Henkilötietojen käsittelyä finanssialalla koskevat käytännesäännöt 1.12.2017

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

FINANSSIALA

Sisällysluettelo

Itämerenkatu 11-13
00180 Helsinki
Puh: +358 20 793 4200
Fax: +358 20 793 4202
etunimi.sukunimi@finanssiala.fi
www.finanssiala.fi
Facebook.com/finanssiala
Twitter.com/finanssiala

Itämerenkatu 11-13
00180 Helsinki

Puh: +358 20 793 4200
Fax: +358 20 793 4202
etunimi.sukunimi@finanssiala.fi

www.finanssiala.fi
Facebook.com/finanssiala
Twitter.com/finanssiala

Henkilötietojen käsittelyä finanssialalla koskevat käytännesäännöt

1 Johdanto

EU:n yleinen tietosuoja-asetus tuli voimaan 25.5.2016. Tietosuoja-asetus korvaa voimassa olleen tietosuojadirektiivin, joka on Suomessa implementoitu henkilötietolakiin. Asetusta sovelletaan sekä yksityisellä että julkisella sektorilla 25.5.2018 lähtien.

Tietosuoja-asetusta sovelletaan Suomessa sellaisenaan. Asetus edellyttää kuitenkin Suomessa myös lainsäädäntötoimenpiteitä, sillä jäsenvaltioilla on mahdollisuus antaa asetusta tarkentavaa lainsäädäntöä. Keskeisin kansallinen säädös on valmisteilla oleva tietosuojalaki .

Tietosuoja-asetuksen tarkoituksena on suojella luonnollisia henkilöitä henkilötietojen käsittelyssä. Luonnollisten henkilöiden suojelu henkilötietojen käsittelyn yhteydessä on perusoikeus. Uudistuksen tavoitteena on muun muassa parantaa henkilötietojen suojaa lisäämällä läpinäkyvyyttä sekä parantamalla rekisteröityjen mahdollisuutta valvoa omia tietojaan. Lisäksi tavoitteena on korkeampi harmonisoinnin taso sekä sisämarkkinoiden tukeminen.

Tietosuoja-asetuksessa määritellyt rekisteröidyn oikeudet vastaavat suurelta osin aiempaa sääntelyä. Henkilöllä on edelleen oikeus esimerkiksi tarkastaa itseään koskevat tiedot. Myös aiemman sääntelyn mukaan rekisterinpitäjän oli oikaistava virheelliset tiedot ja poistettava esimerkiksi tarpeeton tai vanhentunut henkilötieto (oikeus tulla unohdetuksi). Asetuksella kuitenkin luodaan myös uusia oikeuksia, joilla nykyaikaistetaan sääntelyä vastaamaan teknologian kehitystä. Rekisteröity voi pääsääntöisesti saada itseään koskevia tietoja sähköisesti ja hän voi siirtää antamansa henkilötiedot järjestelmästä toiseen. Asetus suojaa erityisiä henkilöryhmiä ja rajoittaa esimerkiksi lasten henkilötietojen käsittelyä ilman vanhempien suostumusta. Sillä annetaan myös tietosuojaviranomaiselle, jona Suomessa toimii tietosuojavirasto, valtuudet määrätä huomattavia sanktioita sääntelyn rikkomisesta.

Finanssiyritykset käsittelevät jokapäiväisessä työssään asiakkaita koskevia erilaisia tietoja. Tietosuoja-asetus vaikuttaa tämän vuoksi merkittävällä tavalla finanssialaan.

Näiden käytännesääntöjen tarkoituksena on määrittää finanssialalle henkilötietojen käsittelyn periaatteet. Tavoitteena on edistää hyvää henkilötietojen käsittelytapaa ottaen huomioon finanssialan erityispiirteet ja rekisteröityjen yksityisyyden suoja ja siten lisätä asiakkaiden luottamusta finanssipalveluihin. Säännöt on tarkoitettu finanssiyrityksille niiden itse suorittaman ohjeistuksen, toiminnan suunnittelun ja opastuksen tueksi. Yksityiskohtaisen ohjeistuksen tarvetta säännöt eivät lähtökohdastaan johtuen kykene poistamaan.

