



**Suunised andmete ülekandmise õiguse kohta**

**Vastu võetud 13. detsembril 2016  
Viimati läbi vaadatud ja vastu võetud 5. aprillil 2017**

Töörühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Tegemist on Euroopa sõltumatu nõuandeorganiga andmekaitse ja eraelu puutumatuse küsimustes. Töörühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaaditeenused tagab Euroopa Komisjoni õigus- ja tarbijaküsimuste peadirektoraadi direktoraat C (põhiõigused ja õigusriigi põhimõte), B-1049 Brüssel, Belgia, kabinet nr MO59 05/35.

Veebisait: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm).

## SISUKORD

<b>Kommenteeritud kokkuvõte.....</b>	<b>3</b>
<b>I. Sissejuhatus .....</b>	<b>3</b>
<b>II. Millised on andmete ülekantavuse põhielemendid? .....</b>	<b>4</b>
<b>III. Millal andmete ülekantavust kohaldatakse? .....</b>	<b>8</b>
<b>IV. Kuidas kohaldatakse andmete ülekantavuse suhtes andmesubjektide õigusi reguleerivaid üldeeskirju? .....</b>	<b>13</b>
<b>V. Kuidas tuleb ülekantavad andmed esitada?.....</b>	<b>15</b>

## **Kommenteeritud kokkuvõte**

Isikuandmete kaitse üldmääruse artikliga 20 luuakse uus andmete ülekandmise õigus, mis on tihedalt seotud õigusega tutvuda andmetega, ent erineb sellest mitmel viisil. See võimaldab andmesubjektidel saada isikuandmeid, mille nad on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ja masinloetaval kujul ning edastada need andmed teisele vastutavale töötlejale. Selle uue õiguse eesmärk on suurendada andmesubjekti mõjuvõimu ja anda talle suurem kontroll teda käsitlevate isikuandmete üle.

Kuna andmete ülekandmise õigus võimaldab edastada isikuandmeid otse ühelt vastutavalt töötlejalt teisele, on see ka oluline vahend, mis toetab isikuandmete vaba liikumist ELis ja soodustab vastutavate töötlejate vahelist konkurentsi. See hõlbustab teenuseosutaja vahetamist ja edendab seega uute teenuste väljatöötamist digitaalse ühtse turu strateegia kontekstis.

Käesolevas arvamuses esitatakse suunised selle kohta, kuidas isikuandmete kaitse üldmäärusega kehtestatud andmete ülekandmise õigust tõlgendada ja rakendada. Arvamuse eesmärk on arutada andmete ülekandmise õigust ja selle kohaldamisala. Selles on selgitatud tingimusi, mille korral seda uut õigust kohaldatakse, võttes arvesse andmete töötlemise õiguslikku alust (andmesubjekti nõusolek või vajadus täita lepingut) ja asjaolu, et see õigus piirdub andmesubjekti esitatud isikuandmetega. Ühtlasi sisaldab arvamus konkreetseid näiteid ja kriteeriume, et selgitada olukordi, kus seda õigust kohaldatakse. Sellega seoses on artikli 29 töörihm seisukohal, et andmete ülekandmise õigus hõlmab nii andmeid, mille andmesubjekt on teadlikult ja aktiivselt esitanud, kui ka tema tegevuse tulemusel loodud isikuandmeid. Seda uut õigust ei saa kahjustada ning seda ei saa piirata isikuandmetega, mille andmesubjekt on näiteks elektroonilisel vormil otse esitanud.

Hea tavana peaksid vastutavad töötlejad hakkama välja töötama vahendeid, näiteks allalaadimistööriistu ja rakendusliideseid, mis aitaksid andmete ülekandmise taotlustele vastata. Nad peaksid kindlustama, et isikuandmed edastatakse struktureeritud, üldkasutatavas vormingus ja masinloetaval kujul, ning neid tuleks julgustada tagama andmete ülekandmise taotluse täitmisel esitatud andmete vormingu koostalitlusvõimet.

Arvamus aitab vastutavatel töötlejatel ka selgelt mõista oma vastavaid kohustusi ning selles esitatakse soovitusel parimate tavade ja tööriistade kohta, mis toetavad andmete ülekandmise õiguse täitmist. Samuti soovitatakse arvamuses tööstusharu sidusrühmadel ja kutseorganisatsioonidel töötada üheskoos välja ühised koostalitlevad standardid ja vormingud andmete ülekandmise õigusega seotud nõuete täitmiseks.

## **I. Sissejuhatus**

Isikuandmete kaitse üldmääruse artikliga 20 kehtestatakse uus andmete ülekandmise õigus. See õigus võimaldab andmesubjektidel saada takistusteta isikuandmeid, mille nad on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ja masinloetaval kujul, ning edastada need andmed teisele vastutavale töötlejale. See õigus, mida kohaldatakse teatavatel tingimustel, toetab kasutajate valikuvõimalusi, kasutajate kontrolli ja kasutajate mõjuvõimu suurendamist.

Üksikisikuid, kes kasutasid oma õigust andmetega tutvuda andmekaitse direktiivi 95/46/EÜ alusel, piiras vorming, mille vastutav töötaja taotletud teabe edastamiseks valis. **Uue andmete ülekandmise õiguse eesmärk on suurendada andmesubjektide mõjuvõimu seoses oma isikuandmetega. See parandab nende suutlikkust isikuandmeid hõlpsalt liigutada, kopeerida või ühest IT-keskkonnast teise üle kanda** (olgu selleks siis nende enda süsteemid, usaldusväärsete kolmandate isikute süsteemid või uute vastutavate töötajate süsteemid).

Kuna andmete ülekantavus toetab üksikisikute isiklike õigusi ja kontrolli neid käsitlevate isikuandmete üle, kujutab see endast ka võimalust tasakaalustada andmesubjektide ja vastutavate töötajate suhteid<sup>1</sup>.

Kuigi isikuandmete ülekantavuse õigus võib suurendada ka konkurentsi pakutavate teenuste vahel (hõlbustades teenuse vahetamist), reguleerib isikuandmete kaitse üldmäärus isikuandmeid, mitte konkurentsi. Eelkõige ei piirdu ülekantavad andmed artikli 20 kohaselt selliste andmetega, mis on vajalikud või kasulikud teenuse vahetamise seisukohast<sup>2</sup>.

Kuigi andmete ülekandmine on uus õigus, on muudes õigusvaldkondades (nt lepingute lõpetamise, sideteenuste rändluse ja teenuste piiriülese kättesaadavuse kontekstis<sup>3</sup>) teisi ülekantavuse liike juba käsitletud või arutatud. Ülekantavuse eri liikide vahel võib tekkida teatav koostoime ja need võivad tuua eeliseid üksikisikutele, kui nende pakkumisel kasutatakse kombineeritud lähenemisviisi. Sarnastesse teenustesse tuleks siiski suhtuda ettevaatusega.

Käesolevas arvamuses on esitatud suunised vastutavatele töötajatele, et nad saaksid ajakohastada oma tavasid, protsesse ja tegevuspõhimõtteid, ning selgitatud andmete ülekantavust, et andmesubjektidel oleks võimalik oma uut õigust tulemuslikult kasutada.

## **II. Millised on andmete ülekantavuse põhielemendid?**

Isikuandmete kaitse üldmääruse artikli 20 lõikes 1 on andmete ülekandmise õigus määratletud järgmiselt:

„Andmesubjektil on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötajale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötajale, ilma et vastutav töötaja, kellele kõnealused isikuandmed on esitatud, seda takistaks [...]“.

### **- Õigus saada isikuandmeid**

---

<sup>1</sup> Andmete ülekantavuse põhieesmärk on suurendada üksikisikute kontrolli oma isikuandmete üle ja veenduda, et neil on andmete ökosüsteemis aktiivne roll.

<sup>2</sup> Näiteks võib see õigus võimaldada pankadel pakkuda kasutaja kontrolli all lisateenuseid, kasutades algselt energiavarustusteenuse raames kogutud isikuandmeid.

<sup>3</sup> Vt Euroopa Komisjoni digitaalse ühtse turu tegevuskava aadressil <https://ec.europa.eu/digital-agenda/en/digital-single-market>, eelkõige esimene poliitikasammas „Parem elektrooniline juurdepääs digitaalsetele kaupadele ja teenustele“.

Esiteks on andmete ülekantavus **andmesubjekti õigus saada** teda käsitlevaid **isikuandmeid**, mida vastutav töötleja töötleb, ja säilitada neid andmeid edaspidiseks isiklikuks kasutamiseks. Säilitamine võib toimuda isiklikul seadmel või isiklikus pilves, ilma et andmeid tingimata teisele vastutavale töötlejale edastataks.

Selles osas täiendab andmete ülekantavus õigust tutvuda andmetega. Üks andmete ülekantavuse eripära on asjaolu, et see pakub andmesubjektidele lihtsa võimaluse isikuandmeid ise hallata ja taaskasutada. Kõnealused andmed tuleks saada „struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul“. Näiteks võib andmesubjekt soovida saada kätte oma praeguse esitusnimekirja (või kuulatud lugude ajaloo) muusika voogedastusteenusest, et teha kindlaks, mitu korda ta on teatavaid lugusid kuulanud või millist muusikat ta soovib osta või mõnel muul platvormil kuulata. Samuti võib ta soovida saada kätte kontaktide nimekirja oma veebimeili rakendusest, et koostada näiteks pulmakuulalist nimekiri või saada teavet ostude kohta, mille tegemisel kasutati erinevaid püsikliendikaarte, või määrata oma CO<sub>2</sub>-jalajälg<sup>4</sup>.

