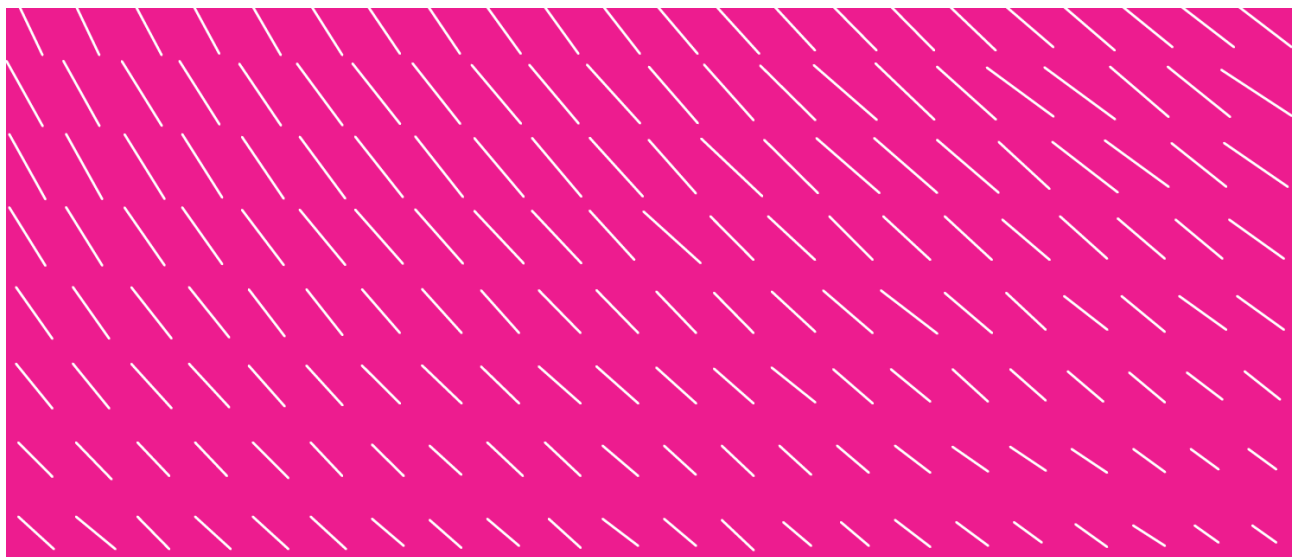




Henkilötietojen käsittelyä koskevat ohjeet finanssialan toimijoille

Nämä ohjeet eivät ole EU:n tietosuoja-asetuksen 40 artiklan mukaiset käytäntösäännöt, vaan ne on tarkoitettu finanssialan yritysten oman ohjeistuksen ja toiminnan suunnittelun avuksi. Tavoitteena on edistää hyvää henkilötietojen käsittelytapaa finanssialalla.

Sisällys

1	Johdanto	3
2	Soveltaminen ja määritelmät.....	3
2.1	Milloin tietosuoja-asetusta ja näitä ohjeita sovelletaan?	3
2.2	Keskeiset käsitteet.....	3
3	Henkilötietojen käsittelyn yleiset edellytykset.....	5
3.1	Henkilötietojen käsittelyä koskevat periaatteet.....	5
3.2	Milloin henkilötietoja voidaan käsitellä?.....	7
3.2.1	Suostumus	7
3.2.2	Sopimus	8
3.2.3	Lakisääteinen velvoite	8
3.2.4	Yleinen etu	9
3.2.5	Oikeutettu etu	9
3.2.6	Elintärkeä etu	11
3.3	Profilointi ja automaattinen päätöksenteko.....	11
3.3.1	Asiakkaiden profilointi.....	11
3.3.2	Automaattinen päätöksenteko	12
3.3.3	Esimerkkejä.....	13
4	Henkilötietojen käsittelyä koskevia erityissäännöksiä ja järjestelyitä	14
4.1	Erityisten henkilötietoryhmien eli nk. arkaluonteisten tietojen käsittely	14
4.2	Finanssirytysten kannalta keskeisiä poikkeuksia erityisiä henkilötietoryhmiä koskevaan käsittelykieltoon	14
4.2.1	Rekisteröidyn nimenomainen suostumus	14
4.2.2	Käsittely on tarpeen vakuutusyhtiön toiminnassa ja sosiaaliturvan alalla	15
4.2.3	Ammattiliittoon kuulumisen.....	15
4.2.4	Rikostuomioihin ja rikoksiin liittyvien henkilötietojen käsittely oikeusvaateiden yhteydessä sekä vakuutusyhtiön vastuun selvittämiseksi	15
4.3	Henkilötietojen käsittely väärinkäytös-, asiakashäiriö- ja vahinkorekisterissä	16
4.4	Eräät vakuutustoiminnassa käsiteltävät tiedot.....	17
4.5	Rahanpesun ja terrorismin rahoittamisen torjunta, kansainväliset talouspakotteet ja kansalliset jäädyttämispäätökset sekä näihin liittyvä henkilötietojen luovuttaminen.....	17
4.5.1	Rahanpesun ja terrorismin rahoittamisen torjunta.....	17
4.5.2	Kansainväliset talouspakotteet ja kansalliset jäädyttämispäätökset	19
4.6	Luottotiedot.....	20
4.7	Henkilötunnuksen käsittely	20
4.7.1	Henkilötunnuksen käsittely finanssirytyksissä	20
4.7.2	Henkilötunnuksen luovuttaminen osoitetietojen päivitystä varten.....	21
4.7.3	Henkilötunnuksen merkitseminen tulosteisiin.....	21
4.8	Turvakielto	21

5	Rekisterinpitäjän velvollisuudet	22
5.1	Sisäänrakennettu ja oletusarvoinen tietosuoja	22
5.2	Osoitusvelvollisuus	23
5.3	Tietosuojavastaavan nimittäminen	23
5.4	Tietosuoja koskeva vaikutustenarviointi ja ennakkuuleminen	24
5.5	Tietoturva: käsittelyn turvallisuus, henkilötietojen suojaaminen ja hävittäminen	25
6	Velvoitteet tietoturvaloukkaustilanteissa	25
6.1	Mikä on henkilötietojen tietoturvaloukkaus?	25
6.2	Ilmoitus tietosuojaviranomaiselle	26
6.3	Tietoturvaloukkauksen dokumentointi	27
6.4	Ilmoitus rekisteröidylle	27
6.5	Muut ilmoitukset tietoturvaloukkauksista	28
7	Rekisteröidyn oikeudet	28
7.1	Oikeus saada tietoa henkilötietojen käsittelystä	28
7.2	Oikeus saada tutustua tietoihin (tarkastusoikeus)	29
7.2.1	Tarkastusoikeus lokitiedoista ilmeneviin tietoihin	30
7.2.2	Rajoitukset rekisterinpitäjän velvollisuuteen toimittaa tietoja rekisteröidylle	31
7.2.3	Vakuutuslääkärin henkilöllisyys	31
7.3	Oikeus tietojen oikaisemiseen	31
7.4	Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")	31
7.5	Oikeus käsittelyn rajoittamiseen	32
7.6	Oikeus vastustaa käsittelyä	33
7.7	Oikeus siirtää tiedot järjestelmästä toiseen	34
7.8	Oikeuksien toteuttamista koskevat periaatteet	34
7.8.1	Toimenpiteistä ilmoittamisen määräaika	35
7.8.2	Kieltäytyminen toimenpiteistä	35
7.8.3	Maksuttomuus	35
7.8.4	Pyynnön esittäjän tunnistaminen	36
8	Henkilötietojen luovuttaminen ja siirto	36
8.1	Henkilötietojen luovuttaminen	37
8.2	Henkilötietojen siirto kolmansiin maihin	37
8.2.1	Siirto tietosuojan riittävyyttä koskevan komission päätöksen perusteella	38
8.2.2	Siirto asianmukaisia suojatoimia soveltaen	38
8.2.3	Eryistä tilanteita koskevat poikkeukset	39
8.3	Henkilötietojen luovutus viranomaisille	40
9	Suoramarkkinointi	40

1 Johdanto

Näiden ohjeiden tavoitteena on edistää hyvää henkilötietojen käsittelytapaa ottaen huomioon finanssialan erityispiirteet ja rekisteröityjen yksityisyyden suojan. Tavoitteena on myös lisätä asiakkaiden luottamusta finanssipalveluihin. Säännöt on tarkoitettu finanssiyrityksille niiden itse suorittaman ohjeistuksen, toiminnan suunnittelun ja opastuksen tueksi. Ohjeet perustuvat yleiseen tietosuoja-asetukseen (EU (2016/679)) ja kansalliseen tietosuojalakiin (1050/2018), joiden lisäksi ohjeet huomioivat voimassa olevaa oikeuskäytäntöä, viranomaisohjeistuksia ja muuta finanssiyrityksiin sovellettavaa lainsäädäntöä. Myös Euroopan tietosuojaneuvoston julkaisemat ohjeet on otettu huomioon soveltuvien osin, joskin on huomattava, että ohjeet eivät ole oikeuslähteinä velvoittavuudeltaan lainsäädännön taseisia.

Tämän ohjeen lukijan on syytä huomioida myös Finanssiala ry:n muut ohjeet ja hyvät käytänteet, kuten Pankkisalaisuusohje, sekä finanssiyrityksen omat ohjeet. Finanssiyrityksellä tarkoitetaan tässä ohjeessa laajasti finanssialalla toimivia yhtiöitä kuten vakuutusyhtiöitä, eläkeyhtiöitä, pankkeja, sijoituspalveluyrityksiä, rahastoyhtiöitä ja vaihtoehtorahastojen hoitajia.

2 Soveltaminen ja määritelmät

2.1 Milloin tietosuoja-asetusta ja näitä ohjeita sovelletaan?

Näitä ohjeita sovelletaan finanssialalla tapahtuvaan luonnollisia henkilöitä koskevaan henkilötietojen käsittelyyn. Käsittelyn kohteena voivat olla muun muassa finanssiyrityksen asiakkaiden, toimihenkilöiden tai päätöksentekijöiden henkilötiedot. Jäljempänä ohjeistetaan lähtökohtaisesti asiakkaita ja näihin rinnastettavia henkilöitä koskevien henkilötietojen käsittelyä.

Henkilötietoa ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Tietosuoja-asetusta ja näitä ohjeita sovellettaessa on kuitenkin otettava huomioon, että asetuksen tarkoituksena on suojata henkilön yksityiselämää ja muuta yksityisyyttä. Myös yritysten yhteyshenkilöiden ja päätöksentekijöiden sekä yksityisten elinkeinonharjoittajien henkilötiedot kuuluvat asetuksen piiriin. Pelkästään yritystä koskevat tiedot sen sijaan eivät kuulu asetuksen eivätkä näiden ohjeiden soveltamisalan piiriin. Yrityksiä koskevien tietojen käsittelyssä on kuitenkin tärkeää huomioida muun muassa liikesalaisuuksien suoja, pankkisalaisuusohjeet ja finanssialan erityislainsäädäntöön sisältyvät salassapitovelvoitteet. Asetusta tai tätä ohjetta ei sovelleta kuolleisiin henkilöihin. On kuitenkin huomattava, että salassapitovelvollisuus ja yksityisyyden suoja jatkuvat myös henkilön kuoleman jälkeen.

2.2 Keskeiset käsitteet

Tietosuoja-asetuksessa (4 Artikla) määritellään keskeiset henkilötietojen käsittelyyn liittyvät käsitteet. Alla on kuvattu tarkempia esimerkkejä näistä käsitteistä finanssialalla.

Henkilötiedon määritelmä on laaja ja kattaa lähtökohtaisesti kaikki luonnolliseen henkilöön liittyvät tiedot, kuten henkilön tunnistetiedot (nimi, syntymäaika ja -paikka,

henkilötunnus, sukupuoli, osoite ja puhelinnumero) sekä varallisuutta ja tuloja koskevat tiedot. Henkilötietoja ovat myös henkilön finanssiyrityksen kanssa tekemiin sopimuksiin sekä palveluiden käyttöön liittyvät keskeiset tiedot. Samoin henkilötietoja ovat kaikki finanssiyritykselle kertyvät tiedot henkilön ominaisuuksista, toimintatavoista tai luotettavuudesta sekä arvostelman luonteiset kuvaukset. Myös henkilön kuva ja esimerkiksi tallennettu puhe ovat henkilötietoa. Henkilötietoja ovat myös henkilön vakuutussopimuksiin liittyvät keskeiset tiedot, kuten tiedot vakuutusturvasta, vakuutetuista, edunsaajista, vakuutettavasta omaisuudesta, sen arvosta ja sijaintipaikasta sekä omistussuhteista. Myös korvaustoimintaan liittyvät luonnollista henkilöä koskevat tiedot ovat lähes poikkeuksetta henkilötietoja.

Käsittelyllä tarkoitetaan kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin. Esimerkiksi tietojen kerääminen, säilyttäminen, käyttö, luovuttaminen ja poistaminen ovat kaikki henkilötietojen käsittelyä. On huomattava, että myös pelkkä tietojen katselu tai henkilötietojen luovuttaminen suullisesti voi täyttää käsittelyn määritelmän.

Rekisterillä tarkoitetaan tietosuoja-asetuksessa mitä tahansa jäsennehtyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Rekisterillä tarkoitetaan siis tiettyä loogista kokonaisuutta, joka voi muodostua useista tietojärjestelmistä ja niiden sisältämistä henkilötiedoista. Finanssialalla rekisterit viittaavat usein tiettyyn käsittelytarkoitukseen, kuten asiakasrekisteriin ja sisäpiirirekisteriin.

Rekisteröityjä ovat käsittelyn kohteena olevat tunnistetut tai tunnistettavissa olevat luonnolliset henkilöt, kuten luottolaitoksen asiakkaat eri ominaisuuksissaan, kuten tallettajina, luotonottajina tai -hakijoina. Rekisteröityjä ovat myös henkilöt, jotka esimerkiksi tehdyn henkilökohtaisen luottotarjouksen perusteella on rekisteröity luottolaitoksen asiakasrekisteriin sekä henkilöt, jotka on merkitty mahdolliseen suoramarkkinointirekisteriin. Vakuutusyhtiöissä rekisteröityjä ovat vastaavasti esimerkiksi vakuutusyhtiön asiakkaat ja asiakkaisiin rinnastuvat tai heitä edustavat henkilöt eri ominaisuuksissaan, kuten vakuutuksenottajina, -hakijoina, vakuutettuina, korvauksenhakijoina ja edunsaajina. Finanssiyrityksissä rekisteröityjä ovat myös yritysasiakkaiden edustajat ja yhteyshenkilöt, potentiaaliset asiakkaat, työntekijät ja työnhakijat.

Rekisterinpitäjä finanssialalla on finanssiyritys, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tyypillisesti IT-palveluntarjoajat ovat tällaisia käsittelijöitä finanssiyrityksellä. On syytä selvyyden vuoksi todeta, ettei yksittäinen työntekijä ole asetuksen tarkoittama henkilötietojen käsittelijä. Vuokratyöntekijät rinnastetaan tietosuoja-asetuksen mukaan lähtökohtaisesti työnantajan omiin työntekijöihin.

Tietosuoja-asetus sisältää myös joukon muita määritelmiä (mm. profilointi ja pseudonymisointi), jotka soveltuvat suoraan myös finanssialalla tapahtuvaan henkilötietojen käsittelyyn.

3 Henkilötietojen käsittelyn yleiset edellytykset

3.1 Henkilötietojen käsittelyä koskevat periaatteet

Finanssiryitysten on henkilötietoja käsitellessään noudatettava lakia, huolellisuutta ja hyvää tietojenkäsittelytapaa ja toimittava muutoinkin niin, ettei pankki- tai vakuutussalaisuutta, asiakkaiden yksityiselämän suojaa tai muita perusoikeuksia loukata. Henkilötietojen käsiteltäessä on noudatettava tietosuojasetuksessa (5 artikla) määriteltyjä periaatteita. Jokainen finanssiryitys vastaa itse henkilötietojen käsittelystä ja oman organisaationsa tekemistä tulkinnoista tietosuojasääntelyn osalta.

Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (*lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaatteet*). Lainmukaisuuden periaatteen mukaan henkilötietojen käsittely on mahdollista vain, kun jokin tietosuoja-asetuksessa määritellyistä käsittelyn edellytyksistä täyttyy. Käsittelyssä on myös muutoin noudatettava tietosuoja-asetusta ja muuta henkilötietojen käsittelyä koskevaa lainsäädäntöä. Kohtuullisuutta koskeva periaate puolestaan edellyttää, että henkilötietojen käsittelyn tulee olla asianmukaista ja kohtuullista suhteessa käsittelyn tarkoitukseen. Käsittelystä on kerrottava ymmärrettävästi, eikä henkilötietoja saa käsitellä rekisteröidyn kannalta ennalta arvaamattomalla tai odottamattomalla tavalla. Henkilötietojen käsittelyn tulee näin ollen olla rekisteröidyn kohtuullisten odotusten mukaista.

Läpinäkyvyys edellyttää, että rekisteröidyn tulee saada helposti selkeää tietoa henkilötietojensa käsittelystä, mukaan lukien tiedot siitä, mihin rekisteröity voi ottaa yhteyttä tietosuojaan ja rekisteröityjen oikeuksiin ja käsittelyn tarkoituksiin liittyvissä asioissa. Rekisteröityjä on informoitava käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää oikeuksiaan.

Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla (*käyttötarkoitussidonnaisuuden periaate*). Käyttötarkoitus tai -tarkoitukset on määritettävä ennen käsittelyn aloittamista ja niistä on kerrottava yksiselitteisesti henkilötietoja kerättäessä, tai pääsääntöisesti viimeistään kuukauden kuluessa, jos tietoja ei ole saatu suoraan rekisteröidyltä itseltään.

