16/EN
WP 242 rev.01

Smjernice o pravu na prenosivost podataka

Donesene 13. prosinca 2016.
Kako su zadnje revidirane i donesene 5. travnja 2017.

Radna skupina osnovana je na temelju članka 29. Direktive 95/46/EZ. Ona je neovisno europsko savjetodavno tijelo za zaštitu podataka i privatnost. Njezine su zadaće opisane u članku 30. Direktive 95/46/EZ i članku 15. Direktive 2002/58/EZ.

Tajništvo osigurava Uprava C (Temeljna prava i vladavina prava) Europske komisije, Glavna uprava za pravosuđe i potrošače, B-1049 Bruxelles, Belgija, ured br. MO-59 05/35.

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

SADRŽAJ

Sažetak

Člankom 20. Opće uredbe o zaštiti podataka uvodi se novo pravo na prenosivost podataka, koje je usko povezano s pravom pristupa, ali ipak se u mnogočemu razlikuje od njega. Njime se ispitanicima omogućuje da prime osobne podatke koje su pružidali voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te da prenesu te podatke drugom voditelju obrade. Svrha je tog novog prava osnažiti ispitanika i omogućiti mu veću kontrolu nad osobnim podacima koji se na njega odnose.

Budući da se njime omogućuje izravan prijenos osobnih podataka od jednog voditelja obrade drugome, pravo na prenosivost podataka važan je alat kojim će se podržati slobodan protok osobnih podataka u EU-u i poticati tržišno natjecanje između voditelja obrade. Njime će se olakšati mijenjanje pružatelja usluga i time poticati razvoj novih usluga u kontekstu strategije jedinstvenog digitalnog tržišta.

Ovim se mišljenjem pružaju smjernice o načinu tumačenja i provedbe prava na prenosivost podataka uvedenog Općom uredbom o zaštiti podataka. Svrha mu je rasprava o pravu na prenosivost i njegovu području primjene. U njemu se pojašnjavaju okolnosti u kojima se primjenjuje to novo pravo, uzimajući u obzir pravnu osnovu obrade podataka (suglasnost ispitanika ili potrebu izvršavanja ugovora) i činjenicu da je to pravo ograničeno na osobne podatke koje pruža ispitanik. U mišljenju se pružaju i konkretni primjeri i kriteriji kojima se objašnjavaju okolnosti u kojima se primjenjuje to pravo. U tom pogledu radna skupina iz članka 29. smatra da su pravom na prenosivost podataka obuhvaćeni podaci koje je ispitanik pružio svjesno i aktivno, kao i osobni podaci prikupljeni iz njegovih aktivnosti. To se novo pravo ne može narušiti i ograničiti na osobne informacije koje ispitanik izravno pruža, primjerice, u internetskom obrascu.

Voditelji obrade trebali bi, kao dobru praksu, početi razvijati načine kojima će se pridonijeti odgovaranju na zahtjeve za prenosivost podataka, kao što su alati za preuzimanje i sučelja za programiranje aplikacija. Trebali bi zajamčiti da se osobni podaci prenose u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te bi ih trebalo poticati da osiguravaju interoperabilnost formata podataka koji se pružaju tijekom izvršavanja zahtjeva za prenosivost podataka.

Mišljenjem se voditeljima obrade pomaže i da jasno shvate svoje obveze te se preporučuju najbolje prakse i alati kojima se podržava usklađenost s pravom na prenosivost podataka. Konačno, u mišljenju se preporučuje da dionici iz industrije i trgovinska udruženja surađuju u izradi zajedničkih interoperabilnih standarda i formata kako bi se ispunili zahtjevi prava na prenosivost podataka.

I. Uvod

Člankom 20. Opće uredbe o zaštiti podataka (OUZP) uvodi se novo pravo na prenosivost podataka. Tim se pravom ispitanicima omogućuje da prime osobne podatke koje su pružili voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te da bez ometanja prenesu te podatke drugom voditelju obrade. Pravo se primjenjuje u određenim uvjetima, a njime se podupiru korisnički izbor, kontrola i osnaživanje korisnika.

Pojedinci koji iskorištavaju svoje pravo na pristup u okviru Direktive o zaštiti podataka 95/46/EZ bili su pri pružanju zatraženih informacija ograničeni formatom koji je odabrao voditelj obrade. **Novo pravo na prenosivost podataka usmjereno je na osnaživanje ispitanika u pogledu vlastitih osobnih podataka jer se njime olakšava njihova mogućnost premještanja, kopiranja ili prijenosa osobnih podataka iz jednog IT okruženja u drugo** (u njihove vlastite sustave, sustave pouzdanih trećih strana ili sustave novih voditelja obrade).

Budući da se njome priznaju osobna prava i kontrola pojedinaca nad osobnim podacima koji se na njih odnose, prenosivost podataka predstavlja i mogućnost ponovne uspostave ravnoteže između ispitanikâ i voditeljâ podataka[1].

Iako se pravom na prenosivost osobnih podataka može unaprijediti i konkurentnost između usluga (olakšavanjem prelaska s usluge na uslugu), Općom uredbom o zaštiti podataka reguliraju se osobni podaci, a ne konkurentnost. Konkretno, člankom 20. prenosivi podaci ne ograničavaju se na one koji su potrebni ili korisni za prelazak s usluge na uslugu[2].

Iako je prenosivost podataka novo pravo, druge vrste prenosivosti već postoje ili se o njima raspravlja u okviru drugih područja zakonodavstva (npr. u kontekstu otkazivanja ugovora, *roaminga* u okviru komunikacijskih usluga te prekograničnog pristupa uslugama[3]). Iz različitih vrsta prenosivosti mogle bi proizaći određene sinergije, čak i koristi za pojedince, ako ih se pruža zajedno, iako bi trebalo zauzeti oprezan stav prema analognim slučajevima.

Ovim se mišljenjem voditeljima obrade pružaju smjernice kako bi mogli unaprijediti svoje prakse, postupke i politike te se pojašnjava pojam prenosivosti podataka kako bi se ispitanicima omogućilo da se učinkovito služe svojim novim pravom.

II. Koji su glavni elementi prenosivosti podataka?

U članku 20. stavku 1. Opće uredbe o zaštiti podataka pravo na prenosivost definirano je kako slijedi:

> *Ispitanik ima pravo zaprimiti osobne podatke koji se odnose na njega, a koje je pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu te ima pravo prenijeti te podatke drugom voditelju obrade bez ometanja od strane voditelja obrade kojem su osobni podaci pruženi [...]*

- Pravo na primanje osobnih podataka

Kao prvo, prenosivost podataka **pravo je ispitanika na primanje podskupa osobnih podataka** koji se odnose na njega i koje je obradio voditelj obrade te na pohranjivanje tih

[1] Glavni je cilj prenosivosti podataka poboljšati kontrolu pojedinaca nad vlastitim osobnim podacima i osigurati da imaju aktivnu ulogu u podatkovnom ekosustavu.
[2] Na primjer, tim se pravom može omogućiti bankama da pružaju dodatne usluge, pod kontrolom korisnika, upotrebom osobnih podataka koji su prvotno prikupljeni u okviru usluge opskrbe energijom.
[3] Vidjeti program Europske komisije za jedinstveno digitalno tržište: https://ec.europa.eu/digital-agenda/en/digital-single-market, a posebno prvi stup politike „Bolji pristup digitalnoj robi i uslugama na internetu".

podataka za daljnju osobnu upotrebu. Pohranjivati ih se može na privatnom uređaju ili u privatnom oblaku bez potrebe za prijenosom podataka drugom voditelju obrade.

Prenosivost podataka u tom pogledu nadopunjuje pravo pristupa. Jedna je od posebnosti prenosivosti podataka činjenica da se njome ispitanicima omogućuje da na jednostavan način sami upravljaju osobnim podacima i ponovno ih upotrebljavaju. Ti bi se podaci trebali primati „*u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu"*. Na primjer, ispitanik bi mogao poželjeti preuzeti svoj trenutačni popis za reprodukciju (ili prošlost slušanih zapisa) iz usluge za reprodukciju glazbe kako bi saznao koliko je puta odslušao neke zapise ili provjerio koju glazbu želi kupiti ili slušati na nekoj drugoj platformi. Slično tomu, može poželjeti preuzeti i popis svojih kontakata iz aplikacije za internetsku poštu (*webmail*) kako bi, primjerice, sastavio popis uzvanika za vjenčanje, informirati se o kupnjama uz upotrebu različitih kartica vjernosti ili procijeniti svoj ugljični otisak[4].

