



Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet

**Hyväksytty 13. joulukuuta 2016
Viimeksi tarkistettu ja hyväksytty 5. huhtikuuta 2017**

Tietosuojatyöryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojan ja yksityisyyden suojaan liittyviä kysymyksiä. Sen tehtävät määritellään direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa.

Työryhmän sihteeristön tehtävistä huolehtii Euroopan komission oikeus- ja kuluttaja-asioiden pääosaston linja C (perusoikeudet ja oikeusvaltioperiaate), toimisto MO59 05/35, B-1049 Bryssel, Belgia.

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

SISÄLLYSLUETTELO

Tiivistelmä.....	3
I. Johdanto	3
II. Mitkä ovat tietojen järjestelmästä toiseen siirtämisen keskeiset osatekijät?	4
III. Milloin oikeutta tietojen siirtämiseen järjestelmästä toiseen sovelletaan? .	9
IV. Miten rekisteröidyn oikeuksien käyttämistä koskevia yleisiä sääntöjä sovelletaan oikeuteen siirtää tietoja järjestelmästä toiseen?	14
V. Miten järjestelmästä toiseen siirrettävät tiedot on toimitettava?	17

Tiivistelmä

Yleisen tietosuoja-asetuksen 20 artiklalla luodaan uusi tietojen siirtämistä järjestelmästä toiseen koskeva oikeus. Se liittyy läheisesti oikeuteen saada pääsy tietoihin mutta poikkeaa siitä monin tavoin. Sen perusteella rekisteröidyllä on oikeus saada rekisterinpitäjälle toimittamansa itseään koskevat henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle. Tämän uuden oikeuden tarkoituksena on vahvistaa rekisteröidyn vaikutusmahdollisuuksia ja hänen kykyään valvoa henkilötietojaan.

Koska oikeus tietojen siirtämiseen järjestelmästä toiseen mahdollistaa henkilötietojen suoran siirron rekisterinpitäjältä toiselle, se on tärkeä väline myös henkilötietojen vapaan liikkuvuuden tukemiseksi EU:ssa ja rekisterinpitäjien välisen kilpailun edistämiseksi. Se helpottaa palveluntarjoajan vaihtamista ja edistää siten uusien palvelujen kehittämistä digitaalisten sisämarkkinoiden strategian yhteydessä.

Tässä lausunnossa annetaan ohjeita siitä, miten yleisessä tietosuoja-asetuksessa esitettyä oikeutta tietojen siirtämiseen järjestelmästä toiseen on tulkittava ja miten se toteutetaan. Tarkoituksena on käsitellä oikeutta tietojen siirtämiseen järjestelmästä toiseen ja sen soveltamisalaa. Lausunnossa selvennetään uuden oikeuden soveltamisen edellytyksiä ottaen huomioon tietojenkäsittelyn oikeusperusta (joko rekisteröidyn suostumus tai tarpeellisuus sopimuksen täytäntöönpanemiseksi) ja se, että tämä oikeus koskee vain rekisteröidyn toimittamia henkilötietoja. Lausunnossa esitetään myös konkreettisia esimerkkejä ja kriteerejä, jotka kuvaavat sitä, missä olosuhteissa tätä oikeutta voidaan soveltaa. Tältä osin tietosuojatyöryhmä katsoo, että oikeus tietojen siirtämiseen järjestelmästä toiseen kattaa rekisteröidyn tietoisesti ja aktiivisesti toimittamat tiedot sekä hänen toimintansa tuottamat henkilötiedot. Tätä uutta oikeutta ei voi heikentää tai rajoittaa koskemaan henkilötietoja, jotka rekisteröity on antanut suoraan esimerkiksi sähköisellä lomakkeella.

Rekisterinpitäjien olisi hyvänä käytäntönä ryhdyttävä kehittämään rekisteröityjen tietojen siirtämistä järjestelmästä toiseen koskeviin pyyntöihin vastaamisen edistämiseksi erilaisia välineitä, kuten lataustyökaluja tai sovellusliittymiä. Rekisterinpitäjien olisi taattava, että henkilötiedot siirretään jäsennellysti, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja niitä olisi kannustettava varmistamaan tietojen siirtämistä koskevan pyynnön täyttämiseksi käytettyjen tiedostomuotojen yhteentoimivuus.

Lausunnossa autetaan myös rekisterinpitäjiä ymmärtämään selvästi velvollisuutensa ja suositellaan parhaita käytäntöjä ja välineitä, jotka tukevat tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden noudattamista. Lausunnossa suositellaan myös, että alan sidosryhmät ja ammattijärjestöt kehittävät yhdessä yhteentoimivat standardit ja muodot, jotta oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat vaatimukset voidaan täyttää.

I. Johdanto

Yleisen tietosuoja-asetuksen 20 artiklalla otetaan käyttöön uusi tietojen siirtämistä järjestelmästä toiseen koskeva oikeus. Sen perusteella rekisteröidyllä on oikeus saada rekisterinpitäjälle toimittamansa itseään koskevat henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä oikeus siirtää kyseiset tiedot toiselle

rekisterinpitäjälle esteettä. Tämä oikeus koskee rekisteröityä tietyin edellytyksin ja se lisää käyttäjän valinta-, valvonta- ja vaikutusmahdollisuuksia.

Henkilöitä, jotka käyttivät tietosuojadirektiivin 95/46/EY mukaista oikeutta saada pääsy tietoihin, rajoitti rekisterinpitäjän valitsema pyydettyjen tietojen toimitusmuoto. **Uuden tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden tarkoituksena on lisätä rekisteröityjen vaikutusmahdollisuuksia omien henkilötietojensa suhteen, koska se helpottaa henkilötietojen siirtämistä tai kopioimista tietojärjestelmäympäristöstä toiseen** (omiin järjestelmiin, luotettavien kolmansien osapuolten järjestelmiin tai uusien rekisterinpitäjien järjestelmiin).

Oikeus tietojen siirtämiseen järjestelmästä toiseen vahvistaa yksilön henkilökohtaisia oikeuksia ja omien henkilötietojen valvontaa ja tarjoaa myös tilaisuuden korjata rekisteröityjen ja rekisterinpitäjien välisen suhteen tasapaino.¹

Vaikka oikeus henkilötietojen siirtämiseen järjestelmästä toiseen voi lisätä palveluiden välistä kilpailua (helpottamalla palvelun vaihtamista), yleisellä tietosuoja-asetuksella ei ole tarkoitus säädellä kilpailua vaan henkilötietoja. Asetuksen 20 artikla ei rajoita oikeutta tietojen siirtämiseen koskemaan vain niitä tietoja, jotka ovat palvelun vaihtamisen kannalta välttämättömiä tai hyödyllisiä.²

Vaikka oikeus tietojen siirtämiseen järjestelmästä toiseen on uusi, muun tyyppisiä siirtämistä koskevia oikeuksia on jo olemassa tai niistä keskustellaan lainsäädännön muilla osa-alueilla (esimerkiksi sopimuksen päättämisen, viestintäpalvelujen verkkovierailujen ja palvelujen rajatylittävän saannin yhteydessä³). Järjestelmästä toiseen siirtämisen eri muodot voivat luoda synergiaa ja jopa hyötyjä yksittäisille henkilöille, jos niihin sovelletaan yhteensovitettua lähestymistapaa, vaikka analogioihin olisikin suhtauduttava varauksella.

Tässä lausunnossa annetaan rekisterinpitäjille ohjeita siitä, miten ne voivat päivittää käytäntöjään, prosessejaan ja toimintaperiaatteitaan, ja selvennetään, mitä tietojen siirtäminen järjestelmästä toiseen tarkoittaa, jotta rekisteröidyt voivat hyödyntää tehokkaasti uutta oikeuttaan.

II. Mitkä ovat tietojen järjestelmästä toiseen siirtämisen keskeiset osatekijät?

Oikeus tietojen siirtämiseen järjestelmästä toiseen määritellään yleisen tietosuoja-asetuksen 20 artiklan 1 kohdassa seuraavasti:

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu [...].

¹ Tietojen järjestelmästä toiseen siirtämisen ensisijaisena tavoitteena on parantaa yksilön mahdollisuuksia valvoa omia henkilötietojaan ja varmistaa, että yksilöllä on aktiivinen rooli tiedon ekosysteemissä.

² Tämä oikeus voi esimerkiksi mahdollistaa sen, että pankit tarjoavat (käyttäjän valvonnassa) lisäpalveluja käyttäen henkilötietoja, jotka on alun perin kerätty osana energiantoimituspalveluja.

³ Ks. Euroopan komission digitaalisten sisämarkkinoiden strategia: <https://ec.europa.eu/digital-agenda/en/digital-single-market>, erityisesti sen ensimmäinen pilari, joka koskee digitaalisten tuotteiden ja palvelujen saannin parantamista verkossa.

- Oikeus saada henkilötietoja

Ensinnäkin oikeus tietojen siirtämiseen järjestelmästä toiseen tarkoittaa **rekisteröidyn oikeutta saada itseään koskevat rekisterinpitäjän käsittelemät henkilötiedot** ja tallentaa ne henkilökohtaista käyttöä varten. Tallennuspaikka voi olla oma laite tai yksityinen pilvipalvelu, jolloin tietoja ei välttämättä siirretä toiselle rekisterinpitäjälle.

