdelave ali na druge[102].

**Primer 39 (mizar):** Posameznik, na katerega se nanašajo osebni podatki, **vsaka dva meseca** vloži zahtevo za dostop pri mizarju, ki mu je izdelal mizo. Mizar je v celoti odgovoril na prvo zahtevo. Pri odločanju o tem, ali je pretekel razumen časovni presledek, bi bilo treba upoštevati, da mizar obdeluje in zbira osebne podatke le občasno (prva alinea zgoraj) in ne v okviru svoje glavne dejavnosti, še manj verjetno pa je, da pogosto opravlja storitve za istega posameznika, na katerega se nanašajo osebni podatki. V tem primeru mizar posamezniku, na katerega se nanašajo osebni podatki, dejansko ni zagotovil več kot ene storitve, zato je malo verjetno, da je prišlo do sprememb nabora podatkov, ki se nanaša na tega posameznika. Zlasti glede na naravo in količino obdelanih osebnih podatkov se lahko tveganja, povezana z obdelavo, štejejo za nizka (druga alinea zgoraj), namen obdelave (zaračunavanje in izpolnjevanje obveznosti vodenja evidenc) pa verjetno ne bo škodoval posamezniku, na katerega se nanašajo osebni podatki (tretja alinea zgoraj). Poleg tega se zahteva nanaša na iste informacije kot zadnja zahteva (četrta alinea zgoraj). Take zahteve se zato lahko štejejo za pretirane, ker se ponavljajo.

**Primer 40 (platforma družbenih medijev):** Platforma družbenih medijev, katere glavna dejavnost je zbiranje in/ali obdelava osebnih podatkov posameznika, na katerega se nanašajo osebni podatki, izvaja obsežne kompleksne in stalne dejavnosti obdelave. Posameznik, na katerega se nanašajo osebni podatki in ki uporablja storitve platforme, predloži zahtevo za dostop **vsake tri mesece**. V tem primeru so pogoste spremembe osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, zelo verjetne (prva alinea zgoraj), širok nabor zbranih podatkov pa vključuje povzete občutljive osebne podatke (druga alinea zgoraj), ki se obdelujejo za namen prikaza ustrezne vsebine in članov mreže posamezniku, na katerega se nanašajo osebni podatki (tretja alinea). Zahteve za dostop vsake tri mesece se v teh okoliščinah načeloma ne bi štele za pretirane, čeprav se ponavljajo.

**Primer 41 (bonitetne agencije):** Tako kot pri družbenih omrežjih ni mogoče izključiti, da se bodo zadevni podatki, ki jih hranijo bonitetne agencije, spreminjali v veliko krajših časovnih presledkih kot na drugih področjih (prva alinea zgoraj). Vzrok za to so številni dejavniki, ki jih posameznik, na katerega se nanašajo osebni podatki, kot oseba od zunaj običajno ne pozna zaradi zapletenosti poslovnega modela. Odgovor na vprašanje, katere vrste podatkov je upravljavec zbral za izračun vrednosti ocene in ki so trenutno vključeni v izračun, lahko zato zagotovi le bonitetna agencija sama. Poleg tega imata lahko obdelava podatkov prek bonitetnih agencij in dobljena vrednost ocene daljnosežne posledice za posameznika, na katerega se nanašajo osebni podatki, v zvezi z načrtovanimi pravnimi posli, kot je sklepanje pogodb o nakupu, najemu ali zakupu (tretja alinea zgoraj).