Henkilötietojen käsittely muita kuin alkuperäisiä tarkoituksia varten on sallittua vain, jos käsittely ei ole yhteensopimatonta alkuperäisten käyttötarkoitusten kanssa.

Punnitessaan myöhemmän käsittelyn tarkoituksen yhteensopivuutta niiden tarkoitusten kanssa, joita varten henkilötiedot alun perin kerättiin, finanssiyrityksen on ensinnäkin huomioitava alkuperäisten tarkoitusten ja suunnitellun myöhemmän käsittelyn tarkoitusten väliset yhteydet. Finanssiyrityksen tulee huomioida asiayhteys, jossa henkilötiedot on kerätty, ja tähän liittyen erityisesti myöhempään käsittelyyn liittyvät rekisteröidyn kohtuulliset odotukset, jotka perustuvat hänen ja finanssiyrityksen väliseen suhteeseen. Henkilötietojen luonne, suunnitellun myöhemmän käsittelyn seuraukset rekisteröidyille ja asianomaisten suojatoimien olemassaolo sekä alkuperäisessä että suunnitellussa käsittelyssä on myös huomioitava.

Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (*tietojen minimoinnin periaate*). Henkilötietoja tulee käsitellä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.

Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä (*täsmällisyyden periaate*). Finanssiyrityksen on kohtuullisin toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Esimerkkinä kohtuullisesta toimenpiteestä voidaan pitää asiakastietojen säännöllistä päivittämistä luotettavaksi katsottavasta lähteestä, kuten väestötietojärjestelmästä tai Postin rekistereistä. On huomioitava, että erityislainsäädäntö, kuten kansainvälistä veroraportointia koskevat säännökset, voi sisältää tietojen päivittämistä koskevia velvoitteita. Velvoite ilmoittaa muuttuneista tiedoista voi koskea myös asiakasta.

Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (*säilytyksen rajoittamisen periaate*). Finanssiyrityksen tulee määrittää henkilötiedoille etukäteen säilytysajat tai säilytysajan määräytymiskriteerit, joiden mukaisesti henkilötiedot on poistettava tai anonymisoitava. Erityisesti finanssialalla on toimialakohtaisessa erityislainsäädännössä asetettu finanssiyrityksille useita tietojen säilyttämistä koskevia velvoitteita, jotka yritysten tulee ottaa huomioon säilytysaikojen määrittämisessä. Finanssiyrityksen tulee myös huolehtia mainittujen säilytysaikojen toteutumisesta esimerkiksi tietojärjestelmissään ja näin varmistettava, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (*eheyden ja luottamuksellisuuden periaate*). Näin muun muassa ehkäistään luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoihin sekä tällaisten tietojen tai laitteistojen luvaton käyttö. Henkilötietojen käsittelyn ja suojaamisen asianmukainen turvallisuustaso on ratkaistava jokaisessa finanssiyrityksessä tapauskohtaisesti yrityksen omaan riskiperusteiseen arviointiin nojautuen.

Tämän lisäksi on syytä huomioida, että finanssiyritysten toimihenkilöillä ja toimielimien jäsenillä on lakiin perustuva salassapitovelvollisuus, jolla varmistetaan asiakkaiden asioiden luottamuksellinen käsittely. Toimihenkilöt saavat käsitellä asiakastietoja ja muita henkilötietoja vain työtehtäviensä edellyttämässä laajuudessa. Käytännössä tämä tarkoittaa muun muassa sitä, että toimihenkilö voi käsitellä vain niiden asiakkaiden tietoja, joiden tietojen käsittelyä toimihenkilön työtehtävät edellyttävät. Toimihenkilö ei saa käsitellä esimerkiksi lähipiirinsä tietoja tai katsoa omia asiakastietojaan asiakastietojärjestelmien kautta. Jos työntekijä syyllistyy oikeudettomaan henkilötietojen käsittelyyn, voi hän joutua oikeudelliseen vastuuseen ja rikosoikeudellisten seuraamusten kohteeksi. Pankki- ja vakuutuslaitokset käsittelevät kaikki ne seikat, jotka finanssiyrityksen toimi- tai luottamushenkilö työssään saa tietoonsa asiakkaan tai muun sen toimintaan liittyvän henkilön taloudellisesta

asemasta, henkilökohtaisia oloja koskevasta tiedosta tai liike- tai ammattisalaisuudesta.

Sisäänrakennetun ja oletusarvoisen tietosuoja-asetuksen sekä osoitusvelvollisuuden periaatteita käsitellään luvussa 5.

3.2 Milloin henkilötietoja voidaan käsitellä?

Finanssiryityksellä on oikeus käsitellä toimintansa kannalta tarpeellisia henkilötietoja. Käsitteily on perustuttava tietosuoja-asetukseen (6 artikla) ja, jos kyse on rekisterinpitäjän lakisääteisen velvoitteen, yleistä etua koskevan tehtävän suorittamisen tai julkisen vallan käyttämisen nojalla suoritettavasta käsitteilystä (6 artiklan 1 kohdan c ja e alakohdat), Euroopan unionin tai jäsenvaltion lainsäädäntöön. Finanssialalla on tavanomaista, että henkilötietojen käsitteilyyn liittyy useampi käsitteilyperuste samanaikaisesti. Tiettyä henkilötietoa voidaan käsitellä siten useampaan tarkoitukseen ja useamman käsitteilyperusteen nojalla. Finanssiryitykset huomioivat asian henkilötietojen käsitteilyn suunnittelussa sekä käytännön toteutuksessa. Esimerkiksi sopimukseen perustuvan käsitteilyn päätyttyä henkilötietoja saatetaan käsitellä lakisääteisten velvoitteiden noudattamiseksi. Erityisiin henkilötietoryhmiin kuuluvien henkilötietojen, kuten terveydentilatietojen, käsitteilyä varten on säädetty omat vaatimuksensa tietosuoja-asetuksen 9 artiklassa, ja niitä käsitellään tarkemmin tämän ohjeen luvussa 4.

Tietosuoja-asetuksen mukaiset henkilötietojen käsitteilyn oikeusperusteet on esitelty seuraavissa alaluvuissa.

3.2.1 Suostumus

Henkilötietoja voidaan käsitellä, jos rekisteröity on antanut suostumuksensa henkilötietojensa käsitteilyyn yhtä tai useampaa erityistä tarkoitusta varten.

Suostumuksen pitää olla tarpeellinen palvelun tarjoamisen kannalta. Suostumuksella ei siten tule kerätä ylimääräisiä tai käsitteilytarkoitukseen nähden tarpeettomia tietoja. Jos käsitteilyllä on useita tarkoituksia, suostumus on annettava kaikkia käsitteilytarkoituksia varten erikseen. Suostumusta ei voida pitää vapaaehtoisesti annettuna, jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemminkään kieltäytyä suostumuksen antamisesta tai peruuttaa sitä milloin tahansa ilman, että siitä aiheutuu hänelle haittaa.

Suostumus on annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, sähköisellä tai suullisella lausumalla, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsitteilyn.

Finanssialalla alle 18-vuotiaan alaikäisen lapsen osalta henkilötietojen käsitteilyyn liittyvän suostumuksen antaa lähtökohtaisesti lapsen huoltaja. Tapauskohdaisen arvioinnin perusteella voi olla tarpeen pyytää suostumusta myös alaikäiseltä itseltään, kun kysymyksessä on nuori, joka voi ymmärtää antamansa suostumuksen merkityksen. Tästä poikkeuksena on esimerkiksi tilanne, jossa on kyse

tietoyhteiskunnan palveluiden tarjoamisesta lapselle: Suomen tietosuojalaissa on säädetty, että 13-vuotias lapsi voi antaa suostumuksen kyseisiin palveluihin itse.

On hyvä huomioida, että muussa lainsäädännössä käytetty termi 'suostumus' ei välttämättä tarkoita tietosuoja-asetuksen mukaista suostumusta henkilötietojen käsittelylle. Asiaa tulee aina arvioida kyseessä olevaan tilanteeseen soveltuvan sääntelyn puitteissa.

3.2.2 Sopimus

Henkilötietoja voidaan käsitellä, jos käsittely on tarpeen sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osapuolena, tai jos se on tarpeen sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

Finanssirytyksessä asiakasta koskevien henkilötietojen käsittely perustuu pääsääntöisesti asiakkaan kanssa tehtyyn sopimukseen. Tällä perusteella voidaan käsitellä esimerkiksi asiakasta koskevia tietoja asiakkaan hankkiman palvelun tarjoamiseksi, vaikkapa lainan hakijan tietoja tarjouksen antamista varten tai vakuutushakemukseen sisältyviä asiakasta koskevia tietoja ennen vakuutus sopimuksen tekemistä.

3.2.3 Lakisääteinen velvoite

Henkilötietoja voidaan käsitellä, jos se on tarpeen finanssirytyksen lakisääteisen velvoitteen noudattamiseksi.

Käsittelyn tulee perustua Euroopan unionin tai sen jäsenvaltion lainsäädäntöön, ja myös käsittelyn tarkoituksen tulee olla määritelty lainsäädännössä. Viranomaistulkintojen mukaan lakisääteisen velvoitteen tulee olla riittävän selvä sen edellyttämän henkilötietojen käsittelyn suhteen. Tämä tarkoittaa, että velvoitteeseen ei saa liittyä valinnanvaraa sen suhteen, täyttääkö rekisterinpitäjä velvoitteen, eikä kohtuutonta harkinnanvaraa sen suhteen, miten velvoitetta tulee tietojenkäsittelyn osalta noudattaa. Toimet, joissa henkilötietoja käsitellään laajemmin kuin lainsäädännössä edellytetään, eivät kuulu lakisääteistä velvoitetta koskevan käsittelyperusteen soveltamisalaan.

Esimerkiksi lakisääteisten vakuutusten hoitoon liittyvä henkilötietojen käsittely perustuu siihen, että vakuutusyhtiöt hoitavat lakisääteisiä vakuutuksia koskevissa erityislaeissa määritellyjä tehtäviä.

Lisäksi esimerkiksi luottolaitosten ja sijoituspalveluyritysten on säilytettävä tallenteet sellaisia liiketoimia koskevista puhelinkeskusteluista ja sähköisistä viesteistä, jotka liittyvät sen rahoitusvälineiden kaupankäyntiin tai mahdolliseen muuhun kaupankäyntiin omaan lukuun, tai asiakastoimeksiantojen vastaanottamiseen, välittämiseen ja toteuttamiseen liittyvään palvelun tarjoamiseen.

Yksittäisiä tietojenkäsittelytilanteita varten ei kuitenkaan vaadita erityislakia, vaan yksi laki voi oikeuttaa useita käsittelytoimia. Näin ollen esimerkiksi rahanpesulaki

mahdollistaa mm. sekä asiakastietojen keräämisen että asiakassuhteen seurannan (kuten esimerkiksi asiakkaan transaktioiden seurannan).

3.2.4 Yleinen etu

Henkilötietoja voidaan käsitellä, jos käsittely on *tarpeen yleistä etua koskevan tehtävän suorittamiseksi* tai rekisterinpitäjälle kuuluvan *julkisen vallan käyttämiseksi*. Asetuksessa on annettu tämän käsittelyperusteen osalta jäsenvaltioille mahdollisuus ottaa käyttöön kansallisesti yksityiskohtaisempia säännöksiä. Tällaista yksityiskohtaisempaa kansallista sääntelyä on annettu esimerkiksi tietosuojalaissa, luottolaitoslaissa ja vakuutusyhtiölaissa.

3.2.5 Oikeutettu etu

Henkilötietoja voidaan käsitellä, jos käsittely on tarpeen finanssirytyksen tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi silloin kun henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Oikeutetun edun valitseminen käsittelyperusteeksi tulee kyseeseen silloin kun se on tilanteeseen sopivin, edellyttäen, että oikeutetulle edulle asetetut edellytykset täyttyvät. Ennen oikeutetun edun valintaa käsittelyperusteeksi on siis syytä pohtia, olisivatko esimerkiksi suostumus tai sopimuksen täytäntöönpano sopivampia käsittelyperusteita. Jotta etu voidaan katsoa oikeutetuksi, tulee sen olla lainmukainen, selkeästi ilmaistu ja sen tulee edustaa todellista ja välitöntä tarvetta. Oikeutettua etua käytetään finanssialalla tyypillisesti esimerkiksi kamera- ja kulunvalvonnassa, suoramarkkinoinnissa ja petosten torjunnassa. Palveluiden ja liiketoiminnan kehittäminen on myös yksi hyvin tyypillinen oikeutetun edun käyttötilanne.

Oikeutetun edun käyttäminen edellyttää, että rekisteröidyn ja rekisterinpitäjän välillä on asianmukainen suhde. Asiakassuhteen lisäksi tietojen käsittelyyn oikeuttavan asianmukaisen suhteen voidaan katsoa olevan olemassa silloinkin, kun henkilö ei itse ole sopimusosapuoli, vaan esimerkiksi vakuutussopimusten tapauksessa edunsaaja. Kaikki vahinkoon osalliset eivät välttämättä ole vakuutusyhtiön asiakkaita, mutta myös heidän henkilötietojensa käsittelyn saatetaan katsoa olevan oikeutettua oikeutetun edun perusteella. Henkilötietojen käsittelyn tulee olla tarpeellista kyseisen oikeutetun edun tarkoituksissa.

Jotta oikeutettua etua voidaan käyttää käsittelyperusteena, rekisteröidyn edut ja oikeudet tulee huomioida erityisen tarkkaan, sillä luonnollisen henkilön edut ja oikeudet ovat lähtökohtaisesti rekisterinpitäjän etuja ja oikeuksia suojatumpia. Oikeutettua etua henkilötietojen käsittelylle ei synny, jos rekisteröidyn edut tai oikeudet syrjäyttävät rekisterinpitäjän tai kolmannen osapuolen edun. Näin voi olla esimerkiksi tilanteessa, jossa rekisteröity ei voi kohtuudella odottaa kysymyksessä olevaa henkilötietojen käsittelyä. Oikeutetun edun käyttäminen käsittelyperusteena edellyttääkin rekisterinpitäjän tai kolmannen osapuolen edun punnintaa rekisteröidyn etuja ja oikeuksia vastaan. Se, voidaanko etu katsoa oikeutetuksi, saadaan selville tasapainotestillä. Tietosuojaviranomaiset ovat julkaisseet erilaisia ohjeita tasapainotestistä ja sen sisällöstä. Jokaisen finanssirytyksen tulee rekisterinpitäjänä

itse määritellä menetelmänsä tasapainotestin suorittamiselle. Tasapainotesti on finanssiyrityksen sisäinen asiakirja, eikä finanssiyrityksillä ole velvoitetta luovuttaa sitä rekisteröidylle.

Kun henkilötietojen käsittelyperusteeksi on määritetty oikeutettu etu, rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä. Rekisteröidylle on ilmoitettava tästä oikeudesta. Jos rekisteröity vastustaa henkilötietojensa käsittelyä, rekisterinpitäjän tulee arvioida käsittelyn tarvetta uudelleen rekisteröidyn esittämien henkilökohtaisten perusteluiden valossa. Henkilötietojen käsittely tulee lopettaa käsittelyä vastustaneen rekisteröidyn osalta, jollei rekisterinpitäjä kykene osoittamaan, että käsittelylle on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut ja oikeudet. Henkilötietojen käsittelyä on mahdollista jatkaa myös silloin, kun käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Henkilötietojen käsittelyä ei sen sijaan saa jatkaa esimerkiksi suoramarkkinointitarkoituksessa. Rekisteröidyn ei tällöin tarvitse esittää perusteluja vastustamiselleen, vaan kieltä on noudatettava.

Tietojen käsittelyä petosten estämistarkoituksessa voidaan pitää rekisterinpitäjän oikeutettuna etuna. Esimerkiksi vakuutusyhtiöiden yhteiseen vahinkorekisteriin sisältyvien henkilötietojen käsittely on mahdollista oikeutetun edun perusteella. Vahinkorekisterissä on kyse vahinkoja koskevista tiedoista, joita vakuutusyhtiöt luovuttavat toisilleen vakuutuslaitoksiin kohdistuvan rikollisuuden estämiseksi. Vahinkorekisteriin liittyvää henkilötietojen käsittelyä koskevat tarkemmat linjaukset löytyvät vahinkorekisteriä koskevista ohjeista kohdassa 4.3.

Oikeutettu etu voi mahdollistaa myös tietojen käsittelyn konsernin, konsolidointiryhmän, luottolaitosten yhteenliittymän, rahoitus- ja vakuutusryhmittymän tai taloudellisen yhteenliittymän sisällä. Tällaisessa tietojen käsittelyssä tulee kuitenkin huomioida tietojen luovuttamista rajoittavat pankki- ja vakuutussalaisuus sekä muut soveltuvat salassapitosäännökset. Lisäksi rekisterinpitäjän on harkittava, milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät oikeutetun edun käsittelyperusteen.

Oikeutettu etu voi mahdollistaa henkilötietojen käsittelyn esimerkiksi tilanteissa, joissa on kyse entisiä asiakkaita koskevista maksurästeistä. Näillä tiedoilla voi olla merkitystä arvioitaessa henkilön taloudellista asemaa, sitoumusten hoitokykyä ja luotettavuutta. Finanssiyritysten voi olla perusteltua säilyttää maksun viivästymistietoja jonkin aikaa asiakassuhteen katkeamisen jälkeenkin, koska asianomainen voi lyhyessäkin ajassa hakeutua uudestaan yhteisön asiakkaaksi, jolloin maksun viivästymistä koskevien tietojen käsittely voi olla tarpeellista finanssiyrityksen oikeutetun edun toteuttamiseksi ja luoton- ja sitoumustenantoon liittyvien riskien pienentämiseksi.