- **Pravo prijenosa osobnih podataka od jednog voditelja obrade drugom**

Kao drugo, člankom 20. stavkom 1. ispitanicima je osigurano **pravo prenošenja osobnih podataka od jednog voditelja obrade drugom** „bez ometanja". Podaci se mogu prenijeti i izravno od jednog voditelja obrade drugom na zahtjev ispitanika te ako je to tehnički izvedivo (članak 20. stavak 2.). U tom se pogledu uvodnom izjavom 68. potiče voditelje obrade na razvoj interoperabilnih formata koji omogućuju prenosivost podataka[5], ali bez stvaranja obveze za voditelja obrade da upotrebljava ili održava tehnički kompatibilne sustave za obradu[6]. Međutim, Općom uredbom o zaštiti podataka voditeljima obrade zabranjuje se da postavljaju prepreke za prijenos.

Tim se elementom prenosivosti podataka ispitanicima u osnovi omogućuje ne samo da prime i ponovno upotrijebe, već i da prenesu podatke koje pružaju drugom pružatelju usluga (u istom poslovnom sektoru ili u nekom drugom). Uz to što osigurava osnaživanje potrošača sprečavanjem „ovisnosti o dobavljačima", očekuje se da će se pravom na prenosivost podataka poticati prilike za inovacije i razmjenu osobnih podataka između voditelja obrade na siguran i zaštićen način pod kontrolom ispitanika[7]. Prenosivost podataka može promicati kontrolirano i ograničeno dijeljenje podataka ispitanika između organizacija te tako unaprijediti usluge i iskustva potrošača[8]. Prenosivost podataka može olakšati prijenos i ponovnu upotrebu osobnih podataka koji se odnose na korisnike u okviru različitih usluga koje ih zanimaju.

[4] U tim slučajevima obrada koja se izvršava na podacima ispitanika može biti obuhvaćena područjem primjene koje se odnosi na kućne aktivnosti, gdje se cjelokupna obrada izvršava pod isključivom kontrolom ispitanika, ili je može izvršiti druga strana u ime ispitanika. U potonjem slučaju drugu bi stranu trebalo smatrati voditeljem obrade, čak i za isključivu svrhu pohrane osobnih podataka, a ta druga strana mora poštovati načela i obveze utvrđene Općom uredbom o zaštiti podataka.

[5] Vidjeti i odjeljak V.

[6] Zbog toga bi trebalo posebnu pozornost obratiti na format podataka koji se prenose kako bi se zajamčilo da ispitanik ili drugi voditelj obrade može jednostavno ponovno upotrijebiti podatke. Vidjeti i odjeljak V.

[7] Vidjeti nekoliko pokusnih primjena u Europi, na primjer MiData u Ujedinjenoj Kraljevini, MesInfos/SelfData koje pruža FING u Francuskoj.

[8] Takozvani *quantified self* i industrije interneta stvari pokazali su koje su prednosti (i rizici) povezivanja osobnih podataka iz različitih aspekata života pojedinca kao što su kondicija, tjelesna aktivnost i unos kalorija kako bi se dobila bolja slika o životu pojedinca u jednoj datoteci.

- **Kontrola**

Prenosivost podataka jamči pravo primanja i obrade osobnih podataka u skladu sa željama ispitanika[9].

Voditelji obrade koji odgovaraju na zahtjeve za prenosivost podataka u skladu s uvjetima iz članka 20. nisu odgovorni za obradu koju provodi ispitanik ili neko drugo društvo koje prima osobne podatke. Oni djeluju u ime ispitanika, uključujući i kad se osobni podaci izravno prenose drugom voditelju obrade. U tom smislu voditelj obrade nije odgovoran za usklađenost voditelja obrade koji prima podatke s pravom zaštite podataka jer voditelj obrade koji šalje podatke nije taj koji odabire primatelja tih podataka. Voditelj bi istodobno trebao uspostaviti zaštitne mjere kako bi osigurao da zaista djeluje u ime ispitanika. Na primjer, mogu se uspostaviti postupci kojima se osigurava da je vrsta podataka koji se prenose zaista ona vrsta koju ispitanik želi prenijeti. To se može učiniti tako da se od ispitanika dobije potvrda prije prijenosa ili još ranije, kad se prvi put daje suglasnost za obradu podataka ili se sklapa ugovor.

Voditelji obrade koji odgovaraju na zahtjev za prenosivost podataka nisu posebno obvezni provjeravati i potvrđivati kvalitetu podataka prije njihova prijenosa. Naravno, ti bi podaci već trebali biti točni i ažurni, u skladu s načelima navedenima u članku 5. stavku 1. Opće uredbe o zaštiti podataka. Osim toga, prenosivost podataka ne nameće voditelju obrade obvezu zadržavanja osobnih podataka dulje no što je to potrebno ili nakon isteka određenog razdoblja zadržavanja[10]. Važno je napomenuti da nema dodatnog zahtjeva za zadržavanje podataka nakon isteka inače primjenjivih razdoblja zadržavanja samo kako bi ih se iskoristilo za mogući budući zahtjev za prenosivost podataka.

Ako zatražene osobne podatke obrađuje voditelj obrade, ugovor sklopljen u skladu s člankom 28. Opće uredbe o zaštiti podataka mora uključivati obvezu pomaganja „voditelju obrade putem odgovarajućih tehničkih i organizacijskih mjera, [...] u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika". Voditelj obrade stoga bi u suradnji sa svojim izvršiteljima obrade trebao uvesti posebne postupke radi odgovaranja na zahtjev za prenosivost podataka. U slučaju zajedničke kontrole, ugovorom bi trebalo jasno raspodijeliti odgovornosti između svih voditelja obrade u pogledu obrade zahtjeva za prenosivost podataka.

Nadalje, voditelj obrade koji prima podatke[11] odgovoran je osigurati da su pruženi prenosivi podaci relevantni i da nisu prekomjerni s obzirom na novu obradu podataka. Na primjer, ako se zahtjev za prenosivost podataka dostavlja pružatelju usluge internetske pošte, pri čemu ispitanik zahtjev upotrebljava radi primanja poruka e-pošte i njihova slanja na sigurnu platformu za arhiviranje, novi voditelj obrade ne mora obrađivati podatke za kontakt ispitanikovih korespondenata. Ako te informacije nisu relevantne u odnosu na svrhu nove obrade, ne bi ih trebalo čuvati i obrađivati. U svakom slučaju, voditelji obrade koji primaju podatke nisu obvezni prihvatiti i obrađivati osobne podatke koji se prenose nakon zahtjeva za prenosivost podataka. Slično tomu, ako ispitanik zatraži prijenos podataka o svojim bankovnim transakcijama usluzi koja pomaže u upravljanju njegovim proračunom, voditelj

[9] Pravo na prenosivost podataka nije ograničeno na osobne podatke koji su korisni i relevantni za slične usluge koje pružaju konkurenti voditelja obrade.

[10] U prethodnom primjeru, ako voditelj podataka ne čuva zapis o pjesmama koje je korisnik slušao, ti se osobni podaci ne mogu uključiti u zahtjev za prenosivost podataka.

[11] Odnosno onaj koji prima podatke nakon zahtjeva za prenosivost podataka koji je ispitanik podnio drugom voditelju obrade.

obrade koji prima podatke ne mora prihvatiti sve podatke ili zadržati sve pojedinosti o transakcijama nakon što ih se označi za potrebe nove usluge. Drugim riječima, podaci koji se primaju i zadržavaju trebali bi biti samo oni koji su potrebni i relevantni za uslugu koju pruža voditelj obrade koji prima podatke.

Organizacija koja prima podatke postaje novi voditelj obrade za te osobne podatke i mora poštovati načela navedena u članku 5. Opće uredbe o zaštiti podataka. Stoga taj „novi" voditelj obrade mora jasno i izravno navesti svrhu nove obrade prije zahtjeva za prijenos prenosivih podataka u skladu sa zahtjevima o transparentnosti iz članka 14.[12] Kad je riječ o drugoj obradi podataka koja se provodi pod njegovom odgovornošću, voditelj obrade trebao bi primjenjivati načela propisana člankom 5. kao što su zakonitost, pravednost i transparentnost, ograničavanje svrhe, smanjenje količine podataka, točnost, cjelovitost i povjerljivost, ograničenje pohrane i pouzdanost[13].