V skladu z drugim stavkom člena 12(5) splošne uredbe o varstvu podatkov na splošno ni mogoče določiti posebnega časovnega presledka predložitve nadaljnje zahteve za dostop, v katerem bi se ta lahko štela za pretirano. Treba je celostno preučiti okoliščine posameznega primera. Vendar je glede na pomen obdelave podatkov za vsakdanje življenje posameznikov, na katere se nanašajo osebni podatki, mogoče domnevati, da bo **enoletni časovni presledek** med brezplačno zagotovljenimi

[102] Če se naknadna zahteva nanaša na isto vrsto informacij po obsegu IN času, ne gre za vprašanje pretiranosti, temveč za zahtevo za dodatno kopijo (glej oddelek 2.2.2.2).

informacijami v vsakem primeru predolg, da bi se lahko štelo, da je zahteva pretirana. Če se zahteva vloži v zelo kratkem časovnem presledku, bi moralo biti odločilno, ali ima posameznik, na katerega se nanašajo osebni podatki, razlog za domnevo, da se je informacija ali obdelava od zadnje zahteve spremenila. Na primer, če je posameznik, na katerega se nanašajo osebni podatki, izvedel finančno transakcijo, kot je najem posojila, bi moral imeti pravico zahtevati dostop do kreditnih informacij, čeprav je tako zahtevo predložil le malo pred tem in nanjo prejel odgovor.

186. Kadar je informacije mogoče enostavno zagotoviti z elektronskimi sredstvi ali daljinskim dostopom do varnega sistema, kar pomeni, da izpolnjevanje takih zahtev dejansko ne obremenjuje upravljavca, je malo verjetno, da bi se poznejše zahteve lahko štele za pretirane.

187. Če se zahteva prekriva s prejšnjo zahtevo, se lahko prekrivajoča zahteva na splošno šteje za pretirano, če in kolikor zajema popolnoma enake informacije ali dejavnosti obdelave in upravljavec prejšnje zahteve še ni izpolnil in ni zagotovil izpolnitve „brez nepotrebnega odlašanja“ (glej člen 12(3) splošne uredbe o varstvu podatkov). V praksi se lahko posledično obe zahtevi združita.

188. Dejstvo, da bi upravljavec potreboval veliko časa in truda za zagotovitev informacij ali kopije posamezniku, na katerega se nanašajo osebni podatki, samo po sebi ne more povzročiti pretirane zahteve[103]. Če so dejavnosti obdelave številne, to običajno pomeni večja prizadevanja pri izpolnjevanju zahtev za dostop. Toda kot je navedeno zgoraj, se lahko zahteve v nekaterih okoliščinah štejejo za pretirane zaradi drugih razlogov in ne, ker se ponavljajo. Evropski odbor za varstvo podatkov meni, da to zajema zlasti primere zlorabe sklicevanja na člen 15 splošne uredbe o varstvu podatkov, kar pomeni primere, ko posamezniki, na katere se nanašajo osebni podatki, čezmerno uresničujejo pravico do dostopa zgolj zato, da upravljavcu povzročijo škodo.

189. Glede na navedeno se zahteva ne bi smela šteti za pretirano, ker:

- posameznik, na katerega se nanašajo osebni podatki, ne navede nobenega razloga za zahtevo ali upravljavec meni, da zahteva ni smiselna;
- posameznik, na katerega se nanašajo osebni podatki, uporablja neprimeren ali nevljuden jezik;
- namerava posameznik, na katerega se nanašajo osebni podatki, podatke uporabiti za vložitev nadaljnjih zahtevkov zoper upravljavca[104].

190. Po drugi strani pa se zahteva lahko šteje za pretirano, na primer, če:

- posameznik vloži zahtevo, vendar hkrati ponudi, da jo bo umaknil, če od upravljavca prejme določeno korist; ali
- je zahteva zlonamerna in se uporablja za nadlegovanje upravljavca ali njegovih zaposlenih zgolj z namenom povzročanja motenj, na primer na podlagi dejstva, da:
    - je posameznik v sami zahtevi ali v drugih sporočilih izrecno navedel, da je njegov edini namen povzročiti motnje; ali

[103] Brez preskusa sorazmernosti, glej odstavek 166 zgoraj.
[104] To ne posega v katero koli veljavno nacionalno pravo, ki je v skladu z zahtevami iz člena 23 splošne uredbe o varstvu podatkov, glej poglavje 6.4.

- posameznik upravljavcu sistematično, npr. enkrat tedensko, pošilja različne zahteve v okviru kampanje, katerih namen in učinek je povzročitev motenj[105].