#### - **Õigus edastada andmeid ühelt vastutavalt töötlejalt teisele**

Teiseks on artikli 20 lõikes 1 sätestatud andmesubjekti **õigus edastada isikuandmeid ühelt vastutavalt töötlejalt teisele vastutavale töötlejale**, ilma et seda takistataks. Andmeid saab andmesubjekti taotluse korral ka ühelt vastutavalt töötlejalt otse teisele vastutavale töötlejale edastada, kui see on tehniliselt teostatav (artikli 20 lõige 2). Sellega seoses julgustatakse põhjenduses 68 vastutavaid töötlejaid arendama koostalitlevaid vorminguid, mis võimaldavad andmete ülekantavust,<sup>5</sup> kuid sellega ei tekitata vastutavatele töötlejatele kohustust võtta kasutusele või hoida töös tehniliselt ühilduvaid andmetöötlussüsteeme<sup>6</sup>. Isikuandmete kaitse üldmäärusega keelatakse aga vastutavatel töötlejatel luua edastamisele takistusi.

Põhimõtteliselt võimaldab see andmete ülekantavuse element andmesubjektidel esitatud andmeid mitte üksnes saada ja taaskasutada, vaid need ka teisele teenuseosutajale edastada (kas samas või mõnes muus ärivaldkonnas). Lisaks tarbijate mõjuvõimu suurendamisele andmete n-ö lukustamise vältimise teel soodustab andmete ülekandmise õigus eelduste kohaselt ka innovatsioonivõimalusi ning isikuandmete ohutut ja turvalist jagamist vastutavate töötlejate vahel nii, et andmesubjektil on selle üle kontroll<sup>7</sup>. Andmete ülekantavus võib soodustada seda, et kasutajad jagavad oma isikuandmeid organisatsioonide vahel kontrollitult ja piiratud, ning täiustada seeläbi teenuseid ja parandada klientide kogemusi<sup>8</sup>. Andmete ülekantavus võib hõlbustada kasutajaid käsitlevate isikuandmete edastamist ja taaskasutamist mitmesuguste teenuste vahel, mille vastu nad huvi tunnevad.

---

<sup>4</sup> Sellistel juhtudel võib andmete töötlemine andmesubjekti poolt kuuluda koduse tegevuse alla, kui andmesubjektil on kogu töötlemise üle ainukontroll, või sellega võib andmesubjekti nimel tegeleda mõni teine isik. Viimasel juhul tuleks asjaomast teist isikut käsitada vastutava töötlejana (isegi kui ainus eesmärk on isikuandmete säilitamine), kes peab järgima isikuandmete kaitse üldmääruses sätestatud põhimõtteid ja kohustusi.

<sup>5</sup> Vt ka V peatükk.

<sup>6</sup> Seega tuleks pöörata eritähelepanu edastatavate andmete vormingule tagamaks, et andmesubjektil või teisel vastutaval töötlejal on võimalik andmeid suurema pingutuseta taaskasutada. Vt ka V peatükk.

<sup>7</sup> Vt mitu eksperimentaalset rakendust Euroopas, näiteks [MiData](#) Ühendkuningriigis ja FINGi hallatav [MesInfos / SelfData](#) Prantsusmaal.

<sup>8</sup> Nn enesemõõtmise (*quantified self*) ja asjade interneti tööstusharud on näidanud, millised eelised (ja riskid) kaasnevad üksikisiku elu eri tahke, näiteks füüsilist vormi, aktiivsust ja kaloreid tarbimist käsitlevate isikuandmete ühendamise, et saada ühesainsas failis terviklikum pilt inimese elust.

## - Vastutus

Andmete ülekantavus tagab õiguse saada ja töödelda isikuandmeid vastavalt andmesubjekti soovile<sup>9</sup>.

Artiklis 20 sätestatud tingimuste kohaselt ei vastuta andmete ülekandmise taotlustele vastavad vastutavad töötlejad töötlemise eest, mida teeb andmesubjekt või mõni teine ettevõtja, kes isikuandmed vastu võtab. Nad tegutsevad andmesubjekti nimel, sealhulgas siis, kui isikuandmed edastatakse otse teisele vastutavale töötlejale. Sellega seoses ei vastuta vastutav töötleja selle eest, kas andmeid vastuvõttev vastutav töötleja täidab andmekaitsealaseid õigusakte, sest saatev vastutav töötleja ei vali andmete vastuvõtjat. Samal ajal peaksid vastutavad töötlejad kehtestama kaitsemeetmed selle tagamiseks, et nad tõepoolest tegutsevad andmesubjekti nimel. Näiteks saavad nad seada sisse menetlused, millega tagatakse, et edastatakse ka tegelikult sellist liiki isikuandmeid, mida andmesubjekt soovib edastada. Selleks võib hankida andmesubjekti kinnituse kas enne andmete edastamist või varem, töötlemiseks algse nõusoleku andmise või lepingu sõlmimise ajal.

Andmete ülekandmise taotlustele vastavatel vastutavatel töötlejal ei ole erikohustust kontrollida ja tõendada enne andmete edastamist nende kvaliteeti. Kooskõlas isikuandmete kaitse üldmääruse artikli 5 lõikes 1 sätestatud põhimõtetega peaksid need andmed loomulikult juba olema õiged ja ajakohased. Peale selle ei kaasne andmete ülekantavusega vastutavale töötlejale kohustust säilitada isikuandmeid võimalikust kindlaksmääratud säilitamisajast või vajalikust kauem<sup>10</sup>. Oluline on ka see, et ei ole mingit lisanõuet säilitada andmeid juba kohaldatavast säilitamisajast kauem lihtsalt selleks, et täita võimalikke tulevasi andmete ülekandmise taotlusi.

Kui vastutav töötleja taotletud isikuandmeid töötleb, peab isikuandmete kaitse üldmääruse artikli 28 kohaselt sõlmitud leping sisaldama kohustust aidata „vastutaval töötlejal asjakohaste tehniliste ja korralduslike meetmete abil [...] vastata taotlustele [...] andmesubjekti õiguste teostamiseks“. Seepärast peaks vastutav töötleja rakendama koostöös oma volitatud töötlejatega erimenetlusi andmete ülekandmise taotluste täitmiseks. Ühise vastutuse korral tuleks lepingus selgelt kindlaks määrata iga vastutava töötleja kohustused andmete ülekandmise taotluste töötlemisel.

Peale selle on vastuvõttev vastutav töötleja<sup>11</sup> kohustatud tagama, et esitatud ülekantavad andmed on andmete uue töötlemise jaoks asjakohased ega ole selleks ülemäärased. Näiteks ei pea uus vastutav töötleja töötleva andmesubjekti korrespondentide kontaktandmeid veebimeili teenuse osutajale esitatud andmete ülekandmise taotluse puhul, kui andmesubjekt kasutab taotlust e-kirjade saamiseks ja nende turvalisse arhiiviplatvormi saatmiseks. Kui see teave ei ole uue töötlemise eesmärgi täitmiseks asjakohane, ei tuleks seda säilitada ega töödelda. Igal juhul ei ole vastuvõtavad vastutavad töötlejad kohustatud andmete ülekandmise taotluse põhjal edastatud isikuandmeid vastu võtma ja töötleva. Samamoodi ei pea vastuvõttev vastutav töötleja juhul, kui andmesubjekt taotleb oma pangatehingute andmete edastamist sellise teenuse osutajale, mis aitab tal oma eelarvet hallata, kõiki andmeid vastu

---

<sup>9</sup> Andmete ülekandmise õigus ei piirdu selliste isikuandmetega, mis on kasulikud ja asjakohased vastutava töötleja konkurentide pakutavate sarnaste teenuste jaoks.

<sup>10</sup> Eespool esitatud näite puhul ei saa juhul, kui vastutav töötleja ei säilita kasutaja kuulatud laulude andmeid, selliseid isikuandmeid andmete ülekandmise taotlusse lisada.

<sup>11</sup> St see vastutav töötleja, kes saab isikuandmeid andmete ülekandmise taotluse põhjal, mille andmesubjekt on esitanud mõnele teisele vastutavale töötlejale.

võtma ega säilitama kõiki tehingute üksikasju pärast seda, kui need on uue teenuse jaoks märgistatud. Teiste sõnadega tuleks vastu võtta ja säilitada ainult selliseid andmeid, mis on vastuvõtva vastutava töötaja osutatava teenuse jaoks vajalikud ja asjakohased.