Suomalaisissa luottolaitoksissa ja vakuutusyhtiöissä on liki 20 vuoden ajan ollut käytössään Finanssialan Keskusliitossa ja sen edeltäjissä valmistellut, tietosuojavaltuutetun tarkastamat käytännesäännöt, joita on hyödynnetty uusien käytännesääntöjen laatimisessa. Nykyisen Finanssiala ry:n jäsenistöön kuuluu myös rahoitusyhtiöitä, sijoituspalveluyrityksiä, rahastoyhtiöitä sekä vaihtoehtorahastojen hoitajia. Näiden yhtiöiden osalta on hyvä huomioida, että käytännesääntöjen kirjaukset soveltuvat suurimmilta osin myös niiden toimintaan ja vastaavat kirjaukset, jotka löytyvät käytännesäännöistä viitatuista luottolaitoslaista ja vakuutusyhtiölaista,

ovat myös kyseisiä toimijoita koskevissa erityislaeissa. Näin ollen käytännesäännöt ovat käyttökelpoiset soveltuvin osin myös niiden toiminnassa. Sen sijaan tietosuoja-asetuksen edellyttämät muutokset lakisääteisiä vakuutuksia koskevaan erityislainsäädäntöön ja samoin näitä vakuutuslajeja koskeva ohjeistus on vielä työnalla, joten käytännesäännöissä ei oteta yksityiskohtaisesti kantaa kyseisten vakuutuslajien osalta. Lopuksi on syytä huomioida, että käytännesäännöt eivät sisällä finanssiyritysten omien työntekijöiden henkilötietojen käsittelyä koskevia periaatteita.

2 Soveltaminen ja määritelmät

2.1 Milloin tietosuoja-asetusta ja käytännesääntöjä sovelletaan?

Tietosuoja-asetusta ja näitä käytännesääntöjä sovelletaan finanssialalla luonnollisia henkilöitä koskevaan jäsenneltyyn henkilötietojen käsittelyyn, tapahtuipa tietojen käsittely automaattisesti tai manuaalisesti. Käsittelyn kohteena voivat olla muun muassa finanssiyrityksen asiakkaiden, toimihenkilöiden tai hallintohenkilöiden henkilötiedot. Näistä henkilöryhmistä voidaan muodostaa henkilörekistereitä eri käyttötarkoituksen mukaisesti (esim. asiakas- ja vakuutusrekisteri, markkinointirekisteri, korvausrekisteri, henkilöstörekisteri ja sisäpiirirekisteri). Jäljempänä ohjeistetaan lähtökohtaisesti asiakkaita ja näihin rinnastettavia henkilöitä koskevien henkilötietojen käsittelyä.

Lähtökohtana henkilötietoa määriteltäessä ovat kaikki luonnollista henkilöä koskevat tiedot. Asetusta ja käytännesääntöjä sovellettaessa on kuitenkin otettava huomioon, että asetuksen tarkoituksena on suojata henkilön yksityiselämää ja muuta yksityisyyttä. Näin ollen esimerkiksi ammatinharjoittajan tai yritystoimintaa harjoittavan henkilön kyseiseen ammatti- ja yritystoimintaan liittyvät asiat kuuluvat yksityisyyden suojan piiriin vain siltä osin kuin tiedot koskevat kyseistä henkilöä. Sen sijaan esimerkiksi yritystä koskevat tiedot eivät kuulu asetuksen ja käytänne-sääntöjen soveltamisalan piiriin.

2.2 Tietosuoja-asetuksen ja käytännesääntöjen keskeisten käsitteiden määritelmät

Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity), liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

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 luottolaitoksen kanssa tekemiin sopimuksiin sekä palveluiden käyttöön liittyvät keskeiset tiedot. Samoin henkilötietoja ovat kaikki luottolaitokseen kertyvät tiedot henkilön ominaisuuksista, toimintatavoista, luotettavuudesta ja arvostelman luonteiset kuvaukset. Myös henkilön kuva ja esimerkiksi tallennettu puhe ovat henkilötietoa.