### 6.3.3 Posledice

191. V primeru očitno neutemeljene ali pretirane zahteve za pravico do dostopa lahko upravljavci v skladu s členom 12(5) splošne uredbe o varstvu podatkov bodisi zaračunajo razumno pristojbino (pri čemer upoštevajo upravne stroške posredovanja informacij ali sporočila ali izvajanja zahtevanega ukrepa) bodisi zavrnejo izpolnitev zahteve.

192. Evropski odbor za varstvo podatkov poudarja, da po eni strani upravljavcem pred zavrnitvijo ukrepanja v zvezi z zahtevo na splošno ni treba zaračunati razumne pristojbine. Po drugi strani pa ne morejo popolnoma prosto izbirati med obema možnostma. Dejansko morajo sprejeti ustrezno odločitev glede na posebne okoliščine primera. Čeprav si je težko predstavljati, da je zaračunavanje razumne pristojbine primeren ukrep v primeru očitno neutemeljenih zahtev, bo za pretirane zahteve – v skladu z načelom preglednosti – pogosto primerneje zaračunati pristojbino kot nadomestilo za upravne stroške, ki nastanejo zaradi ponavljajočih se zahtev.

193. Upravljavci morajo biti zmožni dokazati, da je zahteva očitno neutemeljena ali pretirana (tretji stavek člena 12(5) splošne uredbe o varstvu podatkov). Zato se priporoča, da se zagotovi ustrezna dokumentacija o dejstvih zadevnega primera. V skladu s členom 12(4) splošne uredbe o varstvu podatkov morajo upravljavci, če v celoti ali delno zavrnejo ukrepanje v zvezi z zahtevo za dostop, o tem brez odlašanja, najpozneje pa v enem mesecu po prejemu zahteve, obvestiti posameznika, na katerega se nanašajo osebni podatki:

- o razlogu za to,
- o pravici do vložitve pritožbe pri nadzornem organu,
- o možnosti uveljavljanja pravnih sredstev.

194. Preden zaračunajo razumno pristojbino na podlagi člena 12(5) splošne uredbe o varstvu podatkov, bi morali upravljavci posameznikom, na katere se nanašajo osebni podatki, sporočiti svojo namero. Slednjim je treba omogočiti, da se odločijo, ali bodo umaknili zahtevo, da bi se izognili pristojbini.

195. Neupravičene zavrnitve zahtev za pravico do dostopa se lahko štejejo za kršitve pravic posameznikov, na katere se nanašajo osebni podatki, v skladu s členi 12 do 22 splošne uredbe o varstvu podatkov, zato lahko pristojni nadzorni organi izvajajo popravljalna pooblastila, vključno z upravnimi globami na podlagi člena 83(5)(b) splošne uredbe o varstvu podatkov. Če posamezniki, na katere se nanašajo osebni podatki, menijo, da so bile kršene njihove pravice, imajo pravico do vložitve pritožbe na podlagi člena 77 splošne uredbe o varstvu podatkov.

## 6.4 Morebitne omejitve v pravu Unije ali držav članic na podlagi člena 23 splošne uredbe o varstvu podatkov in odstopanja

[105] „Sistematično pošiljanje v okviru kampanje“ pomeni, da posameznik, na katerega se nanašajo osebni podatki, umetno razdeli zahteve, ki bi jih bilo mogoče zlahka združiti, na ne le nekaj, ampak veliko posameznih delov z očitnim namenom povzročiti motnje.

196. Obseg obveznosti in pravic iz člena 15 splošne uredbe o varstvu podatkov se lahko omeji z zakonodajnimi ukrepi v pravu Unije ali držav članic[106].

197. Upravljavci, ki se nameravajo sklicevati na omejitev, ki temelji na nacionalnem pravu, morajo skrbno preveriti zahteve določbe zadevne nacionalne zakonodaje. Poleg tega je treba opozoriti, da morajo omejitve pravice do dostopa v pravu držav članic (ali Unije), ki temeljijo na členu 23 splošne uredbe o varstvu podatkov, strogo izpolnjevati pogoje iz te določbe. Evropski odbor za varstvo podatkov je izdal Smernice 10/2020 o omejitvah iz člena 23 splošne uredbe o varstvu podatkov z dodatnimi pojasnili v zvezi s tem. Kar zadeva pravico do dostopa, Evropski odbor za varstvo podatkov opozarja, da bi morali upravljavci omejitve preklicati takoj, ko okoliščine, ki jih upravičujejo, ne veljajo več[107].