Vastuvõtvast organisatsioonist saab kõnealuste isikuandmete puhul uus vastutav töötaja ja ta peab järgima isikuandmete kaitse üldmääruse artiklis 5 sätestatud põhimõtteid. Seepärast peab uus vastuvõttev vastutav töötaja enne mis tahes taotlust ülekantavate andmete edastamise kohta täpsustama kooskõlas artiklis 14 sätestatud läbipaistvusnõuetega selgelt ja otseselt uue töötlemise eesmärgi<sup>12</sup>. Nagu mis tahes muu tema vastutusel toimuva andmete töötlemise puhul peaks vastutav töötaja kohaldama artiklis 5 sätestatud põhimõtteid, nagu seaduslikkus, õiglus ja läbipaistvus, eesmärgi piirang, võimalikult väheste andmete kogumine, õigus, usaldusväarsus ja konfidentsiaalsus, säilitamise piirang ning vastutus<sup>13</sup>.

Isikuandmeid hoidvad vastutavad töötajad peaksid olema valmis toetama oma andmesubjektide õigust andmete ülekandmisele. Samuti võivad vastutavad töötajad otsustada andmeid andmesubjektilt vastu võtta, kuid nad ei ole selleks kohustatud.

#### - **Andmete ülekantavus vs. andmesubjektide muud õigused**

**Kui isik teostab oma õigust andmete ülekandmisele, siis ei piira ta sellega mingeid muid õigusi (nagu ka kõikide teiste isikuandmete kaitse üldmääruses sisalduvate õiguste puhul).** Andmesubjekt võib jätkata vastutava töötaja teenuse kasutamist ja sellest kasu saamist ka pärast andmete ülekandmise toimingut. Andmete ülekandmisega ei kaasne automaatselt andmete kustutamist<sup>14</sup> vastutava töötaja süsteemidest ning see ei mõjuta edastatud andmete suhtes kehtivat algset säilitamisega. Andmesubjekt saab teostada oma õigusi nii kaua, kui vastutav töötaja veel andmeid töötleb.

Kui andmesubjekt soovib teostada oma õigust andmete kustutamisele (artikli 17 kohast „õigust olla unustatud“), ei saa vastutav töötaja kasutada andmete ülekandmist sellise kustutamiseks viivitamiseks või sellest keeldumiseks.

Kui andmesubjekt avastab, et andmete ülekandmise õiguse alusel taotletud isikuandmed ei vasta täielikult tema taotlusele, tuleks kooskõlas isikuandmete kaitse üldmääruse artikliga 15 täielikult täita andmetega tutvumise õiguse alusel esitatud võimalikud täiendavad isikuandmete taotlused.

Peale selle tuleb juhul, kui mõnda muud valdkonda käsitlevas ELi või liikmesriigi eriõigusaktis on sätestatud asjaomaste andmete teatavas vormis ülekantavus, võtta isikuandmete kaitse üldmääruse kohase andmete ülekandmise taotluse täitmisel arvesse ka selliste eriõigusaktidega ette nähtud tingimusi. Esiteks ei kohaldata juhul, kui andmesubjekti esitatud taotluse põhjal on selge, et ta ei kavatse teostada oma õigusi isikuandmete kaitse üldmääruse alusel, vaid üksnes valdkondlike õigusaktide alusel, sellise taotluse suhtes

---

<sup>12</sup> Peale selle ei tohiks uus vastutav töötaja töödelda isikuandmeid, mis ei ole asjakohased, ning töötlemine peab piirduma uueks eesmärgiks vajaliku, isegi kui isikuandmed moodustavad osa ülekandmisprotsessi kaudu edastatud üldisemast andmekogumist. Isikuandmed, mis ei ole uue töötlemise eesmärgi saavutamiseks vajalikud, tuleks võimalikult kiiresti kustutada.

<sup>13</sup> Kui vastutav töötaja on andmete ülekandmise õiguse alusel saadetud isikuandmed kätte saanud, võib neid käsitada andmesubjekti poolt „esitatutena“ ja vastavalt andmete ülekandmise õigusele uuesti edastada sel määral, mil on täidetud muud kõnealuse õiguse suhtes kohaldatavad tingimused (st töötlemise õiguslik alus, ...).

<sup>14</sup> Nagu on sätestatud isikuandmete kaitse üldmääruse artiklis 17.

andmete ülekandmist käsitlevaid isikuandmete kaitse üldmääruse sätteid<sup>15</sup>. Teisalt, kui taotlus käsitleb ülekantavust isikuandmete kaitse üldmääruse alusel, siis ei tühista kõnealuste erioigusaktide olemasolu andmete ülekandmise põhimõtte üldist kohaldatavust mis tahes vastutava töötaja suhtes, nagu on ette nähtud isikuandmete kaitse üldmäärusega. Selle asemel tuleb iga juhtumi puhul eraldi hinnata, kuidas (kui üldse) võib selline erioigusakt andmete ülekandmise õigust mõjutada.

### **III. Millal andmete ülekantavust kohaldatakse?**

#### **- Milliseid töötlemistoiminguid andmete ülekandmise õigus hõlmab?**

Isikuandmete kaitse üldmääruse nõuete täitmiseks peab vastutavatel töötajatel olema isikuandmete töötlemiseks selge õiguslik alus.

Kooskõlas isikuandmete kaitse üldmääruse artikli 20 lõike 1 punktiga a peavad töötlemistoimingud selleks, et **need jääksid andmete ülekantavuse kohaldamisalasse**, põhinema:

- andmesubjekti nõusolekul (vastavalt artikli 6 lõike 1 punktile a või isikuandmete eriliikide puhul artikli 9 lõike 2 punktile a) või
- andmesubjekti osalusel sõlmitud lepingul vastavalt artikli 6 lõike 1 punktile b.

Isikuandmed, mis üldiselt jäävad andmete ülekantavuse kohaldamisalasse, on näiteks isiku poolt elektroonilisest raamatupoest ostetud raamatute pealkirjad või laulud, mida ta muusika voogedastusteenuse kaudu kuulab, sest nende töötlemine põhineb andmesubjekti osalusel sõlmitud lepingu täitmisel.

Isikuandmete kaitse üldmäärusega ei ole kehtestatud üldist andmete ülekandmise õigust selliste juhtumite puhul, mil isikuandmete töötlemine ei põhine nõusolekul või lepingul<sup>16</sup>. Näiteks ei ole finantsasutustel kohustust vastata selliseid isikuandmeid käsitlevale andmete ülekandmise taotlusele, mida töödeldakse osana nende kohustusest ennetada ja avastada rahapesu ja muid finantskuritegusid; samamoodi ei hõlma andmete ülekantavus ettevõtetevaheliste suhete raames töödeldavaid ametialaseid kontaktandmeid juhul, kui töötlemine ei põhine ei andmesubjekti nõusolekul ega tema osalusel sõlmitud lepingul.

Töötajate andmete puhul kohaldatakse andmete ülekandmise õigust tavaliselt vaid siis, kui töötlemine põhineb andmesubjekti osalusel sõlmitud lepingul. Paljudel juhtudel leitakse, et

---

<sup>15</sup> Näiteks kui andmesubjekti taotlus käsitleb konkreetselt kontoga seotud teabeteenuse osutajale tema pangakonto ajaloole juurdepääsu andmist teises makseteenuste direktiivis täpsustatud eesmärkidel, tuleb selline juurdepääs anda kooskõlas kõnealuse direktiivi sätetega.

<sup>16</sup> Vt isikuandmete kaitse üldmääruse põhjendus 68 ja artikli 20 lõige 3. Artikli 20 lõikes 3 ja põhjenduses 68 on sätestatud, et andmete ülekantavust ei kohaldata juhul, kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötaja avaliku võimu teostamiseks või kui vastutav töötaja täidab oma avalikke või juriidilisi kohustusi. Seepärast ei ole vastutavatel töötajatel kohustust sellistel juhtudel ülekandmist võimaldada. On aga hea tava töötada välja ülekandmise taotlustele automaatse vastamise menetlused, järgides andmete ülekandmise õigust reguleerivaid põhimõtteid. Selle näide on valitsuse pakutav teenus, mis võimaldab hõlpsalt alla laadida üksikisiku varasemaid tuludeklaratsioone. Andmete ülekantavuse kui hea tava kohta juhul, kui töötlemise õiguslik alus on selle vajalikkus õigustatud huvide ja olemasolevate vabatahtlike kavade jaoks, vt artikli 29 töörihma arvamus 06/2014 õigustatud huvide kohta (WP 217), lk 47 ja 48.



sellises kontekstis ei ole nõusolek vabatahtlikult antud, sest tööandja ja töötaja vahel puudub võimutasakaal<sup>17</sup>. Teatava inimressurssidega seotud töötlemise õiguslik alus on seevastu õigustatud huvi või on see vajalik tööhõive valdkonnas kehtivate konkreetsete juriidiliste kohustuste täitmiseks. Praktikaks on andmete ülekandmise õigus inimressursside kontekstis kahtlemata seotud teatavate töötlemistoimingutega (nagu palga ja hüvitiste maksmise teenused, asutusesisene värbamine), kuid paljudes muudes olukordades tuleb käsitleda iga juhtumit eraldi ja kontrollida, kas kõik andmete ülekandmise õiguse suhtes kohaldatavad tingimused on täidetud.

Samuti kehtib andmete ülekandmise õigus ainult juhul, kui andmeid „töödeldakse automatiseeritult“ – seega ei hõlma see enamikku paberkanalil toimikuid.

