



Smernice o pravici do prenosljivosti podatkov

**Sprejete 13. decembra 2016
Kot so bile nazadnje revidirane in sprejete 5. aprila 2017**

Ta delovna skupina je bila ustanovljena v skladu s členom 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Naloge skupine so opredeljene v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES.

Naloge sekretariata opravlja Direktorat C (Temeljne pravice in pravna država) Evropske komisije, Generalni direktorat za pravosodje in potrošnike, B-1049 Bruselj, Belgija, pisarna št. MO59 05/35.

Spletišče: http://ec.europa.eu/justice/data-protection/index_en.htm

KAZALO

Povzetek 3

I.	Uvod	3
II.	Kateri so glavni elementi prenosljivosti podatkov?	4
III.	Kdaj se uporablja prenosljivost podatkov?	9
IV.	Kako se splošna pravila, ki urejajo uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, uporabljajo za prenosljivost podatkov?	15
V.	Kako je treba zagotoviti prenosljive podatke?	17

Povzetek

V členu 20 Splošne uredbe o varstvu podatkov je določena nova pravica do prenosljivosti podatkov, ki je tesno povezana s pravico dostopa, vendar se v več vidikih razlikuje od nje. Posameznikom, na katere se nanašajo osebni podatki, omogoča, da prejmejo osebne podatke, ki so jih zagotovili upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter da te podatke posredujejo drugemu upravljavcu podatkov. Namen te nove pravice je opolnomočiti posameznika, na katerega se nanašajo osebni podatki, in mu zagotoviti večji nadzor nad osebnimi podatki v zvezi z njim.

Ker pravica do prenosljivosti podatkov omogoča neposreden prenos osebnih podatkov od enega upravljavca podatkov k drugemu, je tudi pomembno orodje, ki bo podprlo prosti pretok osebnih podatkov v EU in spodbudilo konkurenco med upravljavci. Pravica bo olajšala zamenjavo ponudnika storitev in torej spodbudila razvoj novih storitev v okviru strategije za enotni digitalni trg.

To mnenje vsebuje smernice za razlago in izvajanje pravice do prenosljivosti podatkov, kot jo uvaja Splošna uredba o varstvu podatkov. Njegov cilj je razprava o pravici do prenosljivosti podatkov in njenem obsegu. Pojasnjuje pogoje, pod katerimi se ta nova pravica uporablja, pri čemer upošteva pravno podlago za obdelavo podatkov (privolitev posameznika, na katerega se nanašajo osebni podatki, ali potreba po izvajanju pogodbe) in dejstvo, da je ta pravica omejena na osebne podatke, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki. Mnenje vsebuje tudi dejanske primere in merila za razlago okoliščin, v katerih se ta pravica uporablja. V zvezi s tem delovna skupina iz člena 29 meni, da pravica do prenosljivosti podatkov zajema podatke, ki jih zavestno in dejavno zagotovi posameznik, na katerega se nanašajo osebni podatki, ter osebne podatke, ustvarjene na podlagi njegove dejavnosti. Te nove pravice ni mogoče oslabiti ali omejiti na osebne informacije, ki jih neposredno sporoči posameznik, na katerega se nanašajo osebni podatki, na primer prek spletnega obrazca.

Upravljavci podatkov bi morali v skladu z dobro prakso začeti razvijati sredstva, ki bodo prispevala k odgovorom na zahteve za prenosljivost podatkov, kot so orodja za nalaganje in vmesniki za aplikacijsko programiranje. Zagotoviti bi morali, da se osebni podatki posredujejo v strukturirani, splošno uporabljani in strojno berljivi obliki, pri čemer bi jih bilo treba spodbuditi, naj zagotovijo interoperabilnost oblike podatkov, ki se posredujejo pri izpolnjevanju zahteve za prenosljivost podatkov.

Mnenje upravljavcem podatkov pomaga tudi jasno razumeti njihove obveznosti ter priporoča dobre prakse in orodja, ki podpirajo izpolnjevanje pravice do prenosljivosti podatkov. Nazadnje mnenje priporoča sodelovanje med deležniki iz industrije in panožnimi združenji, da si bodo skupaj prizadevali za splošen sklop interoperabilnih standardov in oblik za izpolnitev zahtev v zvezi s pravico do prenosljivosti podatkov.

I. Uvod

Člen 20 Splošne uredbe o varstvu podatkov uvaja novo pravico do prenosljivosti podatkov. Ta pravica posameznikom, na katere se nanašajo osebni podatki, omogoča, da prejmejo osebne podatke, ki so jih zagotovili upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki ter da te podatke neovirano posredujejo drugemu upravljavcu podatkov. Ta

pravica, ki se uporablja pod nekaterimi pogoji, podpira izbiro uporabnika, nadzor uporabnika in opolnomočenje uporabnika.

Posamezniki, ki so uresničevali svojo pravico dostopa na podlagi Direktive 95/46/ES o varstvu podatkov, so bili omejeni z obliko, ki jo je izbral upravljavec podatkov, ko je zagotovil zahtevane informacije. **Cilj nove pravice do prenosljivosti podatkov je posameznike, na katere se nanašajo osebni podatki, opolnomočiti glede njihovih osebnih podatkov, saj jim omogoča enostaven premik, kopiranje ali prenos osebnih podatkov iz enega okolja IT v drugo** (v lastne sisteme, sisteme zaupanja vrednih tretjih oseb ali sisteme novih upravljavcev podatkov).

S potrditvijo osebnostnih pravic posameznikov in nadzora nad osebnimi podatki v zvezi z njimi je prenosljivost podatkov tudi priložnost za ponovno vzpostavitev ravnovesja med posamezniki, na katere se nanašajo osebni podatki, in upravljavci podatkov¹.

Čeprav bi lahko pravica do prenosljivosti osebnih podatkov okrepila tudi konkurenčnost storitev (z olajšanjem menjave storitev), Splošna uredba o varstvu podatkov ne ureja konkurence, ampak osebne podatke. Zlasti člen 20 ne omejuje prenosljivih podatkov na tiste, ki so potrebni ali uporabni za zamenjavo storitev².

Čeprav je prenosljivost podatkov nova pravica, druge vrste prenosljivosti že obstajajo oziroma se obravnavajo na drugih področjih zakonodaje (npr. v zvezi s prekinitvijo pogodbe, gostovanjem komunikacijskih storitev in čezmejnem dostopom do storitev³). Med različnimi vrstami prenosljivosti lahko nastanejo sinergije ali celo koristi za posameznike, če se zagotovijo s kombiniranim pristopom, čeprav bi bilo treba analogije obravnavati previdno.

To mnenje vsebuje smernice za upravljavce podatkov, da lahko posodobijo svoje prakse, postopke in politike, ter pojasnjuje pomen prenosljivosti podatkov, da bodo lahko posamezniki, na katere se nanašajo osebni podatki, učinkovito uporabljali svojo novo pravico.

II. Kateri so glavni elementi prenosljivosti podatkov?

V splošni uredbi o varstvu podatkov je pravica do prenosljivosti podatkov v členu 20(1) opredeljena, kot sledi:

„Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posedoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral [...]“.

- Pravica do prejema osebnih podatkov

¹ Glavni cilj prenosljivosti podatkov je krepitev nadzora posameznikov nad njihovimi osebnimi podatki in zagotovitev, da imajo v podatkovnem ekosistemu dejavno vlogo.

² Ta pravica lahko na primer bankam omogoči zagotavljanje dodatnih storitev pod nadzorom uporabnika z uporabo osebnih podatkov, ki so bili sprva zbrani v okviru storitve oskrbe z energijo.

³ Glej načrt Evropske komisije za enotni digitalni trg: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, zlasti prvi steber politike „boljši spletni dostop do digitalnega blaga in storitev“.

Prvič, prenosljivost podatkov je **pravica posameznika, na katerega se nanašajo osebni podatki, da prejme podsklop osebnih podatkov**, ki jih je obdelal upravljavec podatkov in se nanašajo nanj, ter te podatke shrani za nadaljnjo osebno rabo. Shrani jih lahko na zasebni napravi ali v zasebnem oblaku, pri čemer podatkov ni treba posredovati drugemu upravljavcu podatkov.

V tem smislu prenosljivost podatkov dopolnjuje pravico dostopa. Ena izmed posebnosti prenosljivosti podatkov je, da posameznikom, na katere se nanašajo osebni podatki, omogoča, da lahko osebne podatke sami enostavno upravljajo in ponovno uporabijo. Te podatke bi morali prejeti „v strukturirani, splošno uporabljani in strojno berljivi obliki“. Posameznik, na katerega se nanašajo osebni podatki, bi na primer morda želel pridobiti svoj trenutni seznam predvajanja (ali zgodovine poslušanih skladb) v storitvi pretakanja glasbe, da bi izvedel, kolikokrat je poslušal nekatere posnetke, ali preveril, katero glasbo želi kupiti oziroma poslušati na drugi platformi. Podobno bi lahko želel pridobiti seznam stikov iz aplikacije za spletno pošto, da bi na primer sestavil seznam povabljenih na poroko, pridobiti informacije o nakupih z različnimi karticami zvestobe ali oceniti svoj ogljični odtis⁴.