Voditelji obrade koji posjeduju osobne podatke trebali bi biti spremni omogućiti svojim ispitanicima pravo na prenosivost podataka. Voditelji obrade mogu odlučiti i prihvatiti podatke od ispitanika, ali nisu obvezni to učiniti.

- **Prenosivost podataka u usporedbi s drugim pravima ispitanika**

Kad pojedinac ostvaruje svoje pravo na prenosivost podataka, to čini bez dovođenja bilo kojeg drugog prava u pitanje (što vrijedi i za druga prava iz Opće uredbe o zaštiti podataka). Ispitanik se može nastaviti služiti uslugama voditelja obrade podataka i ostvarivati koristi od njih čak i nakon provedbe radnje prenosivosti podataka. Prenosivost podataka ne pokreće automatski brisanje podataka[14] iz sustavâ voditelja obrade te ne utječe na izvorno razdoblje zadržavanja koje se primjenjuje na prenesene podatke. Ispitanik svoja prava može ostvarivati sve dok voditelj obrade podataka i dalje obrađuje podatke.

Isto tako, ako ispitanik želi ostvariti svoje pravo na brisanje („pravo na zaborav" u skladu s člankom 17.), voditelj obrade ne smije se poslužiti prenosivošću podataka za odlaganje ili odbijanje tog brisanja.

Ako ispitanik otkrije da osobni podaci zatraženi u okviru prava na prenosivost podataka ne ispunjuju u potpunosti njegov zahtjev, trebalo bi u potpunosti ispuniti svaki naknadni zahtjev za osobne podatke u okviru prava na pristup, u skladu s člankom 15. Opće uredbe o zaštiti podataka.

Nadalje, ako je određenim europskim propisom ili propisom neke države članice u nekom drugom području isto tako predviđen određeni oblik prenosivosti predmetnih podataka, i uvjeti propisani tim konkretnim pravom moraju se uzeti u obzir pri izvršavanju zahtjeva za prenosivost podataka u okviru Opće uredbe o zaštiti podataka. Kao prvo, ako je iz zahtjeva ispitanika jasno da nema namjeru ostvarivati prava u okviru Opće uredbe o zaštiti podataka,

[12] Osim toga, novi voditelj obrade ne bi trebao obrađivati osobne podatke koji nisu relevantni, a obradu bi trebao ograničiti na ono što je nužno za nove svrhe, čak i ako su ti osobni podaci dio općenitijeg skupa podataka koji se prenosi u okviru postupka prenosivosti. Osobne podatke koji nisu nužni za postizanje svrhe nove obrade trebalo bi obrisati što je prije moguće.

[13] Kad ih voditelj obrade jednom primi, za osobne podatke koji se šalju kao dio prava na prenosivost podataka može se smatrati da ih je „pružio" ispitanik i mogu se ponovno prenijeti u skladu s pravom na prenosivost podataka sve dok se ispunjuju drugi uvjeti primjenjivi na to pravo (odnosno pravna osnova obrade itd.).

[14] Kako je navedeno u članku 17. Opće uredbe o zaštiti podataka.

već samo ostvarivati prava u okviru sektorskog zakonodavstva, odredbe o prenosivosti podataka iz Opće uredbe o zaštiti podataka neće se primjenjivati na taj zahtjev[15]. S druge strane, ako je zahtjev usmjeren na prenosivost u okviru Opće uredbe o zaštiti podataka, činjenica da postoji to posebno zakonodavstvo nema prednost pred općom primjenom načela prenosivosti podataka bilo kojem voditelju obrade, kako je predviđeno Općom uredbom o zaštiti podataka. Umjesto toga, mora se na temelju svakog pojedinačnog slučaja procijeniti kako, ako uopće, to posebno zakonodavstvo može utjecati na pravo na prenosivost podataka.

III. Kad se primjenjuje prenosivost podataka?

- **Koje su radnje obrade obuhvaćene pravom na prenosivost podataka?**

Kako bi bili usklađeni s Općom uredbom o zaštiti podataka, voditelji obrade moraju imati jasnu pravnu osnovu za obradu osobnih podataka.

U skladu s člankom 20. stavkom 1. točkom (a) Opće uredbe o zaštiti podataka, **kako bi se** postupci obrade **uključili u područje primjene prenosivosti podataka**, moraju se temeljiti:

- na privoli ispitanika (u skladu s člankom 6. stavkom 1. točkom (a) ili u skladu s člankom 9. stavkom 2. točkom (a) ako je riječ o posebnim kategorijama osobnih podataka)

- ili na ugovoru u kojem je ispitanik stranka u skladu s člankom 6. stavkom 1. točkom (b).

Na primjer, naslovi knjiga koje je pojedinac kupio iz određene internetske knjižare ili pjesme koje je slušao u okviru usluge za reprodukciju glazbe primjeri su osobnih podataka koji uglavnom jesu uključeni u područje primjene prenosivosti podataka jer ih se obrađuje na temelju izvršavanja ugovora u kojem je ispitanik stranka.

Općom uredbom o zaštiti podataka ne utvrđuje se općenito pravo na prenosivost podataka za slučajeve u kojima se obrada osobnih podataka ne temelji na suglasnosti ili ugovoru[16]. Na primjer, financijske ustanove nisu obvezne odgovoriti na zahtjev za prenosivost podataka koji se odnosi na osobne podatke koji se obrađuju kao dio njihove obveze sprečavanja i otkrivanja pranja novca i drugih financijskih kaznenih djela. Isto tako, prenosivost podataka ne obuhvaća profesionalne podatke za kontakt koji se obrađuju u okviru odnosa između poslovnih

[15] Na primjer, ako se zahtjevom ispitanika konkretno nastoji pružatelju informacijskih usluga omogućiti pristup povijesnim podacima o bankovnom računu ispitanika za potrebe navedene u Drugoj direktivi o platnim uslugama, takav bi pristup trebalo dopustiti u skladu s odredbama te Direktive.

[16] Vidjeti uvodnu izjavu 68. i članak 20. stavak 3. Opće uredbe o zaštiti podataka. Člankom 20. stavkom 3. i uvodnom izjavom 68. predviđeno je da se prenosivost podataka ne primjenjuje kad je obrada podataka nužna za obavljanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti dodijeljene voditelju obrade ili kad voditelj obrade izvršava svoje javne dužnosti ili ispunjava pravnu obvezu. Stoga voditelji obrade u tim slučajevima nisu obvezni osigurati prenosivost. Međutim, dobra je praksa razviti postupke za automatski odgovor na zahtjeve za prenosivost slijedeći načela mjerodavna za pravo na prenosivost podataka. Jedan bi primjer za to mogla biti usluga vladinih tijela za jednostavno preuzimanje prošlih obrazaca za prijavu poreza. Prenosivost podataka kao dobra praksa u slučaju obrade na temelju pravne osnove potrebe za legitimnim interesom i za postojećim dobrovoljnim programima opisana je na stranicama 47. i 48. Mišljenja 6/2014 radne skupine 29. o legitimnim interesima (WP217).

subjekata u slučajevima u kojima se obrada ne temelji ni na suglasnosti ispitanika ni na ugovoru u kojem je stranka.

Kad je riječ o podacima o zaposlenicima, pravo na prenosivost podataka obično se primjenjuje samo ako se obrada temelji na ugovoru čija je ispitanik stranka. U brojnim se slučajevima neće smatrati da je suglasnost dana dobrovoljno u tom kontekstu zbog neravnoteže ovlasti između poslodavca i zaposlenika[17]. Umjesto toga, određene obrade u okviru ljudskih resursa temelje se na pravnoj osnovi legitimnog interesa ili su nužne radi ispunjivanja određenih pravnih obveza u području zapošljavanja. U praksi će se pravo na prenosivost podataka u kontekstu ljudskih resursa nedvojbeno odnositi na određene postupke obrade (kao što su usluge plaćanja i isplate naknada, interno zapošljavanje), ali u brojnim drugim situacijama bit će potrebna provjera svakog pojedinačnog slučaja kako bi se vidjelo jesu li ispunjeni svi uvjeti koji se primjenjuju na pravo na prenosivost podataka.

Konačno, pravo na prenosivost podataka primjenjuje se samo ako se obrada podataka „provodi automatiziranim putem" i stoga ne obuhvaća većinu papirnatih spisa.

- **Koji se osobni podaci moraju uključiti?**

U skladu s člankom 20. stavkom 1., kako bi podaci bili u području primjene prenosivosti podataka, moraju biti:

- osobni podaci koji se odnose na ispitanika i
- podaci koje je ispitanik *pružio* voditelju obrade.