#### - Milliseid isikuandmeid see õigus hõlmab?

Artikli 20 lõike 1 kohaselt peavad andmed selleks, et need jääksid andmete ülekandmise õiguse kohaldamisalasse:

- olema andmesubjekti puudutavad isikuandmed,
- mida ta on vastutavale töötajale *esitanud*.

Ühtlasi on artikli 20 lõikes 4 märgitud, et selle õiguse järgimine ei kahjusta teiste isikute õigusi ja vabadusi.

#### Esimene tingimus: andmesubjekti puudutavad isikuandmed

Andmete ülekandmise taotluse kohaldamisalasse jäävad ainult isikuandmed. Seega jäävad kohaldamisalast välja kõik andmed, mis on anonüümsed<sup>18</sup> või ei puuduta andmesubjekti. Kohaldamisalasse jäävad aga pseudonüümi all esitatud andmed, kui neid on võimalik selgelt andmesubjektiga seostada (nt kui ta on esitanud vastava identifitseerimistunnuse, vt artikli 11 lõige 2).

Paljudes olukordades töötlevad vastutavad töötajad teavet, mis sisaldab mitme andmesubjekti isikuandmeid. Sellisel juhul ei peaks vastutavad töötajad lauset „andmesubjekti puudutavad isikuandmed“ liiga rangelt tõlgendama. Näiteks võivad telefonikõnede, isikutevahelise sõnumivahetuse või IP-kõnede salvestised sisaldada (abonendi konto ajaloo) üksikasju sissetulevates ja väljaminevates kõnedes osalevate kolmandate isikute kohta. Kuigi salvestised sisaldavad seega mitut inimest käsitlevaid isikuandmeid, peaks abonentidel olema võimalik selliseid salvestisi andmete ülekandmise taotluse põhjal saada, sest salvestised käsitlevad (ka) andmesubjekti. Kui sellised salvestised edastatakse aga seejärel uuele vastutavale töötajale, ei tohiks see uus vastutav töötaja töödelda neid ühelgi eesmärgil, mis kahjustaks kolmandate isikute õigusi ja vabadusi (vt kolmas tingimus allpool).

#### Teine tingimus: andmesubjekti esitatud andmed

Teise tingimusega kitsendatakse kohaldamisala andmetele, mille on „esitanud“ andmesubjekt.

On palju näiteid isikuandmete kohta, mille andmesubjekt on teadlikult ja aktiivselt „esitanud“, nagu elektrooniliste vormide kaudu esitatud kontoandmed (nt meiliaadress, kasutajanimi,

<sup>17</sup> Nagu artikli 29 töörihm kirjeldas oma 13. septembri 2001. aasta arvamuses 8/2001 (WP 48).

<sup>18</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216\\_et.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf).

vanus). Sellest hoolimata saadakse andmesubjekti „esitatud“ andmeid ka tema tegevuse jälgimise tulemusel. Seetõttu leiab artikli 29 töörihm, et kõnealusele uuele õigusele selle täieliku väärtuse andmiseks peaks väljend „esitanud“ hõlmama ka kasutajate tegevuse jälgimise teel saadud isikuandmeid, nagu aruka arvesti või muud liiki ühendatud seadmete töödeldud toorandmed,<sup>19</sup> tegevuslogid, veebisaitide külastamise või otsingute ajalugu.

Viimati nimetatud andmekategooria ei hõlma andmeid, mille on loonud vastutav töötaja (kasutades jälgimise teel saadud või otseselt sisendina esitatud andmeid), nagu aruka arvesti kogutud toorandmete analüüsimise teel koostatud kasutajaprofiil.

Sõltuvalt andmete päritolust saab eristada mitmesuguseid andmekategooriaid, et teha kindlaks, kas need on hõlmatud andmete ülekandmise õigusega. „Andmesubjekti esitatud“ andmeteks saab liigitada järgmised kategooriad:

- **andmed, mille andmesubjekt on aktiivselt ja teadlikult esitanud** (näiteks e-posti aadress, kasutajanimi, vanus jne);
- **jälgimise teel saadud andmed, mille andmesubjekt on esitanud teenuse või seadme kasutamise teel.** Need võivad hõlmata näiteks isiku tehtud otsingute ajalugu, andmeliiklusandmeid ja asukohaandmeid. Samuti võivad need hõlmata muid toorandmeid, nagu kantava seadme kaudu jälgitavad südamelöögid.

Kaudsed ja tuletatud andmed seevastu loob vastutav töötaja „andmesubjekti esitatud“ andmete põhjal. Näiteks kasutaja tervist käsitleva hinnangu tulemuste või riskijuhtimise ja finantseeskirjade kontekstis loodud profiili puhul (nt krediidi hinnangu määramiseks või rahapesuvastaste eeskirjade täitmiseks) ei saa iseenesest väita, et andmesubjekt on need „esitanud“. Kuigi sellised andmed võivad moodustada osa vastutava töötaja hoitavast profiilist ja need on kaudselt saadud või tuletatud andmesubjekti poolt (näiteks tema tegevuse kaudu) esitatud andmete analüüsist, ei käsitata selliseid andmeid tavaliselt „andmesubjekti esitatud“ andmetena ja seega ei kuulu need kõnealuse uue õiguse kohaldamisalasse<sup>20</sup>.

Arvestades andmete ülekandmise õiguse valdkondlikke eesmärke, tuleks väljendit „andmesubjekti esitatud“ üldjuhul tõlgendada laialt ning selle alla ei tohiks kuuluda „kaudsed andmed“ ega „tuletatud andmed“, mis hõlmavad teenuseosutaja loodud andmeid (näiteks algoritmide kasutamisel saadud tulemusi). Vastutav töötaja võib need kaudsed andmed välja jätta, ent ta peaks lisama kõik muud isikuandmed, mille andmesubjekt on vastutava töötaja pakutud tehniliste vahendite kaudu esitanud<sup>21</sup>.

---

<sup>19</sup> Kui andmesubjektil on võimalik saada kätte tema tegevuse jälgimisest tulenevad andmed, saab ta ka parema ülevaate sellest, millises ulatuses on vastutav töötaja otsustanud jälgimise teel saadud andmeid kasutada, ning tal on parem teha valikuid selle kohta, milliseid andmeid ta on nõus sarnase teenuse saamiseks esitama, ja võimalik olla teadlikum sellest, mil määral austatakse tema õigust eraelu puutumatusel.

<sup>20</sup> Isikuandmete kaitse üldmääruse artikli 15 (mis käsitleb õigust tutvuda andmetega) kohaselt saab andmesubjekt sellest hoolimata kasutada oma õigust „saada vastutavalt töötajalt kinnitust selle kohta, kas teda käsitlevaid isikuandmeid töödeldakse, ning sellisel juhul tutvuda isikuandmetega“ ja teabega „artikli 22 lõigetes 1 ja 4 osutatud automatiseeritud otsuste, sealhulgas profiilanalüüsi tegemise kohta ning vähemalt nendel juhtudel [sisulise teabega] kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks“.

<sup>21</sup> Need hõlmavad kõiki andmeid, mis on saadud andmesubjekti sellise tegevuse jälgimise teel, mille kohta andmeid kogutakse, nagu tehingute ajalugu või külastuslogi. Andmesubjekti jälgimise ja tema tegevuse salvestamise kaudu (näiteks südamelööke salvestav rakendus või sirvimiskäitumise jälgimiseks kasutatav tehnoloogia) kogutud andmeid tuleks samuti käsitada tema „esitatud“ andmetena isegi juhul, kui neid ei ole edastatud aktiivselt ja teadlikult.

Seega hõlmab väljend „esitatud“ ka isikuandmeid, mis käsitlevad andmesubjekti tegevust või on saadud üksikisiku käitumise jälgimise tulemusel, kuid mitte selliseid andmeid, mis tulenevad selle käitumise hilisemast analüüsimisest. Seevastu mis tahes isikuandmed, mille vastutav töötleja on loonud andmete töötlemise osana, näiteks isikustamise või soovitude esitamise protsessi, kasutajate liigitamise või profiilide koostamise teel, on andmesubjekti esitatud isikuandmetest tuletatud või nende põhjal kaudselt saadud andmed ega ole andmete ülekandmise õigusega hõlmatud.

Kolmas tingimus: andmete ülekandmise õigus ei kahjusta teiste isikute õigusi ja vabadusi

### **Teisi andmesubjekte käsitlevate isikuandmete puhul**

Kolmanda tingimuse eesmärk on vältida teiste (nõusolekut mitte andnud) andmesubjektide isikuandmeid sisaldavate andmete kättesaamist ja edastamist uuele vastutavale töötlejale juhul, kui selliseid andmeid töödeldakse tõenäoliselt viisil, mis võib kahjustada teiste andmesubjektide õigusi ja vabadusi (isikuandmete kaitse üldmääruse artikli 20 lõige 4)<sup>22</sup>.

Selline kahjustamine toimuks näiteks juhul, kui andmete edastamine ühelt vastutavalt töötlejalt teisele takistaks kolmandatel isikutel teostada andmesubjektidena oma isikuandmete kaitse üldmääruse kohaseid õigusi (nagu õigus saada teavet, õigus tutvuda andmetega jne).