- **Pravica do prenosa osebnih podatkov od enega upravljavca podatkov k drugemu upravljavcu podatkov**

Drugič, člen 20(1) posameznikom, na katere se nanašajo osebni podatki, zagotavlja **pravico do prenosa osebnih podatkov od enega upravljavca podatkov k drugemu upravljavcu podatkov**, „ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral“. Podatki se lahko prenesejo tudi neposredno od enega upravljavca podatkov k drugemu, in sicer na zahtevo posameznika, na katerega se nanašajo osebni podatki, in kadar je to tehnično izvedljivo (člen 20(2)). V zvezi s tem uvodna izjava 68 upravljavce podatkov spodbuja, naj razvijejo interoperabilne oblike, ki omogočajo prenosljivost podatkov⁵, vendar to ne pomeni obveznosti za upravljavce, da morajo uvesti ali vzdrževati sisteme za obdelavo, ki so tehnično združljivi⁶. Vendar pa v skladu s Splošno uredbo o varstvu podatkov upravljavci ne smejo ustvarjati ovir za posredovanje.

Ta element prenosljivosti podatkov v bistvu posameznikom, na katere se nanašajo osebni podatki, omogoča, da podatke, ki so jih zagotovili, ne le pridobijo in ponovno uporabijo, ampak tudi prenesejo k drugemu upravljavcu podatkov (v istem ali drugem poslovnem sektorju). Poleg tega, da opolnomoča potrošnika s preprečevanjem vezanosti na ponudnika, naj bi pravica do prenosljivosti podatkov spodbujala priložnosti za inovacije ter varno in zanesljivo izmenjavo osebnih podatkov med upravljavci podatkov pod nadzorom posameznika, na katerega se nanašajo osebni podatki⁷. Prenosljivost podatkov lahko spodbuja

⁴ V teh primerih lahko obdelava podatkov, ki jo izvede posameznik, na katerega se nanašajo osebni podatki, spada med domače dejavnosti, če se celotna obdelava izvede pod izključnim nadzorom posameznika, na katerega se nanašajo osebni podatki, ali pa jo lahko v imenu posameznika, na katerega se nanašajo osebni podatki, izvede druga oseba. V slednjem primeru bi se morala druga oseba šteti za upravljavca podatkov, čeprav izključno za namen shranjevanja osebnih podatkov, pri čemer mora izpolnjevati načela in obveznosti iz Splošne uredbe o varstvu podatkov.

⁵ Glej tudi oddelek V.

⁶ Posledično bi bilo treba posebno pozornost nameniti obliki posredovanih podatkov za zagotovitev, da lahko posameznik, na katerega se nanašajo osebni podatki, ali drug upravljavec podatkov podatke z malo napora ponovno uporabi. Glej tudi oddelek V.

⁷ Glej različne eksperimentalne aplikacije v Evropi, na primer [MiData](#) v Združenem kraljestvu in [MesInfos/SelfData](#) družbe FING v Franciji.

nadzorovano in omejeno izmenjavo osebnih podatkov med organizacijami, ki jo opravijo uporabniki, ter s tem bogati storitve in izkušnje uporabnikov⁸. Prenosljivost podatkov lahko olajša posredovanje in ponovno uporabo osebnih podatkov v zvezi z uporabniki med različnimi storitvami, za katere se zanimajo.

⁸ Področji tako imenovanega samosledenja in interneta stvari sta pokazali koristi (in tveganja) povezovanja osebnih podatkov z različnih področij posameznikovega življenja, kot so telesna pripravljenost, dejavnost in vnos kalorij, za zagotavljanje celovitejše podobe posameznikovega življenja v eni datoteki.

- Upravljanje

Prenosljivost podatkov zagotavlja pravico do prejema osebnih podatkov in njihove obdelave v skladu z željami posameznika, na katerega se nanašajo osebni podatki⁹.

Upravljalci podatkov, ki odgovorijo na zahteve za prenosljivost podatkov v skladu s pogoji iz člena 20, niso odgovorni za obdelavo, ki jo izvede posameznik, na katerega se nanašajo osebni podatki, ali druga družba, ki prejme osebne podatke. Delujejo v imenu posameznika, na katerega se nanašajo osebni podatki, tudi kadar se osebni podatki neposredno prenesejo k drugemu upravljavcu podatkov. V tem smislu upravljavec podatkov ni odgovoren za skladnost upravljavca podatkov, ki prejme podatke, s pravom o varstvu podatkov, saj prejemnika ne izbere upravljavec podatkov, ki podatke pošlje. Hkrati bi moral upravljavec določiti zaščitne ukrepe za zagotovitev, da dejansko deluje v imenu posameznika, na katerega se nanašajo osebni podatki. Vzpostavijo lahko na primer postopke za zagotovitev, da so posredovani osebni podatki dejansko tiste vrste, ki jo želi posredovati posameznik, na katerega se nanašajo osebni podatki. To je mogoče storiti s pridobitvijo potrditve posameznika, na katerega se nanašajo osebni podatki, pred posredovanjem ali prej, ko se zagotovi izvorna privolitev v obdelavo ali ko se sklene pogodba.

Za upravljavce podatkov, ki odgovorijo na zahtevo za prenosljivost podatkov, ne velja posebna obveznost, da bi morali pred posredovanjem podatkov preveriti in potrditi kakovost podatkov. Ti podatki bi v skladu z načeli iz člena 5(1) Splošne uredbe o varstvu podatkov seveda že morali biti točni in posodobljeni. Poleg tega prenosljivost podatkov ne pomeni obveznosti za upravljavca podatkov, da osebne podatke hrani dlje, kot je potrebno, ali dlje od določenega obdobja hrambe¹⁰. Pomembno je, da ni dodatne zahteve, da se podatki hranijo dlje od obdobja hrambe, ki se sicer uporabljajo, zgolj zaradi izpolnitve morebitne prihodnje zahteve za prenosljivost podatkov.

Če zahtevane osebne podatke obdeluje obdelovalec podatkov, mora pogodba, sklenjena v skladu s členom 28 Splošne uredbe o varstvu podatkov, vključevati njegovo obveznost, da pomaga „upravljavcu z ustreznimi tehničnimi in organizacijskimi ukrepi [...], da odgovori na zahteve za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki“. Upravljavec podatkov bi torej moral skupaj s svojimi obdelovalci podatkov izvesti posebne postopke, da odgovori na zahteve za prenosljivost podatkov. V primeru skupnega upravljanja bi morale biti odgovornosti v zvezi z obdelavo zahtev za prenosljivost podatkov v pogodbi jasno razdeljene med posamezne upravljavce podatkov.

Poleg tega je upravljavec podatkov, ki podatke prejme¹¹, odgovoren za zagotovitev, da so zagotovljeni prenosljivi podatki relevantni in ne pretirani, kar zadeva novo obdelavo podatkov. Če na primer posameznik, na katerega se nanašajo osebni podatki, pri storitvi spletne pošte vloži zahtevo za prenosljivost podatkov, da bi pridobil e-poštna sporočila in jih poslal varni platformi za arhiviranje, novemu upravljavcu podatkov ni treba obdelati kontaktnih podatkov korespondentov posameznika, na katerega se nanašajo osebni podatki. Če te informacije niso relevantne za namen nove obdelave, se ne bi smele hraniti in

⁹ Pravica do prenosljivosti podatkov ni omejena na osebne podatke, ki so uporabni in relevantni za podobne storitve, ki jih zagotavljajo konkurenti upravljavca podatkov.

¹⁰ Če v zgornjem primeru upravljavec podatkov ne hrani evidence skladb, ki jih je uporabnik predvajal, ti osebni podatki ne morejo biti vključeni v zahtevo za prenosljivost podatkov.

¹¹ Tj. upravljavec, ki prejme osebne podatke na podlagi zahteve za prenosljivost podatkov, ki jo posameznik, na katerega se nanašajo osebni podatki, vloži pri drugem upravljavcu podatkov.

obdelovati. Upravljavcem podatkov, ki prejmejo podatke, v nobenem primeru ni treba sprejeti in obdelati osebnih podatkov, posredovanih na podlagi zahteve za prenosljivost podatkov. Podobno tudi kadar posameznik, na katerega se nanašajo osebni podatki, zahteva posredovanje podrobnosti o njegovih bančnih transakcijah službi, ki pomaga upravljati njegov proračun, upravljavcu podatkov, ki prejme podatke, ni treba sprejeti vseh podatkov ali hraniti vseh podrobnosti o transakcijah, ko so označene za namene nove storitve. To pomeni, da bi bilo treba sprejeti in hraniti samo tiste podatke, ki so potrebni in relevantni za storitev, ki jo zagotavlja upravljavec podatkov, ki prejme podatke.