Oikeus tietojen siirtämiseen järjestelmästä toiseen täydentää tässä suhteessa oikeutta saada pääsy tietoihin. Yksi tietojen järjestelmästä toiseen siirtämisen erityispiirre on, että se tarjoaa rekisteröidylle helpon keinon hallita henkilötietojaan itse ja käyttää niitä uudelleen. Nämä tiedot pitäisi saada ”jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa”. Rekisteröity voisi esimerkiksi haluta hakea nykyisen soittolistansa (tai tiedot kuunnelluista kappaleista) musiikin suoratoistopalvelusta selvittääkseen, kuinka monta kertaa hän on kuunnellut tiettyjä kappaleita, tai tarkistaakseen, mitä musiikkia hän haluaa ostaa tai kuunnella toiselta alustalta. Vastaavasti hän voisi myös haluta hakea yhteystietolistansa selainsähköpostisovelluksesta esimerkiksi laatiakseen häävieraslistan, tai saada tietoja eri kanta-asiakaskorteilla tekemistään ostoista arvioidakseen oman hiilijalanjälkensä.⁴

- Oikeus siirtää henkilötietoja rekisterinpitäjältä toiselle

Toiseksi 20 artiklan 1 kohdassa vahvistetaan rekisteröidyn **oikeus siirtää henkilötietoja rekisterinpitäjältä toiselle** rekisterinpitäjän tätä ”estämättä”. Tiedot voidaan siirtää rekisteröidyn pyynnöstä myös suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista (20 artiklan 2 kohta). Tähän liittyen johdanto-osan 68 kappaleessa kannustetaan rekisterinpitäjiä kehittämään yhteentoimivia muotoja, jotka mahdollistavat tietojen järjestelmästä toiseen siirtämisen⁵, luomatta kuitenkaan rekisterinpitäjille velvoitetta hyväksyä tai ylläpitää tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia.⁶ Yleisessä tietosuojasetuksessa kielletään kuitenkin rekisterinpitäjiä luomasta esteitä siirtämiselle.

Perimmiltään tietojen järjestelmästä toiseen siirtämisen avulla rekisteröidyt voivat saada antamansa tiedot ja käyttää niitä uudelleen ja lisäksi siirtää tiedot toiselle rekisterinpitäjälle (joko samalla tai eri alalla toimivalle). Sen lisäksi, että oikeus tietojen siirtämiseen lisää kuluttajan vaikutusmahdollisuuksia estämällä riippuvuussuhteen syntymisen, tämän oikeuden odotetaan edistävän mahdollisuuksia innovointiin ja henkilötietojen jakamiseen rekisterinpitäjien välillä turvallisesti rekisteröidyn valvonnassa.⁷ Tietojen siirtäminen järjestelmästä toiseen voi edistää käyttäjien harjoittamaa hallittua ja rajattua henkilötietojen

⁴ Näissä tapauksissa rekisteröidyn suorittama tietojenkäsittely voi kuulua kotitaloutta koskevaan toimintaan, jos kaikki käsittely tapahtuu yksistään rekisteröidyn valvonnassa, tai sen voi suorittaa toinen osapuoli rekisteröidyn puolesta. Viimeksi mainitussa tapauksessa toista osapuolta on pidettävä rekisterinpitäjänä myös silloin, kun tietoja säilytetään vain henkilökohtaista käyttöä varten, ja sen on noudatettava yleisessä tietosuojasetuksessa vahvistettuja periaatteita ja velvoitteita.

⁵ Ks. myös V osa.

⁶ Sen vuoksi olisi kiinnitettävä erityistä huomiota siirrettävien tietojen muotoon, jotta taataan, että rekisteröity tai toinen rekisterinpitäjä voi käyttää tietoja uudelleen pienellä vaivalla. Ks. myös V osa.

⁷ Ks. useat kokeelliset sovellukset Euroopassa, esimerkiksi [MiData](#) Yhdistyneessä kuningaskunnassa ja [Fingin MesInfos / SelfData](#) Ranskassa.

jakamista organisaatioiden välillä ja siten parantaa palveluja ja asiakaskokemuksia.⁸ Tietojen siirtäminen järjestelmästä toiseen voi helpottaa käyttäjiä koskevien henkilötietojen siirtämistä ja uudelleenkäyttöä erilaisten heitä kiinnostavien palveluiden kesken.

- Rekisterinpito

Tietojen siirtäminen järjestelmästä toiseen takaa oikeuden saada henkilötietoja ja käsitellä niitä rekisteröidyn toiveiden mukaisesti.⁹

Rekisterinpitäjät, jotka vastaavat tietojen siirtämistä koskeviin pyyntöihin 20 artiklassa esitettyjen edellytysten mukaisesti, eivät ole vastuussa henkilötiedot saavan rekisteröidyn tai toisen yrityksen suorittamasta käsittelystä. Rekisterinpitäjät toimivat rekisteröidyn puolesta myös silloin, kun henkilötiedot siirretään suoraan toiselle rekisterinpitäjälle. Tässä suhteessa rekisterinpitäjä ei ole vastuussa siitä, että tiedot vastaanottava rekisterinpitäjä noudattaa tietosuojalainsäädäntöä, koska tiedot lähettävä rekisterinpitäjä ei valitse vastaanottajaa. Samanaikaisesti rekisterinpitäjien on määriteltävä suojatoimet sen varmistamiseksi, että ne toimivat aidosti rekisteröidyn puolesta. Ne voivat esimerkiksi luoda menettelyjä, joilla varmistetaan, että siirretyt henkilötiedot ovat tyypiltään sellaisia, kuin rekisteröity haluaa siirtää. Tämä voidaan tehdä pyytämällä rekisteröidyltä vahvistus ennen siirtoa tai aiemmin ajankohtana, jolloin alkuperäinen suostumus käsittelyyn annetaan tai sopimus tehdään.

Tietojen siirtämistä järjestelmästä toiseen koskevaan pyyntöön vastaavilla rekisterinpitäjillä ei ole erityistä velvollisuutta tarkistaa ja todentaa tietojen laatua ennen niiden siirtämistä. Näiden tietojen pitäisi luonnollisesti olla jo täsmällisiä ja päivitettyjä yleisen tietosuoja-asetuksen 5 artiklan 1 kohdassa esitettyjen periaatteiden mukaisesti. Tietojen siirtäminen järjestelmästä toiseen ei myöskään tarkoita sitä, että rekisterinpitäjä olisi velvollinen säilyttämään henkilötietoja pidempään kuin on tarpeen tai määritellyn säilytysajan jälkeen.¹⁰ Asetuksessa ei ole vaatimusta siitä, että tietoja pitäisi säilyttää tavanomaisia säilytysaikoja pidempään vain tulevien tietojen siirtämistä koskevien pyyntöjen vuoksi.

Silloin kun pyydettyjä henkilötietoja käsittelee henkilötietojen käsittelijä, yleisen tietosuoja-asetuksen 28 artiklan mukaisesti tehtyyn sopimukseen täytyy sisältyä velvollisuus ”auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, (...)” vastaamaan ”pyyntöihin, jotka koskevat (...) rekisteröidyn oikeuksien käyttämistä”. Siksi rekisterinpitäjän olisi otettava käyttöön erityisiä menettelyjä yhteistyössä henkilötietojen käsittelijänsä kanssa tietojen siirtämistä järjestelmästä toiseen koskeviin pyyntöihin vastaamiseksi. Jos on kyse yhteisestä rekisterinpidosta, sopimuksessa olisi jaettava selvästi kunkin rekisterinpitäjän vastuut tietojen siirtämistä koskevien pyyntöjen käsittelyssä.

⁸ Niin sanotun omamittauksen ja esineiden internetin alat ovat osoittaneet, mitä hyötyjä (ja riskejä) on yksilön elämän eri osa-alueisiin, kuten kuntoiluun, aktiivisuuteen ja kaloreiden saantiin, liittyvien henkilötietojen yhdistämisestä yhdeksi tiedostoksi kokonaisvaltaisemman kuvan saamiseksi henkilön elämästä.

⁹ Oikeus tietojen siirtämiseen järjestelmästä toiseen ei rajoitu henkilötietoihin, jotka ovat rekisterinpitäjän kilpailijoiden tarjoamien vastaavien palvelujen kannalta hyödyllisiä ja olennaisia.

¹⁰ Jos edellä esitetyn esimerkin rekisterinpitäjä ei säilytä luetteloa käyttäjän soittamista kappaleista, näitä henkilötietoja ei voida sisällyttää tietojen siirtämistä koskevaan pyyntöön.

Lisäksi vastaanottavan rekisterinpitäjän¹¹ vastuulla on varmistaa, että järjestelmästä toiseen siirrettävät tiedot ovat olennaisia ja etteivät ne ole kohtuuttomia uutta tietojen käsittelyä ajatellen. Jos tietojen siirtämistä järjestelmästä toiseen koskeva pyyntö on esimerkiksi esitetty selainsähköpostipalvelulle ja rekisteröity pyytää itselleen sähköpostiviestejä lähettääkseen ne suojatulle arkistoalustalle, uuden rekisterinpitäjän ei tarvitse käsitellä rekisteröidyn kanssa viestejä vaihtavien yhteystietoja. Jos nämä tiedot eivät ole uuden käsittelyn tarkoituksen kannalta olennaisia, niitä ei pitäisi säilyttää eikä käsitellä. Vastaanottavat rekisterinpitäjät eivät joka tapauksessa ole velvollisia hyväksymään ja käsittelemään henkilötietoja, jotka on siirretty tietojen siirtämistä koskevan pyynnön perusteella. Vastaavasti silloin, kun rekisteröity pyytää siirtämään tiedot pankkitapahtumistaan palvelulle, joka auttaa häntä hänen taloutensa hallinnassa, vastaanottavan rekisterinpitäjän ei tarvitse hyväksyä kaikkia tietoja tai säilyttää kaikkia tietoja tapahtumista sen jälkeen, kun tiedot on valittu uuden palvelun käyttötarkoituksia varten. Toisin sanoen ainoastaan sellaiset tiedot olisi hyväksyttävä ja säilytettävä, jotka ovat vastaanottavan rekisterinpitäjän tarjoaman palvelun kannalta tarpeellisia ja olennaisia.