Andmesubjekt, kes algatab oma andmete edastamise teisele vastutavale töötlejale, annab uuele vastutavale töötlejale töötlemiseks nõusoleku või sõlmib temaga lepingu. Kui andmekogum sisaldab kolmandate isikute isikuandmeid, tuleb töötlemiseks kindlaks määrata mõni muu õiguslik alus. Näiteks võib vastutav töötleja artikli 6 lõike 1 punkti f alusel tugineda õigustatud huvile, eelkõige kui vastutava töötleja eesmärk on pakkuda andmesubjektile teenust, mis võimaldab viimasel töödelda isikuandmeid eranditult isiklikel või kodustel eesmärkidel. Töötlemistoimingute eest, mille andmesubjekt algatab isikliku tegevuse käigus ning mis puudutavad ja võivad mõjutada kolmandaid isikuid, vastutab andmesubjekt sel määral, mil vastutav töötleja ei tee töötlemise kohta mingil viisil otsuseid.

Näiteks võib veebimeili teenus võimaldada luua kataloogi andmesubjekti kontaktide, sõprade, sugulaste, pereliikmete ja laiema keskkonna kohta. Kuna need andmed käsitlevad (ja need on loonud) tuvastatav üksikisik, kes soovib teostada oma õigust andmete ülekandmisele, peaksid vastutavad töötlejad edastama sellele andmesubjektile kogu sissetulevate ja väljaminevate e-kirjade kataloogi.

Samamoodi võib andmesubjekti pangakonto sisaldada isikuandmeid, mis on seotud mitte üksnes kontoomaniku, vaid ka teiste isikute tehingutega (nt kui nad on kontoomanikule rahaülekande teinud). Kontoomanikule andmete ülekandmise taotluse põhjal pangakonto kohta teabe edastamine nende kolmandate isikute õigusi ja vabadusi tõenäoliselt ei kahjusta, tingimusel et mõlema näite puhul kasutatakse andmeid samal eesmärgil (st ainult andmesubjekti kasutatav kontaktaadress või andmesubjekti pangakonto ajalugu).

Seevastu ei austata kolmandate isikute õigusi ja vabadusi juhul, kui uus vastutav töötleja kasutab nende isikuandmeid muudel eesmärkidel, nt kui vastuvõttev vastutav töötleja kasutab

---

<sup>22</sup> Põhjenduses 68 on sätestatud: „Kui teatud isikuandmed puudutavad enam kui üht andmesubjekti, ei tohiks isikuandmete saamise õigus piirata teiste andmesubjektide käesoleva määruse kohaseid õigusi ja vabadusi“.

andmesubjekti kontaktide kataloogis sisalduvaid teiste isikute isikuandmeid turundamise eesmärgil.

Et vältida kahjulikku mõju asjaomastele kolmandatele isikutele, lubatakse uuel vastutaval töötlejal seepärast selliseid isikuandmeid töödelda ainult sel määral, mil taotluse esitanud kasutajal on andmete üle ainukontroll ja neid hallatakse eranditult isiklikel või kodustel eesmärkidel. Vastuvõttev uus vastutav töötleja (kellele võib andmed kasutaja taotlusel edastada) ei tohi kasutada kolmandate isikute kohta edastatud andmeid oma tarbeks, nt kõnealustele kolmandatele isikutele turundustoodete ja -teenuste soovitamiseks. Näiteks ei tohi kasutada sellist teavet ilma kolmandast isikust andmesubjekti teadmise ja nõusolekuta tema profiili täiendamiseks ja tema sotsiaalse keskkonna ümberkujundamiseks<sup>23</sup>. Samuti ei tohi seda kasutada selliste kolmandate isikute kohta teabe saamiseks ja konkreetsete profiilide loomiseks, isegi kui vastutaval töötlejal on nende isikuandmed juba olemas. Vastasel korral on selline töötlemine tõenäoliselt ebaseaduslik ja ebaõiglane, eriti kui asjaomaseid kolmandaid isikuid ei teavitata ja nad ei saa andmesubjektidena oma õigusi teostada.

Peale selle on kõikide vastutavate töötlejate (nii andmeid saatvate kui ka vastuvõtivate poolte) puhul levinud tava rakendada vahendeid, mis võimaldavad andmesubjektidel valida asjakohased andmed, mida nad soovivad saada ja edastada, ja vajaduse korral teiste isikute andmed välja jätta. See aitab veelgi vähendada riske kolmandate isikute jaoks, kelle isikuandmeid võidakse üle kanda.

Lisaks peaksid vastutavad töötlejad kasutama mehhanisme teistelt asjaomastelt andmesubjektidelt nõusoleku saamiseks, et hõlbustada andmete edastamist juhtudel, mil kõnealused isikud soovivad nõusoleku anda, nt kui nad soovivad samuti oma andmeid mõnele teisele vastutavale töötlejale edastada. Selline olukord võib tekkida näiteks sotsiaalvõrgustike puhul, kuid vastutavad töötlejad peavad ise otsustama, millist head tava nad järgivad.

### **Intellektuaalomandi ja ärisaladusega hõlmatud andmed**

Artikli 20 lõikes 4 on mainitud teiste isikute õigusi ja vabadusi. Kuigi need ei ole otseselt seotud ülekandmisega, võib mõista, et need hõlmavad „ärisaladusi ja intellektuaalomandit ning eelkõige tarkvara kaitsvat autoriõigust“. Neid õigusi tuleks enne ülekandmise taotlusele vastamist küll kaaluda, ent „[s]ellise kaalumise tulemus ei tohiks olla andmesubjektile teabe andmisest keeldumine“. Peale selle ei tohiks vastutav töötleja andmete ülekandmise taotlust tagasi lükata mõne muu lepingulise õiguse rikkumise põhjal (näiteks tasumata võlg või ärikonflikt andmesubjektiga).

Andmete ülekandmise õigus ei ole üksikisiku õigus kasutada teavet viisil, mida võib pidada ebaausaks tavaks või mille näol võib olla tegemist intellektuaalomandi õiguste rikkumisega.

Võimalikku äririski iseenesest ei saa aga kasutada ülekandmise taotlusele vastamisest keeldumise alusena ja vastutavad töötlejad saavad edastada andmesubjektide esitatud isikuandmeid sellises vormis, mille puhul ei avaldata ärisaladuse või intellektuaalomandi õigusega hõlmatud teavet.

---

<sup>23</sup> Sotsiaalvõrgustikuteenuste osutajad ei tohi täiendada oma liikmete profiile, kasutades isikuandmeid, mille andmesubjekt on oma andmete ülekandmise õiguse alusel edastanud, ilma et nad järgiksid seejuures läbipaistvuse põhimõtet ja ühtlasi veenduksid, et nad tuginevad selle konkreetse töötlemistoimingu puhul asjakohasele õiguslikule alusele.

#### **IV. Kuidas kohaldatakse andmete ülekantavuse suhtes andmesubjektide õigusi reguleerivaid üldeeskirju?**

##### **- Milline eelnev teave tuleb andmesubjektile esitada?**

Uue andmete ülekandmise õiguse järgimiseks peavad vastutavad töötajad andmesubjekte sellest õigusest teavitama. Kui asjaomaseid isikuandmeid kogutakse otse andmesubjektilt, peab see toimuma „isikuandmete saamise ajal“. Kui isikuandmed ei ole saadud andmesubjektilt, peab vastutav töötaja esitama artikli 13 lõike 2 punktiga b ja artikli 14 lõike 2 punktiga c nõutud teabe.

„Kui isikuandmed ei ole saadud andmesubjektilt“, siis nõutakse artikli 14 lõikega 3, et teave tuleb esitada mõistliku aja, kuid hiljemalt ühe kuu jooksul pärast andmete saamist, andmesubjekti esmakordse teavitamise ajal või isikuandmete kolmandatele isikutele avaldamise ajal<sup>24</sup>.

Nõutava teabe esitamisel peavad vastutavad töötajad tagama, et nad eristavad andmete ülekandmise õigust muudest õigustest. Seepärast soovib artikli 29 tööriühm eelkõige, et vastutavad töötajad selgitavad üheselt erinevusi andmeliikide vahel, mida andmesubjekt võib saada andmetega tutvumise õiguse alusel ja andmete ülekandmise õiguse alusel.

Peale selle soovib tööriühm vastutavatel töötajatel alati esitada teavet andmete ülekandmise õiguse kohta enne seda, kui andmesubjekt oma võimaliku konto sulgeb. See võimaldab kasutajatel saada oma isikuandmetest ülevaade ja andmed enne lepingu lõpetamist hõlpsalt oma seadmele kanda või mõnele teisele teenuseosutajale edastada.

Samuti soovib artikli 29 tööriühm vastuvõtvatel vastutavatel töötajatel esitada andmesubjektidele levinud tavana kogu teave selle kohta, millist laadi isikuandmed on nende teenuste pakkumisel asjakohased. Lisaks õiglase töötlemise toetamisele võimaldab see kasutajatel piirata kolmandatele isikutele tekkida võivaid riske ning ka muud ebavajalikku isikuandmete dubleerimist isegi siis, kui teised andmesubjektid ei ole hõlmatud.