Oikeutettu etu voi toimia käsittelyperusteena myös suoramarkkinoinnille, joka kohdistetaan asiakkaaseen tai asiakassuhteeseen rinnastettavissa olevassa suhteessa olevaan henkilöön, esimerkiksi entiseen asiakkaaseen tai potentiaaliseen uuteen asiakkaaseen. Käyttäessään asiakasrekisterinsä tietoja suoramarkkinointitarkoituksiin, finanssiyrityksen on kuitenkin huomioitava, että sellaisia asiakkaan tuntemistietoja ja muita henkilötietoja, jotka on hankittu ainoastaan rahanpesulain tarkoittamiin käyttötarkoituksiin ja yksinomaan rahanpesusääntelyn

perusteella, ei saa käyttää näiden tarkoitusten kanssa yhteensopimattomaan tarkoitukseen, kuten markkinointiin (ks. tarkemmin rahanpesusääntelyä koskeva kohta 4.4). Suoramarkkinointia käsitellään tarkemmin luvussa 9.

3.2.6 Elintärkeä etu

Edellä esitettyjen käsittelyperusteiden lisäksi tietosuoja-asetuksen 6 artiklassa on yhtenä käsittelyperusteena elintärkeä etu. Finanssiyritysten kohdalla elintärkeä etu on harvoin sovellettava käsittelyperuste. Kyseinen käsittelyperuste saattaa tulla kyseeseen tilanteessa, jossa on kyse asiakkaan tai finanssiyrityksen toimihenkilöiden terveydestä tai turvallisuudesta. Käsittelyperusteen mahdollinen soveltuvuus tulee aina arvioida tapauskohtaisesti kussakin organisaatiossa.

3.3 Profilointi ja automaattinen päätöksenteko

3.3.1 Asiakkaiden profilointi

Profiloinnilla tarkoitetaan tietosuoja-asetuksessa (4 artikla) mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia. Kun profiloinnissa hyödynnetään henkilöihin yhdistettävissä olevia tietoja, kuten nimen tai muun tunnisteen perusteella identifioitun henkilön käyttäytymiseen liittyviä tietoja, kysymys on henkilötietojen käsittelystä.

Finanssiyrityksessä profilointia voi esiintyä muun muassa suoramarkkinoinnissa, kun markkinointi tapahtuu kohdennetusti henkilön tiettyjä ominaisuuksia huomioiden. Profilointia tehdään tyypillisesti myös mm. asiakkaan luottokelpoisuuden arvioinnin yhteydessä. Profilointia varten finanssiyritys voi kerätä asiakkaita koskevia tietoja paitsi asiakkailta, myös luotettavista ulkopuolisista lähteistä, joilla on oikeus luovuttaa tietoja. Kuten muukin asiakastietojen käyttöön liittyvä toiminta, myös asiakkaiden profilointi on suunniteltava etukäteen, ja sen on oltava perusteltua ja tarpeellista. Profiloinnin voidaan katsoa olevan perusteltua esimerkiksi silloin, kun asiakas voi hyötyä profiloinnista siten, että finanssiyritys pystyy tarjoamaan hänen elämäntilanteeseensa soveltuvia tuotteita ja palveluja.

Profilointiin sovelletaan sellaisenaan henkilötietojen käsittelyä koskevia säännöksiä, kuten käsittelyn oikeudellisia perusteita ja tietosuojaperiaatteita. Kun finanssiyritys harkitsee asiakkaidensa profiloinnin aloittamista, sen tulee ottaa huomioon, mitä käyttötarkoituksia se on määritellyt henkilötietojen käsittelylle. Kaikilla asiakkailla on oikeus tietää ja saada ilmoitus henkilötietojen käsittelyn tarkoituksista ja kyseisen käsittelyn mahdollisista seurauksista myös silloin, kun käsittely perustuu profilointiin.

Jotta voidaan varmistaa asianmukainen ja läpinäkyvä käsittely, finanssiyrityksen on käytettävä profiloinnissa asianmukaisia matemaattisia tai tilastollisia menetelmiä ja toteutettava asianmukaisia teknisiä ja organisatorisia toimenpiteitä, jotta varmistetaan, että henkilötietojen virheellisyys johtavat tekijät korjataan ja virheriski minimoidaan. Lisäksi henkilötiedot on turvattava siten, että asiakkaiden etuihin ja oikeuksiin kohdistuvat mahdolliset riskit otetaan huomioon ja syrjintä estetään. Profilointia hyödyntävien järjestelmien suunnittelussa ja käyttöönottossa on mahdollisesti

huomioitava myös muu sääntely, kuten esimerkiksi EU:n tekoälysäädös. On kuitenkin huomattava, että kaikki rekisteröityjen ominaisuuksiin perustuva luokittelu tai segmentointi ei välttämättä ole profilointia.

3.3.2 Automaattinen päätöksenteko

Rekisteröidyllä on pääsääntöisesti oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn ilman ihmisen osallistumista ja jossa arvioidaan hänen henkilökohtaisia ominaisuuksiaan ja joka aiheuttaa hänelle kielteisiä oikeusvaikutuksia tai vaikuttaa häneen muutoin vastaavalla tavalla merkittävästi (jäljempänä *automatisoitu päätöksenteko*). Automatisoidusta päätöksenteosta ei ole kyse esimerkiksi silloin, kun järjestelmästä saatu päätös menee aina toimihenkilön uudelleen harkittavaksi ennen päätöksen antamista asiakkaalle. Tässä yhteydessä on myös huomioitava, että finanssiyrityksellä on useissa tapauksissa velvollisuus perustella päätökset ja pääsääntöisesti myös velvollisuus liittää päätöksiin muutoksenhakuohjeet.

Automatisoidulla päätöksenteolla tarkoitetaan tietosuoja-asetuksen määritelmän mukaisesti päätöstä, joka vaikuttaa merkittäväällä tavalla rekisteröityyn henkilöön, jota päätös koskee. Esimerkiksi kun finanssiyritys valitsee asiakastiedoistaan tietyt kriteerit täyttäviä henkilöasiakkaitaan kohteiksi suoramarkkinointiaineiston postitukseen, kyse ei ole automatisoidusta päätöksenteosta, koska tarjouksista ei aiheudu asiakkaalle merkittäviä vaikutuksia.

Automatisoitu päätöksenteko on sallittua seuraavissa tapauksissa: kun se on tarpeen rekisteröidyn ja finanssiyrityksen välisen sopimuksen tekemistä tai täytäntöönpanoa varten, kun se on tarpeen finanssiyrityksen tarjoaman palvelun turvallisuuden ja luotettavuuden varmistamiseksi, kun se on hyväksytty EU:n tai sen jäsenvaltion lainsäädännössä (tällaista sääntelyä liittyy finanssialalla muun muassa rahanpesun, petosten ja verovilpin torjuntaan), tai kun päätös perustuu rekisteröidyn nimenomaiseen suostumukseen.

Kansallisessa lainsäädännössä on erityisiä määräyksiä esimerkiksi niin sanottuja lakisääteisiä vakuutuslajeja koskien. Hallintolaki ja tiedonhallintalaki mahdollistavat automatisoidun päätöksenteon lakisääteisissä vakuutuslajeissa (työtapaturma-, työeläke-, liikenne- ja potilasvakuutus) laeissa tarkemmin säädettyjen edellytysten mukaisesti.

Sopimukseen ja suostumukseen liittyvässä automatisoidussa päätöksenteossa on aina sovellettava seuraavia suoja-toimia ja rekisteröidyn oikeuksia:

- käsittelystä tiedottaminen ja rekisteröidyn oikeus vaatia ihmisen osallistumista tietojen käsittelemiseen,
- rekisteröidyn oikeus esittää kantansa, ja
- oikeus saada selvitys kyseisen arvioinnin jälkeen tehdystä päätöksestä ja oikeus riitauttaa päätös.

Finanssiyritys voi myöntää esimerkiksi henkilöasiakkailleen tarkoitettuja luottoja tai vakuutuksia verkkosivuillaan täysin automatisoidusti. Jos luotto tai vakuutus evätään

tällaisessa prosessissa, on kyse automatisoidusta päätöksenteosta, ja rekisteröidyllä on oltava mahdollisuus ottaa yhteyttä finanssiyrityksen asiakaspalveluun hakemuksen manuaalista käsittelyä varten. Näin rekisteröity voi esittää finanssiyritykselle kantansa ja sellaisia asiaan vaikuttavia tietoja, joita finanssiyrityksellä mahdollisesti ei ennestään ole hallussa. Rekisteröidyllä on oltava myös mahdollisuus saada tietoja niistä perusteista, joita finanssiyritys on päätöksenteossaan käyttänyt. Tarkat päätöksenteossa käytettävät luokitusperusteet kuuluvat finanssiyritysten liikesalaisuuden piiriin.

Jos automatisoidussa päätöksenteossa käytetään tietosuoja-asetuksen 9 artiklan mukaisiin erityisiin henkilötietoryhmiin kuuluvia tietoja (esimerkiksi terveydentilatiedot), käsittely on rajoitetumpaa kuin muissa tilanteissa. Silloin automatisoitu päätöksenteko on mahdollista, mikäli rekisteröity, johon automatisoitu päätöksenteko kohdistuu, on antanut nimenomaisen suostumuksensa automaattiselle päätöksenteolle, taikka mikäli henkilötietojen käsittelystä automaattisen päätöksenteon keinoin on säädetty EU:n tai sen jäsenvaltion lainsäädännön nojalla. Lisäksi edellytetään asianmukaisten suojatoimenpiteiden toteuttamista.

Automatisoitua päätöksentekoa voidaan kohdistaa lapseen sillä edellytyksellä, että automatisoitu lapseen kohdistuva päätöksentekoprosessi on finanssiyritykselle välttämätön. Tällöin tulee kuitenkin kiinnittää erityistä huomiota siihen, että käsittelyn yhteydessä tarjotaan asianmukaiset ja kattavat suojatoimenpiteet, kuten mahdollisuus saada asia uudelleen käsiteltyksi ihmisen toimesta, joilla varmistetaan lasten oikeuksien ja etujen tehokas suojaaminen.

Automatisoidun päätöksenteon ei katsota kohdistuvan lapseen tilanteessa, jossa lapseen liittyvällä päätöksellä ei ole oikeudellisia tai muita vastaavalla tavalla merkittäviä vaikutuksia suoraan lapseen. Kun päätös koskee esimerkiksi sopimukseen liittyviä oikeuksia ja velvollisuuksia, ei päätöksen katsota kohdistuvan lapseen, jollei lapsi ole sopimuksen sopijapuoli ja jollei päätöksellä ole suoria merkittäviä vaikutuksia lapseen. Automatisoitu päätöksenteko ei näin ollen kohdistu lapseen esimerkiksi silloin, kun lapsi on vahinkovakuutuksen vakuutettu ja korvaus vakuutuksesta maksetaan vakuutus sopimuksen osapuolena olevalle lapsen huoltajalle eikä lapselle itselleen. Tämä mahdollistaa esimerkiksi kertakorvausluontoisen lapsen lääkärikulun korvausta koskevan päätöksenteon automatisoinnin, kunhan automatisoidun päätöksenteon muut edellytykset täyttyvät.

3.3.3 Esimerkkejä

Kohdehenkilöiden valinta suoramarkkinoinnissa

- Finanssiyritys valitsee asiakastiedoistaan tietyt kriteerit täyttäviä henkilöasiakkaitaan suoramarkkinoinnin kohteiksi. Vaikka menettely olisi täysin automatisoitu, ei se ole asetuksen tarkoittamaa automatisoitua päätöksentekoa, koska tarjouksesta ei aiheudu asiakkaalle oikeusvaikutuksia, eikä se muuten vaikuta häneen vastaavalla tavalla merkittävästi.

Automatisoitu luoton myöntäminen

- Luottolaitos myöntää henkilöasiakkailleen tarkoitettuja luottoja verkkosivuillaan tarjottavan palvelun välityksellä. Järjestelmä saattaa olla automatisoitu niin, että luotto myönnetään, jos luottolaitoksen tietokannoissa ei ole asiakkaasta esimerkiksi hänen maksukäyttäytymistään tai varallisuusasemaansa koskien sellaisia tietoja, jotka ovat perusteena luottihakemuksen hylkäämiselle. Jos tällaisia tietoja on, ei luottoa myönnetä tai se myönnetään hakemuksesta poikkeavin ehdoin. Tällöin kyseessä on automatisoitu päätös, josta aiheutuu kielteisiä oikeusvaikutuksia asiakkaalle.

On syytä huomata, että edellä olevassa esimerkissä automatisoidusta päätöksenteosta ei olisi kyse, mikäli järjestelmästä saatu päätös menisi aina toimihenkilön uudelleen harkittavaksi ennen päätöksen antamista asiakkaalle.

Automatisoitu vakuutuksen myynti

- Vakuutusyhtiö myy henkilöasiakkailleen tarkoitettuja vakuutuksia verkkosivuillaan tarjottavan palvelun välityksellä. Järjestelmä on täysin automatisoitu niin, että vakuutus myönnetään, jos vakuutusyhtiön tietokannoissa ei ole asiakkaasta esimerkiksi hänen maksukäyttäytymistään koskien sellaisia tietoja, jotka ovat perusteena vakuutushakemuksen hylkäämiselle. Jos tällaisia tietoja on, ei vakuutusta myönnetä tai se myönnetään hakemuksesta poikkeavin ehdoin. Kun asiakkaalle aiheutuu päätöksestä lisäksi oikeusvaikutuksia, kyseessä on automatisoitu päätös. Järjestelmä on varustettava ominaisuuksilla, joiden avulla varmistetaan rekisteröidyn oikeuksien suojaaminen.

4 Henkilötietojen käsittelyä koskevia erityissäännöksiä ja järjestelyitä

4.1 Erityisten henkilötietoryhmien eli nk. arkaluonteisten tietojen käsittely

Tietosuoja-asetuksen mukaan sellaisten henkilötietojen käsittely on kiellettyä, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. Myös geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä. Jotta erityisiin henkilötietoryhmiin kuuluvia tietoja voidaan käsitellä, tulee tietojen käsittelyyn olla jokin tietosuoja-asetuksessa säädetty erityisperuste.

4.2 Finanssiyritysten kannalta keskeisiä poikkeuksia erityisiä henkilötietoryhmiä koskevaan käsittelykieltoon

Erityisiä henkilötietoryhmiä voidaan käsittelykiellon estämättä käsitellä, jos jokin seuraavista poikkeusperusteista täyttyy.

4.2.1 Rekisteröidyn nimenomainen suostumus

Käsittelykielto ei estä finanssiyritystä käsittelemästä tietoja, jos rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten. Nimenomainen suostumus edellyttää yleensä kirjallisesti tai muulla tavoin todisteellisesti annettua suostumusta, josta ilmenee,

minkälaiseen henkilötietojen käsittelyyn lupa on annettu. Suostumuksen on oltava yksilöity, tietoinen, vapaaehtoinen ja yksiselitteinen tahdonilmaisu, jonka tulee täyttää myös muut tietosuojaa-asetuksessa tarkemmin säädetty suostumuksen edellytykset.

4.2.2 Käsittely on tarpeen vakuutusyhtiön toiminnassa ja sosiaaliturvan alalla

Erityisiä henkilötietoryhmiä on mahdollista käsitellä myös silloin, kun käsittely on tarpeen vakuutusyhtiön tai asiakkaan velvoitteiden ja erityisten oikeuksien noudattamiseksi sosiaaliturvan alalla tai kun käsittely on tarpeen erityislainsäädännön nojalla. Sosiaaliturvaan katsotaan kuuluviksi lakisääteinen työtapaturma- ja ammattitautivakuutus sekä työeläkevakuutus.

4.2.3 Ammattiliittoon kuuluminen

Finanssiyritykset voivat käsitellä tietoa asiakkaansa kuulumisesta ammattiliittoon silloin, kun tällainen tieto kuuluu ammattiliittotoiminnan laillisen toiminnan piiriin, kuten ammattiliittojen jäsenilleen ottamiin ryhmävakuutuksiin tai jäsenten henkilökohtaisiin vakuutuksiin, joihin on myönnetty jäsenyyteen perustuvia etuja (ns. ryhmäetuvakuutukset), tai esimerkiksi silloin, kun ammattiliitot tarjoavat toiminnassaan jäsenetuja luottolaitoksen kanssa tekemänsä sopimuksen perusteella ja luovuttavat edun saamiseksi välttämättömän ammattiliiton jäsenyystiedon edun tarjoavalle luottolaitokselle. Lisäksi edellytetään, että liitto on informoinut jäseniään tietojen luovuttamisesta finanssiyritykselle ja huolehtinut jäsenten antamista suostumuksista tietojen luovuttamiseen. Finanssiyritykset voivat käsitellä tietoa ammattiliittoon kuulumisesta vain siinä määrin, kuin se on välttämätöntä esimerkiksi jäsenille myönnettävien etujen antamiseksi.

4.2.4 Rikostuomioihin ja rikoksiin liittyvien henkilötietojen käsittely oikeusvaateiden yhteydessä sekä vakuutusyhtiön vastuun selvittämiseksi

Rikostuomioihin ja rikoksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja saa käsitellä vain viranomaisen valvonnassa tai silloin kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä. Näitä henkilötietoja voidaan käsitellä esimerkiksi oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi oikeudellisessa menettelyssä tai hallinnollisessa tai tuomioistuimen ulkopuolisessa menettelyssä. Suomessa tällaisia tuomioistuimen ulkopuolisia menettelyjä ovat lautakuntamenettelyt, kuten FINEn pankki-, vakuutus- ja arvopaperilautakunnat sekä kuluttajariitalautakunta. Oikeusvaateeseen katsotaan lautakuntakäsittelyssäkin kuuluvan asian selvittämiseen kuuluva henkilötietojen käsittely.