”Vastaanottavasta” organisaatiosta tulee näiden henkilötietojen uusi rekisterinpitäjä, jonka on noudatettava yleisen tietosuoja-asetuksen 5 artiklassa vahvistettuja periaatteita. Siksi ”uuden” vastaanottavan rekisterinpitäjän on selvästi ja suoraan ilmoitettava uuden käsittelyn tarkoitus ennen kuin tietojen siirtämistä järjestelmästä toiseen koskeva pyyntö esitetään 14 artiklassa vahvistettujen läpinäkyvyysvaatimusten mukaisesti.¹² Rekisterinpitäjän olisi sovellettava samalla tavoin kuin muuhun sen vastuulla olevaan tietojen käsittelyyn 5 artiklassa vahvistettuja periaatteita, jotka ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, eheys ja luottamuksellisuus, säilytyksen rajoittaminen ja osoitusvelvollisuus.¹³

Henkilötietoja säilyttävien rekisterinpitäjien olisi oltava valmiita edistämään rekisteröidyn oikeutta siirtää tiedot järjestelmästä toiseen. Rekisterinpitäjät voivat myös tarvittaessa hyväksyä rekisteröidyn tiedot, mutta niillä ei ole siihen velvollisuutta.

- Oikeus siirtää tietoja järjestelmästä toiseen vs. rekisteröityjen muut oikeudet

Kun henkilö käyttää oikeuttaan siirtää tietoja järjestelmästä toiseen, se ei rajoita minkään muun oikeuden käyttöä (kuten on myös yleisen tietosuoja-asetuksen muiden oikeuksien tapauksessa). Rekisteröity voi edelleen käyttää rekisterinpitäjän palvelua ja hyötyä siitä myös tietojen siirto-operaation jälkeen. Tietojen siirtäminen järjestelmästä toiseen ei automaattisesti käynnistä tietojen poistamista¹⁴ rekisterinpitäjän järjestelmästä eikä vaikuta alkuperäiseen säilytysaikaan, jota sovelletaan siirrettyihin tietoihin. Rekisteröity voi käyttää oikeuksiaan niin kauan kuin rekisterinpitäjä käsittelee tietoja.

¹¹ Rekisterinpitäjä, joka vastaanottaa henkilötiedot rekisteröidyn toiselle rekisterinpitäjälle esittämän tietojen siirtämistä järjestelmästä toiseen koskevan pyynnön mukaisesti.

¹² Uusi rekisterinpitäjä ei myöskään saa käsitellä henkilötietoja, jotka eivät ole olennaisia, ja käsittely on rajoitettava siihen, mikä on uusien käyttötarkoitusten kannalta tarpeen, vaikka henkilötiedot olisivat osa yleisempää tietokokonaisuutta, joka siirretään tietojen siirtämistä järjestelmästä toiseen koskevan prosessin kautta. Henkilötiedot, jotka eivät ole tarpeen uuden käsittelyn tarkoituksen saavuttamiseksi, olisi poistettava mahdollisimman pian.

¹³ Kun rekisterinpitäjä on saanut henkilötiedot, jotka on lähetetty osana oikeutta siirtää tiedot järjestelmästä toiseen, niiden voidaan katsoa olevan rekisteröidyn toimittamia ja ne voidaan siirtää uudelleen tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden perusteella, mikäli muut tähän oikeuteen sovellettavat edellytykset (eli käsittelyn oikeusperusta, ...) täyttyvät.

¹⁴ Yleisen tietosuoja-asetuksen 17 artiklan mukaisesti.

Vastaavasti jos rekisteröity haluaa käyttää oikeuttaan tietojen poistamiseen (17 artiklan mukainen ”oikeus tulla unohdetuksi”), rekisterinpitäjä ei voi käyttää oikeutta tietojen siirtämiseen järjestelmästä toiseen keinona viivyttää tällaista poistamista tai kieltäytyä siitä.

Jos rekisteröity huomaa, että tietojen siirtämistä koskevan oikeuden perusteella pyydetty henkilötiedot eivät vastaa täysin hänen pyyntöään, hänen esittämänsä henkilötietoihin pääsyä koskevaan lisäpyyntöön on vastattava yleisen tietosuoja-asetuksen 15 artiklan mukaisesti.

Jos jollakin unionin tai jäsenvaltion toisen alan säädöksellä säädetään jostakin kyseisten tietojen järjestelmästä toiseen siirtämisen muodosta, kyseisessä säädöksessä vahvistetut edellytykset on myös otettava huomioon täytettäessä yleisen tietosuoja-asetuksen mukaista tietojen siirtämistä koskevaa pyyntöä. Ensinnäkin jos rekisteröidyn esittämästä pyynnöstä käy selvästi ilmi, että hänen tarkoituksenaan ei ole käyttää yleisen tietosuoja-asetuksen mukaisia oikeuksiaan vaan pikemminkin vain alakohtaisen lainsäädännön mukaisia oikeuksiaan, yleisen tietosuoja-asetuksen tietojen siirtämistä järjestelmästä toiseen koskevia säännöksiä ei sovelleta tähän pyyntöön.¹⁵ Toisaalta jos pyyntö kohdistuu yleisen tietosuoja-asetuksen mukaiseen tietojen siirtämiseen järjestelmästä toiseen, tällaisen erityislainsäädännön olemassaolo ei syrjäytä tietojen siirtämistä järjestelmästä toiseen koskevan periaatteen yleistä soveltamista mihin tahansa rekisterinpitäjään, kuten yleisessä tietosuoja-asetuksessa säädetään. Sen sijaan on arvioitava tapauskohtaisesti, vaikuttaako tällainen erityislainsäädäntö oikeuteen siirtää tietoja järjestelmästä toiseen ja miten se vaikuttaa.

III. Milloin oikeutta tietojen siirtämiseen järjestelmästä toiseen sovelletaan?

- Mitkä käsittelytoimet oikeus tietojen siirtämiseen järjestelmästä toiseen kattaa?

Yleisen tietosuoja-asetuksen noudattaminen edellyttää sitä, että rekisterinpitäjillä on selvä henkilötietojen käsittelemistä koskeva oikeusperusta.

Yleisen tietosuoja-asetuksen 20 artiklan 1 kohdan a alakohdan mukaan käsittelytoimet **kuuluvat tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden soveltamisalaan**, jos ne perustuvat

- rekisteröidyn suostumukseen (6 artiklan 1 kohdan a alakohdan nojalla tai 9 artiklan 2 kohdan a alakohdan nojalla, jos on kyse erityisistä henkilötietoryhmistä)
- tai sopimukseen, jossa rekisteröity on osapuolena (6 artiklan 1 kohdan b alakohdan nojalla).

Henkilön verkkokirjakaupasta ostamien kirjojen nimet tai musiikin suoratoistopalvelun kautta kuuntelemat kappaleet ovat esimerkkejä henkilötiedoista, joita oikeus tietojen siirtämiseen järjestelmästä toiseen yleensä koskee, koska niitä käsitellään sellaisen sopimuksen täytäntöönpanon perusteella, jossa rekisteröity on osapuolena.

¹⁵ Jos esimerkiksi rekisteröidyn pyyntö koskee nimenomaisesti hänen pankkitilinsä tapahtumatietoihin pääsyn sallimista tilitietopalvelujen tarjoajalle toisessa maksupalveludirektiivissä vahvistettuihin käyttötarkoituksiin, pääsy on myönnettävä kyseisen direktiivin säännösten mukaisesti.

Yleisessä tietosuoja-asetuksessa ei säädetä yleisestä oikeudesta tietojen siirtämiseen järjestelmästä toiseen tapauksissa, joissa henkilötietojen käsittely ei perustu suostumukseen tai sopimukseen.¹⁶ Esimerkiksi rahoituslaitoksilla ei ole velvollisuutta vastata pyyntöihin, jotka koskevat niiden rahanpesun ja muiden talousrikosten ehkäisemiseen ja paljastamiseen liittyvien velvoitteiden vuoksi käsittelemien henkilötietojen siirtämistä. Oikeus tietojen siirtämiseen järjestelmästä toiseen ei myöskään koske yritysten välisissä liikesuhteissa käsiteltäviä ammattilaisten yhteystietoja tapauksissa, joissa käsittely ei perustu rekisteröidyn suostumukseen tai sopimukseen, jonka osapuoli henkilö on.

Kun on kyse työntekijöiden tiedoista, oikeutta tietojen siirtämiseen järjestelmästä toiseen sovelletaan vain, jos käsittely perustuu sopimukseen, jonka osapuoli rekisteröity on. Monissa tapauksissa suostumusta ei katsota tässä yhteydessä vapaaehtoiseksi työnantajan ja työntekijän välisen vallan epätasapainon vuoksi.¹⁷ Jotkin henkilöstöhallinnon käsittelyt perustuvat sen sijaan oikeudellisen intressin oikeudelliseen perusteeseen tai ovat tarpeen erityisten työsuhteisiin liittyvien oikeudellisten velvoitteiden täyttämiseksi. Käytännössä oikeus tietojen siirtämiseen järjestelmästä toiseen henkilöstöhallinnon yhteydessä koskee väistämättä joitakin käsittelytoimia (kuten palkkoihin ja korvauksiin liittyviä palveluja tai sisäistä rekrytointia), mutta monissa muissa tilanteissa on tapauskohtaisesti varmistettava, täytyvätkö kaikki oikeutta tietojen siirtämiseen koskevat edellytykset.

Oikeutta siirtää tietoja järjestelmästä toiseen sovelletaan vain, jos tietojen käsittely ”suoritetaan automaattisesti”, eikä se siksi kata suurinta osaa paperiasiakirjoja.

- Mitä henkilötietoja on siirrettävä?

Asetuksen 20 artiklan 1 kohdan mukaan tiedot kuuluvat tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden soveltamisalaan, jos ne ovat

- henkilöä itseään koskevia henkilötietoja ja
- hän on *toimittanut* ne rekisterinpitäjälle.

Asetuksen 20 artiklan 4 kohdassa todetaan myös, että tämän oikeuden käyttäminen ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin.