##### **- Kuidas saab vastutav töötaja andmesubjekti enne tema taotlusele vastamist tuvastada?**

Isikuandmete kaitse üldmäärusega ei ole ette nähtud mingeid nõudeid andmesubjekti autentimise kohta, ent selle artikli 12 lõikes 2 on sätestatud, et vastutav töötaja ei keeldu meetmete võtmisest andmesubjekti taotlusel tema õiguste (sealhulgas andmete ülekandmise õiguse) kasutamiseks, välja arvatud juhul, kui vastutav töötaja töötleb andmeid eesmärgil, milleks ei ole vaja andmesubjekti tuvastamist, ja kui ta saab tõendada, et ta ei suuda andmesubjekti tuvastada. Vastavalt artikli 11 lõikele 2 võib andmesubjekt sellistel juhtudel esitada lisateavet, mis võimaldab teda tuvastada. Lisaks on artikli 12 lõikes 6 sätestatud, et kui vastutaval töötajal on põhjendatud kahtlused andmesubjekti identiteedi suhtes, võib ta nõuda lisateavet andmesubjekti isiku kinnitamiseks. Kui andmesubjekt esitab lisateavet, mis võimaldab teda tuvastada, siis ei keeldu vastutav töötaja taotluse täitmiseks meetmeid võtmast. Kui elektrooniliselt kogutud teave ja andmed on seotud pseudonüümide või kordumatute identifikaatoritega, võivad vastutavad töötajad rakendada asjakohaseid

---

<sup>24</sup> Artikliga 12 nõutakse, et vastutavad töötajad teavitavad andmesubjekti „kokkuvõtlikult, selgelt, arusaadavalt ning lihtsalt kättesaadavas vormis, kasutades selget ja lihtsat keelt, eelkõige konkreetselt lapsele suunatud teabe korral“.

menetlusi, mis võimaldavad isikul esitada andmete ülekandmise taotluse ja saada teda käsitlevaid andmeid. Igal juhul peavad vastutavad töötledjad rakendama autentimismenetlust, et oma isikuandmeid taotleva või laiemalt isikuandmete kaitse üldmäärusega antud õigusi teostava andmesubjekti isik kahtlusteta kindlaks teha.

Sellised menetlused on sageli juba kehtestatud. Tihti autendib vastutav töötledja andmesubjekte enne nendega lepingu sõlmimist või töötlemiseks nende nõusoleku saamist. Selle tagajärjel võib töötlemisega seotud isiku registreerimiseks kasutatud isikuandmeid kasutada ka tõendina andmesubjekti autentimiseks andmete ülekandmise eesmärgil<sup>25</sup>.

Kuigi sellistel juhtudel võib andmesubjektide eelnevaks tuvastamiseks olla vaja nõuda nende juriidilise identiteedi tõendamist, ei pruugi selline kontrollimine olla asjakohane andmete ja asjaomase isiku vahelise seose hindamiseks, sest selline seos ei tulene ametlikust või juriidilisest identiteedist. Põhimõtteliselt ei saa asjaolu, et vastutav töötledja saab taotleda isiku identiteedi tuvastamiseks lisateavet, tuua kaasa liigseid nõudmisi ega selliste isikuandmete kogumist, mis ei ole asjakohased või vajalikud isiku ja taotletavate isikuandmete vahelise seose kinnitamiseks.

Paljudel juhtudel on sellised autentimismenetlused juba kehtestatud. Näiteks kasutatakse sageli kasutajanimed ja salasõnu, et lubada isikutele juurdepääs andmetele nende e-posti kontodel, sotsiaalvõrgustike kontodel ja mitmesuguste muude teenuste osutamiseks kasutatavatel kontodel, millest mõnda otsustasid nad kasutada ilma oma täielikku nime ja identiteeti avalikustamata.

Kui andmesubjekti taotletud andmete mahu tõttu on neid interneti teel raske edastada, võib vastutaval töötledjal selle asemel, et kasutada taotluse täitmiseks maksimaalselt kolme kuu pikkust pikendatud ajavahemikku,<sup>26</sup> olla vaja kaaluda ka alternatiivseid võimalusi andmete esitamiseks, näiteks voogedastuse kasutamist või CD- või DVD-kettale või muule füüsilisele andmekandjale salvestamist või isikuandmete otse teisele vastutavale töötledjale edastamise lubamist (vastavalt isikuandmete kaitse üldmääruse artikli 20 lõikele 2, kui see on tehniliselt teostatav).

#### **- Milline on andmete ülekandmise taotlusele vastamiseks kehtestatud ajaline piirang?**

Artikli 12 lõikega 3 nõutakse, et vastutav töötledja esitab andmesubjektile „teabe [...] võetud meetmete kohta“ „tarbetu viivitusega“, kuid mitte hiljem kui „ühe kuu jooksul pärast taotluse saamist“. Keeruliste juhtumite puhul võib seda ühekuulist perioodi pikendada maksimaalselt kolme kuuni, tingimusel et andmesubjekti on teavitatud sellise viivituse põhjustest ühe kuu jooksul alates algse taotluse saamisest.

Infoühiskonna teenuseid osutavatel vastutavatel töötledjatel on tõenäoliselt parem võimalus taotlusi väga lühikese aja jooksul täita. Et vastata kasutajate ootustele, on hea tava määrata kindlaks ajavahemik, mille jooksul andmete ülekandmise taotlusele suudetakse tavaliselt vastata, ja andmesubjekte sellest teavitada.

---

<sup>25</sup> Näiteks kui andmete töötlemine on seotud kasutajakontoga, võib andmesubjekti tuvastamiseks olla piisav, kui esitatakse vastav kasutajatunnus ja salasõna.

<sup>26</sup> Artikli 12 lõige 3: „Vastutav töötledja esitab [...] teabe [...] taotluse alusel võetud meetmete kohta“.

Artikli 12 lõike 4 kohaselt teatab vastutav töötaja, kes keeldub ülekandmise taotlusele vastamast, andmesubjektile hiljemalt ühe kuu jooksul alates taotluse saamisest „meetmete võtmata jätmise põhjused ning selgitab talle võimalust esitada järelevalveasutusele kaebus ja kasutada õiguskaitsevahendeid“.

**Vastutavad töötajad peavad täitma kohustuse vastata ettenähtud tähtaja jooksul isegi siis, kui tegemist on keeldumisega. Teiste sõnadega ei saa vastutav töötaja jätta reageerimata, kui tal palutakse andmete ülekandmise taotlusele vastata.**

- **Millisel juhul võib andmete ülekandmise taotluse tagasi lükata või tasu nõuda?**

Artikliga 12 keelatakse vastutaval töötajal isikuandmete esitamise eest tasu nõuda, välja arvatud juhul, kui vastutav töötaja suudab tõendada, et taotlused on selgelt põhjendamatud või ülemäärased, „eelkõige oma korduva iseloomu tõttu“. Isikuandmete automatiseeritud töötlemisele spetsialiseerunud infoühiskonna teenuste puhul võib selliste automatiseeritud süsteemide nagu rakendusliideste<sup>27</sup> kasutamine hõlbustada teabevahetust andmesubjektiga ja vähendada seega korduvatest taotlustest tingitud koormust. Seepärast peaks esinema väga vähe juhtumeid, kus vastutav töötaja suudab põhjendada taotletud teabe esitamisest keeldumist, isegi mitme andmete ülekandmise taotluse puhul.

Peale selle ei tohiks taotluse ülemäärasuse kindlaksmääramisel arvesse võtta andmete ülekandmise taotlustele vastamiseks loodud protsesside üldkulu. Tegelikult keskendutakse isikuandmete kaitse üldmääruse artiklis 12 ühe andmesubjekti esitatud taotlustele, mitte vastutava töötaja saadud taotluste koguarvule. Selle tulemusel ei tohiks süsteemi rakendamise üldkulusid andmesubjektidelt sisse nõuda ega kasutada neid kulusid ülekandmise taotlusele vastamisest keeldumise põhjendusena.

## **V. Kuidas tuleb ülekantavad andmed esitada?**

- **Milliseid vahendeid peaks vastutav töötaja andmete esitamiseks eeldatavalt kasutama?**

Isikuandmete kaitse üldmääruse artikli 20 lõikes 1 on sätestatud, et andmesubjektidel on õigus edastada andmed teisele vastutavale töötajale, ilma et vastutav töötaja, kellele isikuandmed on esitatud, seda takistaks.

Sellist takistamist võib iseloomustada kui mis tahes õiguslikku, tehnilist või rahalist tõket, mille vastutav töötaja on loonud selleks, et muuta võimatuks või aeglustada andmetega tutvumist ja nende edastamist või taaskasutamist andmesubjekti või teise vastutava töötaja poolt. Kõnealused takistused võivad olla näiteks andmete esitamise eest nõutavad tasud, andmevormingu või rakendusliidese või ettenähtud vormingu koostalitlusvõime ja juurdepääsetavuse puudumine, ülemäärane viivitus või keerukus kogu andmekogumi kättesaamisel, andmekogumi tahtlik segaseks muutmine või konkreetset ja ebavajalikud või ülemäärased valdkondlikud standardid või akrediteerimismõuded<sup>28</sup>.

<sup>27</sup> Rakendusliideseid on rakenduste või veebiteenuste liideseid, mille vastutavad töötajad teevad kättesaadavaks selleks, et muud süsteemid või rakendused saaksid nende süsteemidega ühenduse luua ja töötada.