198. Zakonodajni ukrepi, ki določajo omejitve v skladu s členom 23 splošne uredbe o varstvu podatkov, lahko določajo tudi, da se uresničevanje pravice časovno odloži, da se pravica uresničuje deloma ali omeji na nekatere vrste podatkov ali da se pravica lahko uresničuje posredno prek neodvisnega nadzornega organa[108].

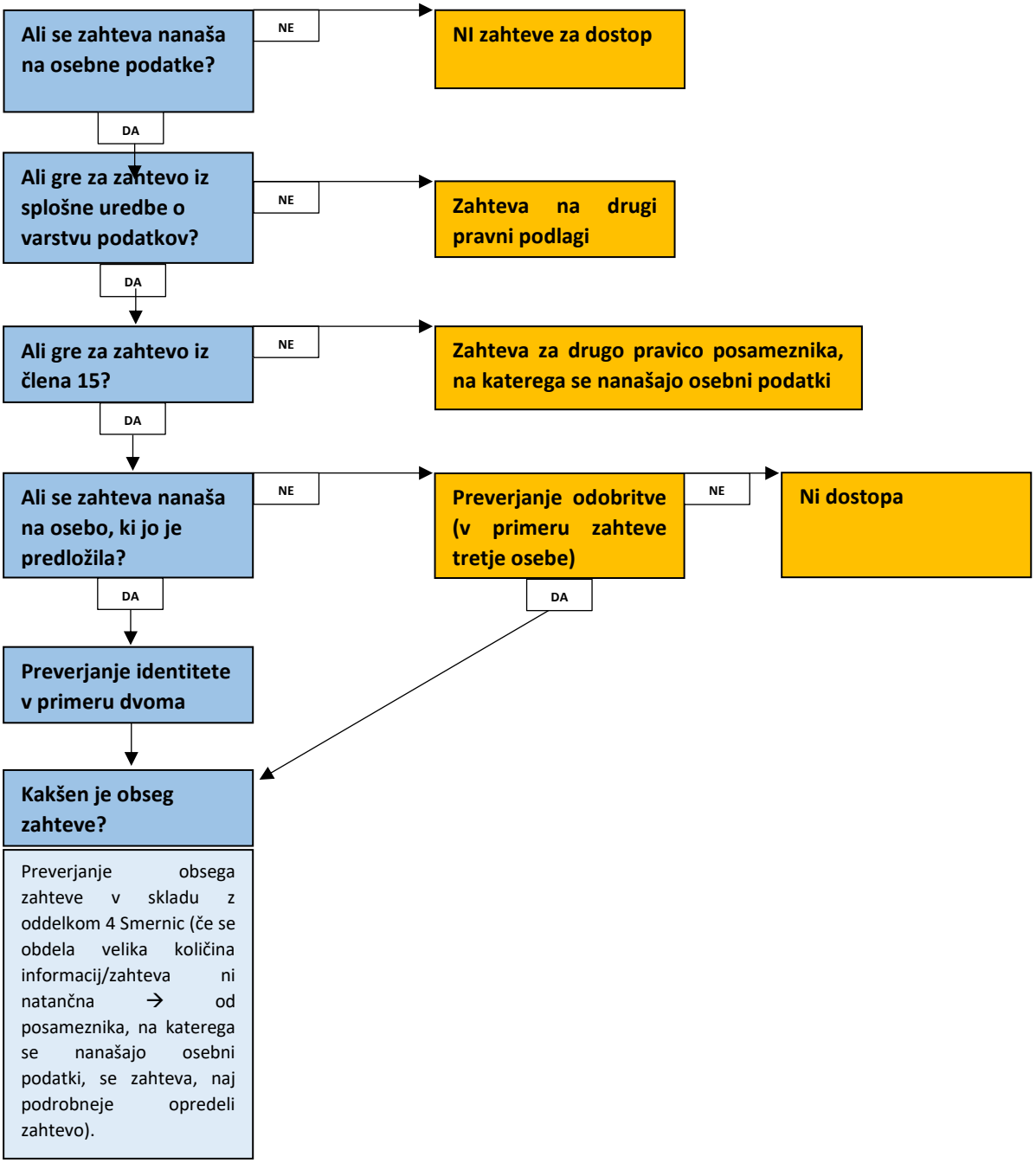
[106] Glej na primer člene 32 do 37 nemškega zveznega zakona o varstvu podatkov (BDSG), člena 16 in 17 norveškega zakona o osebnih podatkih ter poglavje 5 švedskega zakona o varstvu podatkov.