Kansallisen tietosuojalain mukaan vakuutusyhtiöillä on oikeus käsitellä rikostuomioihin ja rikoksiin liittyviä henkilötietoja myös silloin, jos ne ovat tarpeen vakuutusyhtiön vastuun selvittämiseksi. Oikeusvaadetta koskevia tietoja käsitellään vakuutusyhtiöissä esimerkiksi silloin, kun yhtiö vetoaa vakuutussopimuslain (543/94) 75 §:n mukaiseen takautumisoikeuteensa ja hakee vakuutussopimuksen perusteella suorittamaansa korvausta takaisin vakuutustapahtuman tahallisesti tai törkeän huolimattomasti aiheuttaneelta henkilöltä.

Vakuutusyhtiöllä on oikeus käsitellä rikostietoja ja muita asian ajamisessa tarpeellisia arkaluonteisia tietoja myös silloin, kun vakuutusyhtiö pyrkii selvittämään sen vakuutustoimintaa vastaan suunnattua rikosta. Vakuutusyhtiölain säännösten mukaan vakuutuslaitoksilla on oikeus luovuttaa toisille vakuutuslaitoksille vaitiolovelvollisuuden piiriin kuuluvia tietoja niihin kohdistuneista rikoksista sekä niille ilmoitetuista vahingoista.

Esimerkiksi liikennevahinkojen korvauskäsittelyn yhteydessä vakuutusyhtiön on liikennevakuutuslain (460/2016) 33 §:n mukaan ratkaistava yhteenajoissa se, minkä ajoneuvon vakuutuksesta vahingot maksetaan eli kumman kuljettajan tuottamuksesta vahinko on aiheutunut. Liikennevahinkojen korvauskäsittelyn yhteydessä vakuutusyhtiöön kertyy tämän vuoksi tietoja liikenne rikoksista.

Vastaavasti rikostietoja saadaan korvauskäsittelyn yhteydessä muissakin vakuutuslajeissa esimerkiksi vastuuvahingoissa. Kaikissa näissä tilanteissa rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta koskevia tietoja käsitellään tavanomaisena osana vakuutusyhtiön korvaustoimintaa. Rikostiedot kertyvät osaksi kunkin vahinkotapahtuman tausta-aineistoa.

Finanssiryityksellä on velvollisuus laatia tietosuojaa koskeva vaikutustenarviointi tietojenkäsittelystä, joka kohdistuu laajamittaisesti erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin. Vaikutustenarviointia käsitellään tarkemmin kohdassa 5.4.

4.3 Henkilötietojen käsittely väärinkäytös-, asiakashäiriö- ja vahinkorekisterissä

Vakuutusyhtiö saa käsitellä ja rekisteröidä tiedon sen harjoittamaan vakuutustoimintaan kohdistuneista rikoksista ja niiden epäilyistä ylläpitämäänsä rekisteriin. Tietoja saa käsitellä vain siinä laajuudessa, kuin se on välttämätöntä vakuutustoimintaan kohdistuvien rikosten estämiseksi ja selvittämiseksi.

Vakuutusyhtiö voi luovuttaa salassapitovelvollisuuden estämättä näitä tietoja toiselle vakuutusyhtiölle vakuutusyhtiöihin kohdistuvan rikollisuuden ehkäisemiseen liittyvän tärkeän edun vuoksi. Väärinkäytösrekisterissä käsiteltävät tietokategoriat sekä niiden käsittelyn säännöt on määritetty tarkemmin vakuutusyhtiölaissa (30 luvun 3 a §) ja laissa ulkomaisista vakuutusyhtiöistä (11 luvun 81 §).

Luottolaitos ja rahoituslaitos voivat käsitellä tietoja asiakashäiriöihin liittyvistä henkilötiedoista ja ylläpitää niitä koskevaa rekisteriä (asiakashäiriörekisteri) siinä laajuudessa kuin se on välttämätöntä niiden toimintaan välittömästi kohdistuvien asiakashäiriöiden, rikosten tai rikkomusten estämiseksi ja selvittämiseksi. Asiakashäiriörekisteristä on säännökset luottolaitoslain 15 luvussa.

Vahinkorekisteriin merkitään vakuutusyhtiölle ilmoitettuja vahinkoja koskevat perustiedot (henkilötunnus tai yritystunnus, vakuutuksen myöntänyt vakuutuslaitos, vahingon tapahtuma-aika, vahinkonumero, ajoneuvon tai veneen rekisteritunnus, vakuutuslaji koodina ja vahinkotyyppi koodina). Vahinkorekisteriin ei merkitä tietoja luotto-, takaus-, oikeusturva- ja sairausvakuutuksista eikä työtapaturma- ja ammattitautilain mukaisista pakollisista vakuutuksista. Vahinkorekisterin pitäminen on

ennen tietosuoja-asetuksen soveltamisen alkamista perustunut tietosuojalautakunnan lupaan. Vakuutusyhtiölain muutosten esitöissä (HE 87/2019) on kuitenkin todettu, että vahinkorekisteriin liittyvä tietojen käsittely on tarpeen rekisterinpitäjän eli vakuutusyhtiön oikeutetun edun toteuttamiseksi. Näin ollen suomalaiset vakuutusyhtiöt ovat jatkaneet vahinkorekisteriin perustuvaa tietojenkäsittelyä oikeutetun edun nojalla

Edellä mainittuja alan yhteisiä rekistereitä ylläpitää ulkopuolinen toimija finanssiyritysten puolesta ja lukuun.

4.4 Eräät vakuutustoiminnassa käsiteltävät tiedot

Tietosuojalaki antaa vakuutusyhtiöille mahdollisuuden käsitellä arkaluontoisiksi katsottavia tietoja tietyissä tilanteissa ilman rekisteröidyn suostumusta. Vakuutuslaitoksella on siten lakiin perustuva oikeus käsitellä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi. Nämä tiedot ovat keskeisiä muun muassa korvaustoiminnassa.

Suomessa toimivat vahinkovakuutusyhtiöt ovat mukana vakuutus- ja vahinkohistoriatietojen välitysjärjestelmässä (VVH-järjestelmä). Kyseessä on sanomavälitysjärjestelmä, jolla yhtiöt voivat pyytää ja välittää liikennevakuutusten hinnanlaskentaa varten tarvittavat vakuutus- ja vahinkohistoriatiedot yhtiöiden välillä. VVH-järjestelmän keskitetyn tietovaraston avulla vakuutusyhtiöt voivat lisäksi ylläpitää vakuutettujen ajoneuvojen vakuutusten vahinkohistorioita siten, että muut yhtiöt voivat pyytää niitä keskinäisten sopimustensa antamassa laajuudessa suoraan järjestelmästä. Kaikki järjestelmässä mukana olevat vakuutusyhtiöt toimivat rekisterinpitäjinä omien tietojensa osalta.

4.5 Rahanpesun ja terrorismin rahoittamisen torjunta, kansainväliset talouspakotteet ja kansalliset jäädyttämispäätökset sekä näihin liittyvä henkilötietojen luovuttaminen

4.5.1 Rahanpesun ja terrorismin rahoittamisen torjunta

Finanssiyritysten velvollisuus tuntea asiakkaansa perustuu muun muassa luottolaitoslain 15 luvun 18 §:ään, sijoituspalvelulain 12 luvun 3 §:ään, sijoitusrahastolain 26 luvun 15 §:ään, vaihtoehtorahastojen hoitajista annetun lain 12 luvun 8 §:ään ja vakuutusyhtiölain 6 luvun 13 §:ään. Asiakkaan tuntemista koskevat aineelliset vaatimukset sisältyvät rahanpesulakiin (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017).

Asiakkaan tuntemista koskevien yleisten vaatimusten ohella rahanpesulaki asettaa finanssiyrityksille velvoitteita, jotka tähtäävät nimenomaisesti rahanpesun ja terrorismin rahoittamisen torjuntaan. Kyseessä on kaksi toisistaan poikkeavaa henkilötietojen käsittelyn tarkoitusta, perustetta ja rekisterinpitäjän tehtävää.

Rahanpesun ja terrorismin rahoittamisen torjunta on yleisen tietosuoja-asetuksen 23 artiklassa tarkoitettua rikosten ennalta estämistä, tutkintaa ja torjuntaa. Rahanpesulaki velvoittaa finanssiyrityksiä tallentamaan ja käsittelemään lukuisia

henkilötietoja. Tällöin asetuksen mukainen käsittelyperuste on rekisterinpitäjän lakisääteinen velvollisuus. Lisäksi rahanpesun ja terrorismin rahoittamisen torjunnassa voidaan käsitellä myös muita kuin laissa nimenomaisesti määritellyjä henkilötietoja, jos käsittelylle on tietosuoja-asetuksen mukainen peruste.

Finanssirytyksen¹ hankkimien asiakkaan tuntemistietojen laajuus voi vaihdella riskiperusteiseen arviointiin pohjautuen. Myös finanssirytyksen käytössä olevilla riskienhallintakeinoilla on vaikutusta siihen, kuinka kattavasti asiakkaasta tulee kerätä tietoja. Rahanpesulain vaatimusten täyttäminen voi edellyttää finanssirytykseltä henkilötietojen käsittelyä myös ilman asiakkuussuhdetta.

Suomessa lainsäädäntö ei tätä kirjoittaessa mahdollista rikostuomioihin ja rikoksiin liittyvien henkilötietojen käsittelyä asiakkaan tuntemistietoina, joten niitä koskevia tietoja ei tule tallentaa luonnollisesta henkilöstä. Vuonna 2027 tulee kuitenkin sovellettavaksi EU:n uusi rahanpesusäätelyn kokonaisuus, joka tulee muuttamaan oikeustilan muun muassa rikostietojen käsittelyn osalta.² Voimaan tulevat muutokset ovat kuitenkin riippuvaisia siitä, miten kansallinen implementointi tullaan toteuttamaan.

Laki ei määrittele tietolähteitä, joita finanssirytyksen tulee tai on sallittua hyödyntää asiakkaan tuntemista tai muita rahanpesulain mukaisia velvoitteita täyttäessään. Finanssirytyksen tulee riskiperusteista lähestymistapaa käyttäen määritellä, mistä lähteistä ja miten asiakkaan tuntemistietoja kerätään. Lähteinä voidaan käyttää erilaisia viranomaislähteitä sekä muita uskottavia ja luotettavia tietoja, mutta osa tiedoista voidaan kerätä suoraan asiakkaalta. Tietolähteiden luotettavuuden aste on harkittava osana asiakkaaseen liittyvien rahanpesun ja terrorismin rahoittamisen riskien arviointia. Varmistaakseen tiedon uskottavuuden ja luotettavuuden finanssirytyksen voi olla tarpeen selvittää tiedon todenperäisyyttä useammista luotettavaksi arvioimistaan tietolähteistä.

Yksinomaan rahanpesulain vaatimusten täyttämiseksi hankitut tiedot tulee pitää erillään muista asiakastiedoista, eikä niitä saa käyttää muuhun kuin rahanpesulaissa säädettyyn tarkoitukseen. Henkilötietoja, jotka on hankittu ainoastaan rahanpesun ja terrorismin rahoittamisen estämiseksi ja paljastamiseksi, ei saa käyttää tarkoitukseen, joka on yhteensopimaton näiden tarkoitusten kanssa, kuten esimerkiksi finanssirytyksen tuotteiden tai palveluiden markkinointiin.

Rahanpesulain mukaan finanssirytyksen on ilmoitettava asiakkaalle, että rahanpesulain mukaisia asiakkaan tuntemistietoja ja muita henkilötietoja voidaan käyttää rahanpesun ja terrorismin rahoittamisen estämiseen, paljastamiseen ja selvittämiseen sekä muihin lainkohdassa mainittuihin tarkoituksiin.

Rahanpesuilmoituksen tekemistä tai selvittelyä ei saa paljastaa epäilyn kohteelle tai muulle henkilölle. Rajoituksen piiriin kuuluvat muun muassa sovellettuja

¹ Lukijan on hyvä huomioida, että rahanpesusäätelyssä viitataan terminologisesti yleensä "ilmoitusvelvolliseen" ja viranomaisen viittaa usein myös "valvottaviin".

² [EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS \(EU\) 2024/1624, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen](#) (ks. Artikla 76) sekä [EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI \(EU\) 2024/1640, jäsenvaltioissa käyttöön otettavista mekanismeista rahoitusjärjestelmän käytön estämiseksi rahanpesuun ja terrorismin rahoitukseen, direktiivin \(EU\) 2019/1937 muuttamisesta sekä direktiivin \(EU\) 2015/849 muuttamisesta ja kumoamisesta](#)

riskienhallintatoimenpiteitä, asiakkaan riskiluokitusta tai asiakkaan luottotietojen tarkastamista rahanpesuepäilyn yhteydessä koskevat tiedot. Finanssiyritys saa kuitenkin salassapitovelvoitteen estämättä luovuttaa tiedon rahanpesulaissa säädetyin rajoituksin muun muassa samaan rahoitus- ja vakuutusryhmittymään kuuluvalla toimiluvan saaneelle yhteisölle, jos tiedon luovuttaminen on välttämätöntä epäilyttävän liiketoimen arvioimiseksi eikä rahanpesun selvittelykeskus ole pyytänyt rajoittamaan tiedon luovuttamista.

Asiakkaan tuntemista koskevat tiedot on säilytettävä viiden vuoden ajan vakituisen asiakassuhteen päättymisestä tai laissa tarkoitetun satunnaisen liiketoimen suorittamisesta.

Ilmoitusvelvollisuuden täyttämiseksi hankitut tiedot ja asiakirjat on poistettava viiden vuoden kuluttua asiakassuhteen päättymisestä tai epäilyttävän liiketoimen suorittamisesta, ellei niiden edelleen säilyttäminen ole tarpeen esim. rikostutkinnan turvaamiseksi. Edelleen säilyttämisen tarpeellisuus on tutkittava viimeistään kolmen vuoden kuluttua edellisestä säilyttämisen tarpeellisuuden tarkistamisesta.

Rekisteröidyllä ei ole oikeutta tarkastaa ilmoitus- tai selonottovelvollisuuden täyttämiseksi hankittuja tietoja ja asiakirjoja, mutta tietosuojavaltuutettu voi rekisteröidyn pyynnöstä tarkastaa näiden tietojen käsittelyn lainmukaisuuden.

4.5.2 Kansainväliset talouspakotteet ja kansalliset jäädyttämispäätökset

Kansainvälisillä talouspakotteilla pyritään jäädyttämään pakotteiden kohteena olevien tahojen omistuksessa, hallussa tai määräysvallassa olevat varat ja muut taloudelliset resurssit. Lisäksi pakotteet saattavat sisältää kiellon rahoittaa mainittuja tahoja tai kiellon luovuttaa tai välittää varoja mainituille tahoille.

Finanssiyritykset ovat velvollisia seuraamaan kansainvälisiä pakotteita ja kansallisia jäädyttämispäätöksiä ja niiden muutoksia, tarkistamaan asiakasrekisterinsä säännöllisesti sekä seuraamaan maksuliikennettä ja muita liiketoimia varmistaakseen, että ne menettelevät pakotteiden ja jäädyttämispäätösten luomien velvoitteiden mukaisesti. Pakotteiden ja jäädyttämispäätösten noudattamisessa tarvittavien henkilötietojen käsittely on tarpeen finanssiyritystä sitovan lakisääteisen velvoitteen noudattamiseksi.

Suomea sitovat kansainväliset talouspakotteet perustuvat YK:n turvallisuusneuvoston ja EU:n neuvoston päätöksiin. EU:ssa pakotteita koskevat tarkemmat määräykset annetaan neuvoston asetuksina, jotka ovat suoraan sovellettavaa lainsäädäntöä kaikissa EU:n jäsenmaissa. Pakotteiden kohteena olevien henkilöiden, yhteisöjen, ryhmien tai muiden tahojen nimet julkaistaan pakotesäädösten liitteissä. Kansallisesti keskusrikospoliisi tekee päätökset varojen jäädyttämiseksi. Päätökset perustuvat kansalliseen lakiin (325/2013), joka koskee varojen jäädyttämistä terrorismin torjumiseksi.

YK:n ja EU:n asettamien talouspakotteiden lisäksi useilla valtioilla ja viranomaisilla on omia kansallisia pakotteita, esimerkiksi Yhdysvaltojen Office of Foreign Assets Control (OFAC) -viranomaisen listaukset henkilöistä ja yhteisöistä, joiden varat tulee OFACin

mukaan jäädyttää. Finanssivalvonta on suosittanut³ ohjeissaan valvottavaa huomioimaan riskienhallinnassaan kolmansien maiden pakotteet niissä tapauksissa, joissa kyseisen kolmannen maan pakotteiden rikkominen voi aiheuttaa valvottavan maksuvalmiudelle tai vakavaraisuudelle huomattavan taloudellisen riskin, vaikka kyseiset pakotteet eivät olisi Suomessa oikeudellisesti sitovia.

4.6 Luottotiedot

Luottotietojen käyttämisestä säädetään luottotietolaissa, ja positiiviseen luottotietorekisteriin talletettavista luottotiedoista ja niiden käsittelystä säädetään laissa positiivisesta luottotietorekisteristä. Luottotietoja saa käyttää se, joka tarvitsee tietoa luoton myöntämistä tai luoton valvontaa varten tai muuhun laissa yksilöityyn tarkoitukseen. Luottotiedot voidaan tarkastaa myös vakuutuksen myöntämistä varten. Finanssiyrityksen toimihenkilö saa tehdä luottotietokyselyn ainoastaan silloin, kun hänen työtehtävänsä sitä edellyttävät.