<sup>28</sup> Tekkida võib teatavaid seadusest tulenevaid takistusi, nagu need, mis on seotud artikli 20 lõikes 4 mainitud teiste isikute õiguste ja vabadustega või vastutavate töötajate enda süsteemide turvalisusega. Vastutava töötaja

Artikli 20 lõikega 2 pannakse vastutavatele töötajatele ka kohustus edastada ülekantavad andmed otse teistele vastutavatele töötajatele, „kui see on tehniliselt teostatav“.

Seda, kas andmete edastamine andmesubjekti kontrolli all ühelt vastutavalt töötajalt teisele on tehniliselt teostatav, tuleks hinnata iga juhtumi puhul eraldi. „Tehnilise teostatavuse“ piire on täiendavalt selgitatud põhjenduses 68, kus on märgitud, et see „ei peaks tekitama vastutavale töötajale kohustust võtta kasutusele või hoida töös tehniliselt ühilduvaid andmetöötlussüsteeme“.

Vastutavate töötajatelt eeldatakse isikuandmete edastamist koostalitavas vormingus, ent see ei tekita teistele vastutavatele töötajatele kohustust selliseid vorminguid toetada. Seega võib andmete otsene edastamine ühelt vastutavalt töötajalt teisele leida aset juhul, kui kaks süsteemi suudavad omavahel turvaliselt<sup>29</sup> suhelda ja kui vastuvõttev süsteem on tehniliselt suuteline sissetulevaid andmeid vastu võtma. Kui tehnilised takistused ei võimalda otsest edastamist, selgitab vastutav töötaja neid takistusi andmesubjektidele, sest vastasel korral on tema otsus oma laadilt sarnane keeldumisega andmesubjekti taotluse põhjal meetmeid võtta (artikli 12 lõige 4).

Tehnilisel tasandil peaksid vastutavad töötajad uurima ja hindama kahte erinevat ja vastastikku täiendavat võimalust ülekantavate andmete andmesubjektidele või teistele vastutavatele töötajatele kättesaadavaks tegemiseks:

- kogu ülekantava andmekogumi (või kogu andmekogumi mitme osa väljavõtete) otsene edastamine;
- automatiseeritud vahend, mis võimaldab asjakohastest andmetest väljavõtte teha.

Keeruliste ja suurte andmekogumite puhul võivad vastutavad töötajad eelistada teist moodust, sest see võimaldab teha väljavõtte andmekogumi mis tahes osast, mis on andmesubjekti jaoks tema taotluse põhjal asjakohane, ning võib aidata minimeerida riski ja võimaldada kasutada andmete sünkroniseerimise mehhanisme<sup>30</sup> (nt vastutavate töötajate vahelise regulaarse teabevahetuse kontekstis). See võib olla parem võimalus tagada, et uus vastutav töötaja täidab nõudeid, ja selle näol oleks tegemist hea tavaga eraelu puutumatuses seotud riskide vähendamiseks algse vastutava töötaja poolt.

Neid kahte erinevat ja potentsiaalselt vastastikku täiendavat võimalust asjakohaste ülekantavate andmete esitamiseks saab kasutada, tehes andmed kättesaadavaks mitmesuguste vahendite, näiteks turvalise sõnumside, turvalise failiedastusprotokolliga (SFTP) serveri, turvalise veebipõhise rakendusliidese või veebiportaali kaudu. Andmesubjektidel peaks olema võimalik kasutada isikuandmete hoidmiseks ja säilitamiseks isiklikku andmehoidlat, isikuandmete haldamise süsteemi<sup>31</sup> või muud liiki usaldusväärseid kolmandaid isikuid ning

---

kohustus on põhjendada, miks sellised takistused on seaduslikud ja miks ei ole nende näol tegemist takistamisega artikli 20 lõike 1 tähenduses.

<sup>29</sup> Autenditud teabevahetuse kaudu, mille puhul andmed on piisaval tasemel krüpteeritud.

<sup>30</sup> Andmete sünkroniseerimise mehhanismid võivad aidata täita üldisi kohustusi vastavalt isikuandmete kaitse üldmääruse artiklile 5, mille kohaselt „[i]sikuandmete töötlemisel tagatakse, et [...] isikuandmed on õiged ja vajaduse korral ajakohastatud“.

<sup>31</sup> Isikuandmete haldamise süsteemide kohta vt näiteks Euroopa Andmekaitseinspektori aramus 9/2016, mis on kättesaadav aadressil

[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20\\_PIMS\\_opinion\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf).



anda vastutavatele töötajatele õigus isikuandmete vajaduse korral juurde pääseda ja neid töödelda.

- **Milline on andmete eeldatav vorming?**

Isikuandmete kaitse üldmäärusega nõutakse vastutavalt töötajatelt, et nad esitaksid isiku taotletud isikuandmed taaskasutamist toetavas vormingus. Täpsemalt on isikuandmete kaitse üldmääruse artikli 20 lõikes 1 märgitud, et isikuandmed tuleb esitada „struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul“. Põhjenduses 68 on täiendavalt selgitatud, et selline vorming peaks olema koostalitlev; see termin on ELis määratletud<sup>32</sup> järgmiselt:

„disparaatsete ja erilaadsete organisatsioonide suutlikkus toimida koos vastastikku kasulike ja omavahel kokku lepitud ühiste eesmärkide nimel, sh organisatsioonide vahel nende poolt toetatavate äriprotsesside kaudu teabe ja teadmiste vahetamine, mis toimub andmete vahetamise kaudu vastavate IKT-süsteemide vahel.“

Terminite „struktureeritud“, „üldkasutatav“ ja „masinloetav“ näol on tegemist miinimumnõuete kogumiga, mis peaks hõlbustama vastutava töötaja kasutatava andmete vormingu koostalitlusvõimet. Seega kirjeldatakse terminitega „struktureeritud“, „üldkasutatav“ ja „masinloetav“ vahendeid, samas kui soovitud tulemus on koostalitlusvõime.

Direktiivi 2013/37/EL<sup>33,34</sup> põhjenduses 21 on „masinloetav“ määratletud järgmiselt:

„failivorming, mis on struktureeritud selliselt, et tarkvararakendused suudavad spetsiifilisi andmeid, sealhulgas üksikuid faktiväiteid, ja nende sisemist struktuuri kergelt tuvastada, ära tunda ja välja lugeda. Masinloetavas vormingus struktureeritud failides sisalduvad andmed on masinloetavad andmed. Masinloetavad vormingud võivad olla avatud või litsentsitud; nad võivad, kuid ei pruugi olla ametlikud standardid. Dokumente, mis on sellises automaatselt töötlemist piiravas failivormingus, et andmeid kas ei saa või ei saa kergesti dokumendist kätte, ei tuleks pidada masinloetavas vormingus dokumentideks. Liikmesriigid peaksid soodustama masinloetavate avatud vormingute kasutamist, kui see on asjakohane.“

Arvestades seda, et vastutav töötaja võib töödelda väga erinevat liiki andmeid, ei ole isikuandmete kaitse üldmääruses tehtud konkreetseid soovitusi esitatavate isikuandmete vormingu kohta. Kõige sobilikum vorming on sektorite lõikes erinev ja vastavad vormingud võivad juba olemas olla ning valiku tegemisel tuleks alati lähtuda eesmärgist, et vorming oleks tõlgendatav ja võimaldaks andmesubjektile ulatuslikku andmete ülekantavust. Seega ei peeta piisavaks lähenemisviisiks vorminguid, mille suhtes kehtivad litsentseerimisega seotud kulukad piirangud.

Põhjenduses 68 on selgitatud, et „[a]ndmesubjekti õigus edastada või saada teda puudutavaid isikuandmeid ei peaks tekitama vastutavatele töötajatele kohustust võtta kasutusele või hoida

<sup>32</sup> Euroopa Parlamendi ja nõukogu 16. septembri 2009. aasta otsuse nr 922/2009/EÜ (Euroopa haldusametuste koosvõimealaste lahenduste (ISA) kohta (ELT L 260, 3.10.2009, lk 20)) artikkel 2.

<sup>33</sup> Millega muudetakse direktiivi 2003/98/EÜ avaliku sektori valduses oleva teabe taaskasutamise kohta.

<sup>34</sup> ELi sõnastikus (<http://eur-lex.europa.eu/eli-register/glossary.html?locale=et>) on täiendavalt selgitatud käesolevates suunistes kasutatud põhimõtetega seotud eeldusi, näiteks *masinloetav*, *koostalitlusvõime*, *avatud vorming*, *standard*, *metaandmed*.

töös tehniliselt ühilduvaid andmetöötlussüsteeme<sup>35</sup>. **Seega on ülekantavuse eesmärk luua koostalitlevad, mitte ühilduvad süsteemid<sup>35</sup>.**

Eeldatakse, et isikuandmed esitatakse sellises vormingus, mis on võimalikest asutusesisestest või litsentsitud vormingutest märkimisväärselt üldistatum. Seega eeldab andmete ülekantavus vastutavatelt töötajatelt täiendavat andmetöötluse kihti, et andmeid platvormilt kätte saada ja eraldada ülekantavuse kohaldamisalast väljapoole jäävad isikuandmed, nagu kaudsed andmed või süsteemide turvalisusega seotud andmed. Sel viisil õhutatakse vastutavaid töötajaid tegema oma süsteemides eelnevalt kindlaks need andmed, mis jäävad ülekantavuse kohaldamisalasse. Seda täiendavat andmetöötlust peetakse põhilise andmetöötluse kõrvaltoiminguks, sest seda ei tehta vastutava töötaja määratletud uue eesmärgi saavutamiseks.