Organizacija, „ki prejme podatke“, postane nov upravljavec teh osebnih podatkov in mora upoštevati načela iz člena 5 Splošne uredbe o varstvu podatkov. Zato mora „novi“ upravljavec podatkov, ki prejme podatke, jasno in neposredno navesti namen nove obdelave, preden se vloži kakršna koli zahteva za posredovanje prenosljivih podatkov v skladu z zahtevami glede preglednosti iz člena 14¹². Upravljavce podatkov bi moral tako kot za vsako drugo obdelavo podatkov, izvedeno v okviru njegove odgovornosti, uporabiti načela iz člena 5, kot so zakonitost, pravičnost in preglednost, omejitev namena, najmanjši obseg podatkov, točnost, celovitost in zaupnost, omejitev shranjevanja ter odgovornost¹³.

Upravljavci podatkov, ki imajo osebne podatke, bi morali biti pripravljeni svojim posameznikom, na katere se nanašajo osebni podatki, olajšati uresničevanje pravice do prenosljivosti podatkov. Upravljavci podatkov se lahko tudi odločijo, da bodo sprejeli podatke posameznika, na katerega se nanašajo osebni podatki, vendar k temu niso zavezani.

- Prenosljivost podatkov v primerjavi z drugimi pravicami posameznikov, na katere se nanašajo osebni podatki

Ko posameznik uresničuje svojo pravico do prenosljivosti podatkov, pri tem ne posega v nobeno drugo pravico (kot velja za vse druge pravice iz Splošne uredbe o varnosti podatkov). Posameznik, na katerega se nanašajo osebni podatki, lahko tudi po dejanju prenosljivosti podatkov še naprej uporablja storitev upravljavca podatkov in ima koristi od nje. Prenosljivost podatkov samodejno ne sproži izbrisa podatkov¹⁴ iz sistemov upravljavca podatkov in ne vpliva na izvirno obdobje hrambe, ki se uporablja za posredovane podatke. Posameznik, na katerega se nanašajo osebni podatki, lahko svoje pravice uresničuje, če upravljavec podatkov še vedno obdeluje podatke.

Tudi če želi posameznik, na katerega se nanašajo osebni podatki, uresničiti svojo pravico do izbrisa („pravica do pozabe“ iz člena 17), upravljavec podatkov prenosljivosti podatkov ne more uporabiti za odlašanje ali zavrnitev takšnega izbrisa.

Če posameznik, na katerega se nanašajo osebni podatki, ugotovi, da osebni podatki, ki jih je zahteval na podlagi pravice do prenosljivosti podatkov, njegove zahteve ne izpolnjujejo v

¹² Poleg tega novi upravljavec podatkov ne bi smel obdelovati osebnih podatkov, ki niso relevantni, obdelava pa mora biti omejena na tisto, kar je potrebno za nove namene, čeprav so osebni podatki del splošnejšega nabora podatkov, posredovanega s postopkom prenosljivosti. Osebne podatke, ki niso potrebni za doseganje namena nove obdelave, bi bilo treba čim prej izbrisati.

¹³ Ko upravljavec podatkov prejme osebne podatke, poslane na podlagi pravice do prenosljivosti podatkov, se ti lahko štejejo za podatke, „ki jih posreduje“ posameznik, na katerega se nanašajo osebni podatki, in se lahko v skladu s pravico do prenosljivosti podatkov ponovno posredujejo, če so izpolnjeni drugi pogoji, ki se uporabljajo za to pravico (tj. pravna podlaga obdelave itd.).

¹⁴ Kakor je opredeljen v členu 17 Splošne uredbe o varstvu podatkov.

celoti, bi morale biti v skladu s členom 15 Splošne uredbe o varnosti podatkov na podlagi pravice dostopa v celoti izpolnjene vse morebitne dodatne zahteve glede osebnih podatkov.

Nadalje, če tudi posebna evropska zakonodaja ali zakonodaja držav članic na drugem področju zagotavlja nekakšno obliko prenosljivosti zadevnih podatkov, je treba pri izpolnjevanju zahteve za prenosljivost podatkov na podlagi Splošne uredbe o varstvu podatkov upoštevati tudi to posebno zakonodajo. Če je na eni strani iz zahteve, ki jo vloži posameznik, na katerega se nanašajo osebni podatki, jasno, da njegov namen ni uresničitev pravic na podlagi Splošne uredbe o varstvu podatkov, ampak le uresničitev pravic na podlagi sektorske zakonodaje, se določbe glede prenosljivosti podatkov iz Splošne uredbe o varstvu podatkov za to zahtevo ne bodo uporabljale¹⁵. Če je na drugi strani cilj zahteve prenosljivost na podlagi Splošne uredbe o varstvu podatkov, obstoj takšne posebne zakonodaje ne prevlada nad splošno uporabo načela prenosljivosti podatkov v zvezi s katerim koli upravljavcem podatkov, kot je določeno v Splošni uredbi o varstvu podatkov. Namesto tega je treba na podlagi posameznega primera oceniti, kako, če sploh, lahko takšna posebna zakonodaja vpliva na pravico do prenosljivosti podatkov.

III. Kdaj se uporablja prenosljivost podatkov?

- Katera dejanja obdelave zajema pravica do prenosljivosti podatkov?

Za skladnost s Splošno uredbi o varstvu podatkov morajo imeti upravljavci podatkov jasno pravno podlago za obdelavo osebnih podatkov.

Da dejanja obdelave v skladu s členom 20(1)(a) Splošne uredbe o varnosti podatkov **spadajo na področje prenosljivosti podatkov**, morajo temeljiti:

- na privolitvi posameznika, na katerega se nanašajo osebni podatki (v skladu s členom 6(1)(a) ali v skladu s členom 9(2)(a), če gre za posebne kategorije osebnih podatkov),
- ali na pogodbi, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 6(1)(b).

Na primer naslovi knjig, ki jih posameznik kupi v spletni knjigarni, ali skladbe, ki jih poslušajo prek storitve pretakanja glasbe, so primeri osebnih podatkov, ki običajno spadajo na področje prenosljivosti podatkov, saj se obdelajo na podlagi izvajanja pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki.

Splošna uredba o varnosti podatkov ne vzpostavlja splošne pravice do prenosljivosti podatkov v primerih, v katerih obdelava osebnih podatkov ne temelji na privolitvi ali pogodbi¹⁶.

¹⁵ Če je na primer cilj zahteve posameznika, na katerega se nanašajo osebni podatki, predvsem zagotoviti ponudniku storitev zagotavljanja informacij o računih dostop do zgodovine njegovega bančnega računa za namene iz revidirane direktive o plačilnih storitvah (PSD2), bi se moral tak dostop odobriti v skladu z določbami iz navedene direktive.

¹⁶ Glej uvodno izjavo 68 in člen 20(3) Splošne uredbe o varstvu podatkov. V členu 20(3) in uvodni izjavi 68 je določeno, da se pravica do prenosljivosti podatkov ne uporablja, če je obdelava potrebna za opravljanje naloge, ki se izvaja v javnem interesu, ali pri izvajanju javne oblasti, dodeljene upravljavcu podatkov, ali če upravljavec podatkov izvaja svoje naloge v javnem interesu ali izpolnjuje pravno obveznost. V teh primerih upravljavci

Finančnim institucijam na primer ni treba odgovoriti na zahtevo za prenosljivost podatkov, ki se nanaša na osebne podatke, obdelane v okviru njihovih obveznosti v zvezi s preprečevanjem in odkrivanjem pranja denarja in drugega finančnega kriminala, prenosljivost podatkov pa prav tako ne zajema službenih kontaktnih podatkov, ki se obdelajo v okviru medsebojnega odnosa dveh podjetij, kadar obdelava ne temelji niti na privolitvi posameznika, na katerega se nanašajo osebni podatki, niti na pogodbi, katere pogodbeni stranka je.

Kar zadeva podatke delodajalcev, se pravica do prenosljivosti podatkov običajno uporablja le, če obdelava temelji na pogodbi, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki. V številnih primerih se privolitev v tem smislu zaradi neuravnoteženosti moči med delodajalcem in zaposlenim ne bo štela za dano prostovoljno¹⁷. Namesto tega nekatere obdelave podatkov o človeških virih temeljijo na pravni podlagi pravnega interesa oziroma so potrebne za izpolnitev specifičnih pravnih obveznosti na področju zaposlitve. V praksi se bo na področju človeških virov pravica do prenosljivosti podatkov za nekatera dejanja obdelave (kot so storitve v zvezi s plačili in nadomestili, notranje zaposlovanje) zagotovo uporabljala, medtem ko bo v številnih drugih primerih treba za vsak primer posebej preveriti, ali so izpolnjeni vsi pogoji, ki veljajo za pravico do prenosljivosti podatkov.

Nazadnje, pravica do prenosljivosti podatkov se uporablja le, če se obdelava podatkov „izvaja z avtomatiziranimi sredstvi“, in torej večine papirnih datotek ne zajema.

- **Katere osebne podatke je treba vključiti?**

Da bi podatki spadali na področje pravice do prenosljivosti, morajo v skladu s členom 20(1) biti:

- osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki, in
- podatki, ki jih je posameznik *posredoval* upravljavcu podatkov.