Ensimmäinen edellytys: rekisteröityä koskevat henkilötiedot

¹⁶ Ks. yleisen tietosuoja-asetuksen johdanto-osan 68 kappale ja 20 artiklan 3 kohta. Asetuksen 20 artiklan 3 kohdassa ja johdanto-osan 68 kappaleessa säädetään, että oikeutta tietojen siirtämiseen ei sovelleta, jos tietojen käsittely on tarpeen yleisen edun vuoksi toteutettavan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten tai jos rekisterinpitäjä hoitaa julkisia velvollisuuksiaan tai noudattaa lakisääteistä velvoitetta. Näin ollen rekisterinpitäjillä ei näissä tapauksissa ole mitään velvollisuutta mahdollistaa tietojen siirtämistä järjestelmästä toiseen. On kuitenkin hyvän käytännön mukaista kehittää prosesseja, joilla automatisoidaan tietojen siirtämistä koskeviin pyyntöihin vastaaminen oikeutta tietojen siirtämiseen koskevien periaatteiden mukaisesti. Yksi esimerkki tästä olisi valtion palvelu, jonka avulla voisi helposti ladata aiemmat henkilökohtaisen tuloverotuksen tiedot. Tietojen siirtämistä järjestelmästä toiseen hyvänä käytäntönä silloin, kun on kyse käsittelystä, jonka oikeudellinen peruste on välttämättömyys oikeutetun intressin ja olemassa olevien vapaaehtoisten järjestelmien vuoksi, käsitellään tietosuojatyöryhmän oikeutettuja intressejä koskevan lausunnon 6/2014 (WP 217) sivuilla 47 ja 48.

¹⁷ Kuten tietosuojatyöryhmä esitti 13. syyskuuta 2001 antamassaan lausunnossa 8/2001 (WP 48).

Vain henkilötiedot kuuluvat tietojen siirtämistä järjestelmästä toiseen koskevan pyynnön soveltamisalaan. Siksi tiedot, jotka ovat anonyymejä¹⁸ tai eivät koske rekisteröityä, eivät kuulu sen soveltamisalaan. Soveltamisalaan kuuluvat kuitenkin pseudonymisoidut tiedot, jotka voidaan helposti yhdistää rekisteröityyn (esimerkiksi niin, että hän toimittaa asiaankuuluvan tunnusteen, vrt. 11 artiklan 2 kohta).

Rekisterinpitäjät käsittelevät monissa tilanteissa tietoja, jotka sisältävät useiden eri rekisteröityjen henkilötietoja. Tällaisessa tapauksessa rekisterinpitäjien ei pitäisi tulkita liian tiukasti ilmausta ”rekisteröityä koskevat henkilötiedot”. Esimerkiksi puhelu-, sanomanvälitys- tai internetpuhelutietueet voivat sisältää (tilaajan tilitiedoissa) tietoja tulevien tai lähtevien puhelujen kolmansista osapuolista. Vaikka tietueissa on näin ollen useita henkilöitä koskevia henkilötietoja, tilaajien olisi voitava saada nämä tietueet vastauksena tietojen siirtämistä järjestelmästä toiseen koskeviin pyyntöihin, koska tietueet koskevat (myös) rekisteröityä. Jos tällaiset tietueet siirretään sitten uudelle rekisterinpitäjälle, tämä uusi rekisterinpitäjä ei saisi käsitellä niitä mihinkään sellaiseen tarkoitukseen, joka voisi vaikuttaa epäedullisesti kolmansien osapuolten oikeuksiin ja vapauksiin (ks. kolmas edellytys jäljempänä).

Toinen edellytys: rekisteröidyn toimittamat tiedot

Toinen edellytys supistaa soveltamisalan rekisteröidyn ”toimittamiin” tietoihin.

On useita esimerkkejä henkilötiedoista, jotka rekisteröity ”toimittaa” tietoisesti ja aktiivisesti, kuten verkkolomakkeiden kautta annettavat tilitiedot (esimerkiksi postiosoite, käyttäjänimi ja ikä). Rekisteröidyn ”toimittamat” tiedot voivat myös olla hänen toimintansa havainnoinnin tulosta. Siksi tietosuojatyöryhmä katsoo, että tämän uuden oikeuden täysimääräinen hyödyntäminen edellyttää sitä, että ”toimittaminen” koskee myös henkilötietoja, jotka ovat käyttäjän toiminnan havainnoinnin tulosta, kuten älymittarin tai muun tyyppisten liitettyjen laitteiden¹⁹ käsittelemät raakatiedot, toimintalokit, verkkosivuston käyttöhistoria tai tehdyt haut.

Jälkimmäinen tietoryhmä ei sisällä tietoja, jotka rekisterinpitäjä luo (käyttäen havainnoituja tietoja tai suoraan toimitettuja tietoja), kuten käyttäjäprofiili, joka luodaan analysoimalla älymittarilla kerätty raakatiedot.

Eri tietoryhmät voidaan erottaa toisistaan niiden alkuperän mukaan, jotta voidaan määrittää, koskeeko oikeus tietojen siirtämiseen niitä. Seuraavat ryhmät voidaan määritellä ”rekisteröidyn toimittamiksi” tiedoiksi:

- **Rekisteröidyn aktiivisesti ja tietoisesti toimittamat tiedot** (esimerkiksi postiosoitteet, käyttäjänimi ja ikä).
- **Havainnoidut tiedot, jotka rekisteröity on toimittanut käyttämällä palvelua tai laitetta.** Näitä voivat olla esimerkiksi henkilön hakuhistoria, liikennetiedot ja sijaintitiedot. Ne voivat sisältää myös muita raakatietoja, kuten sydämen sykettä tarkkailevan puettavan laitteen tallentamat tiedot.

¹⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf

¹⁹ Kun rekisteröity voi hakea toimintansa havainnoinnin tuloksena saadut tiedot, hänen on myös helpompi saada kuva rekisterinpitäjän tekemistä havainnoitujen tietojen laajuutta koskevista valinnoista ja hänen on helpompi valita, mitä tietoja hän haluaa toimittaa vastaavan palvelun saadakseen. Silloin hän on myös tietoinen siitä, miten pitkälle hänen oikeuttaan yksityisyyteen kunnioitetaan.

Sitä vastoin rekisterinpitäjä luo pääteltyjä tietoja ja johdettuja tietoja ”rekisteröidyn toimittamien” tietojen perusteella. Esimerkiksi käyttäjän terveyttä koskevan arvioinnin tulosta tai riskinhallinnan ja rahoitussäännösten yhteydessä (esimerkiksi luottoluokituksen antamiseksi tai rahanpesun torjuntaa koskevien sääntöjen noudattamiseksi) luotua profiilia ei itsessään voida pitää rekisteröidyn ”toimittamana”. Vaikka tällaiset tiedot voivat olla osa rekisterinpitäjän ylläpitämää profiilia ja ne on päätelty tai johdettu analysoimalla rekisteröidyn (esimerkiksi toimiensa kautta) toimittamia tietoja, niiden ei yleensä katsota olevan ”rekisteröidyn toimittamia” eivätkä ne siksi kuulu uuden oikeuden soveltamisalaan.²⁰

Ottaen huomioon oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat poliittiset tavoitteet, termiä ”rekisteröidyn toimittama” on tulkittava laajasti ja sen ulkopuolelle olisi jätettävä ”päätelty tiedot” ja ”johdetut tiedot”, joihin kuuluvat rekisterinpitäjän luomat henkilötiedot (esimerkiksi algoritmien tulokset). Rekisterinpitäjä voi jättää nämä päätellyt tiedot pois, mutta sen olisi otettava mukaan kaikki muut henkilötiedot, jotka rekisteröity on toimittanut rekisterinpitäjän tarjoamien teknisten välineiden avulla.²¹

Näin ollen termi ”toimittama” kattaa henkilötiedot, jotka liittyvät rekisteröidyn toimintaan tai saadaan henkilön käyttäytymisen havainnoinnin tuloksena, mutta se ei kata tietoja, jotka saadaan kyseisen käyttäytymisen myöhemmän analysoinnin tuloksena. Sitä vastoin henkilötiedot, jotka rekisterinpitäjä on luonut osana tietojen käsittelyä, esimerkiksi yksilöinti- tai suositusprosessissa tai käyttäjiä luokittelemalla tai profiloimalla, ovat tietoja, jotka on johdettu tai päätelty rekisteröidyn toimittamista henkilötiedoista eikä oikeus tietojen siirtämiseen järjestelmästä toiseen kata niitä.

Kolmas edellytys: oikeus tietojen siirtämiseen järjestelmästä toiseen ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin

Muita rekisteröityjä koskevat henkilötiedot:

Kolmannen edellytyksen tarkoituksena on välttää muiden rekisteröityjen (jotka eivät ole antaneet siihen suostumustaan) henkilötietoja sisältävien tietojen hakeminen ja siirtäminen uudelle rekisterinpitäjälle silloin, kun näitä tietoja todennäköisesti käsitellään tavalla, joka voisi vaikuttaa haitallisesti muiden rekisteröityjen oikeuksiin ja vapauksiin (yleisen tietosuojasetuksen 20 artiklan 4 kohta).²²

²⁰ Rekisteröidyllä on silti yhä ”oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin” sekä tieto automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolosta, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle yleisen tietosuojasetuksen 15 artiklan mukaisesti (joka koskee oikeutta saada pääsy tietoihin).

²¹ Niihin kuuluvat kaikki rekisteröidystä sellaisen toimien aikana havainnoidut tiedot, joita varten tietoja kerätään, kuten tapahtumatiedot tai käyttöpäiväkirja. Rekisteröidyn tarkkailun ja jäljityksen aikana kerättyjä tietoja (esimerkiksi sovelluksella, joka tallentaa sydämen sykkeen, tai teknologialla, jolla tarkkaillaan selailukäyttäytymistä), on myös pidettävä hänen ”toimittaminaan”, vaikka tietoja ei ole siirretty aktiivisesti tai tietoisesti.

²² Johdanto-osan 68 kappaleessa säädetään, että ”jos tietyssä henkilötietoja sisältävässä tietojoukossa tiedot koskevat useampia kuin yhtä rekisteröityä, oikeus vastaanottaa henkilötietoja ei saisi rajoittaa toisten rekisteröityjen tämän asetuksen mukaisia oikeuksia ja vapauksia”.

Tällainen haittavaikutus ilmenisi esimerkiksi silloin, jos tietojen siirtäminen rekisterinpitäjältä toiselle estäisi kolmansia osapuolia käyttämästä yleisen tietosuoja-asetuksen mukaisia oikeuksiaan rekisteröityinä (kuten oikeuksia tiedon saantiin tai tietoihin pääsyyn).