Kun henkilöluottotiedot tarkastetaan ulkopuolisesta luottotietorekisteristä, asiakkaalle tulee ilmoittaa henkilöluottotietojen käytöstä sekä siitä, mistä rekisteristä luottotiedot hankitaan tai on hankittu. Sen sijaan mikäli luottotiedot tarkastetaan rahanpesuepäilyn yhteydessä, siitä ei saa ilmoittaa asiakkaalle. Henkilöluottotietojen käytöstä voidaan ilmoittaa esimerkiksi luottolaitosten palveluita koskevissa hakemuksissa tai palveluiden yleisissä ehdoissa. Ilmoittaminen voidaan hoitaa tarvittaessa myös suullisesti.

Jos luottolaitos hylkää luottihakemuksen tai vakuutusyhtiö vakuutushakemuksen ulkopuolisesta luottotietorekisteristä saatujen henkilöluottotietojen perusteella, tulee myös huomioida se, että luottolaitoksen tai vakuutusyhtiön on välittömästi päätöksen jälkeen ilmoitettava luoton- tai vakuutushakijalle tällaisesta luottotietojen käytöstä ja siitä, mistä luottotietorekisteristä tiedot ovat peräisin.

Henkilöllä on oikeus saada tietää, mitä häntä koskevia tietoja luottotietorekisteriin on talletettu tai ettei rekisterissä ole häntä koskevia tietoja. Tätä oikeutta käyttävä henkilö tulee ohjata ottamaan yhteyttä luottotietorekisterin pitäjään.

Myös luottolaitoksen asiakasrekistereissä olevat tiedot voivat olla luottotietoja silloin, kun niitä käytetään luottoa myönnettäessä.

4.7 Henkilötunnuksen käsittely

Henkilötunnuksen käsittelyn edellytykset määritellään tietosuojalain 5 luvun 29 §:ssä.

4.7.1 Henkilötunnuksen käsittely finanssiyrityksissä

Finanssiyritysten toiminnassa on tärkeää, että toimintaan liittyvät henkilöt (kuten tallettajat, maksajat, takaaajat, käyttöoikeudenhaltijat, luoton- ja vakuutushakijat, vakuutuksenottajat, vakuutetut, edunsaajat ja vahingonkärsineet) voidaan yksilöidä täysin yksiselitteisesti. Tämän vuoksi tietosuojalakiin on otettu nimenomainen maininta

³ Finanssivalvonnan määräykset ja ohjeet 4/2023 pakotesäätelyn ja kansallisten jäädyttämispäätösten noudattamiseen liittyvästä asiakkaan tuntemisesta (voimaan 1.3.2024), ks. luku 10.

siitä, että henkilötunnuksen käsittely on finanssiryitysten toiminnassa sallittua, jos se on tarpeen rekisteröidyn yksiselitteiseksi yksilöimiseksi.

Vakuutusyhtiö voi esimerkiksi pyytää vakuutuksen hakijaa ilmoittamaan henkilötunnuksensa ennen kuin yhtiö tekee itseään sitovan vakuutustarjouksen. Lisäksi vakuutusyhtiö voi kysyä vakuutuksenhakijan tai vakuutettavan henkilön henkilötunnusta myös verkkopalveluissaan (esim. hintalaskurit). Henkilötunnusta käsitellään myös esimerkiksi luottotietojen tarkastamisen yhteydessä. Henkilötunnus varmistetaan yleensä joko finanssiryityksen omasta asiakasrekisteristä tai väestötietojärjestelmästä. Finanssiryityksen tulee henkilötunnusta kysyessään informoida asianomaista henkilöä läpinäkyvästi siitä, miksi henkilötunnuksen antaminen on tarpeellinen ja mistä lähteistä se tarkistetaan. Lain nojalla vakuutusyhtiö voi myös esimerkiksi tallettaa henkivakuutuksen yhteyteen tiedon edunsaajan henkilötunnuksesta. On kuitenkin huomattava, että finanssiryityksen ei ole sallittua käyttää rekisteröidyn henkilöllisyyden tunnistamiseen yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää.

4.7.2 Henkilötunnuksen luovuttaminen osoitetietojen päivitystä varten

Finanssiryitys voi saada henkilötunnuksen ulkopuoliselta taholta (esim. väestörekisteristä) osoitetietojen päivittämiseksi tai moninkertaisten postilähetysten välttämiseksi, jos henkilötunnus on jo finanssiryityksen käytettävissä.

4.7.3 Henkilötunnuksen merkitseminen tulosteisiin

Finanssiryityksen on huolehdittava siitä, että henkilötunnusta ei tarpeettomasti merkitä tulostettuihin tai laadittuihin asiakirjoihin. Henkilötunnusta ei saa näkyvästi käyttää esimerkiksi postilähetyksissä tai markkinointikirjeissä. Sen sijaan esimerkiksi viranomaiskäyttöön tarkoitetussa asiakirjassa henkilötunnus voi olla tarpeellinen. Esimerkiksi sosiaalivakuuttamisessa henkilötunnus on tärkeä yksilöivä tunnistus, jota käytetään asioitaessa viranomaisten kanssa sekä henkilöä koskevissa virallisissa asiakirjoissa.

4.8 Turvakielto

Turvakielto on väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain 4 luvun 36 §:n mukainen tietojenluovutuskielto, jolla rajoitetaan henkilön yhteystietojen luovuttamista väestötietojärjestelmästä. Turvakielto koskee usein koko perhettä. Mikäli asiakkaalla on turvakielto, Digi- ja väestötietovirasto ei välitä asiakkaan osoitetietoja finanssiryitykselle. Turvakieltoasiakkaan tulee itse ilmoittaa finanssiryitykselle turvakiellostaan, sillä turvakieltopäätös velvoittaa ainoastaan viranomaisia.

Esimerkiksi luottolaitoksen järjestelmissä oleva tieto asiakkaan turvakiellostaan ei estä asiakkaan yhteystietojen välittämistä luottolaitoksen asiakastietojärjestelmästä niille tahoille (esim. korttimaksunsaajat, viranomaiset), joille luottolaitos voi lainsäädännön ja sopimusehtojen mukaan välittää asiakkaan tietoja. Lisäksi tietoa asiakkaan turvakiellostaan ja turvakielto määräyksen suojaamista yhteystiedoista voidaan käsitellä

ja välittää lainsäädännön mahdollistamissa tilanteissa sen konsernin tai muun yhteisörakenteen sisällä, johon finanssiyritys kuuluu.

Turvakieltoasiakkaan tulee ilmoittaa finanssiyritykselle mihin osoitteeseen hän haluaa postinsa toimitettavan. Tämä osoite voi olla esimerkiksi postilokero-osoite, joka voi välittyä edellä mainituissa tilanteissa ulkopuolisille tahoille. Säännökset asiakkaan tuntemisesta edellyttävät kuitenkin, että finanssiyrityksellä on oikeus vaatia turvakieltoasiakasta toimittamaan myös varsinaisen osoitteensa, joka asiakasrekisteriin tallennettuna tietona on pankki- ja vakuutussalaisuuden alainen tieto.

5 Rekisterinpitäjän velvollisuudet

5.1 Sisäänrakennettu ja oletusarvoinen tietosuojaja

Sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus tarkoittaa sitä, että finanssiyrityksen on suunniteltava ja toteutettava henkilötietojen käsittelyä koskevat prosessinsa siten, että henkilötietojen käsittelyä koskevat tietosuojaperiaatteet toteutuvat käsittelyn jokaisessa vaiheessa. Sisäänrakennettu ja oletusarvoinen tietosuoja on huomioitava esimerkiksi kehitettäessä uusia tuotteita, palveluita, järjestelmiä ja sovelluksia ja suunniteltaessa hankintoja ja projekteja.

Tietosuoja-asetuksen mukaan rekisterinpitäjän on, ottaen huomioon tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset ja käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit yksilölle, toteutettava henkilötietojen käsittelytapojen määrittämisen ja käsittelyn yhteydessä asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta käsittely vastaa tietosuoja-asetuksen vaatimuksia ja rekisteröidyn oikeuksia suojataan. Jotta näihin vaatimuksiin voidaan vastata, tulee organisaatiossa arvioida näitä vaatimuksia yhteistyössä eri alojen asiantuntijoiden kesken. Sääntely edellyttää, että organisaatiot itse arvioivat ja määrittävät asianmukaisten toimenpiteiden tason.

Asetuksen tarkoittamia teknisiä toimenpiteitä ovat muun muassa tietojen suojauskäytännöt, käyttövaltuuksien hallinta, lokit ja muut tekniset kontrollit, tietojen pseudonymisointi ja anonymisointi sekä tietojen arkistointi ja hävittäminen. Organisatorisia toimenpiteitä ovat esimerkiksi henkilötietojen käsittelyyn liittyvien tehtävien ja vastuiden määrittely, sisäiset ohjeet ja koulutus sekä esihenkilövalvonta. Myös muusta sääntelystä tulevat vaatimukset saattavat vaikuttaa sisäänrakennetun ja oletusarvoisen tietosuojan tason vaatimuksiin.

Lisäksi rekisterinpitäjän on oletusarvoisen tietosuojan vaatimuksen mukaisesti toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että se käsittelee oletusarvoisesti vain kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Tarkoitus on varmistaa, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

5.2 Osoitusvelvollisuus

Tietosuoja-asetuksessa säädetään osoitusvelvollisuuden periaatteesta (artikla 5.2). Osoitusvelvollisuus tarkoittaa sitä, että finanssiyrityksen on rekisterinpitäjänä pystyttävä käytännössä osoittamaan, että se noudattaa tietosuoja-asetusta. Esimerkiksi tietoturvaloukkaustilanteissa osoitusvelvollisuuden avulla voidaan näyttää, että rekisterinpitäjällä on käytössään tarvittavat menettelytavat ja tekniset suojaustoimenpiteet rekisteröityjen oikeuksien turvaamiseksi ja henkilötietojen suojaamiseksi. Osoitusvelvollisuus tarkoittaa myös dokumentointivelvollisuutta, ja se on huomioitava jo henkilötietojen käsittelyn suunnitteluvaiheessa.

Tietosuojavaltuutettu on julkaissut omilla verkkosivuillaan listauksen osoitusvelvollisuuden toteuttamiseksi mahdollisesti tarvittavista toimenpiteistä ja dokumenteista. Osoitusvelvollisuuden ja sitä koskevien vaatimusten laajuus riippuu muun muassa organisaation koosta, henkilötietojen määrästä ja siitä, millaisia henkilötietoja rekisterinpitäjä käsittelee. Oleellisia dokumentteja ovat esimerkiksi:

- informointikäytännöt (esimerkiksi tietosuojaselosteet)
- seloste käsittelytoimista
- tietosuoja- ja tietoturvapoliitikat
- tietojen käsittelyä finanssiyrityksessä koskevat ohjeistukset
- koulutukset
- tietosuojaa koskevat vaikutustenarvioinnit, tasapainotestit
- tietoturvaloukkauksia koskeva dokumentointi
- tietosuojavastaavan asemaa koskevat dokumentit
- henkilötietojen käsittelyä koskevat sopimukset.

5.3 Tietosuojavastaavan nimittäminen

Tietosuoja-asetuksessa säädetään niistä tilanteista, joissa tietosuojavastaavan nimittäminen on pakollista. Finanssialan toimijat usein katsovat perustelluksi nimittää tietosuojavastaavan, jos niissä käsitellään laajasti asiakastietoja. Tietosuoja-asetus sisältää yksityiskohtaiset säännökset tietosuojavastaavan asemasta ja tehtävistä. Konserni voi nimittää yhden tietosuojavastaavan edellyttäen, että konsernin jokaisesta toimipaikasta voidaan helposti ottaa tähän yhteyttä. Lähtökohtaisesti yhdellä yhteisöllä (y-tunnuksellinen organisaatio) ei voi olla useampia tietosuojavastaavia.

Tietosuojavastaavalla voi kuitenkin olla apunaan asiantuntijaorganisaatio. On tärkeää huolehtia myös varahenkilöjärjestelyistä mahdollisia poissaolo- tai sijaistustilanteita varten. Nimitettäessä tietosuojavastaavaa tulee ottaa huomioon henkilön ammattipätevyys ja asiantuntemus erityisesti tietosuojalainsäädännöstä ja alan käytänteistä.

Tietosuojavastaavan on oltava asetuksen tarkoittamalla tavalla riippumaton, eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Tietosuojavastaava ei saa esimerkiksi määritellä henkilötietojen käsittelyn tarkoituksia. Tietosuojavastaavan tehtävänä on muun muassa seurata ja valvoa henkilötietojen käsittelyn

lainmukaisuutta ja auttaa organisaatiota noudattamaan tietosuojalainsäädännön asettamia velvoitteita antamalla tietoja ja neuvoja tietosuoja koskevista vaatimuksista organisaation johdolle ja henkilöstölle. Tietosuojavastaava ei kuitenkaan ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta, vaan vastuu kuuluu organisaation johdolle. Finanssialalla tietosuojavastaavan rooli tyypillisesti rinnastuu vastaaviin riippumattomiin toimintoihin kuten compliance-toimintoon ja sisäiseen tarkastukseen.

Tietosuojavastaavan tehtävänä on myös toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Organisaation on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle.

5.4 Tietosuoja koskeva vaikutustenarviointi ja ennakkokuuleminen

Kun henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille, on rekisterinpitäjän tehtävä tietosuoja koskeva vaikutustenarviointi. Finanssialan käsittelytoimenpiteet ovat usein sellaisia, että niistä tulee tehdä vaikutustenarviointi. Vaikutustenarviointia vaativat tilanteet on listattu tietosuoja-asetuksessa, ja tietosuojavaaltuutettu on täydentänyt tätä listaa ohjeistuksella, joka on saatavilla tietosuojavaaltuutetun sivuilta.⁴ Asetuksen ja valtuutetun listaukset eivät kuitenkaan ole tyhjentyviä, ja vaikutustenarvioinnin tarve tulee arvioida aina tapauskohtaisesti. Tyypillisesti finanssialalla tehdään vaikutustenarviointeja esimerkiksi automaattista päätöksentekoa tai profilointia koskevissa käyttötapauksissa. Vaikka käsittely ei olisi ns. korkean riskin käsittelyä, vaikutustenarvioinnin voi aina tehdä. Toisin sanoen vaikutustenarviointia voi hyödyntää työkaluna tietosuoja vaatimusten toteuttamisen dokumentoinnissa ja osoitusvelvollisuuden täyttämisessä.

Rekisterinpitäjän on tarvittaessa varmistettava, että henkilötietojen käsittely tosiasiallisesti tapahtuu vaikutustenarvioinnin mukaisesti, etenkin silloin, jos käsittelytoimien sisältämä riski muuttuu. Vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja organisaation tietosuojavastaavalta, jos sellainen on nimitetty.

Jos vaikutustenarvioinnin perusteella riskin taso on korkea, eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi, on rekisterinpitäjän kuultava valvontaviranomaista ennen käsittelyn aloittamista (ennakkokuulemisvelvoite). Rekisterinpitäjän on toimitettava valvontaviranomaiselle kuulemista varten tarvittavat tiedot.

Ennakkokuulemisen perusteella viranomainen voi antaa ohjeita toimista riskien pienentämiseksi tai ryhtyä muihin toimenpiteisiin kuten antaa varoituksen. Ohjeen mukaiset lisätoimenpiteet tulee tehdä ennen kuin käsittely aloitetaan, jotta käsittely olisi lainmukaista.

⁴ [Luettelo vaikutustenarviointia edellyttävistä käsittelytoimista | Tietosuojavaaltuutetun toimisto](#)

5.5 Tietoturva: käsittelyn turvallisuus, henkilötietojen suojaaminen ja hävittäminen

Finanssirytyksen on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten käyttöoikeuksien hallinta, käytön valvonta, tietojen minimointi ja sisäinen ohjeistus. Ohjeistuksessa tulee kiinnittää huomiota muun muassa siihen, että henkilötietojen käyttö on sallittua vain työtehtävien hoitamiseksi. Ohjeistuksen noudattamista ja henkilötietojen käsittelyä tulee myös seurata ja valvoa.

Henkilötiedot tulee suojata siirron, tallennuksen ja käsittelyn aikana tapahtuvalta oikeudettomalta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai tietoihin pääsylvä. Tietojen suojaamisesta on huolehdittava käsittelyn kaikissa vaiheissa alkaen tietojen keräämisestä ja päättyen niiden tuhoamiseen. Sekä manuaalisesti että automaattisesti käsiteltävät henkilötiedot on suojattava.

Finanssirytysten tietoturvasuvelvoitteista on olemassa erityislainsäädäntöä, kuten DORA-asetus (asetus finanssialan digitaalisesta häiriönsietokyvystä) ja sitä tukevaa viranomaisohjeistusta⁵, jotka täytyy ottaa huomioon mietittäessä teknisiä ja organisatorisia toimenpiteitä. Lisäksi kansallisessa lainsäädännössä on myös paljon säännöksiä finanssirytyksiin soveltuvista vaatimuksista, kuten laki sähköisen viestinnän palveluista. Samoin esimerkiksi luottotietolaki määrittelee erikseen hyvän luottotietotavan, jonka perusteella luottotietojen käyttäjän on noudatettava toiminnassaan huolellisuutta ja varmistuttava siitä, että luottotietojen laadusta, rekisteröityjen oikeuksien toteutumisesta, tietoturvasuvelvuksesta ja luottotietojen käytön valvonnasta huolehditaan.