V členu 20(4) je določeno tudi, da izpolnjevanje te pravice ne vpliva negativno na pravice in svoboščine drugih.

Prvi pogoj: osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki

Na področje zahteve za prenosljivost podatkov spadajo le osebni podatki. Zato anonimni¹⁸ 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)).

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 torej niso zavezani k zagotovitvi prenosljivosti. Vendar je razvoj postopkov za samodejno odgovarjanje na zahteve za prenosljivost ob upoštevanju načel, ki urejajo pravico do prenosljivosti podatkov, dobra praksa. Primer bi bil vladna storitev, ki zagotavlja enostavno nalaganje preteklih osebnih napovedi za odmero davka od dohodkov. Za prenosljivost podatkov kot dobro prakso v primeru obdelave, ki temelji na pravni podlagi potrebe za pravni interes in obstoječe prostovoljne sisteme, glej strani 47 in 48 Mnenja št. 6/2014 delovne skupine iz člena 29 o pravnih interesih (WP217).

¹⁷ Kot je delovna skupina iz člena 29 poudarila v svojem Mnenju št. 8/2001 z dne 13. septembra 2001 (WP48).

¹⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_sl.pdf.

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 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).

Drugi pogoj: podatki, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki.

Drugi pogoj zoži področje uporabe na podatke, „ki jih posreduje“ posameznik, na katerega se nanašajo osebni podatki.

Obstajajo številni primeri osebnih podatkov, ki jih bo zavestno in dejavno „posredoval“ posameznik, na katerega se nanašajo osebni podatki, kot so podatki o računu (npr. e-poštni naslov, uporabniško ime, starost), predloženi prek spletnih obrazcev. Vendar podatki, „ki jih posreduje“ posameznik, na katerega se nanašajo osebni podatki, izhajajo tudi iz spremljanja njegove dejavnosti. Zato delovna skupina iz člena 29 meni, da bi moral za zagotovitev polne vrednosti te nove pravice izraz „ki jih posreduje“ vključevati tudi osebne podatke, ugotovljene na podlagi dejavnosti uporabnikov, kot so neobdelani podatki, ki se obdelajo s pametnim merjenjem, ali druge vrste povezanih predmetov¹⁹, dnevniki aktivnosti, zgodovina uporabe spletišč ali dejavnosti iskanja.

Ta zadnja kategorija podatkov ne vključuje podatkov, ki jih ustvari upravljavec podatkov (tako da kot vhodne podatke uporabi ugotovljene ali neposredno zagotovljene podatke), kot je profil uporabnika, ustvarjen z analizo zbranih neobdelanih podatkov za pametno merjenje.

Na podlagi izvora podatkov se lahko razlikuje med različnimi kategorijami podatkov, da se ugotovi, ali jih pravica do prenosljivosti podatkov zajema. Podatki iz naslednjih kategorij se lahko opredelijo kot podatki, „ki jih posreduje posameznik, na katerega se nanašajo osebni podatki“:

- **podatki, ki jih dejavno in zavestno posreduje posameznik, na katerega se nanašajo osebni podatki** (na primer e-poštni naslov, uporabniško ime, starost itd.);
- **ugotovljeni podatki, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki, z uporabo storitev ali naprave.** To bi lahko na primer vključevalo posameznikovo zgodovino iskanja, podatke o prometu in podatke o lokaciji. Vključuje lahko tudi druge neobdelane podatke, kot so srčni utrip, ki ga spremlja nosljiva naprava.

Nasprotno povzete in izpeljane podatke ustvari upravljavec podatkov na podlagi podatkov, „ki jih posreduje posameznik, na katerega se nanašajo osebni podatki“. Rezultat ocene zdravja uporabnika ali profil, ustvarjen v okviru obvladovanja tveganja in finančnih predpisov (npr.

¹⁹ Ko se posamezniku, na katerega se nanašajo osebni podatki, omogoči pridobitev podatkov, ki izhajajo iz spremljanja njegove dejavnosti, bo imel tudi boljši pregled nad odločitvami glede izvajanja, ki jih sprejme upravljavec podatkov, kar zadeva obseg ugotovljenih podatkov, bolje se bo lahko odločil, katere podatke želi posredovati, da bi pridobil dostop do znane storitve, in se seznanil, v kolikšnem obsegu se spoštujejo njegove pravice do zasebnosti.

za dodelitev kreditnih točk ali izpolnjevanje pravil o preprečevanju pranja denarja), se na primer sam po sebi ne more šteti za podatek, „ki ga posreduje posameznik, na katerega se nanašajo osebni podatki“. Čeprav so takšni podatki lahko del profila, ki ga hrani upravljavec podatkov, in so povzeti ali izpeljani iz analize podatkov, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki (na primer s svojimi dejanji), se ti podatki običajno ne bodo šteli za podatke, „ki jih posreduje posameznik, na katerega se nanašajo osebni podatki“, in torej ne bodo spadali na področje uporabe te nove pravice²⁰.

Na splošno je treba glede na cilje politike pravice do prenosljivosti podatkov izraz „ki jih posreduje posameznik, na katerega se nanašajo osebni podatki,“ razlagati široko, pri čemer bi bilo treba izključiti „povzete podatke“ in „izpeljane podatke“, ki vključujejo osebne podatke, ki jih ustvari ponudnik storitve (na primer algoritemske rezultate). Upravljavec podatkov lahko te povzete podatke izključi, vendar pa bi moral vključiti vse druge osebne podatke, ki jih posameznik, na katerega se nanašajo osebni podatki, posreduje s tehničnimi sredstvi, ki jih zagotovi upravljavec²¹.

Zato izraz „ki jih posreduje“ vključuje osebne podatke, ki so povezani z dejavnostjo posameznika, na katerega se nanašajo osebni podatki, ali izhajajo iz spremljanja posameznikovega vedenja, vendar ne vključuje podatkov, ki izhajajo iz naknadnih analiz tega vedenja. Nasprotno pa so vsi osebni podatki, ki jih je ustvaril upravljavec podatkov kot del obdelave podatkov, npr. s postopkom personalizacije ali priporočil, kategorizacijo uporabnika ali profiliranjem, podatki, ki izhajajo ali so povzeti iz osebnih podatkov, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki, in jih pravica do prenosljivosti podatkov ne zajema.

Tretji pogoj: pravica do prenosljivosti podatkov ne vpliva negativno na pravice in svoboščine drugih

Kar zadeva osebne podatke v zvezi z drugimi posamezniki, na katere se nanašajo osebni podatki:

Namen tretjega pogoja je preprečiti pridobivanje podatkov, ki vsebujejo osebne podatke drugih posameznikov, na katere se nanašajo osebni podatki (ki niso dali privolitve), in posredovanje teh podatkov novemu upravljavcu podatkov v primerih, v katerih bi ti podatki verjetno bili obdelani na način, ki bi negativno vplival na pravice in svoboščine drugih

²⁰ Kljub temu lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 15 Splošne uredbe o varstvu podatkov (ki se nanaša na pravico dostopa) še vedno izkoristi svojo „pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov“ ter informacije o „obstoj[u] avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki“.

²¹ To vključuje vse podatke o posamezniku, na katerega se nanašajo osebni podatki, ugotovljene med dejavnostmi, za namen katerih se podatki zbirajo, kot je zgodovina transakcij ali dnevnik dostopov. Tudi podatki, zbrani s spremljanjem in snemanjem posameznika, na katerega se nanašajo osebni podatki (kot je aplikacija, ki snema srčni utrip, ali tehnologija, ki se uporablja za spremljanje vedenja pri brskanju), bi se morali šteti za podatke, „ki jih posreduje“ posameznik, čeprav niso posredovani dejavno ali zavestno.

posameznikov, na katere se nanašajo osebni podatki (člen 20(4) Splošne uredbe o varstvu podatkov)²².

Takšen negativni vpliv bi na primer bil, če bi se s prenosom podatkov od enega upravljavca podatkov k drugemu tretjim osebam preprečilo uresničevanje njihovih pravic, ki jih imajo na podlagi Splošne uredbe o varnosti podatkov kot posamezniki, na katere se nanašajo osebni podatki (kot sta pravica do informacij, pravica dostopa itd.).

Posameznik, na katerega se nanašajo osebni podatki, ki sproži prenos svojih podatkov od enega upravljavca podatkov k drugemu, da novemu upravljavcu podatkov privolitev v obdelavo ali z njim sklene pogodbo. Če nabor podatkov vključuje osebne podatke tretjih oseb, je treba opredeliti drugo pravno podlago za obdelavo. Upravljavec podatkov se lahko na primer v skladu s členom 6(1)(f) sklicuje na zakoniti interes, zlasti če je namen upravljavca podatkov posamezniku, na katerega se nanašajo osebni podatki, zagotoviti storitev, ki mu omogoča obdelavo osebnih podatkov za izključno osebno ali domačo dejavnost. Za dejanja obdelave, ki jih v okviru osebne dejavnosti sproži posameznik, na katerega se nanašajo osebni podatki, in ki zadevajo tretje osebe in bi lahko vplivala nanje, ostaja odgovoren posameznik, če takšne obdelave na noben način ne določi upravljavec podatkov.