U članku 20. stavku 4. navedeno je i da to pravo ne smije negativno utjecati na prava i slobode drugih.

Prvi uvjet: osobni podaci koji se odnose na ispitanika

U područje primjene zahtjeva za prenosivost podataka uključeni su samo osobni podaci. Stoga svi podaci koji su anonimni[18] ili se ne odnose na ispitanika neće biti uključeni u to područje primjene. Međutim, pseudonimizirani podaci koji se mogu jasno povezati s ispitanikom (npr. tako da ispitanik pruži odgovarajući identifikator, vidjeti članak 11. stavak 2.) uključeni su u područje primjene.

U brojnim će okolnostima voditelji obrade obrađivati informacije koje sadržavaju osobne podatke o nekoliko ispitanika. U tom slučaju voditelji obrade ne bi trebali prestrogo tumačiti rečenicu „osobni podaci koji se odnose na ispitanika". Na primjer, telefonski zapisi, razmjena poruka među osobama ili zapisi prijenosa govora putem internetskog protokola (VoIP) mogu uključivati (u povijesti računa korisnika) pojedinosti o trećim osobama uključenima u ulazne i izlazne pozive. Iako će zbog toga zapisi sadržavati osobne podatke koji se odnose na više ljudi, trebalo bi ih moći pružiti korisnicima kao odgovor na zahtjeve za prenosivost podataka jer se zapisi odnose (i) na ispitanika. Međutim, ako se ti zapisi zatim prenose novom voditelju obrade, taj novi voditelj obrade ne bi ih trebao obrađivati ni za jednu svrhu koja bi negativno utjecala na prava i slobode trećih osoba (vidjeti u nastavku: treći uvjet).

Drugi uvjet: podaci koje je pružio ispitanik

[17] Kako je radna skupina iz članka 29. naglasila u svojem Mišljenju 8/2001 od 13. rujna 2001. (WP48).
[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_hr.pdf

Drugi uvjet sužava područje primjene na podatke koje je „pružio" ispitanik.

Brojni su primjeri osobnih podataka koje će ispitanik svjesno i aktivno „pružiti", kao što su podaci o računu (poštanska adresa, korisničko ime, dob) dostavljeni putem internetskih obrazaca. Ipak, podaci koje „pruži" ispitanik isto tako potječu od promatranja njegovih aktivnosti. Zbog toga radna skupina iz članka 29. smatra da bi se radi ostvarivanja potpune vrijednosti tog novog prava u podatke koje su „pružili" korisnici trebali uključiti i osobni podaci zabilježeni na temelju aktivnosti korisnikâ, kao što su sirovi podaci koji se obrađuju pametnim mjerenjem ili neke druge vrste povezanih objekata[19], zapisnici aktivnosti, povijest upotrebe internetskih stranica ili aktivnosti pretraživanja.

Ta potonja kategorija podataka ne uključuje podatke koje stvara voditelj obrade (upotrebom zabilježenih podataka ili podataka koji su izravno pruženi kao ulazni podaci), kao što je korisnički profil kreiran analizom sirovih podataka dobivenih pametnim mjerenjem.

Moguće je razlikovati različite kategorije podataka ovisno o njihovu podrijetlu kako bi se utvrdilo jesu li obuhvaćeni pravom na prenosivost podataka. Sljedeće se kategorije mogu klasificirati kao „podaci koje je pružio ispitanik":

- **podaci koje je ispitanik pružio aktivno i svjesno** (na primjer poštanska adresa, korisničko ime, dob itd.),
- **zabilježeni podaci koje je ispitanik pružio upotrebom usluge ili uređaja**. Oni mogu, na primjer, uključivati povijest pretraživanja, podatke o prometu i podatke o lokaciji pojedinca. Mogu uključivati i druge sirove podatke kao što je praćenje otkucaja srca s pomoću uređaja koji pojedinac nosi na sebi (eng. *wearable device*).

S druge strane, podatke koji se zaključuju ili izvode stvara voditelj obrade na temelju podataka koje je „pružio ispitanik". Na primjer, ne može se smatrati da je rezultate procjene koja se odnosi na stanje korisnika ili profila izrađene u kontekstu upravljanja rizikom i financijskih propisa (npr. radi ocjene kreditne sposobnosti ili usklađivanja s pravilima protiv pranja novca) „pružio" ispitanik. Iako takvi podaci mogu biti dio profila koji održava voditelj obrade te ih se zaključuje ili izvodi na temelju analize podataka koje je pružio ispitanik (na primjer u okviru svojih aktivnosti), obično se neće smatrati da je te podatke „pružio ispitanik" te neće biti obuhvaćeni tim novim pravom[20].

Općenito, imajući na umu ciljeve politike prava na prenosivost podataka, izraz „pružio ispitanik" mora se široko tumačiti te bi se trebali isključiti „podaci koji se zaključuju" i „podaci koji se izvode", što uključuje osobne podatke koje stvara pružatelj usluge (na primjer rezultate iz algoritama). Voditelj obrade može isključiti te podatke koji se zaključuju, ali

[19] Ako ispitanik može preuzeti podatke zabilježene na temelju njegovih aktivnosti, moći će i dobiti bolji uvid u odluke o provedbi koje je donio voditelj obrade u pogledu područja primjene zabilježenih podataka i bit će u boljem položaju za odabir podataka koje želi pružiti radi dobivanja slične usluge te biti svjestan mjere u kojoj se poštuje njegovo pravo na privatnost.

[20] Ipak, ispitanik svejedno može iskoristiti svoje „pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima", kao i informaciju o „postojanju automatiziranog donošenja odluka, što uključuje izradu profila iz članka 22. stavaka 1. i 4. te, barem u tim slučajevima, smislenim informacijama o tome o kojoj je logici riječ, kao i važnosti i predviđenim posljedicama takve obrade za ispitanika", u skladu s člankom 15. Opće uredbe o zaštiti podataka (koji se odnosi na pravo na pristup).

trebao bi uključiti sve druge osobne podatke koje je pružio ispitanik putem tehničkih sredstava koje je omogućio voditelj obrade[21].

Stoga izraz „pružio" obuhvaća osobne podatke koji se odnose na aktivnost ispitanika ili proizlaze iz promatranja ponašanja pojedinca, ali ne obuhvaća podatke koji potječu iz naknadne analize tog ponašanja. S druge strane, svi osobni podaci koje je stvorio voditelj obrade tijekom obrade podataka, na primjer u okviru postupka personalizacije ili davanja preporuka, kategorizacijom korisnika ili izradom profila podaci su koji se izvode ili zaključuju na temelju osobnih podataka koje je pružio ispitanik i nisu obuhvaćeni pravom na prenosivost podataka.

Treći uvjet: pravo na prenosivost podataka ne smije negativno utjecati na prava i slobode drugih

U pogledu osobnih podataka koji se odnose na druge ispitanike

Trećim se uvjetom nastoji izbjeći da novi voditelj obrade pronalazi i prenosi podatke koji sadržavaju osobne podatke o drugim ispitanicima (koji nisu dali suglasnost) u slučajevima u kojima je vjerojatno da bi se ti podaci mogli obrađivati na način koji bi negativno utjecao na prava i slobode drugih ispitanika (članak 20. stavak 4. Opće uredbe o zaštiti podataka)[22].

Do takvog bi negativnog utjecaja moglo doći, na primjer, ako bi se prijenosom podataka od jednog voditelja obrade drugom spriječilo treće osobe u ostvarivanju prava koja imaju kao ispitanici u okviru Opće uredbe o zaštiti podataka (kao što su pravo na informiranje, pravo na pristup itd.).

Ispitanik koji pokreće prijenos svojih podataka drugom voditelju obrade daje suglasnost novom voditelju obrade za tu obradu ili sklapa ugovor s tim voditeljem obrade. Ako su u skup podataka uključeni osobni podaci trećih osoba potrebno je utvrditi drugu pravnu osnovu za obradu. Na primjer, voditelj obrade može slijediti legitimni interes na temelju članka 6. stavka 1. točke (f), posebno ako je svrha voditelja obrade da ispitaniku pruži uslugu koja mu omogućuje da obrađuje osobne podatke isključivo u okviru osobne ili kućne aktivnosti. Ispitanik ostaje odgovoran za postupke obrade koje je započeo u kontekstu osobnih aktivnosti te koji se odnose na treće osobe i mogli bi na njih utjecati, ako o toj obradi ni na koji način ne odlučuje voditelj obrade.