[107] Odstavek 76 Smernic 10/2020 o omejitvah iz člena 23 splošne uredbe o varstvu podatkov, različica 2.0, sprejetih 13. oktobra 2021.

[108] Odstavek 12 Smernic 10/2020 o omejitvah iz člena 23 splošne uredbe o varstvu podatkov, različica 2.0, sprejetih 13. oktobra 2021. Člen 34(3) nemškega zveznega zakona o varstvu podatkov na primer določa, da če javni organ posamezniku, na katerega se nanašajo osebni podatki, zaradi nekaterih omejitev ne zagotovi informacij v skladu z zahtevo za pravico do dostopa, se takšne informacije na zahtevo posameznika, na katerega se nanašajo osebni podatki, posredujejo zveznemu nadzornemu organu, razen če pristojni vrhovni zvezni organ (za organ, na katerega se nanaša zahteva) v posameznem primeru ugotovi, da bi to ogrozilo varnost federacije ali zvezne dežele. Italijanski zakonik o varstvu podatkov določa posreden dostop (prek organa), če bi dostop lahko negativno vplival na številne interese (npr. interes za boj proti pranju denarja), glej člen 2-L italijanskega zakonika o varstvu podatkov.

# PRILOGA – DIAGRAM PRETOKA

**1. korak: Kako razlagati in presojati zahtevo?**



### 2. korak: Kako odgovoriti na zahtevo (1)?

| Trije glavni sestavni deli pravice do dostopa (struktura člena 15) | | |
|---|---|---|
| Potrditev, ali se osebni podatki obdelujejo ali ne | Dostop do osebnih podatkov | Dodatne informacije o namenih, uporabnikih itd. (člen 15(1)(a)–(h)) |