Storitev spletne pošte lahko na primer omogoča oblikovanje imenika kontaktov, prijateljev, sorodnikov, družine in posameznikov iz širšega okolja posameznika, na katerega se nanašajo osebni podatki. Ker so ti podatki povezani s posameznikom (in jih ta ustvari), ki ga je mogoče identificirati in ki želi uresničiti svojo pravico do prenosljivosti podatkov, bi morali upravljavci podatkov celoten imenik vhodnih in izhodnih e-poštnih sporočil posredovati temu posamezniku, na katerega se nanašajo osebni podatki.

Podobno lahko bančni račun posameznika, na katerega se nanašajo osebni podatki, vključuje podatke v zvezi s transakcijami ne le imetnika računa, ampak tudi drugih posameznikov (na primer če so denar prenesli na imetnika računa). Prenos informacij o bančnem računu k imetniku računa na podlagi zahteve za prenosljivost najverjetneje ne bo negativno vplival na pravice in svoboščine teh tretjih oseb, če se bodo podatki v obeh primerih uporabili za isti namen (tj. kontaktni naslov, ki ga uporabi le posameznik, na katerega se nanašajo osebni podatki, ali zgodovina bančnega računa posameznika, na katerega se nanašajo osebni podatki).

Prav nasprotno pa se pravice in svoboščine tretjih oseb ne bodo spoštovale, če bo novi upravljavec podatkov osebne podatke uporabil za druge namene, na primer če upravljavec podatkov, ki prejme podatke, osebne podatke drugih posameznikov, ki so v imeniku stikov posameznika, na katerega se nanašajo osebni podatki, uporabi za namene trženja.

Da bi se torej preprečili negativni vplivi na vključene tretje osebe, je obdelava takšnih osebnih podatkov, ki jo izvede drug upravljavec, dovoljena le, če so podatki pod izključnim nadzorom uporabnika, ki vloži zahtevo, in se upravljajo le za osebne ali domače potrebe. „Novi“ upravljavec podatkov, ki prejme podatke (kateremu se lahko podatki posredujejo na zahtevo uporabnika), posredovanih podatkov tretjih oseb ne sme uporabiti za svoj namen, ne sme na primer predlagati trženja proizvodov in storitev tem tretjim posameznikom, na katere se nanašajo osebni podatki. Te informacije se na primer ne bi smele uporabiti za obogatitev

²² V uvodni izjavi 68 je navedeno, da „[k]adar določeni niz osebnih podatkov zadeva več kot enega posameznika, na katerega se ti podatki nanašajo, pravica do prejemanja osebnih podatkov ne bi smela posegati v pravice in svoboščine drugih posameznikov, na katere se nanašajo osebni podatki, v skladu s to uredbo“.

profila tretje osebe, na katero se nanašajo osebni podatki, in izgradnjo njene družbene skupnosti brez njene seznanjenosti in privolitve²³. Uporabiti se ne smejo niti za pridobivanje informacij o takšnih tretjih osebah in ustvarjanje posebnih profilov, tudi če upravljavec podatkov že ima njihove osebne podatke. V nasprotnem primeru bo takšna obdelava verjetno nezakonita in nepoštena, zlasti če zadevne tretje osebe niso obveščene in ne morejo uresničiti svojih pravic, ki jih imajo kot posamezniki, na katere se nanašajo osebni podatki.

Poleg tega je vodilna praksa vseh upravljavcev podatkov (tako upravljavcev, ki pošljejo podatke, kot upravljavcev, ki prejmejo podatke), da uporabljajo orodja, s katerimi posameznikom, na katere se nanašajo osebni podatki, omogočijo, da izberejo relevantne podatke, ki jih želijo prejeti in posredovati, ter izključijo podatke drugih posameznikov, kadar je to ustrezno. To bo še dodatno prispevalo k zmanjšanju tveganja za tretje osebe, katerih osebni podatki bi se lahko prenesli.

Upravljavci podatkov bi morali izvajati tudi mehanizme privolitve za druge vključene posameznike, na katere se nanašajo osebni podatki, da bi se olajšalo posredovanje podatkov v primerih, v katerih so takšne osebe pripravljene dati privolitev, na primer če tudi same želijo svoje podatke prenesti k nekemu drugemu upravljavcu podatkov. Takšne okoliščine se lahko pojavijo na primer pri socialnih omrežjih, vendar je od upravljavcev podatkov odvisno, katero vodilno prakso bodo upoštevali.

Kar zadeva podatke, ki spadajo na področje intelektualne lastnine in poslovnih skrivnosti:

Pravice in svoboščine drugih so omenjene v členu 20(4). Te se ne nanašajo neposredno na prenosljivost, vendar se lahko razumejo kot „vključno s poslovnimi skrivnostmi ali intelektualno lastnino, ter predvsem [...] avtorsk[imi] pravic[ami], ki ščitijo programsko opremo“. Čeprav bi bilo treba te pravice proučiti, preden se odgovori na zahtevo za prenosljivost podatkov, „[t]o [...] ne bi smelo povzročiti, da se posamezniku, na katerega se nanašajo osebni podatki, zavrne dostop do vseh informacij“. Upravljavec podatkov tudi ne bi smel zavrniti zahteve za prenosljivost podatkov na podlagi kršitve druge pogodbene pravice (na primer izjemnega dolga ali poslovnega spora s posameznikom, na katerega se nanašajo osebni podatki).

Pravica do prenosljivosti podatkov ni pravica posameznika, da lahko zlorabi informacije na način, ki bi se lahko štel za nepošteno prakso ali bi pomenil kršitev pravil intelektualne lastnine.

Vendar pa morebitno poslovno tveganje samo po sebi ne more biti podlaga za zavrnitev odgovora na zahtevo za prenosljivost, pri čemer lahko upravljavci podatkov osebne podatke, ki jih posredujejo posamezniki, na katere se nanašajo osebni podatki, posredujejo v obliki, ki ne zajema informacij, ki spadajo na področje poslovnih skrivnosti ali pravic intelektualne lastnine.

²³ Storitve socialnega omrežja ne bi smela bogatiti profilov svojih članov, tako da uporablja osebne podatke, ki jih posameznik, na katerega se nanašajo osebni podatki, posreduje kot del svoje pravice do prenosljivosti, ne da bi upoštevala načelo preglednosti in preverila, ali je pravna podlaga za to posebno obdelavo ustrezna.

IV. Kako se splošna pravila, ki urejajo uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki, uporabljajo za prenosljivost podatkov?

- **Katere predhodne informacije bi bilo treba posredovati posamezniku, na katerega se nanašajo osebni podatki?**

Da bi upravljavci podatkov delovali v skladu z novo pravico do prenosljivosti podatkov, morajo posameznike, na katere se nanašajo osebni podatki, obvestiti o obstoju nove pravice do prenosljivosti. Če upravljavec podatkov zadevne osebne podatke zbere neposredno pri posamezniku, na katerega se ti nanašajo, mora to storiti „takrat, ko pridobi osebne podatke“. Če osebnih podatkov ne pridobi od posameznika, na katerega se ti nanašajo, mora upravljavec podatkov posamezniku, na katerega se nanašajo osebni podatki, zagotoviti informacije, kot je določeno v členih 13(2)(b) in 14(2)(c).

„Kadar osebni podatki niso bili pridobljeni od posameznika, na katerega se ti nanašajo“, člen 14(3) določa, da je treba informacije zagotoviti v razumnem roku po prejemu osebnih podatkov, vendar najpozneje v enem mesecu, ob prvem komuniciranju s posameznikom, na katerega se nanašajo osebni podatki, ali ob razkritju tretjim osebam²⁴.

Upravljavci podatkov morajo pri zagotavljanju zahtevanih informacij zagotoviti, da pravico do prenosljivosti podatkov razlikujejo od drugih pravic. Delovna skupina iz člena 29 torej priporoča zlasti, da upravljavci podatkov natančno pojasnijo razliko med vrstami podatkov, ki jih lahko posameznik, na katerega se nanašajo osebni podatki, prejme na podlagi pravice dostopa in pravice do prenosljivosti podatkov.

Delovna skupina priporoča tudi, naj upravljavci podatkov vedno vključijo informacijo o pravici do prenosljivosti podatkov, preden posamezniki, na katere se nanašajo osebni podatki, zaprejo svoje morebitne račune. To uporabnikom omogoča, da pregledajo svoje osebne podatke in podatke enostavno prenesejo na svojo napravo ali k drugemu ponudniku, preden se pogodba prekine.

Na koncu delovna skupina iz člena 29 priporoča, naj bo vodilna praksa upravljavcev podatkov, ki prejmejo podatke, da posameznikom, na katere se nanašajo osebni podatki, zagotovijo vse informacije o vrsti osebnih podatkov, ki so relevantni za izvajanje njihovih storitev. Navedeno podpira pošteno obdelavo in uporabnikom omogoča, da omejijo tveganja za tretje osebe in tudi vse drugo nepotrebno podvajanje osebnih podatkov, tudi kadar posamezniki, na katere se nanašajo osebni podatki, niso vključeni.