Henkilötietoja ovat myös henkilön vakuutussopimuksiin liittyvät keskeiset tiedot, kuten tiedot vakuutusturvasta, vakuutetuista ja edunsaajista, vakuutettavasta omaisuudesta, sen arvosta ja sijaintipaikasta sekä omistussuhteista. Myös korvaustoimintaan liittyvät luonnollista henkilöä koskevat tiedot ovat lähes poikkeuksetta henkilötietoja. Samoin henkilötietoja ovat kaikki vakuutusyhtiöön kertyvät tiedot henkilön ominaisuuksista, toimintatavoista, luotettavuudesta ja arvostelman luonteiset kuvaukset. Myös henkilön kuva ja esimerkiksi tallennettu puhe ovat henkilötietoa.

Henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä, tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Henkilötiedot saattavat olla jaoteltavissa myös pienemmiksi kokonaisuuksiksi ilman, että niistä muodostuu omaa henkilötietorekisteriään. Esimerkiksi korvauskäsittelyssä syntyvät ns. vahinkokansiot katsotaan kuuluvaksi rekisterin tausta-aineistoon ja ne ovat osa vakuutusyhtiön korvausrekisteriä.

Automaattisen tietojenkäsittelyn avulla toteuttava tekstinkäsittely ei sellaisenaan muodosta laissa tarkoitettua henkilörekisteriä, vaikka siinä käsitellään henkilötietoja. Tietojenkäsittelyllä tuotetusta asiakirjasta voi muodostua kuitenkin henkilörekisterin osa, jos asiakirja säilytetään osana tietojenkäsittelyjärjestelmää.

Asiakasrekisterin osana voi olla myös puhelinnauhoitteita sekä kuva- ja äänitallenteita siltä osin kuin ne sisältävät asiakkaita koskevia tietoja.

Rekisteröity on henkilö, jota henkilötieto koskee.

Luottolaitosten rekistereissä rekisteröityjä ovat siten luottolaitoksen asiakkaat eri ominaisuuksissaan, kuten tallettajina, luotonottajina tai -hakijoina. Rekisteröityjä ovat myös henkilöt, jotka esim. tehdyn henkilökohtaisen luottotarjouksen perusteella on rekisteröity luottolaitoksen asiakasrekisteriin sekä henkilöt, jotka on merkitty mahdolliseen suoramarkkinointirekisteriin.

Vakuutusyhtiöiden rekistereissä rekisteröityjä ovat siten vakuutusyhtiön asiakkaat eri ominaisuuksissaan, kuten vakuutuksenottajina, vakuutettuina, korvauksenhakijoina ja edunsaajina. Rekisteröityjä ovat myös mahdolliseen suoramarkkinointirekisteriin merkityt henkilöt.

Rekisterinpitäjä on finanssiyritys, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjillä, jotka kuuluvat konserniin, konsolidointiryhmään, luottolaitosten yhteenliittymään, rahoitus- ja vakuutusryhmittymään tai taloudelliseen yhteenliittymään, saattaa olla sisäisistä hallinnollisista syistä johtuen oikeutettu etu siirtää henkilötietoja sanotun organisaation sisällä.

Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Selvyyden vuoksi todetaan, ettei yksittäinen työntekijä ole asetuksen tarkoittama henkilötietojen käsittelijä. Vuokratyöntekijät rinnastetaan työnantajan omiin työntekijöihin.

Profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.

Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu.

Anonyymit tiedot ovat tietoja, jotka eivät liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, tai henkilötietoja, joiden tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole enää mahdollista. Anonyymia tietoa voivat olla esim. testitietojen, tilastotarkoituksia tai finanssiyrityksen riskienhallintaa, kuten vakavaraisuuden hallintaa, varten käytettävien tietojen käsittely. Tietosuoja-asetus ei koske tällaisten tietojen käsittelyä. On kuitenkin huomioitava, että henkilötietojen anonymisointi on henkilötietojen käsittelyä.