6 Velvoitteet tietoturvaloukkaustilanteissa

6.1 Mikä on henkilötietojen tietoturvaloukkaus?

Henkilötietojen tietoturvaloukkauskalla tarkoitetaan tapahtumaa, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen tai luvaton luovuttaminen taikka luvattoman tahon pääsy tietoihin.

Finanssirytyksen on rekisterinpitäjänä lähtökohtaisesti ilmoitettava tietoturvaloukkauksista tietosuojaviranomaiselle ja jossain tapauksissa myös rekisteröidylle. Ilmoitusvelvollisuudesta on olemassa joitakin poikkeuksia, joita käsitellään myöhemmin tässä luvussa. Rekisterinpitäjän pitää myös suunnitella, miten mahdollinen tietoturvaloukkaus tunnistetaan, ilmoitetaan, selvitetään ja dokumentoidaan. Tämä on tarpeen, jotta se pystyy toimimaan vahingon minimoimiseksi ja toimintakyvyn palauttamiseksi.

Tietoturvaloukkaukset luokitellaan yleisesti seuraavien tunnettujen tietoturvaperaiaatteiden mukaisesti:

⁵ Finanssivalvonnan määräys ja ohjekokoelmasta esimerkiksi seuraavat ohjeet 6/2015 henki- ja vahinkovakuutusyhtiön toiminnan aloittaminen ja hallintajärjestelmä ja 8/2014 Operatiivisen riskin hallinta rahoitussektorin valvottavissa.

- ”Tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus” – henkilötietojen tahaton tai luvaton luovuttaminen tai käyttöön antaminen.
- ”Tietojen eheyteen vaikuttava tietoturvaloukkaus” – henkilötietojen luvaton tai tahaton muuttaminen.
- ”Tietojen käytettävyyteen vaikuttava tietoturvaloukkaus” – tahaton tai luvaton henkilötietoihin pääsyn menettäminen tai henkilötietojen tuhoaminen.

Tietoturvaloukkauksella saattaa olla useita erilaisia henkilöihin kohdistuvia haittavaikutuksia, jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja. Näitä saattavat olla mm. omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintä, identiteettivarkaus tai petos, taloudelliset menetykset, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen ja salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys. Niihin saattaa sisältyä myös muuta merkittävää taloudellista tai sosiaalista vahinkoa kyseisille henkilöille. Yksi rekisterinpitäjän tärkeimmistä velvoitteista on arvioida näitä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä ja toteuttaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä niihin puuttumiseksi.

Finanssirytyksen toimintavelvoitteet tietoturvaloukkauksen tapahtuessa ovat:

- tietoturvaloukkauksen dokumentointi, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimenpiteet
- mahdollinen ilmoittaminen valvontaviranomaiselle (paitsi, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä)
- ilmoittaminen rekisteröidylle silloin, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Tietoturvaloukkausten käsittely ja ilmoitusvelvollisuuden arviointi edellyttää aina tapauskohtaista harkintaa. Näin ollen finanssirytyksen on suositeltavaa suunnitella toimintamalli tyypillisiä tietoturvaloukkauksia varten esimerkiksi erilaisten malliesimerkkien avulla. Malliesimerkeillä voidaan määrittää alustavasti tyypillisiä rekisteröidylle aiheutuvia riskejä tietystä henkilötietojen tietoturvaloukkauksista (esim. palveluiden käytön estyminen, terveystietojen oikeudeton luovutus väärälle asiakkaalle). Tällaiset malliesimerkit voivat auttaa riskiarviointia todellisissa tilanteissa.

6.2 Ilmoitus tietosuojaviranomaiselle

Rekisterinpitäjänä toimivan finanssirytyksen on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta tietosuojavaltuutetulle. Ilmoitusta ei tarvitse tehdä, jos loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Jos rekisterinpitäjä ei ilmoita ilmoitusvelvollisuuden piiriin kuuluvasta tietoturvaloukkauksesta valvontaviranomaiselle 72 tunnin kuluessa, sen on toimitettava viranomaiselle asiaa koskeva perusteltu selvitys.

Valvontaviranomaiselle annettavan ilmoituksen tulee sisältää vähintään seuraavat tiedot:

- kuvaus henkilötietojen tietoturvaloukkauksesta, sisältäen mahdollisuuksien mukaan tiedot asianomaisten rekisteröityjen ryhmistä ja arvioiduista lukumääristä sekä henkilötietotyyppien ryhmistä ja arvioiduista lukumääristä
- kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteydenottopiste lisätiedon saamiseksi
- kuvaus toimenpiteistä, jotka rekisterinpitäjä on suunnitellut tai toteuttanut tietoturvaloukkauksen johdosta, mukaan lukien toimenpiteet haittavaikutusten lieventämiseksi.

Mikäli kaikkia edellä lueteltuja tietoja ei ole mahdollista toimittaa samanaikaisesti, rekisterinpitäjä voi toimittaa ne vaiheittain, tällöinkin ilman aiheetonta viivytystä.

6.3 Tietoturvaloukkauksen dokumentointi

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, niihin liittyvät seikat, niiden vaikutukset sekä toteutetut korjaavat toimenpiteet.

Dokumentaation on oltava sellainen, että valvontaviranomainen voi sen avulla varmistaa, että asetuksen vaatimuksia on noudatettu. Dokumentointia kannattaa hyödyntää myös organisaation päivittäisessä riskienhallinta- ja tietosuojatyössä sisäisten prosessien parantamiseksi ja tietoturvaloukkausten vähentämiseksi.

6.4 Ilmoitus rekisteröidylle

Mikäli henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjänä toimivan finanssirytyksen on ilmoitettava tietoturvaloukkauksesta valvontaviranomaisen lisäksi rekisteröidylle, jota loukkaus koskee, ilman aiheetonta viivytystä. Tyypillisesti ilmoitusvelvollisuus tulee kyseeseen esimerkiksi tilanteessa, jossa on riski rekisteröidyn tietojen väärinkäytöstä.

Rekisteröidylle annettavassa ilmoituksessa on vähintään kuvattava selkeällä ja yksinkertaisella kielellä tietoturvaloukkauksen luonne, ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteydenottopiste lisätiedon saamiseksi, kuvattava tietoturvaloukkauksen todennäköiset seuraukset sekä kuvattava toimenpiteet, jotka rekisterinpitäjä on suunnitellut tai toteuttanut tietoturvaloukkauksen johdosta, mukaan lukien toimenpiteet haittavaikutusten lieventämiseksi.

Tietoturvaloukkauksesta ei tarvitse ilmoittaa rekisteröidylle, jos jokin seuraavista edellytyksistä täyttyy:

- Rekisterinpitäjä on suojannut tietoturvaloukkauksen kohteena olevat henkilötiedot asianmukaisin teknisin ja organisatorisin suojatoimenpitein, erityisesti sellaisin, joiden avulla henkilötiedot on esimerkiksi salaamalla muutettu muotoon, jossa ne eivät ole ulkopuolisen ymmärrettävissä.
- Rekisterinpitäjä on toteuttanut toimenpiteitä, jotka pienentävät rekisteröityjen oikeuksiin ja vapauksiin kohdistuvan korkean riskin toteutumistodennäköisyyttä.
- Ilmoittaminen vaatisi kohtuutonta vaivaa; tällöin rekisterinpitäjän on käytettävä muuta toimintatapaa, esimerkkinä julkinen tiedonanto, jolla rekisteröidylle tiedotetaan loukkauksesta yhtä tehokkaasti kuin ilmoittamalla.

Tilanteessa, jossa rekisterinpitäjä ei ole vielä ilmoittanut tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia tällaisen ilmoituksen tekemistä.

6.5 Muut ilmoitukset tietoturvaloukkauksista

Tietoturvaloukkaus tai sen uhka voi aiheuttaa finanssiyritykselle muitakin ilmoitusvelvoitteita. Esimerkiksi luottolaitokset sekä tietyt sijoituspalveluyritykset, rahastoyhtiöt, vaihtoehdorahastojen hoitajat ja työeläkevakuutusyhtiöt raportoivat tietoturvaloukkaukset tietyissä tilanteissa myös Finanssivalvonnalle.⁶ Finanssiyrityksen on syytä varmistaa, että se on tietoinen myös tällaisista muista toimintaansa soveltuvista ilmoitusvelvoitteista, jotka voivat olla myös päällekkäisiä tietosuoja sääntelystä seuraavien velvoitteiden kanssa.

Henkilötietojen käsittelijänä toimivan finanssiyrityksen on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan loukkauksen tietoonsa. Ilmoituksessa tulee ottaa huomioon, mitä organisaatioiden välisessä henkilötietojen käsittelyä koskevassa sopimuksessa ja mahdollisessa rekisterinpitäjän antamassa ohjeistuksessa on määrätty esimerkiksi ilmoituksen määräajasta ja sisällöstä.

7 Rekisteröidyn oikeudet

7.1 Oikeus saada tietoa henkilötietojen käsittelystä

Tietosuoja-asetus velvoittaa finanssiyrityksiä informoimaan henkilötietojen käsittelystä. Informoinnin tarkoituksena on, että rekisteröity saa kattavan ja selkeän kuvan henkilötietojen käsittelyn kokonaisuudesta.

Rekisteröidylle on kerrottava muun muassa,

- kuka rekisterinpitäjä on
- mitä tarkoitusta varten rekisteröidyn henkilötietoja käsitellään
- kuinka kauan henkilötietoja tarvitaan

⁶ Finanssivalvonnan määräys ohjekokoelmasta 8/2014 Operatiivisen riskin hallinta rahoitussektorin valvottavissa sekä työeläkevakuutusyhtiöiden osalta määräykset ja ohjeet 2/2017 Työeläkevakuutusyhtiöiden hallinto, johon on 1.4.2024 voimaan tullut muutoksen mukaisesti myös tietyissä tilanteissa raportointivelvollisuus FIVA:lle silloin, kun tehdään ilmoitus tietosuojaviranomaisillekin (kohdassa 11.1).

- luovutetaanko henkilötietoja eteenpäin ja siirretäänkö niitä ETA-maiden ulkopuolelle
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- millaisia riskejä rekisteröidyn oikeuksiin ja vapauksiin kohdistuu.

Rekisterinpitäjän on annettava rekisteröidylle kaikki henkilötietojen käsittelyä koskevat tiedot tiiviissä, läpinäkyvässä, helposti ymmärrettävässä ja selkeässä muodossa. Rekisterinpitäjän tulee arvioida, onko annettu informaatio kielen ja johdonmukaisuuden kannalta ymmärrettävää kohderyhmän näkökulmasta. Läpinäkyvyyden periaatteesta säädetään osana tietosuoja-asetuksen lainmukaisen ja asianmukaisen käsittelyn periaatetta. Henkilötietoja on käsiteltävä rekisteröidyn kannalta läpinäkyvästi, ja rekisterinpitäjän on pystyttävä osoittamaan, että näin on toimittu.

Tietosuojan läpinäkyvyyttä voidaan edistää seuraavilla tekijöillä:

- Selkeys – tiedot on esitettävä selvällä ja yksinkertaisella kielellä.
- Saatavuus – tietojen on oltava helposti rekisteröidyn saatavilla.
- Asiayhteys - tiedot on annettava oikeaan aikaan keräämisen yhteydessä, esimerkiksi ostettaessa vakuutusta finanssiyrityksen verkkosivulta, tärkeimmät tiedot annetaan ostotapahtuman yhteydessä ko. verkkosivulla.
- Monikanavaisuus – tietoa on annettava eri kanavissa ja mahdollisuuksien mukaan myös muita kuin tekstimuotoisia välineitä hyödyntämällä.
- Kerroksellisuus – tietoja voidaan ryhmitellä ja kategorisoida siten, että annettavista tiedoista saadaan sekä kattavia että ymmärrettäviä.

Tietosuoja-asetuksessa ei säädetä tietyistä muodosta (esim. tietosuojaselosteesta), jolla informointivaroituksen alaiset tiedot olisi rekisteröidylle tarjottava. Yleisölle suunnatut tiedot voidaan antaa sähköisessä muodossa esimerkiksi verkkosivuilla. Henkilötietojen käsittelyä koskevat tiedot tulee antaa selkeästi erillään muusta informaatiosta. Informaation tulee olla rekisteröidyn saatavilla maksutta. Pääsääntöisesti tiedot on annettava kirjallisesti.

7.2 Oikeus saada tutustua tietoihin (tarkastusoikeus)

Jokaisella henkilöllä on oikeus saada finanssiyritykseltä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos tietoja käsitellään, oikeus saada kopio niistä. Tarkastusoikeuttaan käyttävän henkilön on annettava ja esitettävä finanssiyritykselle tietojen etsimiseksi tarpeelliset tiedot. Finanssiyrityksen tulee myös varmistua riittävällä tavalla pyynnön esittäjän henkilöllisyydestä. Henkilöllisyyden vahvistaminen ei saa kuitenkaan johtaa tarpeettomien henkilötietojen keräämiseen tai rekisteröidyn oikeuksien käytön vaikeutumiseen.

Tarkastusoikeus tarkoittaa pääsääntöisesti sitä, että finanssiyrityksen on pyydettyäessä toimitettava rekisteröidylle tiedot hänen henkilötietojensa käsittelystä finanssiyrityksen käytössä olevilla menetelmillä, ensisijaisesti sähköisesti.

Edellä mainittuun tarkastusoikeuteen perustuen finanssiyrityksen tulee antaa lisäksi seuraavat käsittelyä koskevat tiedot:

- tietojen käsittelyn tarkoitukset
- henkilötietoryhmät
- vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa
- mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- rekisteröidyn oikeus pyytää finanssiyritykseltä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista taikka henkilötietojen käsittelyn rajoittamista tai vastustaa tällaista käsittelyä
- oikeus tehdä valitus tietosuojaviranomaiselle
- jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot
- automaattisen päätöksenteon, muun muassa profiloinnin, olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Rekisteröidyn tarkastusoikeus rajoittuu kyseisen rekisteröidyn omiin henkilötietoihin, joita finanssiyritys käsittelee. Rekisteröidyn oikeus saada jäljennös tiedoistaan ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin, kuten esimerkiksi toisten henkilöiden henkilötietojen suojaan. Toisinaan on kuitenkin mahdollista, että rekisteröityä koskevissa tiedoissa on esimerkiksi finanssiyrityksen rekistereissä myös muita henkilöitä koskevia tietoja. Tällöin finanssiyrityksen on arvioitava tapauskohtaisesti, voiko heitä koskevien tietojen antaminen tarkastusoikeuttaan käyttävälle rekisteröidylle vaarantaa kyseisten kolmansien osapuolten oikeudet ja vapaudet. Finanssiyritys ei kuitenkaan voi automaattisesti kieltäytyä toimittamasta tietoja rekisteröidylle ainoastaan sen vuoksi, että tiedoissa on myös muita henkilöitä koskevia tietoja. Finanssiyrityksen on toteutettava asianmukaiset toimet, joiden avulla rekisteröidyn tarkastusoikeus toteutetaan mahdollisimman täysimääräisesti. Tämä voi tarkoittaa esimerkiksi muiden henkilöiden henkilötietojen peittämistä.

Tarkastusoikeutta voi käyttää se henkilö, jonka tiedoista on kyse, eli joka on rekisteröidyn asemassa. Lisäksi oikeutta rekisteröidyn puolesta voi käyttää myös kyseessä olevan rekisteröidyn valtuuttama henkilö. Tallennetut tiedot koskevat kaikki sitä henkilöä, jonka nimen alle tiedot on tallennettu, vaikka tiedoissa olisi myös toista henkilöä koskevia tietoja. Kaikki henkilöt eivät siis automaattisesti ole rekisteröidyn asemassa, vaikka heitä koskevia tietoja olisi tallennettu finanssiyrityksen järjestelmään toisen rekisteröidyn nimen yhteyteen (ks. TSV 28/523/2018).

Velvollisuus poistaa henkilötieto, jolle määritelty säilytysaika on päättynyt, saattaa joissakin tapauksissa johtaa siihen, ettei finanssiyrityksestä löydy enää tietoa tai asiakirjaa, jonka rekisteröity tarkastusoikeutensa nojalla haluaisi nähtäväkseen.

7.2.1 Tarkastusoikeus lokitiedoista ilmeneviin tietoihin

EU-tuomioistuimien on todennut ratkaisussaan C 579/21, että henkilöllä on oikeus saada henkilötietoihin tehtyihin kyselyihin liittyvät tiedot kyselyjen ajankohdista ja

tarkoituksista. Tyypillisesti ainakin osa näistä tiedoista voidaan saada lokitietojen avulla. Rekisteröidyllä ei sen sijaan lähtökohtaisesti ole oikeutta saada tietoa hänen tietojaan käsitelleiden työntekijöiden henkilöllisyydestä, kun työntekijät ovat käsitelleet henkilötietoja rekisterinpitäjän alaisuudessa ja sen ohjeiden mukaisesti. Jos tiedot kuitenkin ovat välttämättömiä rekisteröidyn asetukseen perustuvien oikeuksien käyttämiseksi, voidaan tästä lähtökohdasta poiketa. Tällöin on huomioitava myös työntekijöiden oikeudet ja vapaudet, ja ristiriitatilanteissa työntekijän ja rekisteröidyn oikeuksia ja vapauksia on punnittava keskenään.