- **Kako lahko upravljavec podatkov identificira posameznika, na katerega se nanašajo osebni podatki, preden odgovori na zahtevo?**

V Splošni uredbi o varstvu podatkov ni zavezujočih zahtev glede avtentikacije posameznika, na katerega se nanašajo osebni podatki. Kljub temu je v členu 12(2) Splošne uredbe o varstvu podatkov določeno, da upravljavec ne zavrne ukrepanja na zahtevo posameznika, na katerega se nanašajo osebni podatki, za uresničevanje njegovih pravic (vključno s pravico do prenosljivosti podatkov), razen če osebne podatke obdeluje za namen, pri katerem ni potrebna identifikacija posameznika, na katerega se nanašajo osebni podatki, in lahko dokaže, da ne

²⁴ V členu 12 je določeno, da upravljavci podatkov zagotovijo vsa „sporočila [...] v jedrnatih, preglednih, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku, kar velja zlasti za vse informacije, namenjene posebej otroku“.

more identificirati posameznika, na katerega se nanašajo osebni podatki. Vendar lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 11(2) v takih primerih zagotovi več informacij, ki omogočajo njegovo identifikacijo. Poleg tega je v členu 12(6) določeno, da lahko upravljavec podatkov, kadar izrazi upravičen dvom o identiteti posameznika, zahteva dodatne informacije, da potrdi identiteto posameznika, na katerega se nanašajo osebni podatki. Kadar posameznik, na katerega se nanašajo osebni podatki, zagotovi dodatne informacije, ki omogočajo njegovo identifikacijo, upravljavec podatkov ne zavrne odgovora na zahtevo. Kadar so informacije in podatki, zbrani prek spleta, povezani s psevdonimi ali edinstvenimi identifikatorji, lahko upravljavec podatkov izvede ustrezne postopke, ki posamezniku omogočajo, da vloži zahtevo za prenosljivost podatkov in prejme podatke v zvezi z njim. Upravljalci podatkov morajo v vsakem primeru izvesti postopek avtentikacije, da bi z gotovostjo potrdili identiteto posameznika, na katerega se nanašajo osebni podatki, ki zahteva svoje osebne podatke ali splošneje uresničuje pravice, ki jih zagotavlja Splošna uredba o varstvu podatkov.

Ti postopki pogosto že obstajajo. Upravljavce podatkov posameznike, na katere se nanašajo osebni podatki, pogosto avtenticira, 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 prenosljivosti²⁵.

Čeprav je lahko v teh primerih za predhodno identifikacijo posameznikov, na katere se nanašajo osebni podatki, potrebna zahteva za dokazilo njihove pravne identitete, takšno preverjanje morda ne bo relevantno za oceno povezave med podatki in zadevnim posameznikom, saj takšna povezava ni povezana z uradno ali pravno identiteto. Zmožnost upravljavca podatkov, da zahteva dodatne informacije za oceno posameznikove identitete, v svojem bistvu ne more voditi do čezmernih zahtev in zbiranja osebnih podatkov, ki niso relevantni ali potrebni za krepitev povezave med posameznikom in zahtevanimi osebnimi podatki.

V številnih primerih so takšni postopki avtentikacije že vzpostavljeni. Na primer uporabniška imena in gesla se pogosto uporabljajo, da se posameznikom omogoči dostop do njihovih podatkov v njihovih e-poštnih računih, računih socialnih omrežij in računih, ki se uporabljajo za številne druge storitve, pri čemer se posamezniki odločijo, da bodo nekatere od teh storitev uporabljali brez razkritja svojega polnega imena in identitete.

Če je zaradi velikosti podatkov, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, posredovanje prek interneta težavno, bo upravljavec podatkov morda moral namesto morebitnega podaljšanja roka za izpolnitev zahteve na največ tri mesece²⁶ proučiti nadomestna sredstva za posredovanje podatkov, kot je uporaba pretakanja ali shranjevanje na CD, DVD ali drug fizični medij oziroma omogočitev prenosa osebnih podatkov neposredno k drugemu upravljavcu podatkov (v skladu s členom 20(2) Splošne uredbe o varstvu podatkov, kadar je tehnično izvedljivo).

- Kakšen je rok za odgovor na zahtevo za prenosljivost?

²⁵ Če je na primer obdelava podatkov povezana z uporabniškim računom, bo morda za identifikacijo posameznika, na katerega se nanašajo osebni podatki, dovolj, če se zagotovita ustrezno prijavnno ime in geslo.

²⁶ Člen 12(3): „[u]pravljavce informacije o ukrepih, sprejetih na zahtevo [...], zagotovi [...]“.

V členu 12(3) je določeno, da upravljavec podatkov „informacije o ukrepih, sprejetih [...], posamezniku, na katerega se nanašajo osebni podatki, zagotovi brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve“. To enomesečno obdobje se pri kompleksnih zadevah lahko podaljša na največ tri mesece, če je posameznik, na katerega se nanašajo osebni podatki, obveščen o razlogih za takšno zamudo v enem mesecu po prejemu izvirne zahteve.

Upravljavci podatkov, ki upravljajo storitve informacijske družbe, bodo verjetno boljše opremljeni, da lahko izpolnijo zahteve v zelo kratkem času. Dobra praksa, ki zagotavlja izpolnitev pričakovanj uporabnikov, je opredelitev časovnega okvira, v katerem se običajno odgovori na zahteve za prenosljivost podatkov, pri čemer se to sporoči posameznikom, na katere se nanašajo osebni podatki.

Upravljavci podatkov, ki zavrnejo odgovor na zahtevo za prenosljivost, v skladu s členom 12(4) posameznika, na katerega se nanašajo osebni podatki, obvestijo „o razlogih za neukrepanje ter o možnosti vložitve pritožbe pri nadzornem organu in možnosti uveljavljanja pravnih sredstev“ najpozneje en mesec po prejemu zahteve.

Upravljavci podatkov morajo izpolniti obveznost, da odgovorijo v določenih rokih, čeprav gre za zavrnitev. To pomeni, da upravljavec podatkov ne more molčati, če prejme zahtevo za prenosljivost podatkov.

- **V katerih primerih se lahko zahteva za prenosljivost podatkov zavrne ali se lahko zanjo zaračuna pristojbina?**

V skladu s členom 12 upravljavec podatkov ne sme zaračunati pristojbine za zagotavljanje osebnih podatkov, razen če lahko dokaže, da so zahteve očitno neutemeljene ali pretirane „zlasti ker se ponavljajo“. Storitvam informacijske družbe, ki so specializirane za avtomatizirano obdelavo osebnih podatkov, lahko uvedba avtomatiziranih sistemov, kot so vmesniki za aplikacijsko programiranje (API)²⁷, olajša izmenjave s posamezniki, na katere se nanašajo osebni podatki, in torej zmanjša morebitno breme zaradi ponavljajočih se zahtev. Zato bi morale biti zelo malo primerov, v katerih bi lahko upravljavec podatkov utemeljil zavrnitev posredovanja zahtevanih informacij, tudi pri večkratnih zahtevah za prenosljivost podatkov.

Poleg tega se pri določanju tega, ali je zahteva pretirana, ne bi smel upoštevati skupni strošek postopkov, vzpostavljenih za odgovor na zahteve za prenosljivost. Dejansko je člen 12 Splošne uredbe o varstvu podatkov osredotočen na zahteve, ki jih vloži en posameznik, na katerega se nanašajo osebni podatki, in ne na skupno število zahtev, ki jih prejme upravljavec podatkov. Zato se skupni stroški izvajanja sistema ne bi smeli zaračunati posameznikom, na katere se nanašajo osebni podatki, niti uporabiti za utemeljitev zavrnitve odgovora na zahteve za prenosljivost.

V. Kako je treba zagotoviti prenosljive podatke?

- **Katera sredstva naj bi upravljavec podatkov uvedel za posredovanje podatkov?**

²⁷ Vmesniki za aplikacijsko programiranje (API) so vmesniki aplikacij ali spletnih storitev, ki jih dajo na voljo upravljavci podatkov, da se lahko drugi sistemi ali aplikacije povežejo in delujejo z njihovimi sistemi.

V členu 20(1) Splošne uredbe o varnosti podatkov je določeno, da imajo posamezniki, na katere se nanašajo osebni podatki, pravico, da podatke posredujejo drugemu upravljavcu, ne da bi jih upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral.

Za takšno oviranje se lahko štejejo vse pravne, tehnične ali finančne ovire, ki jih postavi upravljavec podatkov, da bi preprečil oziroma upočasnil dostop do podatkov, njihovo posredovanje ali ponovno uporabo s strani posameznika, na katerega se nanašajo osebni podatki, ali drugega upravljavca podatkov. Takšno oviranje bi lahko bile pristojbine, zaračunane za zagotovitev podatkov, pomanjkanje interoperabilnosti ali dostopa do oblike podatkov, API ali zagotovljene oblike, pretirana zamuda ali zapletena pridobitev polnega nabora podatkov, namerna zameglitev nabora podatkov ali posebne in nepotrebne ali pretirane zahteve sektorja glede standardizacije ali akreditacije²⁸.