Luottolaitoksen ja vakuutusyhtiöiden toimihenkilöillä ja toimielimien jäsenillä on lakiin perustuva salassapitovelvollisuus, jolla varmistetaan asiakkaiden asioiden luottamuksellinen käsittely. Toimihenkilöt saavat käsitellä asiakastietoja vain työtehtäviensä edellyttämässä laajuudessa. **Pankki-/ vakuutussalaisuus** käsittää kaikki ne seikat, jotka luottolaitoksen toimi- tai luottamushenkilö työssään saa tietoonsa asiakkaan tai muun sen toimintaan liittyvän henkilön taloudellisesta asemasta tai yksityiskohtaisen henkilön henkilökohtaisia oloja koskevasta tiedosta taikka liike- tai ammattisalaisuudesta.

3 Henkilötietojen käsittelyn yleiset edellytykset

3.1 Henkilötietojen käsittelyä koskevat periaatteet

Finanssiyritysten on henkilötietoja käsitellessään noudatettava lakia, huolellisuutta, hyvää tietojenkäsittelytapaa ja toimittava muutoinkin niin, ettei pankki- tai vakuutussalaisuutta, asiakkaiden yksityiselämän suojaa ja muita perusoikeuksia loukata.

Henkilötietojen käsiteltäessä on noudatettava seuraavia, tietosuoja-asetuksessa määriteltyjä periaatteita.

Henkilötietoja on ensinnäkin 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. Läpinäkyvyys tarkoittaa, että rekisteröity saa helposti selkeää tietoa käsittelystä, kuten esimerkiksi rekisterinpitäjän identiteetistä ja käsittelyn tarkoituksista. Rekisteröidyille tulee tiedottaa 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 ja niistä on kerrottava yksiselitteisesti henkilötietoja kerättäessä. Henkilötietojen käsittely muita kuin alkuperäisiä tarkoituksia varten on sallittua vain, jos käsittely ei ole yhteensopimatonta alkuperäisten käyttötarkoitusten kanssa.

Punnitessaan, onko myöhemmän käsittelyn tarkoitus yhteensopiva 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. Finanssiyritys on itse vastuussa tulkinnastaan.

Myöhempää henkilötietojen käsittelyä yleisen edun mukaisiin arkistointitarkoituksiin taikka tieteellistä tai historiallista tutkimusta tai tilastotarkoitusta varten ei pidetä yhteensopimattomana alkuperäisen käsittelyn tarkoituksen kanssa. Myös lainsäädännön tarjoama käsittelyn oikeusperuste henkilötietojen käsittelylle voi muodostaa käsittelyn oikeusperusteen myöhemmälle käsittelylle.

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. Finanssiyrityksen tulee asettaa määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, ja näin varmistettava, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä (*täsmällisyyden periaate*). Finanssiyrityksen on toteutettava kohtuulliset toimenpiteet sen varmistamiseksi, 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. Laissa voidaan esimerkiksi edellyttää, että asiakas sitoutuu asiakassopimuksessa ilmoittamaan itse muuttuneista tiedoista.

Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (*säilytyksen rajoittamisen periaate*).

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 asianmukainen turvallisuus on ratkaistava tapauskohtaisesti riskiperusteiseen arviointiin nojautuen.

3.2 Milloin henkilötietoja voidaan käsitellä?

Finanssiyrityksellä on oikeus käsitellä toimintansa kannalta tarpeellisia henkilötietoja. Käsittelyn on perustuttava tietosuoja-asetukseen tai Euroopan unionin tai jäsenvaltion lainsäädäntöön. Tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn edellytykset ovat:

- rekisteröity on antanut *suostumuksensa* henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.

- käsittely on tarpeen sellaisen *sopimuksen täytäntöön panemiseksi*, jossa rekisteröity on osapuolena, tai *sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi* rekisteröidyn pyynnöstä.