Na primjer, usluga internetske pošte mogla bi omogućivati stvaranje imenika s kontaktima, prijateljima, rođacima, obitelji i širom okolinom ispitanika. Budući da se ti podaci odnose na pojedinca kojeg je moguće identificirati (te ih on stvara) i koji želi ostvariti svoje pravo na prenosivost podataka, voditelji obrade trebali bi prenijeti cijeli imenik ulaznih i izlaznih poruka e-pošte tom ispitaniku.

[21] To uključuje sve zabilježene podatke o ispitaniku tijekom aktivnosti u čiju se svrhu prikupljaju podaci, kao što je povijest transakcija ili zapisnik o pristupu. Trebalo bi se smatrati da je podatke koji se prikupljaju praćenjem i bilježenjem ispitanika (na primjer s pomoću aplikacije koja bilježi otkucaje srca ili tehnologije koja prati ponašanje pri pregledavanju) „pružio ispitanik" čak i ako se podaci ne prenose aktivno ili svjesno.

[22] U uvodnoj izjavi 68. navedeno je da „ako se određeni skup osobnih podataka odnosi na više ispitanika, pravo na primanje tih osobnih podataka ne bi smjelo dovoditi u pitanje prava i sloboda ostalih ispitanika u skladu s ovom Uredbom".

Slično tomu, bankovni račun ispitanika može sadržavati osobne podatke koji se odnose na transakcije ispitanika, ali i drugih pojedinaca (npr. ako su poslali novac vlasniku računa). Nije vjerojatno da će prijenos informacija o bankovnom računu vlasniku računa nakon zaprimanja zahtjeva za prenosivost negativno utjecati na prava i slobode tih trećih osoba, pod uvjetom da se u oba slučaja podaci upotrebljavaju u istu svrhu (npr. adresa za kontakt koju upotrebljava samo ispitanik ili povijest bankovnog računa ispitanika).

S druge strane, prava i slobode trećih osoba neće se poštovati ako novi voditelj podataka upotrebljava osobne podatke za druge svrhe, na primjer ako voditelj obrade koji prima podatke upotrebljava osobne podatke drugih pojedinaca uključenih u imenik s kontaktima ispitanika u svrhu marketinga.

Stoga, kako bi se spriječili štetni utjecaji na uključene treće osobe, obrada tih osobnih podataka koju provodi neki drugi voditelj obrade dopuštena je samo ako se podaci čuvaju pod isključivom kontrolom korisnika koji ih je zatražio i ako se njima upravlja isključivo u okviru osobne ili kućne aktivnosti. „Novi" voditelj obrade koji prima podatke (kojem se podaci mogu prenijeti na zahtjev korisnika) ne smije upotrebljavati prenesene podatke o trećoj osobi za vlastite potrebe, npr. za promidžbu proizvoda i usluga tim ispitanicima - trećim osobama. Na primjer, te informacije ne bi trebalo upotrebljavati kako bi se upotpunio profil ispitanika - treće osobe i rekonstruiralo njegovo društveno okruženje bez njegova znanja i suglasnosti[23]. Ne može ih se upotrijebiti ni za pronalaženje informacija o tim trećim osobama i stvaranje posebnih profila, čak ni ako voditelj obrade već posjeduje njihove osobne podatke. U suprotnom bi takva obrada vjerojatno bila nezakonita i nepoštena, posebno ako se ne obavijesti dotične treće osobe te one ne mogu ostvariti prava koja imaju kao ispitanici.

Nadalje, učestala je praksa svih voditelja obrade (strana koje „šalju" i onih koje „primaju") upotrebljavati alate kako bi omogućili ispitanicima da odaberu relevantne podatke koje žele primiti i prenijeti te isključe podatke o drugim pojedincima, kad je to relevantno. Time će se dodatno pridonijeti smanjenju rizika za treće osobe čiji bi se osobni podaci mogli prenijeti.

Uz to, voditelji obrade trebali bi upotrebljavati mehanizme suglasnosti za druge uključene ispitanike kako bi olakšali prijenos podataka u slučajevima u kojima su te strane voljne dati suglasnost, na primjer ako i one žele prenijeti svoje podatke nekom drugom voditelju obrade. Do toga bi moglo doći, na primjer, u slučaju društvenih mreža, ali voditelji obrade ti su koji odlučuju o tome koju će praksu slijediti.

U pogledu podataka obuhvaćenih intelektualnim vlasništvom i poslovnim tajnama
Prava i slobode drugih navedeni su u članku 20. stavku 4. Iako to nije izravno povezano s prenosivošću, može se smatrati da „[uključuje] i poslovne tajne ili intelektualno vlasništvo, a osobito autorsko pravo kojima je zaštićen računalni program". Međutim, iako bi ta prava trebalo razmotriti prije odgovaranja na zahtjev za prenosivost podataka, „rezultat tih razmatranja ipak ne bi smjelo biti odbijanje pružanja svih informacija ispitaniku". Nadalje, voditelj obrade ne bi trebao odbiti zahtjev za prenosivost podataka na temelju kršenja nekog drugog ugovornog prava (na primjer, nepodmireni dug ili trgovinski spor s ispitanikom).

[23] Usluge društvenog umrežavanja ne bi trebale upotpunjivati profile svojih korisnika upotrebom osobnih podataka koje ispitanik prenosi u okviru svojeg prava na prenosivost podataka bez poštovanja načela transparentnosti i osiguravajući da se oslanjaju na odgovarajuću pravnu osnovu za tu konkretnu obradu.

Pravo na prenosivost podataka nije pravo pojedinca na zlouporabu informacija na način koji bi se mogao smatrati nepoštenom praksom ili koji bi bio kršenje prava intelektualnog vlasništva.

Međutim, mogući poslovni rizik ne može sam po sebi biti temelj za odbijanje odgovaranja na zahtjev za prenosivost, a voditelji obrade mogu prenositi osobne podatke koje su pružili ispitanici u obliku kojim se ne otkrivaju informacije obuhvaćene poslovnom tajnom ili pravima intelektualnog vlasništva.

IV. Na koji se način opća pravila o ostvarivanju prava ispitanika primjenjuju na prenosivost podataka?

- **Koje bi prethodne informacije trebalo pružiti ispitaniku?**

Kako bi se poštovalo novo pravo na prenosivost podataka, voditelji obrade moraju obavijestiti ispitanike o tome da postoji novo pravo na prenosivost. Ako se predmetni osobni podaci prikupljaju izravno od ispitanika, ispitanike se mora obavijestiti „u trenutku prikupljanja osobnih podataka". Ako osobni podaci nisu dobiveni od ispitanika, voditelj obrade mora pružiti informacije koje se zahtijeva člankom 13. stavkom 2. točkom (b) i člankom 14. stavkom 2. točkom (c).

„Ako osobni podaci nisu dobiveni od ispitanika", u skladu s člankom 14. stavkom 3. informacije se moraju pružiti u razumnom roku od najviše jednog mjeseca nakon prikupljanja podataka, tijekom prvog komuniciranja s ispitanikom ili nakon njihova otkrivanja trećim stranama[24].

Pri pružanju zatraženih informacija voditelji obrade moraju osigurati da razlikuju pravo na prenosivost podataka od drugih prava. Stoga radna skupina iz članka 29. posebno preporučuje da voditelji obrade jasno objasne razliku između vrsta podataka koje ispitanik može primiti na temelju prava na pristup ispitanika i prava na prenosivost podataka.

Osim toga, radna skupina preporučuje voditeljima obrade da uvijek navedu informaciju o pravu na prenosivost podataka prije nego što ispitanici zatvore bilo koji od svojih računa. Time se korisnicima omogućuje da vode računa o svojim osobnim podacima i da jednostavno prenesu podatke na vlastiti uređaj ili drugom pružatelju prije prekida ugovora.

Konačno, kao jednu od glavnih praksi za voditelje obrade koji „primaju" podatke, radna skupina iz članka 29. preporučuje da se ispitanicima pružaju potpune informacije o vrsti osobnih podataka relevantnih za izvršavanje njihovih usluga. Osim što se time podupire poštena obrada, korisnicima se omogućuje i da ograniče rizike za treće osobe, ali i nepotrebno udvostručivanje osobnih podataka čak i kad nisu uključeni drugi ispitanici.