Tudi v členu 20(2) je določeno, da so upravljavci podatkov zavezani k prenosu prenosljivih podatkov neposredno k drugim upravljavcem podatkov, „kadar je to tehnično izvedljivo“.

Tehnična izvedljivost prenosa podatkov od enega upravljavca podatkov k drugemu pod nadzorom posameznika, na katerega se nanašajo osebni podatki, bi se morala oceniti za vsak primer posebej. V uvodni izjavi 68 so nadalje pojasnjene meje „tehnično izvedljivega“, pri čemer je navedeno, da pravica „ne bi smela ustvariti obveznosti za upravljavca, da mora sprejeti ali vzdrževati sisteme za obdelavo, ki so tehnično združljivi“.

Upravljavci podatkov naj bi osebne podatke posredovali v interoperabilni obliki, čeprav to ne pomeni, da morajo drugi upravljavci podatkov podpirati te oblike. Neposreden prenos od enega upravljavca podatkov k drugemu bi se torej lahko vzpostavil, če je med dvema sistemoma možna varna²⁹ komunikacija in če je sistem, ki prejme podatke, tehnično zmožen prejeti vhodne podatke. Če tehnične ovire onemogočajo neposreden prenos, upravljavec podatkov pojasni te ovire posameznikom, na katere se nanašajo osebni podatki, saj bi bil učinek njegove odločitve sicer podoben neukrepanju v zvezi z zahtevo posameznika, na katerega se nanašajo osebni podatki (člen 12(4)).

Na tehnični ravni bi morali upravljavci podatkov proučiti in oceniti dva različna in dopolnjujoča se načina za dajanje prenosljivih podatkov na voljo posameznikom, na katere se nanašajo osebni podatki, ali drugim upravljavcem podatkov:

- neposreden prenos celotnega nabora prenosljivih podatkov (ali več izvlečkov delov splošnega nabora podatkov);
- avtomatizirano orodje, ki omogoča pridobivanje relevantnih podatkov.

Upravljavci podatkov morda dajejo prednost drugemu načinu, in sicer v primerih, ki vključujejo kompleksne in velike napore podatkov, saj omogoča pridobitev katerega koli dela nabora podatkov, ki je glede na zahtevo posameznika, na katerega se nanašajo osebni podatki, relevanten zanj, lahko prispeva k zmanjšanju tveganja in potencialno omogoča uporabo mehanizmov za sinhronizacijo podatkov³⁰ (npr. v smislu redne komunikacije med upravljavci

²⁸ Možne so nekatere zakonite ovire, kot so ovire, povezane s pravicami in svoboščinami drugih, ki so omenjene v členu 20(4), ali ovire, povezane z varnostjo sistemov upravljavcev. Upravljavec podatkov mora utemeljiti, zakaj bi bile takšne ovire zakonite in zakaj ne pomenijo oviranja v smislu člena 20(1).

²⁹ Z avtentificirano komunikacijo s potrebno stopnjo šifriranja podatkov.

³⁰ Mehanizem za sinhronizacijo lahko pomaga izpolniti splošne obveznosti iz člena 5 Splošne uredbe o varstvu podatkov, v katerem je določeno, da so „osebni podatki [...] točni in, kadar je to potrebno, posodobljeni“.

podatkov). Morda je boljši način za zagotovitev skladnosti za „novega“ upravljavca podatkov in bi pomenil dobro prakso pri zmanjševanju tveganja glede zasebnosti, kar zadeva prvotnega upravljavca podatkov.

Ta dva različna in morda dopolnjujoča se načina zagotavljanja relevantnih prenosljivih podatkov bi se lahko izvajala tako, da bi se dali podatki na voljo z različnimi sredstvi, na primer z zaščitenim sporočanjem, strežnikom SFTP, zaščitenim vmesnikom za aplikacijsko programiranje ali spletnim portalom. Posameznikom, na katere se nanašajo osebni podatki, bi bilo treba omogočiti, da za shranjevanje osebnih podatkov in dodelitev dovoljenja upravljavcem podatkov za dostop do osebnih podatkov in njihovo obdelavo, kot je določeno, uporabijo trgovino z osebnimi podatki, sistem za upravljanje osebnih podatkov³¹ ali druge zaupanja vredne tretje osebe.

- **Katera oblika podatkov se pričakuje?**

V Splošni uredbi o varstvu podatkov je določeno, da morajo upravljavci podatkov osebne podatke, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, posredovati v obliki, ki podpira ponovno uporabo. Zlasti v členu 20(1) Splošne uredbe o varstvu podatkov je določeno, da je treba osebne podatke posredovati „v strukturirani, splošno uporabljani in strojno berljivi obliki“. V uvodni izjavi 68 je nadalje pojasnjeno, da bi morala biti ta oblika interoperabilna, pri čemer je ta izraz v EU opredeljen³² kot:

„zmožnost neenakih in različnih organizacij, da sodelujejo pri vzajemno koristnih in dogovorjenih skupnih ciljih, ki vključujejo izmenjavo informacij in znanja med organizacijami prek poslovnih procesov, ki jih podpirajo, z izmenjavo podatkov med zadevnimi sistemi IKT“.

Pojmi „strukturirani“, „splošno uporabljani“ in „strojno berljivi“ so sklop minimalnih zahtev, s katerimi bi se morala olajšati interoperabilnost oblike podatkov, ki jih posreduje upravljavec podatkov. Tako je stavek „v strukturirani, splošno uporabljani in strojno berljivi obliki“ specifikacija za sredstva, interoperabilnost pa želeni rezultat.

V uvodni izjavi 21 Direktive 2013/37/EU^{33,34} je pojem strojno berljivo opredeljen kot:

datotečni format[,] strukturiran tako, da lahko programske aplikacije z lahkoto določajo, prepoznajo in izločajo določene podatke, vključno s posameznimi dejanskimi navedbami in njihovo notranjo strukturo[.] Podatki, kodirani v datotekah, ki so strukturirane v strojno berljivem formatu, so strojno berljivi podatki. Strojno berljivi formati so lahko odprti ali lastniški; lahko so formalni standardi ali ne. Za dokumente, kodirane v datotečnem formatu, ki omejuje samodejno obdelavo, saj iz njih podatkov ni možno ali jih ni možno zlahka izločiti, ne bi smelo veljati, da so v strojno berljivem

³¹ Za sisteme za upravljanje osebnih podatkov (PIMS) glej na primer Mnenje ENVP št. 9/2016, ki je na voljo na naslovu https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf.

³² Člen 2 Sklepa št. 922/2009/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o interoperabilnostnih rešitvah za evropske javne uprave (ISA), UL L 260, 3.10.2009, str. 20.

³³ Direktiva o spremembi Direktive 2003/98/ES o ponovni uporabi informacij javnega sektorja.

³⁴ V glosarju EU (<http://eur-lex.europa.eu/eli-register/glossary.html>) so nadalje pojasnjena pričakovanja v zvezi s pojmi, uporabljenimi v teh smernicah, kot so *strojno berljivo*, *interoperabilnost*, *odprta oblika*, *standard* in *metapodatki*.

formatu. Države članice bi morale, kjer je to primerno, spodbujati uporabo odprtih, strojno berljivih formatov.

Glede na široko paleto možnih vrst podatkov, ki bi jih upravljavec podatkov lahko obdelal, Splošna uredba o varstvu podatkov ne uvaja posebnih priporočil glede oblike osebnih podatkov, ki jih je treba zagotoviti. Najustrežnejše oblike se bodo razlikovale glede na sektor. Ustrezne oblike morda že obstajajo in bi jih bilo treba vedno izbrati tako, da se doseže njihov namen, tj. da so primerni za razlago in posamezniku, na katerega se nanašajo osebni podatki, zagotovijo visoko stopnjo prenosljivosti podatkov. Zato se oblike, ki jih ovira drago licenciranje, ne bi štele za ustrezen pristop.

V uvodni izjavi 68 je pojasnjeno, da „[p]ravica posameznika, na katerega se nanašajo osebni podatki, do posredovanja ali prejemanja osebnih podatkov v zvezi z njim ne bi smela ustvariti obveznosti za upravljavca, da mora sprejeti ali vzdrževati sisteme za obdelavo, ki so tehnično združljivi³⁵. **Cilj prenosljivosti je torej vzpostaviti interoperabilne in ne združljive sisteme³⁵.**

Osebni podatki naj bi se posredovali v oblikah z visoko stopnjo abstrakcije iz katere koli notranje ali lastniške oblike. Prenosljivost podatkov kot takšna pomeni dodatno plast obdelave podatkov, ki jo izvedejo upravljavci podatkov, da se podatki izločijo iz platforme in se izključijo osebni podatki, ki ne spadajo na področje uporabe pravice do prenosljivosti, kot so povzeti podatki ali podatki, povezani z varnostjo sistemov. S tem se upravljavce podatkov spodbuja, naj predhodno opredelijo podatke, ki v njihovih sistemih spadajo na področje uporabe pravice do prenosljivosti. Ta dodatna obdelava podatkov se bo štela za dodatno obdelavo poleg glavne obdelave podatkov, saj se ne izvaja za doseganje novega namena, ki ga določi upravljavec podatkov.