7.2.2 Rajoitukset rekisterinpitäjän velvollisuuteen toimittaa tietoja rekisteröidylle

Rekisterinpitäjällä ei ole velvollisuutta toimittaa rekisteröidylle tietoja, jotka saattavat vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin. Tällaiset tilanteet on arvioitava aina tapauskohtaisesti. Kyse saattaa olla esimerkiksi tilanteesta, jossa rekisteröidyn tietoihin liittyy kolmatta henkilöä koskevia tietoja tai kyse on finanssiyrityksen liikesalaisuuksista. Rekisterinpitäjään saattaa soveltua myös kiello kertoa rekisteröidylle esimerkiksi rekisteröidyn tietoja koskevasta viranomaistiedustelusta. Myös esimerkiksi kansallisessa tietosuojalaissa 34 §:ssa ja rahanpesulain 4 luvun 3 §:ssa on mainittu rajoituksia rekisterinpitäjän velvollisuuteen toimittaa tietoja rekisteröidylle.

7.2.3 Vakuutuslääkärin henkilöllisyys

Asiakkaan tarkastusoikeus ei ulotu vapaaehtoisia vakuutuksia koskevassa vastuunvalinnassa tai korvauskäsittelyssä käytettävän asiantuntijalääkärin henkilöllisyyteen, eikä vakuutusyhtiön siis tarvitse antaa asiakkaalle kyseistä tietoa. Lakisääteisiä vakuutuksia koskevissa päätöksissä vakuutuslääkärin henkilöllisyyttä koskeva tieto on kuitenkin julkista tietoa, sillä vakuutuslääkäri käyttää päätöksissään julkista valtaa. Asiakkaalla on siis julkisuuslain nojalla oikeus saada tieto asiantuntijalääkärin henkilöllisyydestä.

7.3 Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia, että finanssiyritys oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys. Tiedon virheellisyys ratkaistaan tapauskohtaisesti sen perusteella, onko tieto käsittelyn tarkoituksen kannalta virheellinen (tarpeeton, puutteellinen, vanhentunut).

7.4 Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")

Finanssialan sääntelystä johtuen finanssiyrityksen tulee lähtökohtaisesti säilyttää rekisteröidyn tietoja koko asiakassuhteen voimassaolon ajan ja vielä tietyn ajan asiakassuhteen päättymisen jälkeenkin, jos käsittelylle on asianmukainen peruste. Oikeutta omien tietojen poistamiseen ei ole, jos käsittely on tarpeen finanssiyrityksiin sovellettavaan lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen veloitteen noudattamiseksi, tai jos käsittely tapahtuu oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Mikäli edellä mainittuja perusteita ei ole, rekisteröidyllä on oikeus saada finanssiyritys poistamaan häntä koskevat henkilötiedot ilman aiheetonta viivytystä, jos jokin seuraavista perusteista täyttyy:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin.
- Rekisteröity peruuttaa suostumuksen henkilötietojensa käsittelyyn tai nimenomaisen suostumuksensa erityisten henkilötietoryhmien käsittelyyn, eikä käsittelyyn ole muuta laillista perustetta.
- Rekisteröity vastustaa yleiseen etuun tai oikeutettuun etuun perustuvaa käsittelyä eikä käsittelyyn ole olemassa perusteltua syytä, tai rekisteröity vastustaa käsittelyä suoramarkkinointia varten.
- Henkilötietoja on käsitelty lainvastaisesti.
- Henkilötiedot on poistettava lainsäädäntöön perustuvan, finanssiyrityksiin sovellettavan lakisääteisen velvoitteen noudattamiseksi.
- Käsittely kohdistuu alaikäisen henkilötietoihin, ja henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

7.5 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä voi olla oikeus saada aktiivinen tietojensa käsittely rajoitetuksi neljässä eri tilanteessa:

- Jos rekisteröity kiistää henkilötietojen paikkansapitävyyden, on käsittelyä rajoitettava ajaksi, jonka kuluessa finanssiyritys voi varmistaa tietojen paikkansapitävyyden.
- Jos tietojen käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista. Jos tietojen käsittely on lainvastaista, on rekisteröidyllä oltava oikeus vaatia, ettei finanssiyritys hävitä tietoja ja samalla tuhoa näyttöä siitä, että on käsitellyt tietoja lainvastaisesti. Rekisteröity voi tarvita tietoja esimerkiksi oikeusprosessissa finanssiyritystä vastaan oikeuksiensa toteuttamiseksi.
- Jos finanssiyritys ei enää tarvitse henkilötietoja (käsittelyperuste on päättynyt ja finanssiyritys haluaa poistaa tiedot), mutta asiakas tarvitsee tietoja oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
- Jos rekisteröity on vastustanut henkilötietojen käsittelyä henkilökohtaiseen erityiseen tilanteeseen liittyvän perusteen nojalla ja odottaa sen todentamista, syrjäyttävätkö finanssiyrityksen oikeutetut perusteet asiakkaan perusteet.

Oikeus käsittelyn rajoittamiseen on finanssialalla käytännössä erittäin harvoin sovellettu oikeus.

Henkilötietojen käsittelyn rajoittamista koskevia menetelmiä voivat olla esimerkiksi valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estäminen valittuihin henkilötietoihin. Käsittelyn rajoittaminen on ilmaistava järjestelmässä selkeästi ja varmistettava teknisesti niin, etteivät henkilötiedot enää myöhemmin joudu käsittelytoimenpiteiden kohteeksi. Käyttöoikeuksien määrittelyllä ja

lokitiedoilla voidaan tarvittaessa todentaa ja varmistaa, että tietojen käyttöä on rajoitettu ja ettei niitä ole käsitelty.

Jos käsittelyä on rajoitettu, saa henkilötietoja käsitellä ainoastaan rekisteröidyn suostumuksella taikka oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi tahi toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi.

Jos finanssiyritys on luovuttanut rekisteröidyn tietoja kolmannelle, on finanssiyrittäjän ilmoitettava jokaiselle luovutuksensaajalle kaikista rajoittamista koskevista toimenpiteistä, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Finanssiyrittäjän on myös ilmoitettava rekisteröidylle luovutuksensaajista, jos rekisteröity sitä pyytää. Käsittelyä koskevan rajoituksen poistamisesta on tehtävä rekisteröidylle ilmoitus ennen kuin rajoitus poistetaan.

7.6 Oikeus vastustaa käsittelyä

Rekisteröity voi tietyissä tilanteissa vastustaa tietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella. Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä vain, jos tietojen käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai julkisen vallan käyttöön tai finanssiyrittäjän tai kolmannen osapuolen oikeutetun edun toteuttamiseen. Finanssiyrittäjän oikeus käsitellä tietoja perustuu usein muihin käsittelyperusteisiin. Tämä tarkoittaa, että rekisteröidyllä on vain poikkeuksellisesti oikeus vastustaa tietojensa käsittelyä, eikä rekisteröidyn pyyntö käsittelyn vastustamisesta välttämättä aiheuta toimenpiteitä finanssiyrittäjässä.

Rekisteröidyllä voi olla oikeus vastustaa tietojensa käsittelyä esimerkiksi,

- kun käsittely perustuu finanssiyrittäjän tai kolmannen osapuolen oikeutettuun etuun; tai
- kun henkilötietoja käsitellään suoramarkkinointitarkoituksessa.

Jos rekisteröity vastustaa tietojensa käsittelyä, ei tietoja saa enää käsitellä suoramarkkinoinnin tarkoituksiin. Muissa tapauksissa finanssiyritys saa kuitenkin käsitellä tietoja, jos se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi. Arvioinnissa on huomioitava rekisteröidyn ilmoittamat, tämän henkilökohtaiseen erityiseen tilanteeseen liittyvät perustelut vastustamiselle. Rekisteröity voi kuitenkin aina vastustaa tietojensa käsittelyä suoramarkkinointitarkoituksia varten ilman eri perusteluja.

Finanssiyrittäjän on selkeästi kerrottava rekisteröidylle vastustamisoikeudesta. Tieto on esitettävä muusta tiedotuksesta erillään. Finanssiyrittäjissä tämä tyypillisesti tapahtuu finanssiyrittäjissä tietosuojaselosteissa ja muussa tietosuojainformoinnissa. Markkinoinnin osalta asia tulee kertoa markkinointimateriaalissa.

Tietoyhteiskunnan palveluissa, kuten finanssiyrittäjän verkko- ja mobiilipalveluissa, rekisteröidyn on voitava käyttää vastustamisoikeuttaan automaattisesti teknisiä

ominaisuuksia hyödyntäen. Tämä voidaan ratkaista esimerkiksi omien tietojen hallintapaneeleilla mobiilisovelluksen tai verkkosivuston käyttäjän omista asetuksista.

7.7 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada finanssiyritykseltä automaattisen käsittelyn kohteena olevat, häntä itseään koskevat ja finanssiyritykselle toimittamat henkilötiedot itselleen jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä oikeus siirtää nämä tiedot haluamalleen taholle kuten toiselle palveluntarjoajalle.

Tämä siirto-oikeus koskee nimenomaisesti vain tietoja, joiden käsittelyperusteena on joko rekisteröidyn antama suostumus tietojen käsittelylle tai joiden käsittely on tarpeen finanssiyrityksen ja rekisteröidyn välisen sopimuksen täytäntöön panemiseksi. Näin ollen, mikäli käsittelyperusteena on esimerkiksi oikeutettu etu, velvoitetta tietojen siirtämiseen ei ole. Halutessaan finanssiyritykset voivat kuitenkin vapaaehtoisesti tarjota siirtomahdollisuuden rekisteröidylle myös silloin, kun ne perustavat tietojen käsittelyn muuhun käsittelyperusteeseen kuin suostumukseen tai sopimuksen täytäntöönpanoon. Lisäksi, käsittelyn perustuessa oikeutettuun etuun, siirtomahdollisuuden tarjoamisen voidaan katsoa muodostavan yhden tekijän, jolla finanssiyritys voi perustella käsittelyn perusteena olevan oikeutetun etunsa olemassaoloa, sillä siirto-oikeuden takaaminen rekisteröidylle vahvistaa rekisteröidyn kontrollointimahdollisuuksia omiin tietoihinsa ja samalla asemaa suhteessa finanssiyritykseen.

Käytännössä finanssialalla siirto-oikeutta ei kuitenkaan ole käytetty laajasti, sillä finanssialan yritysten järjestelmät eivät ole olleet keskenään yhteensopivia, eikä tietoja siten ole ollut mahdollista siirtää yhden yrityksen järjestelmästä toiseen. EU valmistelee finanssialalle omaa datan jakamista koskevaa asetusta rahoitusdatan käyttökehyksestä (Financial Data Access regulation eli FIDA). Kyseinen sääntely tulee todennäköisesti edellyttämään tietojen jakamisen ja siirtämisen mahdollistamista toimijoiden välillä. Tietojen jakaminen tulee tapahtumaan finanssialan yritysten perustamien tiedonjakojärjestelmien kautta, joissa sovitaan tiedon jakamisen säännöistä ja teknisistä standardeista. Asetus tulee koskettamaan siirto-oikeuden lisäksi finanssialan datan jakamiseen liittyviä sääntöjä myös laajemmin, mutta siirto-oikeuden merkitys rekisteröidyn oikeutena todennäköisesti kasvaa tulevaisuudessa asetuksen myötä.

7.8 Oikeuksien toteuttamista koskevat periaatteet

Finanssiyritysten on varmistettava, että niiden henkilötietojen käsittelyä koskevat prosessit ja tietojärjestelmät kykenevät toteuttamaan rekisteröidyn oikeuksien toteuttamisen. Rekisteröidyn oikeudet on otettava huomioon organisaation henkilötietojen käsittelyyn liittyvien prosessien ja tietojärjestelmien suunnittelussa.

Käsittelyperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeus siirtää tiedot järjestelmästä toiseen ja oikeus vastustaa tietojen käsittelyä ovat mahdollisia vain, jos tietoja käsitellään tietyllä perusteella. Finanssiyritys voi käsitellä tietoja yhdellä tai useammalla perusteella (ks. kohta 3.2). Finanssiyrityksen onkin

oltava tietoinen, millä perusteella se käsittelee tietoja ja mitä oikeuksia käytössä oleviin käsittelyn perusteisiin liittyy.

Finanssirytyksen on helotettava oikeuksien käyttämistä. Henkilökunta on koulutettava niin, että se pystyy auttamaan ja neuvomaan rekisteröityä oikeuksien toteuttamisessa. Rekisteröidyn on saatava tietoa oikeuksien toteuttamisesta helposti. Finanssirytyksen on toimittava oma-aloitteisesti helpottaakseen oikeuksien käyttämistä.

7.8.1 Toimenpiteistä ilmoittamisen määräaika

Finanssirytyksen on ilmoitettava rekisteröidylle toimenpiteistä, joihin se pyynnön johdosta on ryhtynyt. Toimenpiteistä on kerrottava ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaika voidaan tarvittaessa jatkaa enintään kahdella kuukaudella, jos pyyntöjen määrä ja monimutkaisuus sitä edellyttävät. Määräajan jatkamisesta ja viivästymisen syystä on ilmoitettava rekisteröidylle kuukauden kuluessa pyynnön vastaanottamisesta. Mikäli rekisteröidyn pyyntö on joiltain osin epäselvä, tulee sitä pyrkiä selventämään rekisteröidyn kanssa ilman aiheetonta viivytystä.

Jos finanssirytyksellä on perusteltua syytä epäillä pyynnön tehneen rekisteröidyn henkilöllisyyttä, rekisteröityä voidaan pyytää toimittamaan hänen henkilöllisyytensä vahvistamiseksi tarpeelliset tiedot. Näiden tilanteiden osalta oikeuskäytännössä on katsottu, että kuukauden määräaika rekisteröidyn pyyntöön vastaamiseksi on mahdollista laskea vasta siitä hetkestä, kun rekisterinpitäjä on vastaanottanut pyydetyt lisätiedot. Lisätiedot on kuitenkin myös tässä yhteydessä pyydettävä viipymättä.

Jos rekisteröity on pyytänyt tietojen oikaisua, poistamista tai käsittelyn rajoittamista, on finanssirytyksen ilmoitettava toimenpiteistä myös niille tahoille, joille henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa.

Finanssirytyksen on ilmoitettava rekisteröidylle näistä vastaanottajista, jos henkilö sitä pyytää.

7.8.2 Kieltäytyminen toimenpiteistä

Jos finanssirytyks ei toteuta toimenpiteitä rekisteröidyn henkilön pyynnön perusteella, finanssirytyksen on ilmoitettava rekisteröidylle viipymättä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta syyt siihen ja kerrottava mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja.

7.8.3 Maksuttomuus

Oikeuksien käyttämisen ja toteuttamisen lähtökohtana on maksuttomuus. On myös hyvä huomioida, että rekisteröidyllä on oikeus tehdä maksutta esimerkiksi samoja tietoja koskeva tarkastuspyyntö kohtuullisin väliajoin. Jos rekisteröity esittää pyyntöjä toistuvasti, finanssirytyksen on arvioitava tapauskohtaisesti sitä, onko pyyntö esitetty kohtuullisin väliajoin vai toistuvasti ottaen huomioon esimerkiksi, kuinka usein rekisteröidyn tiedoissa voi tapahtua muutoksia.

Jos henkilön pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti, finanssiyritys voi periä tietojen toimittamisesta ja muista toimenpiteistä kohtuullisen maksun ottaen huomioon tietojen tai viestien toimittamisesta tai pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset, tai kokonaan kieltäytyä suorittamasta pyydettyä toimea. Oikeuksien toteuttamisen maksullisuudelle ei kuitenkaan ole lainsäädäntöön perustuvaa aikarajaa. Finanssiyrityksen on otettava huomioon myös mahdolliset rekisteröidyn perustelut sille, miksi pyyntöä ei tulisi pitää toistuvana tai perusteettomana.

7.8.4 Pyyntöjen esittäjän tunnistaminen

Pyyntöjen esittäjän henkilöllisyys on varmistettava finanssialalla noudatettavien käytäntöjen mukaisesti. Näin vältetään tilanteita, joissa muiden henkilöiden oikeuksia tai vapauksia loukattaisiin. Jos finanssiyrityksellä on perusteltua syytä epäillä pyyntöjen tehneen luonnollisen henkilön henkilöllisyyttä, finanssiyritys voi pyytää henkilöä toimittamaan lisätiedot, jotka ovat tarpeen henkilöllisyyden vahvistamiseksi. Jos finanssiyritys ei pysty tunnistamaan henkilöä ja pystyy tämän osoittamaan, voi finanssiyritys kieltäytyä toimimasta henkilön oikeuksien käyttämiseksi.

Finanssiyrityksellä on kuitenkin rekisterinpitäjänä velvollisuus helpottaa rekisteröidyn oikeuksien käyttämistä. Henkilöllisyyden vahvistaminen ei saa johtaa rekisteröidyn oikeuksien käytön vaikeutumiseen tai perusteettomaan rajoittamiseen eikä epäolennaisten tai tarpeettomien henkilötietojen keräämiseen. Esimerkiksi henkilöllisyystodistuksen edellyttämistä henkilöllisyyden vahvistamiseksi rekisteröidyn pyyntöjen yhteydessä on siksi harkittava tarkasti. Finanssiyrityksen tulisi ottaa henkilöllisyyden vahvistamisen tavoissa huomioon myös erilaisten rekisteröityjen ryhmien tilanteet, kuten iäkkäiden, lasten tai haavoittuvassa asemassa olevien henkilöiden asiointimahdollisuudet.