- **Kako voditelj obrade podataka može identificirati ispitanika prije nego što odgovori na njegov zahtjev?**

U Općoj uredbi o zaštiti podataka nema posebnih zahtjeva u pogledu autentifikacije ispitanika. Ipak, u članku 12. stavku 2. Opće uredbe o zaštiti podataka navedeno je da voditelj

[24] Člankom 12. zahtijeva se od voditeljâ obrade da pruže „sve komunikacije [...] u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu".

obrade ne smije odbiti postupiti po zahtjevu ispitanika u svrhu ostvarivanja njegovih prava (uključujući pravo na prenosivost podataka), osim ako je riječ o obradi osobnih podataka u svrhu za koju nije potrebno identificirati ispitanika i može se dokazati da nije moguće identificirati ispitanika. Međutim, u skladu s člankom 11. stavkom 2. u tim slučajevima ispitanik može pružiti dodatne informacije koje omogućuju njegovu identifikaciju. Osim toga, u članku 12. stavku 6. navodi se da, ako voditelj obrade opravdano sumnja u identitet ispitanika, može zatražiti pružanje dodatnih informacija za potvrđivanje identiteta ispitanika. Ako ispitanik pruži dodatne informacije koje omogućuju njegovu identifikaciju, voditelj obrade ne smije odbiti postupiti po zahtjevu. Ako su informacije i podaci koji su prikupljeni na internetu povezani sa pseudonimima ili jedinstvenim identifikatorima, voditelji obrade mogu provesti odgovarajuće postupke kojima se pojedincu omogućuje da podnese zahtjev za prenosivost podataka i primi podatke koji se na njega odnose. Voditelji obrade u svakom slučaju moraju provesti postupak provjere autentičnosti kako bi jasno utvrdili identitet ispitanika koji traži svoje osobne podatke ili općenito izvršava svoja prava u okviru Opće uredbe o zaštiti podataka.

Ti su postupci često već uspostavljeni. Voditelj obrade najčešće je već autentificirao ispitanike prije sklapanja ugovora ili dobivanja njihove suglasnosti za obradu. Zbog toga se osobni podaci koji se upotrebljavaju za registraciju pojedinca na kojeg se obrada odnosi isto tako mogu upotrijebiti kao dokaz za autentifikaciju ispitanika u svrhu prenosivosti[25].

Iako će u tim slučajevima za prethodnu identifikaciju ispitanika možda biti potreban zahtjev za dokazivanje njihova pravnog identiteta, takva provjera možda neće biti relevantna za procjenu poveznice između podataka i dotičnog pojedinca jer takva poveznica nije povezana sa službenim ili pravnim identitetom. Mogućnost voditelja obrade da zatraži dodatne informacije radi procjene identiteta pojedinca u osnovi ne smije dovesti do prekomjernih zahtjeva i do prikupljanja osobnih podataka koji nisu relevantni ili potrebni za jačanje poveznice između pojedinca i zatraženih osobnih podataka.

U brojnim su slučajevima već uspostavljeni takvi postupci autentifikacije. Na primjer, korisnička imena i lozinke često se upotrebljavaju kako bi se pojedincima omogućilo da pristupe svojim podacima na računima e-pošte, društvenim mrežama te računima kojima se služe za različite druge usluge, pri čemu određeni pojedinci odlučuju te usluge upotrebljavati bez otkrivanja svojeg punog imena i identiteta.

Ako zbog veličine podataka koju zatraži ispitanik prijenos internetom bude problematičan, umjesto mogućeg dopuštanja produljenja roka na najviše tri mjeseca radi ispunjavanja zahtjeva[26], voditelj obrade možda će morati razmotriti i alternativne načine pružanja podataka, kao što su reprodukcija ili pohrana na CD-u, DVD-u ili nekom drugom fizičkom mediju, ili omogućiti izravan prijenos osobnih podataka drugom voditelju obrade (u skladu s člankom 20. stavkom 2. Opće uredbe o zaštiti podataka, ako je to tehnički izvedivo).

- **Koji je rok za odgovor na zahtjev za prenosivost?**

Člankom 12. stavkom 3. zahtijeva se da voditelj obrade pruži „informacije o poduzetim radnjama” ispitaniku „bez nepotrebnog odgađanja”, a u svakom slučaju „u roku od mjesec

[25] Na primjer, ako je obrada podataka povezana s korisničkim računom, relevantno korisničko ime i lozinka mogli bi biti dovoljni za identifikaciju ispitanika.
[26] Članak 12. stavak 3.: „Voditelj obrade ispitaniku na zahtjev pruža informacije o poduzetim radnjama”.

dana od zaprimanja zahtjeva". To se razdoblje od jednog mjeseca može produljiti na najviše tri mjeseca kad je riječ o složenim slučajevima, pod uvjetom da je ispitanik obaviješten o razlozima tog odgađanja u roku od jednog mjeseca od izvornog zahtjeva.

Voditelji podataka koji upravljaju uslugama informacijskog društva vjerojatno će biti bolje opremljeni za ispunjavanje zahtjeva u vrlo kratkom roku. Kako bi se ispunila očekivanja korisnikâ, dobra je praksa definirati rok u kojem se obično može odgovoriti na zahtjev za prenosivost podataka te o tom roku obavijestiti ispitanike.

Voditelj obrade koji odbije odgovoriti na zahtjev za prenosivost u skladu s člankom 12. stavkom 4. u roku od najviše jednog mjeseca od zaprimanja zahtjeva obavješćuje ispitanika o „razlozima zbog kojih nije postupio i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženja pravnog lijeka".

Voditelji obrade moraju poštovati obvezu odgovora u zadanom roku, čak i ako je riječ o odbijanju. Drugim riječima, voditelj obrade obvezan je odgovoriti kad se od njega zatraži odgovor na zahtjev za prenosivost podataka.

- **U kojim se slučajevima može odbiti zahtjev za prenosivost podataka ili naplatiti naknada?**

Člankom 12. voditelju obrade zabranjuje se da naplati naknadu za pružanje osobnih podataka, osim ako voditelj obrade može dokazati da su zahtjevi očito neutemeljeni ili pretjerani, „*osobito zbog njihova učestalog ponavljanja*". Kad je riječ o uslugama informacijskog društva specijaliziranih za automatiziranu obradu osobnih podataka, uvođenjem automatiziranih sustava, kao što su sučelja za programiranje aplikacija[27], mogu se olakšati razmjene s ispitanikom te tako smanjiti moguće opterećenje koje proizlazi iz zahtjeva koji se ponavljaju. Stoga bi trebalo biti vrlo malo slučajeva u kojima bi voditelj obrade bio u mogućnosti opravdati odbijanje pružanja zatraženih informacija, čak i kad je riječ o višestrukim zahtjevima za prenosivost podataka.

Osim toga, sveukupan trošak postupaka uspostavljenih radi odgovora na zahtjeve za prenosivost ne bi trebalo uzimati u obzir pri utvrđivanju je li određeni zahtjev prekomjeran. U članku 12. Opće uredbe o zaštiti podataka naglasak je stavljen na zahtjeve koje je podnio jedan ispitanik, a ne na ukupan broj zahtjeva koje je zaprimio voditelj obrade. Zbog toga sveukupne troškove provedbe sustava ne bi trebalo naplatiti ispitanicima niti bi ih trebalo upotrijebiti kao opravdanje za odbijanje odgovora na zahtjeve za prenosivost.

V. <u>Na koji se način moraju dostavljati prenosivi podaci?</u>

- **<u>Koja su očekivana sredstva kojima bi se voditelj obrade trebao služiti za pružanje podataka?</u>**

U članku 20. stavku 1. Opće uredbe o zaštiti podataka navedeno je da ispitanici imaju pravo bez ometanja prenositi podatke drugom voditelju obrade od voditelja obrade kojem su pruženi osobni podaci.

[27] Sučelje za programiranje aplikacija jest sučelje za aplikacije ili internetske usluge koje voditelji podataka stavljaju na raspolaganje kako bi se drugi sustavi ili aplikacije mogli povezati i funkcionirati s njihovim sustavima.

Ometanjem se može smatrati svaka pravna, tehnička ili financijska prepreka kojom se posluži voditelj obrade kako bi zaustavio ili usporio pristup, prijenos ili ponovnu upotrebu podataka ispitanika ili drugog voditelja obrade. Na primjer, takvim bi se ometanjem mogle smatrati naknade koje se traže za dostavu podataka, nedostatak interoperabilnosti ili pristupa određenom formatu podataka, sučelju za programiranje aplikacija ili pruženom formatu, prekomjerno odgađanje ili složeni postupak pronalaženja cjelokupnog skupa podataka, namjerno skrivanje skupa podataka ili posebni i neprimjereni ili prekomjerni sektorski zahtjevi u pogledu normizacije ili akreditacije[28].