  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 vakuutussopimuksen tekemistä.

- käsittely on tarpeen finanssiyrityksen *lakisääteisen velvoitteen noudattamiseksi*. Käsittelyn tulee perustua Euroopan unionin tai sen jäsenvaltion lainsäädäntöön, ja myös käsittelyn tarkoitus tulee määritellä lainsäädännössä.

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

  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 asiakkaan transaktioiden seurannan).

- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön *elintärkeiden etujen suojaamiseksi*

- käsittely on tarpeen *yleistä etua koskevan tehtävän suorittamiseksi* tai rekisterinpitäjälle kuuluvan *julkisen vallan käyttämiseksi*

- käsittely on tarpeen finanssiyrityksen tai kolmannen osapuolen *oikeutettujen etujen toteuttamiseksi*, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Finanssialalla on tavanomaista, että henkilötietojen käsittelyyn liittyy useampi käsittelyperuste samanaikaisesti. Näin ollen yhden käsittelyperusteen päättyminen ei välttämättä päätä oikeutta käsitellä kyseisiä henkilötietoja. Finanssiyritykset huomioivat asian henkilötietojen käsittelyn suunnittelussa sekä käytännön toteutuksessa esimerkiksi käsittelyn laajuuden osalta yhden oikeusperusteen päättymisen jälkeen.

3.2.1 Oikeutettu etu käsittelyperusteena

Oikeutettu etu on olemassa esimerkiksi asiakkuussuhteen perusteella. Esimerkkinä voidaan mainita erilaiset asiakaspalvelutilanteet sekä suoramarkkinointi. Asiakassuhde on finanssiyrityksen kannalta merkittävä tietojen käsittelyperuste.

> Luottolaitoksen asiakkaita ovat esim. tilinomistajat ja -käyttäjät, kortinhaltijat, luotonhakijat ja velalliset, takaajat ja pantinantajat, tallelokeron vuokraajat ja käyttäjät sekä arvopaperiasiakkaat, edunvalvojat ym. asiakkaita edustavat henkilöt. Asiakassuhdetta ei muodostu pelkästään yksittäisen maksutoimeksiannon perusteella, mutta maksutoimeksianto oikeuttaa tarpeellisten tietojen käsittelemisen.
>
> Asiakassuhde on myös vakuutusyhtiön kannalta keskeinen henkilötietojen käsittelyperuste. Vakuutuksenottajia, vakuutettuja, vakuutusten edunsaajia ja korvauksenhakijoita koskevien henkilötietojen käsittely voi perustua asiakassuhteeseen. Tietojen käsittelyyn oikeuttavan asiakassuhteen voidaan katsoa olevan olemassa silloinkin, kun henkilö ei itse tiedä olevansa osallisena vakuutussopimuksessa, esimerkiksi edunsaajana. Kaikki vahinkoon osalliset eivät välttämättä ole vakuutusyhtiön asiakkaita, mutta myös heidän henkilötietojensa käsittelyn voidaan katsoa olevan oikeutettua oikeutetun edun perusteella.

Tietojen käsittelyä petosten estämistarkoituksessa voidaan pitää rekisterinpitäjän oikeutettuna etuna.

> Esimerkiksi vakuutusyhtiöiden 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 käytännesäännöistä.

Oikeutettu etu mahdollistaa myös tietojen käsittelyn konsernin, konsolidointiryhmän, luottolaitosten yhteenliittymän, rahoitus- ja vakuutusryhmittymän ja 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 mahdollistaa henkilötietojen käsittelyn tilanteissa, joissa on kyse entisiä asiakkaita koskevista saamisen maksun viivästymisistä. Saamisen maksun viivästymistä koskevilla tiedoilla on merkitystä arvioitaessa henkilön taloudellista asemaa, sitoumusten hoitokykyä ja luotettavuutta. Finanssiyritysten on tärkeätä säilyttää maksun viivästymistietoja jonkin aikaa asiakassuhteen katkeamisen jälkeenkin, koska asianomainen voi lyhyessäkin ajassa hakeutua uudestaan yhteisön asiakkaaksi, ja siksi maksun viivästymistä koskevien tietojen käsittely voi tarpeellista finanssiyritysten oikeutetun edun toteuttamiseksi ja luoton- ja sitoumustenantoon liittyen riskien pienentämiseksi.