8 Henkilötietojen luovuttaminen ja siirto

Käsitteitä henkilötietojen "luovuttaminen" ja "siirto" käytetään usein synonyymeina. Tämän takia on tärkeää ymmärtää se asiayhteys, jossa termejä käytetään. Perinteisesti termit on ymmärretty niin, että finanssiyritys voi siirtää asiakkaitaan koskevia henkilötietoja esimerkiksi IT-palveluntarjoajalle finanssiyrityksen lukuun tapahtuvien tietojenkäsittelytehtävien suorittamista varten. Tällöin on kyse tietojenkäsittelytehtävien ulkoistamisesta, ja finanssiyrityksellä säilyy tällöin vastuu siitä, että palvelua tarjoava yritys käsittelee henkilötietoja lainsäädännön ja tehdyn sopimuksen mukaisesti. Pelkkä henkilötietojen siirto edellä mainitussa tarkoituksessa ei ole kuitenkaan vielä henkilötietojen luovutusta, koska luovutukselle on olennaista se, että vastaanottajalla on oikeus määrittää tietojen käyttötarkoitus ja käsitellä saamiaan tietoja omassa toiminnassaan. Toisin sanoen luovutuksessa henkilötietojen vastaanottajasta tulee myös rekisterinpitäjä. Luovutuksen ja siirron suhdetta voi lyhyesti kuvailla niin, että tietoja voidaan siirtää vastaanottajalle niitä luovuttamatta, ja toisaalta luovuttaminen tarkoittaa myös yleensä tietojen siirtoa. Henkilötietoja käsiteltäessä on oltava selkeä käsitys tietojen luovutuksen ja siirron suhteista, koska ne ovat lainsäädännön soveltamisen kannalta eri asioita.

8.1 Henkilötietojen luovuttaminen

Tietosuoja-asetuksen mukaan luovutus on yksi henkilötietojen käsittelyn muoto, joten luovutusta sääntelee mm. asetuksen käsittelyn lainmukaisuutta koskeva 6 artikla sekä erityisiä henkilötietoryhmiä koskevien (arkaluonteisten) tietojen osalta asetuksen 9 ja 10 artiklat. Finanssiyritykset ovat toimialakohtaisen sääntelyn nojalla salassapitovelvollisia ja voivat luovuttaa salassapitovelvollisuuden piiriin kuuluvia henkilötietoja vain asianomaisen henkilön luvalla tai silloin, kun tietojen luovuttamisesta on erikseen säädetty. Finanssiyritykset ovat salassapitovelvollisuudesta huolimatta velvollisia luovuttamaan erityislainsäädännössä olevista säännöksistä johtuen tietoja muun muassa vero-, ulosotto- ja sosiaaliviranomaisille.

Finanssiyrityksen on tietoja muilta vastaanottaessaan varmistettava luovutuksen lainmukaisuus sekä otettava huomioon sovellettaviksi tulevat tietosuoja-asetuksen luovuttajaa ja vastaanottajaa koskevat muut säännökset.

Finanssiyrityksellä ja sen kanssa samaan konsolidointiryhmään kuuluvalla yrityksellä on oikeus antaa salassa pidettäviä tietoja samaan konserniin, konsolidointiryhmään tai rahoitus- ja vakuutusryhmittymien valvonnasta annetussa laissa tarkoitettuun rahoitus- ja vakuutusryhmittymään kuuluvalla yhteisölle asiakaspalvelua, muuta asiakassuhteen hoitamista, markkinointia tai riskienhallintaa varten, jos tietojen vastaanottajaa koskee ko. laissa säädetty tai vastaava salassapitovelvollisuus. Sen lisäksi markkinointia sekä asiakaspalvelua ja muuta asiakassuhteen hoitamista varten tarpeellisia tietoja voidaan antaa sellaiselle yhteisölle, joka kuuluu finanssiyrityksen kanssa samaan taloudelliseen yhteenliittymään, jos tietojen vastaanottajaa koskee ko. laissa säädetty tai sitä vastaava salassapitovelvollisuus.

Edellä viitatu poikkeukset eivät kuitenkaan mahdollista esimerkiksi erityisiin henkilötietoryhmiin kuuluvien tietojen luovuttamista tai sellaisten tietojen luovuttamista, jotka perustuvat asiakkaan ja muun kuin ryhmittymään kuuluvan yrityksen välisen maksutietojen rekisteröintiin.

8.2 Henkilötietojen siirto kolmansiin maihin

Yleisessä tietosuoja-asetuksessa on erityisesti säännelty henkilötietojen siirtoja Euroopan talousalueen (ETA) rajojen ulkopuolelle, ns. kolmansiin maihin. Siirroissa on otettava huomioon asetuksen V luvussa esitetyt rajoittavat säännökset, joiden tarkoituksena on varmistaa, että henkilötietojen tietosuojan taso ei vaarannu siirrettäessä tietoja rajojen yli.

Siirroksi katsotaan myös henkilötietoihin pääsy kolmansista maista esimerkiksi etäyhteyden avulla riippumatta siitä, hyödynnetäänkö kyseistä teknistä pääsyä käytännössä. Henkilötietojen siirroksi kolmansiin maihin ei kuitenkaan ole katsottu tilanteita, joissa esimerkiksi työmatkalla oleva työntekijä tilapäisesti käyttää etäyhteyden avulla yrityksen tietokannoissa olevia henkilötietoja.⁷

⁷ Ks. Euroopan tietosuojaneuvoston suuntaviivat 5/2021 3 artiklan soveltamisen ja yleisen tietosuoja-asetuksen V luvun mukaisten kansainvälisiä siirtoja koskevien säännösten vuorovaikutuksesta, kohta 20 esimerkki 8.

Jos tarkoituksena on harjoittaa toimintaa, jonka yhteydessä henkilötietoja joudutaan siirtämään kolmansiin maihin, on varmistettava, että siirto toteutetaan maahan tai kansainväliselle järjestölle, jonka osalta EU:n komissio on antanut tietosuojan riittävyttä koskevan päätöksen. Vaihtoehtoisesti siirto on mahdollista toteuttaa asetuksessa määritettyjä asianmukaisia suojatoimia soveltaen tai, jos sellaisia ei ole, jollakin asetuksessa säädetyllä erityistilanteita koskevalla poikkeusperusteella.

Viitatus siirron oikeusperusteita koskevat vaatimukset koskevat myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle.

Rekisterinpitäjän on lisäksi varmistettava, että käsittelytoimia koskevassa selosteessa on kuvattu tieto siirtämisestä kolmanteen maahan sekä tarvittaessa asianmukaisia suojatoimia koskevat asiakirjat.

8.2.1 Siirto tietosuojan riittävyttä koskevan komission päätöksen perusteella

Henkilötietojen siirto kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos EU:n komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Henkilötietoja voidaan tällöin siirtää suoraan tällaisen ns. riittävyyspäätöksen nojalla, eikä rekisterinpitäjä tarvitse siirrolle esimerkiksi erillistä lupaa tietosuojaviranomaiselta.

Komissio voi suojan riittävyttä arvioituaan päättää, että kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö tarjoaa tietosuojaa-asetuksessa määritetyn riittävän tietosuojan tason (45 artikla, 2 kohta).

Komissio julkaisee Euroopan unionin virallisessa lehdessä ja verkkosivustollaan luettelon niistä kolmansista maista, kolmannen maan alueista ja tietyistä sektoreista sekä kansainvälisistä järjestöistä, joiden osalta se on päättänyt, että tietosuojan taso on tai ei enää ole riittävä. Finanssiyrityksen on hyvä huomioida, että komissio voi myös muuttaa tai peruuttaa antamansa riittävyyspäätöksen. Tällaisessa tilanteessa kyseiseen riittävyyspäätökseen aiemmin perustuneen tiedonsiirron jatkaminen on mahdollista ainoastaan, mikäli siirrolle on jokin muu tietosuoja-asetuksen V luvun mukainen siirtoperuste.

8.2.2 Siirto asianmukaisia suojatoimia soveltaen

Mikäli komissio ei ole tehnyt edellä kuvattua päätöstä kolmannen maan tai kansainvälisen järjestön osalta, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kyseessä olevaan kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet.

Asianmukaisia suojatoimia voivat olla muun muassa seuraavat suojatoimet:

- yritystä koskevat sitovat säännöt (artikla 47)

- komission antamat tietosuojaa koskevat vakiolausekkeet (tarkastettu 93 artiklan 2 kohdan mukaisesti)
- tietosuojaviranomaisen vahvistamat ja komission hyväksymät tietosuojaa koskevat vakiolausekkeet (tarkastettu 93 artiklan 2 kohdan mukaisesti)
- hyväksytyt käytäntösäännöt (40 artikla) yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi
- hyväksytty sertifiointimekanismi (42 artikla) yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi.

Edellä kuvattujen suojatoimien käyttö ei edellytä erityistä valvontaviranomaisen antamaa lupaa, mutta edellyttää, että rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja. Esimerkiksi käytettäessä edellä mainittuja vakiosopimuslausekkeitä on tapauskohtaisesti varmistettava, että kohdemaan lainsäädäntö vastaa EU:n vaatimaa tietosuojan tasoa. Mikäli näin ei ole, niin tulee tilanteessa käyttää ns. täydentäviä suojatoimia eli teknisiä, organisatorisia tai sopimusperusteisia lisäsuojatoimia.

Toimivaltaisen valvontaviranomaisen luvalla asianmukaisia suojatoimia voivat olla myös rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannen maan tai kansainvälisen järjestön rekisterinpitäjän, henkilötietojen käsittelijän tai vastaanottajan väliset sopimuslausekkeet.

8.2.3 Erityistilanteita koskevat poikkeukset

Mikäli komissio ei ole tehnyt edellä kuvattua tietosuojan tason riittävyttä koskevaa päätöstä eikä edellä kuvattuja asianmukaisia suojatoimia ole toteutettu, henkilötietojen siirto kolmanteen maahan tai kansainväliselle järjestölle voidaan suorittaa tietosuojasetuksen 49 artiklassa kuvatulla poikkeuksella.

Finanssirytyksen toiminnan kannalta yleisimmin kyseeseen tulevat poikkeusperusteet ovat seuraavat:

- Rekisteröity on antanut nimenomaisen suostumuksensa ehdotettuun siirtoon sen jälkeen, kun hänelle on ilmoitettu, että tällaiset siirrot voivat aiheuttaa rekisteröidylle riskejä.
- Siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöönpanemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä, kuten maksutoimeksiannon toteuttaminen.
- Siirto on tarpeen rekisterinpitäjän ja toisen luonnollisen henkilön tai oikeushenkilön välisen, rekisteröidyn edun mukaisen sopimuksen tekemiseksi tai täytäntöönpanemiseksi, kuten vakuutuksen hankinta ETA:n ulkopuoliselta palveluntarjoajalta rekisteröidyn eduksi.
- Siirto on tarpeen tärkeää yleistä etua koskevien syiden vuoksi, kuten rahanpesun estämiseksi.
- Siirto on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Finanssialalla on yhteisessä compliance-keskustelussa vuonna 2022 katsottu, että kansainvälisessä maksuliikenteessä on mahdollista nojautua edellä mainittuun poikkeukseen sopimuksen täytäntöönpanosta. Tämä soveltuu muun muassa tiedonsiirtoihin ETA-alueen ulkopuolisille kirjeenvaihtajapankeille ja SWIFT-verkon kautta välitettäviin maksuihin.

Mikäli siirto ei voi perustua komission päätökseen, yritystä koskeviin sitoviin sääntöihin eikä mikään edellä kuvatuista erityistilanteista koskevista poikkeuksista sovellu, henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle ainoastaan, jos siirto ei ole toistuva, koskee ainoastaan rajallista määrää rekisteröityjä ja on tarpeen rekisterinpitäjän sellaisten pakottavien ja oikeutettujen etujen toteuttamiseksi, joita rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä. Tällaisiin siirtoihin liittyy myös lisävaatimuksia, kuten velvollisuus ilmoittaa siirrosta valvontaviranomaiselle

8.3 Henkilötietojen luovutus viranomaisille

Finanssiyrityksellä on velvollisuus antaa erityislainsäädännössä (esimerkiksi luottolaitoslain 15 luvussa ja vakuutusyhtiölain 30 luvussa) salassa pidettäväksi säädettyjä tietoja syyttäjä- ja esitutkintaviranomaiselle rikoksen selvittämiseksi sekä muulle viranomaiselle, jolle finanssiyritys saa salassapitosäännösten estämättä luovuttaa tietoja, ja jolla on lain mukaan oikeus saada sellaisia tietoja. Tällaisia viranomaisia ovat esimerkiksi Finanssivalvonta, rahanpesun selvittelykeskus sekä ulosotto-, vero- ja sosiaaliviranomaiset. Viranomaisen oikeus saada tietoja perustuu sen lakisääteisiin tehtäviin.

Finanssiyrityksen tulee ennen tietojen luovuttamista varmistua viranomaisen ilmoittaman tiedonsaantioikeutensa perusteeksi ilmoittaman säännöksen soveltuvuudesta. Tietoja viranomaiselle annettaessa Finanssiyrityksen tulee omalta osaltaan myös varmistua siitä, mikä on tietojen tietosuoja-asetuksen mukaisen käsittelyperuste sekä noudattaa tietoja annettaessa muitakin asetuksen mukaisia periaatteita, kuten tietojen minimointia ja tietoturvavelvoitteita.

Kolmannen maan tuomioistuimen tai hallintoviranomaisen päätös, jossa rekisterinpitäjältä tai henkilötietojen käsittelijältä vaaditaan henkilötietojen siirtämistä tai luovuttamista, voidaan tunnustaa tai saattaa millään tavoin täytäntöönpanokelpoiseksi vain, jos se perustuu pyynnön esittäneen kolmannen maan ja unionin tai sen jäsenvaltion väliseen voimassa olevaan kansainväliseen sopimukseen, kuten keskinäiseen oikeusapusopimukseen.

Tietojenluovutukseen voi liittyä erityislakiin perustuva tai viranomaisen toimivaltuuksiensa puitteissa antama kielto kertoa luovutuksesta finanssiyrityksen asiakkaalle. Ellei tällaista kieltoa ole tai sen voimassaolo on päättynyt, tietojen luovutus kuuluu asiakkaan tarkastusoikeuden piiriin.

9 Suoramarkkinointi

Suoramarkkinointi on kaupallisessa tarkoituksessa tapahtuvaa yksittäiseen vastaanottajaan kohdennettavaa markkinointiviestintää, jolla pyritään tavarain tai

palvelun myynnin edistämiseen. Suoramarkkinointi kohdennetaan vastaanottajiin esimerkiksi puhelimitse, kirjeitse tai sähköisiä välineitä tai verkkopalvelua hyödyntäen. Selvyyden vuoksi on syytä todeta, että suoramarkkinointia ei ole sellainen asiakasviestintä, joka liittyy asiakassuhteen hoitoon (esimerkiksi sopimukseen liittyvä viestintä). Alla mainitut kiellot eivät sovellu asiakasviestintään. Asiakasviestintä ei tällöin saa kuitenkaan sisältää suoramarkkinointielementtejä. Myöskään asiakastyytyväisyyskyselyt eivät ole suoramarkkinointia.

Sähköistä suoramarkkinointia (esim. sähköpostiviestit, tekstiviestit, automatisoidut soittojärjestelmät, puheviestit ja vastaavat) saa pääsääntöisesti kohdistaa vain sellaisiin henkilöihin, jotka ovat antaneet siihen etukäteen suostumuksensa. Suostumuksen antaminen edellyttää, että rekisteröity on nimenomaan aktiivisesti hyväksynyt sähköisen suoramarkkinoinnin vastaanottamisen. Näin ollen suostumusta ei voi hankkia esimerkiksi valmiiksi rastitetulla valintaruudulla.

Tietyissä rajatuissa tilanteissa sähköistä suoramarkkinointia voidaan kohdentaa rekisteröityyn myös, vaikka rekisteröity ei ole antanut etukäteistä suostumusta sähköiselle suoramarkkinoinnille. Jos finanssiryitys saa asiakkaana olevalta henkilöltä sähköpostiviestiin, tekstiviestiin taikka, puhe-, ääni- tai kuvaviestiin liittyvän yhteystiedon tuotteen tai palvelun myynnin yhteydessä, finanssiryitys voi käyttää tätä yhteystietoa omien samaan tuoteryhmään kuuluvien tai muuten vastaavien tuotteiden ja palvelujen suoramarkkinoinnissa. Finanssiryitys voi siis kohdistaa asiakkaaseensa sähköistä suoramarkkinointia esimerkiksi tekstiviestin välityksellä ilman ennakkosuostumusta, mikäli asiakas on ostanut finanssiryitykseltä palvelun tekstiviestin välityksellä.

Sähköinen suoramarkkinointi yrityksen yleiseen osoitteeseen ei vaadi suostumusta. Myöskään sähköinen suoramarkkinointi yrityksen edustajille ei yleensä edellytä suostumusta, jos suoramarkkinointia vastaanottava henkilö työskentelee yrityksessä sellaisissa tehtävissä, joihin suoramarkkinoinnilla tarjottavat palvelut tai hyödykkeet olennaisesti liittyvät. Tällöin kyseisen henkilön yritykselle kuuluvaan sähköposti-osoitteeseen voi kohdistaa suoramarkkinointia henkilön asemavaltuuden nojalla. Rekisterinpitäjän on kuitenkin varmistuttava henkilön asemavaltuudesta ennen suoramarkkinoinnin lähettämistä. Viesteihin tulee aina sisällyttää selkeä mahdollisuus kieltäytyä jatkossa markkinointiviesteistä.

Pelkkä käyttöliittymän personointi ei ole sähköistä suoramarkkinointia, jolloin se ei edellytä suostumusta suoramarkkinointiin. Jos personoinnissa hyödynnetään evästeitä tai vastaavia teknologioita, tulee kuitenkin varmistaa, että tarvittavat evästesuostumukset on hankittu.