Člankom 20. stavkom 2. uvode se i obveze za voditelje obrade u pogledu izravnog prijenosa prenosivih podataka drugom voditelju obrade „ako je to tehnički izvedivo".

Tehnička izvedivost prijenosa od jednog voditelja obrade drugom, pod kontrolom ispitanika, trebala bi se procjenjivati za svaki pojedinačni slučaj. U uvodnoj izjavi 68. dodatno su pojašnjene granice onoga što je „tehnički izvedivo" i navodi se da se time „ne bi trebalo obvezivati voditelja obrade da upotrebljava ili održava tehnički kompatibilne sustave za obradu".

Od voditelja obrade očekuje se da prenose osobne podatke u interoperabilnom formatu, iako se time ne nameće obveza drugim voditeljima podataka da podrže te formate. Izravni prijenos od jednog voditelja obrade drugom stoga bi se mogao izvršiti kad je na siguran način[29] omogućena komunikacija između dvaju sustava i ako je sustav koji prima podatke tehnički sposoban primiti te ulazne podatke. Ako je izravni prijenos onemogućen zbog tehničkih prepreka, voditelj podataka objašnjava te prepreke ispitanicima jer će u suprotnome njegova odluka imati učinke slične odbijanju poduzimanja radnji u pogledu zahtjeva ispitanika (članak 12. stavak 4.).

Voditelji obrade na tehničkoj bi razini trebali istražiti i procijeniti dva različita i komplementarna načina na koje se prenosivi podaci mogu staviti na raspolaganje ispitanicima ili drugim voditeljima obrade:

- izravan prijenos sveukupnog skupa prenosivih podataka (ili nekoliko izvadaka ili dijelova ukupnog skupa podataka),
- automatizirani alat koji omogućuje izdvajanje relevantnih podataka.

Voditelji podataka možda su skloniji drugom načinu kad je riječ o slučajevima koji uključuju složene i velike skupove podataka, jer on omogućuje izdvajanje bilo kojeg dijela skupa podataka koji je relevantan ispitaniku u kontekstu njegova zahtjeva, čime se pridonosi svođenju rizika na najnižu razinu, a možda se i omogućuje upotreba mehanizama za sinkronizaciju podataka[30] (na primjer u kontekstu redovite komunikacije između voditeljâ obrade). To bi mogao biti bolji način za osiguravanje usklađenosti „novog" voditelja obrade i smatralo bi ga se dobrom praksom početnog voditelja obrade za smanjenje rizika u pogledu privatnosti.

[28] Moglo bi doći do određenih legitimnih prepreka, kao što su one povezane s pravima i slobodama drugih navedene u članku 20. stavku 4. ili one povezane sa zaštitom vlastitih sustava voditeljâ obrade. Voditelj obrade odgovoran je obrazložiti zašto bi te prepreke mogle biti legitimne i zašto ih se ne smatra ometanjem u smislu članka 20. stavka 1.

[29] Na temelju autentificirane komunikacije uz potrebnu razinu enkripcije podataka.

[30] Mehanizmom sinkronizacije može se pridonijeti postizanju općenitih ciljeva u okviru članka 5. Opće uredbe o zaštiti podataka u kojem je navedeno da „osobni podaci moraju biti (...) točni i prema potrebi ažurni".

Ta dva različita i možda komplementarna načina pružanja relevantnih prenosivih podataka mogu se provesti tako da se podaci stave na raspolaganje s pomoću različitih sredstava, na primjer sigurnih poruka, SFTP poslužitelja, sigurnog internetskog sučelja za programiranje aplikacija ili internetskog portala. Ispitanicima bi trebalo omogućiti da se služe osobnom pohranom podataka, sustavom za upravljanje osobnim informacijama[31] ili drugim vrstama pouzdanih trećih strana radi čuvanja i pohranjivanja osobnih podataka i dopuštanja voditeljima obrade da pristupe potrebnim osobnim podacima i obrađuju ih.

- **Koji je očekivani format podataka?**

Općom uredbom o zaštiti podataka uvode se zahtjevi za voditelje obrade u pogledu pružanja osobnih podataka koje pojedinci zatraže u formatu u kojem ih je moguće ponovno upotrebljavati. Konkretno, u članku 20. stavku 1. Opće uredbe o zaštiti podataka navedeno je da se osobni podaci moraju pružati „u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu". U uvodnoj izjavi 68. navedeno je dodatno pojašnjenje u skladu s kojim bi taj format trebao biti interoperabilan, što je pojam definiran[32] u EU-u kao:

> *sposobnost interakcije disparitetnih i raznovrsnih organizacija na obostrano korisnim i dogovorenim zajedničkim ciljevima, uključujući razmjenu informacija i znanja između organizacija, putem poslovnih procesa koje podržavaju, razmjenjujući podatke između svojih sustava IKT-a.*

Pojmovi „strukturiran", „uobičajen" i „strojno čitljiv" čine minimalne zahtjeve koji bi trebali omogućiti interoperabilnost formata podataka koje pruža voditelj obrade. Tako „strukturirani, uobičajeno upotrebljavan i strojno čitljiv" postaju specifikacije sredstva, dok je interoperabilnost željeni rezultat.

U uvodnoj izjavi 21. Direktive 2013/37/EU[33,34] pojam „strojno čitljivo" definiran je kako slijedi:

> *oblik datoteke strukturirane tako da se programske aplikacije mogu lako identificirati, prepoznati te iz nje izvaditi specifične podatke, uključujući pojedinačne obavijesti i njihovu unutarnju strukturu. Podaci kodirani u datotekama koje su u strojno čitljivom obliku jesu strojno čitljivi podaci. Strojno čitljivi oblici mogu biti otvoreni ili zaštićeni; u formalnom standardu ili ne. Za dokumente kodirane u obliku datoteke koja ograničava automatsku obradu, budući da se podaci ne mogu ili ne mogu lako iz nje izvaditi, ne bi se trebalo smatrati da su u strojno čitljivom obliku. Države članice prema potrebi bi trebale poticati uporabu otvorenih, strojno čitljivih oblika.*

Imajući na umu velik raspon mogućih vrsta podataka koje bi mogao obrađivati voditelj obrade, u Općoj uredbi o zaštiti podatka ne navode se konkretne preporuke u pogledu formata

[31] Za više informacija o sustavima za upravljanje osobnim informacijama (PIMS) vidjeti, na primjer, Mišljenje 9/2016 Europskog nadzornika za zaštitu podataka, dostupno na https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

[32] Članak 2. Odluke br. 922/2009/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o interoperabilnim rješenjima za europske javne uprave (ISA) (SL L 260, 3.10.2009., str. 20.).

[33] O izmjeni Direktive 2003/98/EZ o ponovnoj uporabi informacija javnog sektora.

[34] U glosaru EU-a (http://eur-lex.europa.eu/eli-register/glossary.html) navedena su dodatna objašnjenja o očekivanjima povezanima s konceptima upotrijebljenima u ovim smjernicama, kao što su *strojno čitljiv, interoperabilnost, otvoreni format, standard, metapodaci*.

osobnih podataka koje je potrebno pružiti. Najprikladniji formati razlikovat će se od sektora do sektora i moguće je da već postoje prikladni formati, ali format bi uvijek trebalo birati tako da se osigura mogućnost njegova tumačenja i ispitaniku omogući visok stupanj prenosivosti podataka. Zbog toga se formate koji podliježu ograničenjima zbog skupog licenciranja ne bi smatralo prikladnim pristupom.

U uvodnoj izjavi 68. pojašnjeno je da „*pravo ispitanika na prijenos ili primanje osobnih podataka koji se odnose na njega ne bi trebalo obvezivati voditelja obrade da upotrebljava ili održava tehnički kompatibilne sustave za obradu.*" **Stoga se prenosivošću nastoje izraditi interoperabilni sustavi, a ne kompatibilni sustavi**[35].

Osobne podatke trebalo bi pružati u formatima s visokom razinom poopćivanja u odnosu na bilo koji interni ili zaštićeni format. Prenosivost podataka kao takva podrazumijeva dodatni sloj obrade podataka koju provode voditelji obrade radi izdvajanja podataka iz platforme i filtriranja osobnih podataka izvan područja primjene prenosivosti, kao što su podaci koji se zaključuju i podaci povezani sa sigurnošću sustavâ. Time se voditelje obrade potiče da unaprijed utvrde koji su podaci obuhvaćeni područjem primjene prenosivosti u njihovim sustavima. Tu će se dodatnu obradu podataka smatrati pomoćnom radnjom uz obradu glavnih podataka jer se ne provodi radi ostvarivanja nove svrhe koju je definirao voditelj obrade.