Rekisteröity, joka käynnistää tietojensa siirtämisen toiselle rekisterinpitäjälle, antaa uudelle rekisterinpitäjälle suostumuksensa käsittelyyn tai tekee sopimuksen tämän rekisterinpitäjän kanssa. Jos tiedosto sisältää kolmansien osapuolten henkilötietoja, käsittelylle on määriteltävä jokin muu oikeusperusta. Rekisterinpitäjällä voi esimerkiksi olla 6 artiklan 1 kohdan f alakohdan mukainen oikeutettu etu, erityisesti jos rekisterinpitäjän tarkoituksena on tarjota rekisteröidylle palvelu, jonka avulla tämä voi käsitellä henkilötietoja pelkästään henkilökohtaisena tai kotitaloutta koskevana toimintana. Rekisteröidyn henkilökohtaisen toiminnan yhteydessä käynnistämät käsittelytoimet, jotka koskevat kolmansia osapuolia ja mahdollisesti vaikuttavat niihin, ovat edelleen hänen vastuullaan, mikäli rekisterinpitäjä ei ole millään tavalla päättänyt tällaisesta käsittelystä.

Esimerkiksi selainsähköpostipalvelu voi sallia rekisteröidyn yhteystietojen, ystävien, sukulaisten, perheen ja laajemman piirin tiedot sisältävän hakemiston luomisen. Koska nämä tiedot liittyvät tunnistettavaan henkilöön, joka haluaa käyttää oikeuttaan siirtää tietoja järjestelmästä toiseen (ja ovat hänen luomiaan), rekisterinpitäjän olisi siirrettävä koko saapuvien ja lähtevien sähköpostiviestien hakemisto kyseiselle rekisteröidylle.

Vastaavasti rekisteröidyn pankkitili voi sisältää henkilötietoja, jotka liittyvät tilinhaltijan tapahtumien lisäksi myös muiden henkilöiden tapahtumiin (jos he ovat esimerkiksi siirtäneet rahaa tilinhaltijalle). Pankkitilitietojen siirtäminen tilinhaltijalle ei todennäköisesti vaikuttaisi haitallisesti näiden kolmansien osapuolten oikeuksiin ja vapauksiin, kun tietojen siirtämistä koskeva pyyntö on esitetty, mikäli tietoja käytetään kummassakin esimerkissä samaan tarkoitukseen (eli vain rekisteröidyn käyttämä yhteysosoite tai rekisteröidyn pankkitilin tapahtumatiedot).

Sitä vastoin kolmansien osapuolten oikeuksia ja vapauksia ei kunnioiteta, jos uusi rekisterinpitäjä käyttää henkilötietoja muihin tarkoituksiin, kuten jos vastaanottava rekisterinpitäjä käyttää rekisteröidyn yhteystietohakemistoon sisältyvien muiden henkilöiden henkilötietoja markkinointitarkoituksiin.

Kolmansiin osapuoliin kohdistuvien haittavaikutusten estämiseksi toinen rekisterinpitäjä saa käyttää tällaisia henkilötietoja ainoastaan, jos tiedot pysyvät yksistään ne pyytäneen käyttäjän valvonnassa ja niitä hallinnoidaan pelkästään henkilökohtaisia tai kotitalouden tarpeita varten. Vastaanottava uusi rekisterinpitäjä (jolle tiedot voidaan siirtää käyttäjän pyynnöstä) ei saa käyttää siirrettyjä kolmannen osapuolen tietoja omiin tarkoituksiinsa, esimerkiksi markkinointituotteiden tai -palveluiden esittelemiseen näille muille kolmannen osapuolen asemassa oleville rekisteröidyille. Näitä tietoja ei esimerkiksi pitäisi käyttää kolmannen osapuolen asemassa olevan rekisteröidyn profiilin parantamiseen ja hänen sosiaalisen ympäristönsä rakentamiseen uudelleen ilman, että hän on siitä tietoinen ja antaa siihen suostumuksensa.²³ Niitä ei myöskään voida käyttää tällaisia kolmansia osapuolia koskevien tietojen hakemiseen ja erityisprofiilien luomiseen, vaikka heidän henkilötietonsa olisivat jo rekisterinpitäjän hallussa. Muutoin tällainen käsittely on todennäköisesti laitonta ja

²³ Sosiaalisen verkostopalvelun ei pitäisi parantaa jäsentensä profiileja käyttämällä henkilötietoja, jotka rekisteröity on siirtänyt osana oikeuttaan siirtää tietoja järjestelmästä toiseen, jos ne eivät noudata läpinäkyvyyssperiaattia ja varmista myös, että tällä erityiskäsittelyllä on asianmukainen oikeusperusta.

epäoikeudenmukaista, varsinkin jos kyseiset kolmannet osapuolet eivät ole tietoisia oikeuksistaan rekisteröityinä eivätkä voi käyttää näitä oikeuksia.

Kaikkien rekisterinpitäjien (sekä ”lähettävien” että ”vastaanottavien” osapuolten) johtavana käytäntönä on ottaa käyttöön välineitä, joiden avulla rekisteröidyt voivat valita asiaankuuluvat vastaanotettavat ja siirrettävät tiedot sekä jättää tarvittaessa pois muiden henkilöiden tiedot. Tämä auttaa edelleen vähentämään niiden kolmansien osapuolten riskejä, joiden henkilötietoja saatetaan siirtää.

Lisäksi rekisterinpitäjien olisi otettava käyttöön suostumusmekanismeja muita osallisena olevia rekisteröityjä varten tietojen siirtämisen helpottamiseksi tapauksissa, joissa tällaiset osapuolet haluavat antaa suostumuksensa esimerkiksi tietojensa siirtämiseen jollekin toiselle rekisterinpitäjälle. Tällainen tilanne saattaa syntyä esimerkiksi sosiaalisten verkostojen yhteydessä. Silloin rekisterinpitäjä saa päättää, mitä johtavaa käytäntöä se noudattaa.

Tekijänoikeuksien ja liikesalaisuuksien kattamat tiedot:

Muiden oikeudet ja vapaudet on mainittu 20 artiklan 4 kohdassa. Vaikka ne eivät liity suoraan tietojen siirtämiseen järjestelmästä toiseen, niihin voidaan katsoa sisältyvän ”esimerkiksi liikesalaisuudet tai henkinen omaisuus ja erityisesti ohjelmistojen tekijänoikeudet”. Vaikka nämä oikeudet olisi otettava huomioon, ennen kuin vastataan tietojen siirtämistä järjestelmästä toiseen koskevaan pyyntöön, ”näiden seikkojen huomioon ottaminen ei kuitenkaan saisi johtaa siihen, että rekisteröidylle ei anneta minkäänlaista tietoa”. Rekisterinpitäjä ei myöskään saisi hylätä tietojen siirtämistä koskevaa pyyntöä muiden sopimusoikeuksien loukkaamisen (esimerkiksi maksamattoman velan tai rekisteröidyn kanssa käydyn kauppakiistan) perusteella.

Oikeus siirtää tietoja järjestelmästä toiseen ei tarkoita henkilön oikeutta käyttää tietoja väärin tavalla, joka voitaisiin määritellä sopimattomaksi käytännöksi tai joka rikkoisi teollis- ja tekijänoikeuksia.

Mahdollinen liiketoimintariski ei kuitenkaan voi itsessään olla perusteena kieltäytymiselle tietojen siirtämistä koskevaan pyyntöön vastaamisesta, ja rekisterinpitäjät voivat siirtää rekisteröityjen henkilötietoja muodossa, joka ei paljasta liikesalaisuuksia tai teollis- tai tekijänoikeuksia.

IV. Miten rekisteröidyn oikeuksien käyttämistä koskevia yleisiä sääntöjä sovelletaan oikeuteen siirtää tietoja järjestelmästä toiseen?

- Mitä ennakkotietoja on toimitettava rekisteröidylle?

Uuden tietojen siirtämistä järjestelmästä toiseen koskevan oikeuden noudattamiseksi rekisterinpitäjien on ilmoitettava rekisteröidylle tämän uuden oikeuden olemassaolosta. Silloin kun kyseiset henkilötiedot kerätään suoraan rekisteröidyltä, tämän on tapahduttava ”silloin, kun henkilötietoja saadaan”. Jos henkilötietoja ei ole saatu rekisteröidyltä, rekisterinpitäjän on toimitettava tiedot 13 artiklan 2 kohdan b alakohdan ja 14 artiklan 2 kohdan c alakohdan mukaisesti.

”Kun tietoja ei ole saatu rekisteröidyltä”, 14 artiklan 3 kohdassa vaaditaan toimittamaan tiedot kohtuullisessa ajassa viimeistään yhden kuukauden kuluttua tietojen saamisesta, silloin kun

rekisteröityyn ollaan yhteydessä ensimmäisen kerran tai kun tiedot luovutetaan kolmansille osapuolille.²⁴

Kun rekisterinpitäjät toimittavat pyydetty tiedot, niiden on varmistettava, että oikeus tietojen siirtämiseen järjestelmästä toiseen erotetaan muista oikeuksista. Siksi tietosuojatyöryhmä suosittelee erityisesti, että rekisterinpitäjät selittävät selvästi niiden tietojen välisen eron, jotka rekisteröity voi saada tietoon pääsyä ja tietojen siirtämistä koskevien oikeuksien perusteella.

Lisäksi työryhmä suosittelee, että rekisterinpitäjät antavat aina rekisteröidylle tiedon oikeudesta tietojen siirtämiseen järjestelmästä toiseen, ennen kuin tämä sulkee tilinsä. Näin käyttäjät voivat tarkastella henkilötietojaan ja siirtää tiedot helposti omaan laitteeseensa tai toiselle palveluntarjoajalle ennen sopimuksen päättymistä.