Če se v danem sektorju ali okoliščinah ne uporabljajo splošne oblike, **bi morali upravljavci podatkov posredovati osebne podatke v splošno uporabljanih odprtih oblikah (npr. XML, JSON, CSV ...) skupaj z uporabnimi metapodatki v čim večji ločljivosti** in hkrati ohraniti visoko stopnjo abstrakcije. Ustrezne metapodatke bi bilo treba kot takšne uporabiti za točen opis pomena izmenjanih informacij. Ti metapodatki bi morali biti dovolj, da se omogočita uporabnost in ponovna uporaba podatkov, vendar seveda brez razkritja poslovnih skrivnosti. Zato ni verjetno, da bi bile različice PDF e-poštnega nabiralnika, ki se zagotovijo posamezniku, ustrezno strukturirane ali opisne, da bi omogočale enostavno ponovno uporabo podatkov o nabiralniku. Namesto tega bi bilo treba podatke o e-pošti posredovati v obliki, ki ohrani vse metapodatke, da se omogoči učinkovita ponovna uporaba podatkov. Upravljavec podatkov bi moral pri izbiri oblike podatkov, v kateri bo posredoval osebne podatke, upoštevati, kako bo ta oblika vplivala na posameznikovo pravico do ponovne uporabe podatkov ali jo ovirala. Kadar lahko upravljavec podatkov zagotovi posamezniku, na katerega se nanašajo osebni podatki, izbiro glede prednostne oblike osebnih podatkov, bi bilo treba jasno razložiti vpliv izbire. Vendar obdelava dodatnih metapodatkov, ker naj bi bili potrebni ali želeni pri odgovoru na zahtevo za prenosljivost podatkov, ne pomeni zakonitega razloga za takšno obdelavo.

³⁵ V standardu ISO/IEC 2382-01 je interoperabilnost opredeljena kot: „zmogljivost komunikacije, izvajanja programov ali prenosa podatkov med različnimi funkcionalnimi enotami tako, da uporabnik ne potrebuje znanja oziroma ne potrebuje veliko znanja o edinstvenih lastnostih teh enot“.

Delovna skupina iz člena 29 močno spodbuja sodelovanje med deležniki iz industrije in panožnimi združenji, da si bodo skupaj prizadevali za splošen sklop interoperabilnih standardov in oblik za izpolnitev zahtev v zvezi s pravico do prenosljivosti podatkov. Ta izziv je bil obravnavan tudi z evropskim okvirom interoperabilnosti, ki je določil dogovorjeni pristop k interoperabilnosti za organizacije, ki želijo skupaj izvajati javne storitve. Okvir na svojem področju uporabe določa sklop skupnih elementov, kot so slovar, pojmi, načela, politike, smernice, priporočila, standardi, specifikacije in prakse³⁶.

- **Kako obravnavati veliko ali kompleksno zbirko osebnih podatkov?**

V Splošni uredbi o varstvu podatkov ni pojasnjeno, kako obravnavati izziv odgovora v primeru velike zbirke podatkov, kompleksne strukture podatkov ali drugih tehničnih težav, ki bi lahko upravljavcem podatkov ali posameznikom, na katere se nanašajo osebni podatki, povzročile težave.

Vendar je v vseh primerih bistveno, da posameznik v celoti razume opredelitev, sistem in strukturo osebnih podatkov, ki bi jih lahko upravljavec podatkov posredoval. Podatki bi se lahko na primer najprej posredovali v obliki povzetka prek nadzornih plošč, ki posameznikom, na katere se nanašajo osebni podatki, omogočajo prenos podsklopov osebnih podatkov namesto vseh podatkov. Upravljavec podatkov bi moral pregled zagotoviti „v jedrnatih, preglednih, razumljivih in lahko dostopnih oblikah ter jasnem in preprostem jeziku“ (glej člen 12(1) Splošne uredbe o varstvu podatkov), tako da bi imel posameznik, na katerega se nanašajo osebni podatki, vedno jasne informacije o tem, katere podatke v zvezi z danim namenom naj naloži ali prenese k drugemu upravljavcu podatkov. Posameznikom, na katere se nanašajo osebni podatki, bi bilo treba na primer omogočiti uporabo programske opreme, ki mu v svojem okviru omogoča enostavno opredelitev, prepoznavanje in obdelavo posebnih podatkov.

Kot je navedeno zgoraj, bi lahko bil praktičen način, na katerega lahko upravljavec podatkov odgovori na zahteve za prenosljivost podatkov, zagotovitev ustrezno zaščitenega in dokumentiranega API. To bi lahko posameznikom omogočilo, da zahteve glede svojih osebnih podatkov vložijo pri upravljavcu podatkov s svojo ali programsko opremo ali programsko opremo tretjih oseb ali drugim dodelijo dovoljenje, da to storijo v njihovem imenu (vključno z drugim upravljavcem podatkov), kot je določeno v členu 20(2) Splošne uredbe o varstvu podatkov. Z dodelitvijo dostopa do podatkov prek zunanje dostopnega API bi se morda lahko zagotovil tudi naprednejši sistem dostopa, ki posameznikom omogoča naknadne zahteve glede podatkov, in sicer v obliki nalaganja vseh podatkov ali funkcije delta, ki vsebuje le spremembe od zadnjega nalaganja, ne da bi te dodatne zahteve pomenile težave za upravljavca podatkov.

- **Kako se lahko prenosljivi podatki zavarujejo?**

Na splošno bi morali upravljavci podatkov v skladu s členom 5(1)(f) Splošne uredbe o varstvu podatkov zagotoviti „ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi“.

³⁶ Vir: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

Vendar lahko posredovanje osebnih podatkov za posameznika, na katerega se nanašajo osebni podatki, sproža tudi nekatera varnostna vprašanja:

Kako lahko upravljavci podatkov zagotovijo, da se osebni podatki varno prenesejo k pravi osebi?

Ker je cilj prenosljivosti podatkov pridobitev osebnih podatkov iz informacijskega sistema upravljavca podatkov, lahko posredovanje postane možen vir tveganja v zvezi s temi podatki (zlasti kršitve varstva podatkov med posredovanjem). Upravljavec podatkov je odgovoren za sprejetje vseh varnostnih ukrepov, potrebnih za zagotovitev varnega prenosa osebnih podatkov (z uporabo celovitega šifriranja ali šifriranja podatkov) na pravi cilj (z uporabo zanesljivih avtentikacijskih ukrepov), stalne zaščite osebnih podatkov, ki ostanejo v njegovih sistemih, in preglednih postopkov za obravnavanje možnih kršitev varstva podatkov³⁷. Upravljavci podatkov bi morali oceniti posebna tveganja v zvezi s prenosljivostjo podatkov in sprejeti ustrezne ukrepe za zmanjševanje tveganja.

Takšni ukrepi za zmanjševanje tveganja bi lahko vključevali: če je treba posameznika, na katerega se nanašajo osebni podatki, avtenticirati, uporabo dodatnih informacij za avtentikacijo, kot je zaupana skrivnost, ali drugega elementa avtentikacije, kot je enkratno geslo; prekinitvev ali zamrznitev posredovanja, če obstaja sum, da je bil račun ogrožen; v primeru neposrednega prenosa od enega upravljavca podatkov k drugemu bi bilo treba uporabiti avtentikacijo na podlagi pooblastila, kot je avtentikacija na podlagi žetona.

Takšni varnostni ukrepi sami po sebi ne smejo pomeniti ovire in uporabnikom ne smejo preprečiti uresničevanja njihovih pravic, npr. z uvedbo dodatnih stroškov.

Kako uporabnikom pomagati zavarovati hrambo njihovih osebnih podatkov v lastnih sistemih?

Ko uporabniki pridobijo osebne podatke iz spletne storitve, vedno obstaja tveganje, da jih bodo shranili v manj zavarovanih sistemih, kot jih zagotavlja storitev. Posameznik, na katerega se nanašajo osebni podatki, ki podatke zahteva, je odgovoren za opredelitev pravih ukrepov za zavarovanje osebnih podatkov v svojem sistemu. Vendar ga je treba s tem seznaniti, da lahko sprejme ukrepe za zaščito informacij, ki jih je prejel. Kot primer vodilne prakse lahko upravljavci podatkov priporočijo tudi ustrezne oblike, orodja za šifriranje in druge varnostne ukrepe, da bi posamezniku, na katerega se nanašajo osebni podatki, pomagali doseči ta cilj.

* * *

V Bruslju, 13. decembra 2016

*Za delovno skupino
Predsednica
Isabelle FALQUE-PIERROTIN*

³⁷ V skladu z Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

Kot so bile nazadnje revidirane in sprejete
5. aprila 2017

Za delovno skupino

Predsednica

Isabelle FALQUE-PIERROTIN