Ako u određenoj industriji ili određenom kontekstu nema uobičajenih formata, **voditelji obrade trebali bi pružati osobne podatke s pomoću uobičajenih otvorenih formata (npr. XML, JSON, CSV…) zajedno s** korisnim **metapodacima na najvišoj mogućoj razini detalja,** istodobno održavajući visoku razinu apstrakcije. Stoga bi trebalo upotrebljavati odgovarajuće metapodatke kako bi se točno opisalo značenje razmijenjenih informacija. Ti bi metapodaci trebali biti dostatni za omogućivanje funkcioniranja i ponovne upotrebe podataka, ali, naravno, bez otkrivanja poslovnih tajni. Stoga pružanje inačice pretinca ulaznih poruka e-pošte ispitaniku u formatu PDF vjerojatno ne bi bilo dovoljno strukturirano ili deskriptivno da bi se omogućila jednostavna ponovna upotreba podataka iz pretinca ulazne pošte. Umjesto toga, podatke o porukama e-pošte trebalo bi pružati u formatu koji zadržava sve metapodatke kako bi se omogućila učinkovita ponovna upotreba podataka. Stoga bi pri odabiru formata podataka u kojem će se pružati osobni podaci voditelj obrade trebao razmotriti na koji bi način taj format utjecao na pravo pojedinca da ponovno upotrebljava te podatke ili narušio to pravo. Ako voditelj obrade može ispitaniku omogućiti odabir u pogledu željenog formata osobnih podataka, trebalo bi navesti detaljno objašnjenje utjecaja tog odabira. Međutim, obrada dodatnih metapodataka isključivo jer bi mogli biti potrebni ili zatraženi radi odgovora na zahtjev za prenosivost podataka nije legitimna osnova za takvu obradu.

Radna skupina iz članka 29. snažno potiče suradnju dionika iz industrije i trgovinskih udruženja u izradi zajedničkih interoperabilnih standarda i formata kako bi se postigli ciljevi prava na prenosivost podataka. S tim je izazovom bio suočen i Europski okvir interoperabilnosti koji je donio usuglašeni pristup interoperabilnosti za organizacije koje žele zajedno pružati javne usluge. U području primjene tog okvira nalazi se niz zajedničkih elemenata kao što su rječnik, koncepti, načela, politike, smjernice, preporuke, norme, specifikacije i prakse[36].

[35] U normi ISO/IEC 2382-01 interoperabilnost je definirana kako slijedi: „Mogućnost komunikacije, izvršavanja programâ ili prijenosa podataka među različitim funkcionalnim jedinicama na način kojim se od korisnika zahtijeva vrlo malo ili čak nimalo znanja o jedinstvenim svojstvima tih jedinica."

[36] Izvor: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

- **Kako postupati s opsežnim ili složenim prikupljanjem osobnih podataka?**

U Općoj uredbi o zaštiti podataka nije objašnjeno kako riješiti pitanje odgovora u slučaju opsežnog prikupljanja podataka, složene strukture podataka ili drugih tehničkih pitanja koji bi mogli stvoriti poteškoće za voditelje obrade ili ispitanike.

Međutim, u svakom je slučaju najvažnije da pojedinac bude u položaju u kojem može u potpunosti shvatiti definiciju, raspored i strukturu osobnih podataka koje bi mogao pružiti voditelj obrade. Na primjer, podatke bi se prvo moglo pružiti u sažetom obliku s pomoću nadzornih ploča (eng. *dashboard*) čime se ispitaniku omogućuje da prenese podskupove osobnih podataka, a ne sve podatke. Voditelj obrade trebao bi pružiti pregled „u sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika" (vidjeti članak 12. stavak 1. Opće uredbe o zaštiti podataka) tako da se ispitanika uvijek jasno obavijesti o tome koje podatke treba preuzeti ili prenijeti drugom voditelju obrade u vezi s određenom svrhom. Na primjer, ispitanici bi trebali moći upotrebljavati programske aplikacije za jednostavno utvrđivanje, prepoznavanje i obradu određenih podataka iz tog pregleda.

Kako je prethodno navedeno, praktični način na koji voditelj obrade može odgovoriti na zahtjeve za prenosivost podataka može biti ponuda pravilno zaštićenih i dokumentiranih sučelja za programiranje aplikacija. Time bi se moglo pojedincima omogućiti da od voditelja obrade zatraže svoje osobne podatke s pomoću vlastitih programa ili programa trećih strana ili dopustiti drugima da to čine u njihovo ime (uključujući drugog voditelja obrade) kako je navedeno u članku 20. stavku 2. Opće uredbe o zaštiti podataka. Davanjem pristupa podacima s pomoću sučelja za programiranje aplikacija kojem se može pristupiti izvana mogao bi se omogućiti napredniji sustav pristupa koji omogućuje pojedincima da podnose naknadne zahtjeve za podatke, u obliku potpunog preuzimanja ili u obliku delta funkcije koja sadržava samo promjene u odnosu na prethodno preuzimanje, bez opterećivanja voditelja obrade tim dodatnim zahtjevima.

- **Kako se prenosivi podaci mogu zaštititi?**

Općenito, voditelji obrade trebali bi zajamčiti „odgovarajuću sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja, primjenom odgovarajućih tehničkih ili organizacijskih mjera" u skladu s člankom 5. stavkom 1. točkom (f) Opće uredbe o zaštiti podataka.

Međutim, prijenos osobnih podataka ispitaniku može dovesti i do određenih pitanja u pogledu sigurnosti.

<u>Kako voditelji obrade mogu osigurati da se osobni podaci na siguran način dostavljaju pravoj osobi?</u>

Budući da je cilj prenosivosti podataka dobivanje osobnih podataka iz informacijskog sustava voditelja obrade, prijenos može postati mogući izvor rizika kad je riječ o tim podacima (posebno dođe li do povrede podataka tijekom prijenosa). Voditelj obrade odgovoran je za poduzimanje svih zaštitnih mjera potrebnih da bi se zajamčio ne samo siguran prijenos podataka (upotrebom potpune enkripcije ili enkripcije podataka) do odgovarajućeg odredišta (primjenom strogih mjera autentifikacije), nego i nastavak zaštite osobnih podataka koji ostaju u njegovu sustavu kao i transparentnih postupaka za rješavanje mogućih povreda

podataka[37]. Stoga bi voditelji obrade trebali procijeniti konkretne rizike povezane s prenosivošću podataka i poduzeti odgovarajuće mjere za ublažavanje rizika.

Te mjere za ublažavanje rizika mogu biti sljedeće: ako je već potrebno autentificirati ispitanika, upotreba dodatnih informacija za autentifikaciju kao što su zajednička tajna (eng. *shared secret*) ili neki drugi način autentifikacije kao što je jednokratna lozinka, zaustavljanje ili blokiranje transakcije ako postoji sumnja da je račun kompromitiran. U slučajevima izravnog prijenosa od voditelja obrade drugom voditelju obrade trebalo bi upotrebljavati autentifikaciju uz naredbu kao što je autentifikacija na temelju tokena.

Te zaštitne mjere ne smiju biti ometajuće i ne smiju sprečavati korisnike u ostvarivanju vlastitih prava, na primjer uvođenjem dodatnih troškova.

Kako pomoći korisnicima da zaštite pohranjene osobne podatke u vlastitim sustavima?

Preuzimaju li korisnici svoje osobne podatke iz internetske usluge, uvijek postoji rizik da bi ih mogli pohraniti u sustavima koji su manje zaštićeni od onih koje nudi usluga. Ispitanik koji traži podatke odgovoran je za utvrđivanje pravih mjera za zaštitu osobnih podataka u vlastitom sustavu. Međutim, trebalo bi ga o tome obavijestiti kako bi mogao poduzeti korake za zaštitu informacija koje je primio. Još je jedna od glavnih praksi ta da voditelji obrade preporuče odgovarajući format (ili više njih), alate za enkripciju i druge zaštitne mjere kojima se ispitaniku pomaže da postigne svoj cilj.

* * *

Sastavljeno u Bruxellesu 13. prosinca 2016.

Za Radnu skupinu
Predsjednica
Isabelle FALQUE-PIERROTIN

Kako je revidirano i doneseno 5. travnja 2017.

Za Radnu skupinu
Predsjednica
Isabelle FALQUE-PIERROTIN

[37] U skladu s Direktivom (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.