Lopuksi tietosuojatyöryhmä suosittelee ”vastaanottavia” rekisterinpitäjiä ottamaan johtavaksi käytännöksi sen, että ne antavat rekisteröidylle kaikki tiedot palvelujensa suorittamisen kannalta olennaisten henkilötietojen luonteesta. Tämä tukee asianmukaista käsittelyä ja mahdollistaa sen, että käyttäjät voivat rajoittaa kolmansien osapuolten riskiä ja myös henkilötietojen tarpeettomia päällekkäisyyksiä, vaikka asiaan ei liittyisi muita rekisteröityjä.

- Miten rekisterinpitäjä voi tunnistaa rekisteröidyn ennen hänen pyyntöönsä vastaamista?

Yleisessä tietosuoja-asetuksessa ei ole säännöksiä siitä, miten rekisteröidyn henkilöllisyys on todennettava. Asetuksen 12 artiklan 2 kohdassa kuitenkin todetaan, että rekisterinpitäjä ei saa kieltäytyä toimimasta rekisteröidyn pyynnöstä oikeuksien (myös oikeuden tietojen siirtämiseen järjestelmästä toiseen) käyttämiseksi, ellei se käsittele henkilötietoja sellaiseen tarkoitukseen, joka ei edellytä rekisteröidyn tunnistamista, ja voi osoittaa, ettei se pysty tunnistamaan rekisteröityä. Asetuksen 11 artiklan 2 kohdan mukaan rekisteröity voi tällaisissa tilanteissa toimittaa lisätietoja, joiden avulla hänet voidaan tunnistaa. Lisäksi 12 artiklan 6 kohdassa säädetään, että jos rekisterinpitäjällä on perusteltua syytä epäillä rekisteröidyn henkilöllisyyttä, se voi pyytää lisätietoja rekisteröidyn henkilöllisyyden vahvistamiseksi. Jos rekisteröity toimittaa lisätiedot, joiden avulla hänet voidaan tunnistaa, rekisterinpitäjä ei saa kieltäytyä suorittamasta pyydettyä toimea. Jos verkossa kerätyt tiedot on yhdistetty pseudonyymeihin tai yksilöllisiin tunnisteisiin, rekisterinpitäjät voivat ottaa käyttöön asianmukaiset menettelyt, joiden avulla henkilö voi esittää tietojen siirtämistä järjestelmästä toiseen koskevan pyynnön ja vastaanottaa itseensä liittyviä tietoja. Rekisterinpitäjien on joka tapauksessa otettava käyttöön todentamismenettely voidakseen varmasti tunnistaa rekisteröidyn, joka pyytää henkilötietojaan tai käyttää yleisemmin yleisen tietosuoja-asetuksen mukaisia oikeuksiaan.

Nämä menettelyt ovat usein jo olemassa. Rekisterinpitäjä on usein jo todentanut rekisteröidyn henkilöllisyyden ennen sopimuksen tekemistä tai käsittelyä koskevan suostumuksen saamista häneltä. Silloin henkilötietoja, joita on käytetty kyseisen henkilön rekisteröintiin, voidaan

²⁴ Asetuksen 12 artiklassa vaaditaan, että rekisterinpitäjät toimittavat ”[...] tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä varsinkin silloin, kun tiedot on tarkoitettu erityisesti lapselle”.

käyttää myös todisteena rekisteröidyn henkilöllisyyden tunnustamiseksi tietojen siirtämistä varten.²⁵

Näissä tapauksissa rekisteröidyn ennakkotunnistus voi edellyttää pyyntöä hänen oikeushenkilöllisyytensä todistamiseksi, mutta tällainen varmistaminen ei välttämättä ole tietojen ja kyseisen henkilön välisen yhteyden arvioimisen kannalta olennaista, koska tällainen yhteys ei liity viralliseen henkilöllisyyteen tai oikeushenkilöllisyyteen. Periaatteessa rekisterinpitäjän mahdollisuus lisätietojen pyytämiseen henkilöllisyyden arvioimista varten ei voi johtaa kohtuuttomiin vaatimuksiin ja sellaisten henkilötietojen keräämiseen, jotka eivät ole olennaisia tai tarpeellisia henkilön ja pyydettyjen henkilötietojen välisen yhteyden vahvistamiseksi.

Usein tällaisia menettelyjä on jo käytössä. Henkilöt voivat esimerkiksi käyttäjänimien ja salasanojen avulla usein saada käyttöönsä tietoja sähköpostitileistään, verkkoyhteisöpalvelujen tileistään ja erilaisiin muihin palveluihin käytettävistä tileistään, joita jotkut käyttävät paljastamatta koko nimeään ja henkilöllisyytään.

Jos siirtäminen internetin kautta on rekisteröidyn pyytämien tietojen koon vuoksi ongelmallista, rekisterinpitäjä voi joutua harkitsemaan tietojen antamiseen muitakin vaihtoehtoisia keinoja, kuten suoratoistopalvelut tai tallentaminen CD- tai DVD-levylle tai muuhun fyysiseen mediaan, tai mahdollistamaan henkilötietojen siirtämisen suoraan toiselle rekisterinpitäjälle (yleisen tietosuoja-asetuksen 20 artiklan 2 kohdan mukaisesti, jos se on teknisesti mahdollista) sen sijaan, että varaisi enintään kolme kuukautta pidemmän ajan pyyntöön vastaamiseen.²⁶

- Mikä on tietojen siirtämistä järjestelmästä toiseen koskevaan pyyntöön vastaamisen aikaraja?

Tietosuoja-asetuksen 12 artiklan 3 kohdassa edellytetään, että rekisterinpitäjän on toimitettava rekisteröidylle ”tiedot toimenpiteistä, joihin on ryhdytty [...] ilman aiheetonta viivytystä” ja joka tapauksessa ”kuukauden kuluessa pyynnön vastaanottamisesta”. Tämä yhden kuukauden ajanjakso voidaan pidentää enintään kolmeen kuukauteen monimutkaisissa tapauksissa, jos rekisteröidylle on ilmoitettu tällaisen viivästyksen syistä kuukauden kuluessa alkuperäisestä pyynnöstä.

Tietoyhteiskunnan palveluja tarjoavat rekisterinpitäjät pystyvät todennäköisesti paremmin noudattamaan pyyntöjä hyvin lyhyessä ajassa. Käyttäjien odotusten täyttämiseksi on hyvän käytännön mukaan määriteltävä määräaika tietojen siirtämistä koskevaan pyyntöön vastaamiselle ja ilmoitettava siitä rekisteröidylle.

Rekisterinpitäjien, jotka kieltäytyvät vastaamasta tietojen siirtämistä koskevaan pyyntöön, on 12 artiklan 4 kohdan mukaan ilmoitettava rekisterinpitäjälle ”syyt siihen ja kerrottava mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja” yhden kuukauden kuluessa pyynnön vastaanottamisesta.

²⁵ Jos esimerkiksi tietojen käsittely on yhteydessä käyttäjätiliin, asiaankuuluvan käyttäjätunnuksen ja salasanan antaminen saattaisi riittää rekisteröidyn tunnustamiseen.

²⁶ Asetuksen 12 artiklan 3 kohta: ”Rekisterinpitäjän on toimitettava rekisteröidylle tiedot toimenpiteistä, joihin on ryhdytty [...] pyynnön johdosta”.

Rekisterinpitäjien on noudatettava velvollisuutta vastata määräajassa, vaikka kyse olisi kieltäytymisestä. Toisin sanoen rekisterinpitäjä ei voi olla hiljaa, kun sitä pyydetään vastaamaan tietojen siirtämistä koskevaan pyyntöön.

- **Missä tapauksissa tietojen siirtämistä koskeva pyyntö voidaan evätä tai milloin siitä voidaan periä maksu?**

Yleisen tietosuojasetuksen 12 artiklassa kielletään rekisterinpitäjää perimästä maksua henkilötietojen toimittamisesta, ellei rekisterinpitäjä voi osoittaa, että pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, ”erityisesti jos niitä esitetään toistuvasti”. Tietoyhteiskuntapalvelut, jotka erikoistuvat henkilötietojen automaattiseen käsittelyyn ja ottavat käyttöön sovellusliittymien (API)²⁷ kaltaisia automaattisia toteutusjärjestelmiä, voivat auttaa vaihtamaan tietoja rekisteröidyn kanssa, mikä vähentää toistuvien pyyntöjen aiheuttamaa mahdollista rasitetta. Siksi on hyvin harvoja tapauksia, joissa rekisterinpitäjä voi perustellusti kieltäytyä toimittamasta pyydettyjä tietoja. Tämä koskee myös moninkertaisia tietojen siirtämistä koskevia pyyntöjä.

Lisäksi tietojen siirtämistä koskeviin pyyntöihin vastaamista varten luotujen prosessien kokonaiskustannuksia ei pitäisi ottaa huomioon määritettäessä pyynnön kohtuuttomuutta. Yleisen tietosuojasetuksen 12 artikla koskeekin yhden rekisteröidyn esittämiä pyyntöjä eikä rekisterinpitäjän vastaanottamien pyyntöjen kokonaismäärää. Siksi järjestelmän toteutuksen kokonaiskustannuksia ei pitäisi periä rekisteröidyltä eikä niillä pitäisi perustella kieltäytymistä tietojen siirtämistä koskeviin pyyntöihin vastaamisesta.

V. Miten järjestelmästä toiseen siirrettävät tiedot on toimitettava?

- **Mitä keinoja rekisterinpitäjän odotetaan ottavan käyttöön tietojen toimittamista varten?**

Yleisen tietosuojasetuksen 20 artiklan 1 kohdassa säädetään, että rekisteröidyillä on oikeus siirtää tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu.