Kui teatavas majandusharus või teatavas kontekstis puuduvad üldkasutatavad vormingud, **peaksid vastutavad töötajad kasutama isikuandmete esitamiseks avatud vorminguid (nt XML, JSON, CSV, ...) koos kasulike ja parimal üksikasjalikkuse tasemel metaandmetega**, säilitades samal ajal märkimisväärse üldistatuse. Seega tuleks vahetatud teabe tähenduse täpseks kirjeldamiseks kasutada sobilikke metaandmeid. Sellised metaandmed peaksid olema piisavad, et andmed täidaksid oma otstarbe ja neid oleks võimalik taaskasutada, avalikustamata seejuures ärisaladusi. Seepärast ei ole tõenäoline, et isikule e-posti sisendkasti kohta PDF-vormingus dokumentide esitamine on piisavalt struktureeritud või kirjeldav, et see võimaldaks sisendkasti andmeid hõlpsalt taaskasutada. Et andmeid oleks võimalik tõhusalt taaskasutada, tuleks e-kirjade andmed esitada selle asemel vormingus, mille puhul säilivad kõik metaandmed. Seega peaks vastutav töötaja isikuandmete esitamiseks kasutatava andmevormingu valimisel kaaluma, kuidas see vorming võib mõjutada või takistada isiku õigust andmeid taaskasutada. Nendel juhtudel, kui vastutav töötaja suudab pakkuda andmesubjektile valikuvõimalusi seoses isikuandmete eelistatud vorminguga, tuleks valiku mõju arusaadavalt selgitada. Täiendavate metaandmete töötlemine ainult seetõttu, et need võivad olla nõutavad või soovitavad andmete ülekandmise taotlusele vastamiseks, ei kujuta endast aga sellise töötlemise seaduslikku alust.

**Artikli 29 tööriühm õhutab innukalt tööstusharu sidusrühmade ja kutseorganisatsioonide vahelist koostööd, et nad töötaksid üheskoos välja ühised koostalitlevad standardid ja vormingud andmete ülekandmise õigusega seotud nõuete täitmiseks.** Seda küsimust on käsitletud ka Euroopa koosvõimeraamistik (EIF), kes on loonud kokkulepitud lähenemisviisi koostalitlusvõimele selliste organisatsioonide jaoks, kes soovivad ühiselt osutada avalikke teenuseid. Raamistikuga on selle kohaldamisvaldkondades täpsustatud kogum ühiseid elemente, nagu sõnavara, mõisted, põhimõtted, poliitika, suunised, soovitusel, standardid, tehnilised kirjeldused ja tavad<sup>36</sup>.

#### - **Kuidas tulla toime mahukate või keeruliste isikuandmete kogudega?**

Isikuandmete kaitse üldmääruses ei ole selgitatud, kuidas lahendada vastamisega seotud probleem juhul, kui on tegemist suurte andmekogude või keerulise andmestruktuuriga või kui

<sup>35</sup> Standardis ISO/IEC 2382-01 on koostalitlusvõime määratletud järgmiselt: „Funktsionaalüksuste võime omavahel suhelda, programme täita või andmeid edastada nii, et kasutaja ei pea tundma nende üksuste eriomadusi“.

<sup>36</sup> Allikas: [http://ec.europa.eu/isa/documents/isa\\_annex\\_ii\\_eif\\_en.pdf](http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf).

kerkivad muud tehnilised küsimused, mis võivad vastutavatele töötlejatele või andmesubjektidele raskusi tekitada.

Kõikidel juhtudel on aga väga oluline, et isikul oleks võimalik täielikult aru saada nende isikuandmete määratlusest, skeemist ja struktuurist, mida vastutav töötleja võib esitada. Näiteks võib andmed esmalt esitada kokkuvõtlikul kujul, kasutades teabetabeleid, mis võimaldavad andmesubjektil kanda üle isikuandmete alamhulki, mitte kõiki andmeid. Vastutav töötleja peaks esitama ülevaate „kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt“ (vt isikuandmete kaitse üldmääruse artikli 12 lõige 1), nii et andmesubjektil oleks alati selge teave selle kohta, milliseid andmeid teataval eesmärgil alla laadida või teisele vastutavale töötlejale edastada. Näiteks peaks andmesubjektidel olema võimalik kasutada tarkvararakendusi, et ülevaatest konkreetseid andmeid hõlpsalt kindlaks teha ja ära tunda ning neid töödelda.

Nagu eespool osutatud, võib vastutav töötleja ühe andmete ülekandmise taotlustele vastamise praktilise moodusena pakkuda nõuetekohaselt turvalist ja dokumenteeritud rakendusliidest. See võib anda üksikisikutele võimaluse esitada vastutavale töötlejale oma isikuandmete taotlusi enda või kolmanda isiku tarkvara kaudu või lubada teistel (sealhulgas teisel vastutaval töötlejal) seda nende nimel teha, nagu on täpsustatud isikuandmete kaitse üldmääruse artikli 20 lõikes 2. Andmete väliselt juurdepääsetava rakendusliidese kaudu juurdepääsu lubamine võib võimaldada pakkuda ka täiustatumat juurdepääsusüsteemi, mille puhul üksikisikud saavad esitada järgnevaid taotlusi andmete saamiseks, et laadida need alla täies ulatuses või deltafunktsioonina, mis sisaldab vaid eelmisest allalaadimisest saadik tehtud muudatusi, ilma et sellised lisataotlused vastutavale töötlejale koormavad oleksid.

#### - **Kuidas saab tagada ülekantavate andmete turvalisuse?**

Isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkti f kohaselt peaksid vastutavad töötlejad üldiselt tagama „isikuandmete asjakohase turvalisuse, sealhulgas [kaitse] loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustamise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid“.

Isikuandmete andmesubjektile edastamisel võivad aga kerkida ka teatavad turvalisusküsimused.

Kuidas saavad vastutavad töötlejad tagada, et isikuandmed turvaliselt õigele isikule edastatakse?

Kuna andmete ülekandmise eesmärk on saada kätte isikuandmed vastutava töötleja infosüsteemist, võib edastamine muutuda nende andmete puhul võimalikuks riskiallikaks (eelkõige võidakse edastamise ajal toime panna andmetega seotud rikkumisi). Vastutav töötleja vastutab kõikide selliste turvameetmete võtmise eest, mis on vajalikud mitte üksnes selleks, et tagada isikuandmete turvaline edastamine (otspunktkrüpteerimise või andmete krüpteerimise teel) õigel aadressil (tõhusate autentimismetmete kasutamise teel), vaid ka selleks, et jätkuvalt kaitsta tema süsteemidesse jäävaid isikuandmeid. Samuti vastutab ta läbipaistvate menetluste eest andmetega seotud võimalike rikkumiste käsitlemisel<sup>37</sup>. Seega

---

<sup>37</sup> Vastavalt direktiivile (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase liidus.

peaksid vastutavad töötajad hindama andmete ülekantavusega seotud konkreetseid riske ja võtma asjakohaseid riskimaandamismeetmeid.

Sellised riskimaandamismeetmed võivad hõlmata järgmist: täiendava autentimisteabe, näiteks ühissaladuse või mõne muu autentimisteguri, nagu ühekordse salasõna kasutamine juhul, kui andmesubjekti on juba vaja autentida; edastamise peatamine või külmutamine juhul, kui on kahtlus, et konto salajasust on kahjustatud; andmete otsese edastamise puhul ühelt vastutavalt töötlejalt teisele tuleks kasutada volitatud autentimist, näiteks läbipääsuloal põhinevat autentimist.

Sellised turvameetmed ei tohi olla oma laadilt tõkestavad ja need ei tohi näiteks lisakulude kehtestamise kaudu takistada kasutajatel teostada oma õigusi.

#### Kuidas saab aidata kasutajatel oma isikuandmeid turvaliselt enda süsteemides säilitada?

Kui kasutajad oma isikuandmed elektroonilisest teenusest kätte saavad, siis on alati oht, et nad võivad neid säilitada vähem turvalistes süsteemides kui see, mida pakub asjaomase teenuse osutaja. Andmeid taotlev andmesubjekt vastutab selle eest, et teha kindlaks õiged meetmed isikuandmete turvalisuse tagamiseks oma süsteemis. Teda tuleb aga sellest teavitada, et tal oleks võimalik võtta meetmeid saadud teabe kaitsmiseks. Et aidata andmesubjektil seda eesmärki täita, võivad vastutavad töötajad levinud tava näitena soovitada ka sobilikku vormingut (sobilikke vorminguid), krüpteerimisvahendeid ja muid turvameetmeid.

\* \* \*

Brüssel, 13. detsember 2016

*Töörühma nimel*  
*esimees*  
*Isabelle FALQUE-PIERROTIN*

Viimati läbi vaadatud ja vastu võetud 5. aprillil  
2017

*Töörühma nimel*  
*esimees*  
*Isabelle FALQUE-PIERROTIN*