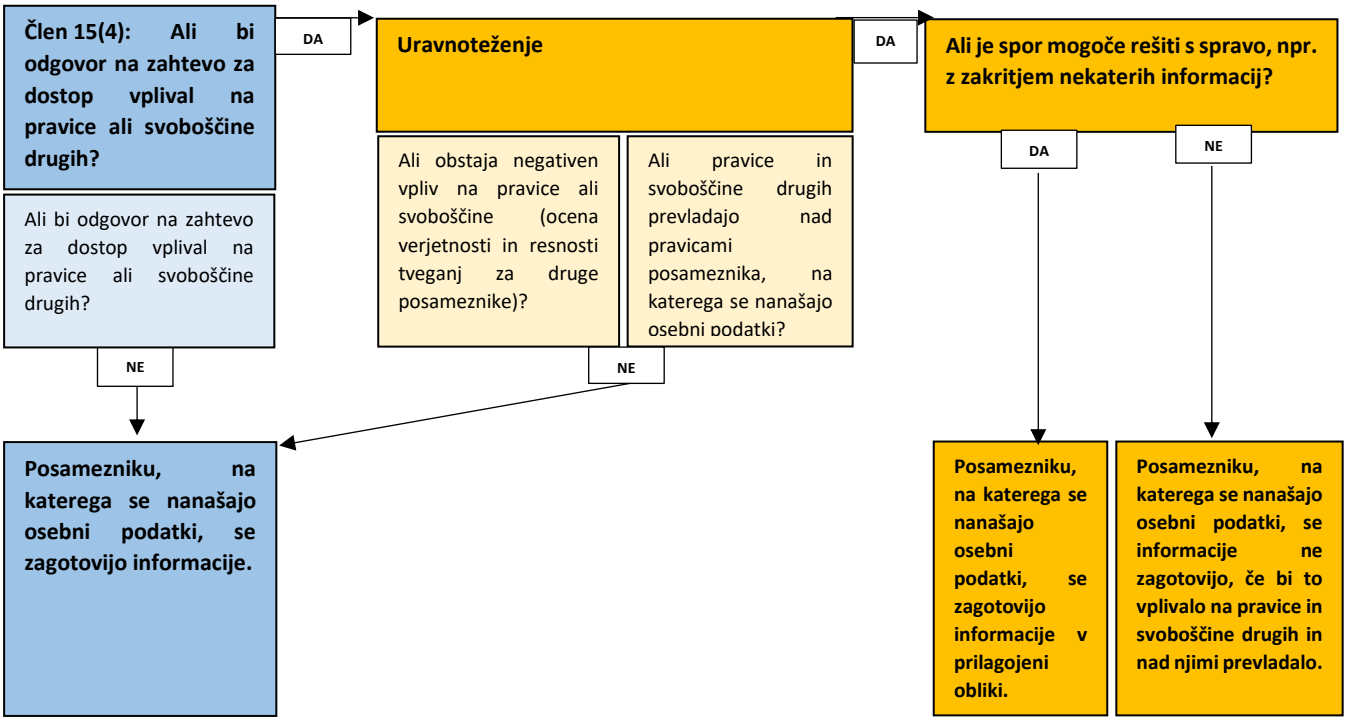
### 2. korak: Kako odgovoriti na zahtevo (2)?

| Sprejetje ustreznih ukrepov | | | |
|---|---|---|---|
| Člen 12(1): jedrnato, pregledno, razumljivo, lahko dostopno | Člen 12(2): olajšanje uresničevanja pravice do dostopa | | |
| Izbira se med različnimi sredstvi | Zagotovi se kopija, če ni dogovorjeno drugače (člen 15(3)) | Po potrebi se uporabi večdelni pristop (najpomembneje v spletnem okolju) | Časovni okvir – brez nepotrebnega odlašanja, v vsakem primeru v enem mesecu (podaljšanje za dodatna dva meseca v izjemnih primerih) (člen 12(3)) |

### 2. korak: Kako odgovoriti na zahtevo (3)?

| Kako lahko upravljavec pridobi vse podatke o posamezniku, na katerega se nanašajo osebni podatki? | | | |
|---|---|---|---|
| Opredelitev meril iskanja – na podlagi tega, kar je zagotovil posameznik, na katerega se nanašajo osebni podatki, drugih informacij, ki jih ima upravljavec o posamezniku, na katerega se nanašajo osebni podatki, in dejavnikov, na podlagi katerih so podatki strukturirani (npr. številka stranke, naslovi IP, poklicni naziv, družinska razmerja itd.). | Opredelitev vseh tehničnih funkcij, ki so lahko na voljo za pridobivanje podatkov. | Iskanje po vseh ustreznih informacijskih sistemih in zbirkah, ki ne temeljijo na informacijski tehnologiji. | Zbiranje, pridobitev izvlečka podatkov ali drugačno zbiranje podatkov o posamezniku, na katerega se nanašajo osebni podatki, na način, ki v celoti odraža obdelavo, tj. vključuje vse osebne podatke v zvezi s posameznikom, na katerega se nanašajo osebni podatki, in mu omogoča, da se seznani z obdelavo in preveri njeno zakonitost. Pridobivanje informacij bi se lahko izvedlo za vsak primer posebej ali, kadar je to ustrezno, z uporabo vgrajenega orodja za zasebnost, ki ga je upravljavec že uvedel. |

### 3. korak: Preverjanje omejitev (1)




### 3. korak: Preverjanje omejitev (2)