Tällaisesta estämisestä on kyse silloin, kun rekisterinpitäjä asettaa mitä tahansa oikeudellisia, teknisiä tai taloudellisia esteitä estääkseen rekisteröityä tai toista rekisterinpitäjää saamasta, siirtämästä tai käyttämästä uudelleen tietoja tai hidastaakseen sitä. Tällaisia esteitä voisivat olla esimerkiksi tietojen toimittamisesta vaaditut maksut, yhteentoimivuuden puute, se, että jokin tiedostomuoto, sovellusliittymä tai toimitettujen tietojen tallennusmuoto ei ole käytettävissä, koko tietoaaineiston hakemisen kohtuuton viivästyminen tai monimutkaisuus, tietoaaineiston tahallinen piilottaminen tai erityiset ja aiheettomat tai kohtuuttomat alakohtaiset standardointi- tai akkreditointivaatimukset.²⁸

²⁷ Sovellusliittymä (API) tarkoittaa sovellusten tai verkkopalvelujen liittymiä, jotka rekisterinpitäjät ovat tarjonneet käytettäväksi niin, että muut järjestelmät tai sovellukset voivat linkittää niiden järjestelmiin ja työskennellä niiden kanssa.

²⁸ Joitakin oikeutettuja esteitä saattaa esiintyä, kuten esteitä, jotka liittyvät 20 artiklan 4 kohdassa mainittuihin muiden oikeuksiin ja vapauksiin tai rekisterinpitäjän omien järjestelmien turvallisuuteen. Rekisterinpitäjän vastuulla on perustella, miksi tällaiset esteet olisivat oikeutettuja ja miksi ne eivät muodosta 20 artiklan 1 kohdassa tarkoitettua estettä.

Asetuksen 20 artiklan 2 kohdassa säädetään myös rekisterinpitäjien velvollisuudesta siirtää tiedot suoraan muille rekisterinpitäjille, ”jos se on teknisesti mahdollista”.

Sitä, onko tietojen siirtäminen rekisterinpitäjältä toiselle rekisteröidyn valvonnassa teknisesti mahdollista, on arvioitava tapauskohtaisesti. Johdanto-osan 68 kappaleessa selvennetään tarkemmin, mitä tarkoittaa ”teknisesti mahdollista”, ja todetaan, että se ”ei saisi luoda rekisterinpitäjille velvoitetta hyväksyä tai ylläpitää tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia”.

Rekisterinpitäjien edellytetään siirtävän henkilötiedot yhteensopivassa muodossa, mutta ei velvoiteta muita rekisterinpitäjiä tukemaan näitä muotoja. Tiedot voidaan siirtää rekisterinpitäjältä toiselle suoraan silloin, kun kahden järjestelmän välinen tietoliikenne on mahdollista suojatusti²⁹ ja kun vastaanottava järjestelmä on teknisesti sellainen, että siihen voidaan vastaanottaa tulevat tiedot. Jos jotkin tekniset seikat estävät suoran siirron, rekisterinpitäjän on selitettävä ne rekisteröidylle, koska rekisterinpitäjän päätöksellä on muuten samanlainen vaikutus kuin kieltäytymisellä rekisteröidyn pyynnön noudattamisesta (12 artiklan 4 kohta).

Teknisellä tasolla rekisterinpitäjien olisi tarkasteltava ja arvioitava kahta toisiaan täydentävää erilaista tapaa siirrettävien tietojen tarjoamiseksi rekisteröityjen tai muiden rekisterinpitäjien saataville:

- siirrettävien tietojen koko tietoaaineiston (tai koko tietoaaineistosta poimittujen useiden otteiden) suora siirto
- automaattinen väline, joka mahdollistaa olennaisten tietojen poimimisen.

Rekisterinpitäjät saattavat pitää parempana toiseksi mainittua keinoa tapauksissa, joihin liittyy monimutkaisia ja suuria tietoaaineistoja, koska se mahdollistaa minkä tahansa osan poimimisen tietoaaineistosta, joka on rekisteröidyn pyynnön kannalta olennainen, saattaa auttaa minimoimaan riskin ja voi mahdollistaa tietojen synkronointimekanismien käytön³⁰ (esimerkiksi rekisterinpitäjien välisen säännöllisen tietoliikenteen yhteydessä). Se voi olla parempi keino varmistaa yhteensopivuus ”uuden” rekisterinpitäjän kanssa ja toimisi hyvänä käytäntönä, jolla vähennetään alkuperäisen rekisterinpitäjän osalta yksityisyydensuojaa koskevia riskejä.

Näitä kahta erilaista ja mahdollisesti toisiaan täydentävää tapaa toimittaa asiaankuuluvat tiedot voidaan täydentää tarjoamalla tiedot saataville eri keinoilla, kuten turvatus sanomavälityksen, SFTP-palvelimen, turvatus WebAPI:n tai WebPortalin kautta. Rekisteröityjen pitäisi voida hyödyntää henkilötietovarastoa, henkilökohtaisten tietojen hallintajärjestelmää³¹ tai muunlaisia luotettavia kolmansia osapuolia henkilötietojen säilyttämiseen ja tallentamiseen ja tarvittaessa henkilötietojen saamista ja käsittelyä koskevan luvan myöntämiseen rekisterinpitäjille.

²⁹ Käyttäen todennettua tietoliikennettä, jossa tiedot on riittävän hyvin salattu.

³⁰ Synkronointimekanismi voi auttaa täyttämään yleisen tietosuojasetuksen 5 artiklan mukaiset yleiset velvollisuudet, joiden mukaan ”henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä”.

³¹ Henkilökohtaisten tietojen hallintajärjestelmien osalta ks. esimerkiksi Euroopan tietosuojavaltuutetun lausunto 9/2016, saatavilla verkko-osoitteessa https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

- **Mikä on edellytetty tiedostomuoto?**

Yleisessä tietosuoja-asetuksessa asetetaan rekisterinpitäjille vaatimuksia henkilön pyytämien henkilötietojen toimittamisesta muodossa, joka tukee niiden uudelleenkäyttöä. Erityisesti asetuksen 20 artiklan 1 kohdassa todetaan, että henkilötiedot on toimitettava ”jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa”. Johdanto-osan 68 kappaleessa selitetään tarkemmin, että tämän muodon olisi oltava yhteentoimiva, mikä tarkoittaa EU:ssa³²

erillisten ja erilaisten organisaatioiden kykyä olla vuorovaikutuksessa niiden yhteistä etua palvelevien ja yhteisesti sovittujen tavoitteiden saavuttamiseksi jakamalla tietoa ja osaamista organisaatioiden kesken niiden käyttämien toimintaprosessien kautta käyttäen niiden tieto- ja viestintätekniikkajärjestelmien välistä tiedonsiirtoa.

Termit ’jäsennelly’, ’yleisesti käytetty’ ja ’koneellisesti luettava’ ovat vähimmäisvaatimuksia, joiden pitäisi helpottaa rekisterinpitäjän käyttämän tiedostomuodon yhteentoimivuutta. Tässä mielessä ”jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa” viittaa keinojen määritelmiin, kun taas yhteensopivuus on haluttu tulos.

Direktiivin 2013/37/EU^{33, 34} johdanto-osan 21 kappaleen mukaan ’koneellisesti luettavalla esitysmuodolla’ tarkoitetaan

tiedostomuotoa, jonka rakenne mahdollistaa sen, että ohjelmistot pystyvät helposti yksilöimään, tunnistamaan ja poimimaan siitä määrättyjä tietoja, yksittäiset tietoalkiot ja niiden rakenne mukaan lukien. Koneellisesti luettavassa muodossa oleviin tiedostoihin koodatut tiedot ovat koneellisesti luettavia tietoja. Koneellisesti luettavissa olevat esitysmuodot voivat olla avoimia tai yksityisiä; ne voivat olla virallisia standardeja, mutta se ei ole välttämätöntä. Asiakirjojen, jotka on koodattu sellaiseen tiedostomuotoon, joka rajoittaa automaattista käsittelyä siksi, että tietoja ei saada poimittua niistä lainkaan tai ei saada poimittua helposti, ei olisi katsottava olevan koneellisesti luettavassa esitysmuodossa. Jäsenvaltioiden olisi tarvittaessa kannustettava avointen koneellisesti luettavien esitysmuotojen käyttöön.

Koska mahdollisia tietoja, joita rekisterinpitäjä voi käsitellä, on montaa eri tyyppiä, yleisessä tietosuoja-asetuksessa ei anneta erityisiä suosituksia annettavien henkilötietojen muodosta. Sopivin muoto vaihtelee eri aloilla. Tarkoituksenmukainen muoto voi jo olla olemassa ja se on aina valittava, jotta saavutetaan tulkittavuuden tavoite ja rekisteröidylle voidaan tarjota hyvät mahdollisuudet tietojen siirtämiseen. Muotoja, joita koskevat kalliit lisenssirajoitukset, ei pidetä tarkoituksenmukaisena lähestymistapana.

Johdanto-osan 68 kappaleessa asiaa selvennetään näin: ”Rekisteröidyn oikeus siirtää tai vastaanottaa häntä koskevia henkilötietoja ei saisi luoda rekisterinpitäjille velvoitetta hyväksyä tai ylläpitää tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia.” **Näin**

³² Yhteentoimivuusratkaisuista eurooppalaisille julkishallinnoille (ISA) 16. syyskuuta 2009 annetun Euroopan parlamentin ja neuvoston päätöksen N:o 922/2009/EY (EUVL L 260, 3.10.2009, s. 20) 2 artikla.

³³ Direktiivi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä annetun direktiivin 2003/98/EY muuttamisesta.

³⁴ Englanninkielisessä EU-sanastossa (<http://eur-lex.europa.eu/eli-register/glossary.html>) selvennetään tarkemmin odotuksia, jotka liittyvät näissä ohjeissa käytettyihin käsitteisiin, kuten *machine-readable* (koneellisesti luettava), *interoperability* (yhteentoimivuus), *open format* (avoin muoto), *standard* (standardi) ja *metadata* (metatieto).

ollen tietojen siirtämisen järjestelmästä toiseen tarkoituksena on tuottaa yhteentoimivia järjestelmiä, ei yhteensopivia järjestelmiä.³⁵

Henkilötiedot edellytetään toimitettavan muodoissa, jotka ovat hyvin kaukana sisäisistä tai yksityisistä muodoista. Tietojen siirtäminen järjestelmästä tarkoittaa sinänsä rekisterinpitäjälle tietojen käsittelyssä lisävaihetta, jossa tiedot haetaan alustasta ja niistä suodatetaan pois henkilötiedot, jotka eivät kuulu tietojen siirtämistä koskevan oikeuden soveltamisalaan, kuten päätellyt tiedot tai järjestelmien turvallisuuteen liittyvät tiedot. Näin rekisterinpitäjiä kannustetaan tunnistamaan etukäteen, mitä niiden omien järjestelmien tietoja oikeus tietojen siirtämiseen järjestelmästä toiseen koskee. Tätä ylimääräistä tietojen käsittelyä pidetään pääasiallista käsittelyä täydentävänä, koska sitä ei suoriteta jonkin rekisterinpitäjän määrittelemän uuden tavoitteen saavuttamiseksi.

Jos tietyllä alalla tai tietyssä yhteydessä ei ole yleisesti käytettyjä muotoja, **rekisterinpitäjien olisi toimitettava henkilötiedot yleisesti käytetyssä avoimessa muodossa (esimerkiksi XML, JSON tai CSV) yhdessä hyödyllisten metatietojen kanssa parhaalla mahdollisella tarkkuustasolla** säilyttäen samalla korkean abstraktiotason. Vaihdetun tietojen merkitys olisi kuvailtava tarkasti käyttämällä sopivia metatietoja. Näiden metatietojen olisi oltava riittävät, jotta mahdollistetaan tietojen käyttö suunniteltuun tarkoitukseen ja niiden uudelleenkäyttö paljastamatta tietenkään liikesalaisuuksia. Siksi on epätodennäköistä, että pdf-version toimittaminen saapuneiden sähköpostiviestien kansioista olisi riittävän jäseneltyä tai kuvailevaa, jotta kansion tietoja olisi helppo käyttää uudelleen. Tietojen tehokkaan uudelleenkäytön mahdollistamiseksi sähköpostitiedot on sen sijaan toimitettava muodossa, joka säilyttää kaikki metatiedot. Kun valitaan tiedostomuoto henkilötietojen toimittamista varten, rekisterinpitäjän on harkittava, miten tämä muoto vaikuttaa henkilön oikeuteen käyttää tietoja uudelleen tai estää sen. Tapauksissa, joissa rekisterinpitäjä pystyy tarjoamaan rekisteröidylle eri vaihtoehtoja henkilötietojen ensisijaiselle muodolle, valinnan vaikutukset on kuvattava selvästi. Lisämetatietojen käsittely pelkäästään sitä varten, että niitä saatetaan tarvita tietojen siirtämistä järjestelmästä toiseen koskevaan pyyntöön vastaamiseen, ei ole oikeutettu peruste tällaiseen käsittelyyn.

Tietosuojatyöryhmä kannustaa voimakkaasti alan sidosryhmiä ja ammattijärjestöjä tekemään yhteistyötä ja laatimaan yhteentoimivat standardit ja muodot, jotta oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat vaatimukset voidaan täyttää. Tähän haasteeseen on vastattu myös eurooppalaisilla yhteentoimivuusperiaatteilla, joilla on luotu sovittu lähestymistapa yhteentoimivuuteen organisaatioille, jotka haluavat tuottaa yhdessä julkisia palveluja. Periaatteiden soveltamisalan puitteissa niissä määritellään yhteiset osatekijät, kuten sanasto, käsitteet, periaatteet, toimintaperiaatteet, ohjeet, suosikset, standardit, erittelyt ja käytännöt.³⁶

- Miten hoidetaan laaja tai monimutkainen henkilötietojen keruu?

Yleisessä tietosuojasetuksessa ei selitetä, kuinka voidaan selviytyä pyyntöön vastaamiseen liittyvistä haasteista, kun on kyse laajasta tiedonkeruusta, monimutkaisesta tietorakenteesta tai

³⁵ ISO/IEC 2382-01 -standardissa määritellään yhteentoimivuus seuraavasti: Kyky kommunikoida, suorittaa ohjelmia tai siirtää tietoja eri toiminnallisten yksiköiden välillä tavalla, joka edellyttää, että käyttäjällä on vähän tai ei ole lainkaan tietämystä näiden yksiköiden ainutlaatuisista ominaisuuksista.

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

muista teknisistä asioista, jotka voivat aiheuttaa ongelmia rekisterinpitäjille tai rekisteröidyille.

Kaikissa tapauksissa on kuitenkin ratkaisevaa, että henkilö ymmärtää täysin niiden henkilötietojen määritelmän, mallin ja rakenteen, joita rekisterinpitäjä voi toimittaa. Tiedot voitaisiin esimerkiksi ensin toimittaa tiivistetyssä muodossa käyttäen koontinäyttöä, jolloin rekisteröity voi siirtää vain osia henkilötiedoista eikä kaikkia. Rekisterinpitäjän olisi annettava yhteenveto ”tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä” (katso yleisen tietosuoja-asetuksen 12 artiklan 1 kohta) sellaisella tavalla, että rekisteröidyllä on aina selvät tiedot siitä, mitkä tiedot on ladattava tai siirrettävä toiselle rekisterinpitäjälle jotain tiettyä käyttötarkoitusta varten. Rekisteröidyillä olisi esimerkiksi oltava mahdollisuus käyttää ohjelmistoja, joiden avulla tietyt tiedot on helppo määritellä, tunnistaa ja käsitellä.

Kuten edellä mainittiin, yksi käytännön keino, jolla rekisterinpitäjä voi vastata tietojen siirtämisestä koskeviin pyyntöihin, voi olla asianmukaisesti suojatun ja dokumentoidun sovellusliittymän tarjoaminen käyttöön. Tällöin käyttäjät voivat esittää rekisterinpitäjälle henkilötietojensa koskevia pyyntöjä oman tai kolmannen osapuolen ohjelmiston avulla tai antaa muille (myös toiselle rekisterinpitäjälle) luvan tehdä se puolestaan yleisen tietosuoja-asetuksen 20 artiklan 2 kohdan mukaisesti. Sallimalla pääsy tietoihin ulkopuolisten käytettävissä olevan sovellusliittymän kautta on myös mahdollista tarjota kehittyneempi liittymäjärjestelmä, jonka avulla käyttäjät voivat esittää myöhempiä tietopyyntöjä joko lataamalla kaikki tiedot uudelleen tai delta-toimintona, joka sisältää vain edellisen latauksen jälkeen tehdyt muutokset, ilman että nämä lisäpyynnöt aiheuttaisivat rekisterinpitäjälle liikaa lisätöitä.

- Miten siirrettävät tiedot voidaan suojata?

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan mukaan rekisterinpitäjien on taattava ”henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia”.

Henkilötietojen siirtäminen rekisteröidylle voi kuitenkin myös herättää joitakin turvallisuuskysymyksiä:

Miten rekisterinpitäjät voivat varmistaa, että henkilötiedot toimitetaan turvallisesti oikealle henkilölle?

Koska tietojen siirtämisen tavoitteena on saada henkilötiedot ulos rekisterinpitäjän tietojärjestelmästä, siirtäminen voi aiheuttaa näille tiedoille mahdollisen riskin (erityisesti tietoturvaloukkausten riskin siirron aikana). Rekisterinpitäjän vastuulla on toteuttaa kaikki turvatoimenpiteet, joita tarvitaan sen varmistamiseksi, että henkilötiedot siirretään turvallisesti (päästä-päähän- tai tiedonsalauksella) oikeaan kohteeseen (vahvan todentamisen toimenpiteillä) ja että sen järjestelmään jäävät henkilötiedot suojataan edelleen, sekä läpinäkyvät menettelyt mahdollisten tietoturvaloukkausten käsittelyyn.³⁷ Rekisterinpitäjien on

³⁷ Toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa annetun direktiivin (EU) 2016/1148 mukaisesti.

arvioitava tietojen siirtämiseen järjestelmästä toiseen liittyvät erityiset riskit ja toteutettava tarvittavat toimenpiteet riskien lieventämiseksi.

Tällaisiin riskejä lieventäviin toimenpiteisiin voivat kuulua seuraavat: jos rekisteröity on jo todennettava, lisätodentamistietojen käyttö, kuten jaettu salaisuus, tai muu todentamisen tekijä, kuten kertakäyttöinen salasana; siirron keskeyttäminen tai jäädyttäminen, jos epäillään, että tili on vaarantunut; kun on kyse suorasta siirrosta rekisterinpitäjältä toiselle, olisi käytettävä toimivaltuuksilla tehtyä todentamista, kuten tunnistevälineeseen perustuvaa todentamista.

Tällaiset turvallisuustoimenpiteet eivät saa olla luonteeltaan hidastavia eivätkä ne saa estää käyttäjiä käyttämästä oikeuksiaan esimerkiksi aiheuttamalla lisäkustannuksia.

Miten käyttäjiä autetaan suojaamaan henkilötietojensa tallennus omiin järjestelmiinsä?

Kun käyttäjät hakevat henkilötietojaan verkkopalvelusta, on aina olemassa riski, että he tallentavat tiedot heikommin suojattuihin järjestelmiin kuin palvelun tarjoama järjestelmä. Tietoja pyytävä rekisteröity on vastuussa oikeiden toimenpiteiden määrittelystä henkilötietojen suojaamiseksi omassa järjestelmässään. Hänelle olisi kuitenkin tiedotettava tästä, jotta hän voi toteuttaa toimia vastaanottamiensa tietojen suojaamiseksi. Esimerkkinä johtavasta käytännöstä rekisterinpitäjät voivat myös suositella tarkoituksenmukaisia muotoja, salausvälineitä ja muita suojaustoimenpiteitä auttaakseen rekisteröityä saavuttamaan tämän tavoitteen.

* * *

Tehty Brysselissä 13. joulukuuta 2016

Tietosuojatyöryhmän puolesta
Puheenjohtaja
Isabelle FALQUE-PIERROTIN

Viimeksi tarkistettu ja hyväksytty 5. huhtikuuta 2017

Tietosuojatyöryhmän puolesta
Puheenjohtaja
Isabelle FALQUE-PIERROTIN