3.2.2 Suostumus käsittelyperusteena

Suostumus henkilötietojenkäsittelyn lainmukaisena käsittelyperusteena edellyttää, että rekisteröity on antanut suostumuksen yhtä tai useampaa erityistä tarkoitusta varten. Suostumuksen pitää olla tarpeellinen palvelun tarjoamisen kannalta. Jos käsittelyllä on useita tarkoituksia, suostumus olisi annettava kaikkia käsittelytarkoituksia varten.

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

Suostumuksen tulee olla suostumuksen antajan aktiivinen toimi, jolla hän selkeästi osoittaa hyväksymisensä henkilötietojensa käyttöön tässä asiayhteydessä. Suostumusta ei voida siten antaa vaikenemalla, valmiiksi rastitetulla ruudulla tai jättämällä jokin toimi toteuttamatta.

Ennen suostumuksen antamista rekisteröidylle tulee selvittää suostumuksen merkitys. Rekisteröidyn tulee tietää vähintään rekisterinpitäjän identiteetti ja ne käyttötarkoitukset, joita varten henkilötietoja on määrä käsitellä. 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 ilman, että siitä aiheutuu hänelle haittaa.

Rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn. Suostumus on dokumentoitava, koska näyttövelvollisuus siitä, että suostumus henkilötietojen käsittelyyn on ollut olemassa, on rekisterinpitäjällä.

Suostumusta koskevan pyynnön tulee olla yksilöity ja pyyntö on esitettävä rekisteröidylle selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeästi ja yksinkertaisella kielellä. Suostumuksen edellytyksenä ei saa olla kohtuuttomia ehtoja.

Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa. Oikeudesta peruuttaa suostumus on ilmoitettava rekisteröidylle ennen kuin tämä antaa suostumuksen. Suostumuksen peruuttaminen ei vaikuta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen. Suostumus tulee voida peruuttaa yhtä selkeästi ja helposti kuin suostumuksen voi antaa.

Alle 13/15 -vuotiaan lapsen osalta henkilötietojen käsittelyyn liittyvän suostumuksen antaa lapsen laillinen huoltaja. Alaikäisen lapsen suostumuksen osalta noudatetaan muutoin lakia holhoustoimesta.

Rekisterinpitäjällä on velvollisuus kohtuullisin toimenpitein tarkistaa lapsen suostumuksen olemassaolo.

3.2.3 Suoramarkkinointi

Mitä on suoramarkkinointi

Suoramarkkinointi on kaupallisessa tarkoituksessa tapahtuvaa yksittäiseen vastaanottajaan kohdennettavaa markkinointiviestintää, jolla pyritään tavaran tai palvelun myynnin edistämiseen. Suoramarkkinointi kohdennetaan vastaanottajiin esimerkiksi puhelimitse, kirjeitse tai sähköisiä välineitä hyödyntäen. Koska suoramarkkinointi kohdennetaan aina yksittäiseen rekisteröityyn, edellyttää suoramarkkinointi rekisteröidyn henkilötietojen käsittelyä, jolloin noudatettavaksi tulevat sekä tietosuojalainsäädännön yleiset velvoitteet että myös erityiset nimenomaan suoramarkkinointia koskevat velvoitteet (vastustamisoikeus ja ennakkosuostumus sähköiseen suoramarkkinointiin).

Suoramarkkinointia ei ole sellainen asiakasviestintä, jossa on kyse olemassa olevan asiakassuhteen hoitamiseksi tarvittavasta yhteydenpidosta ja joka ei sisällä markkinointia. Asiakasviestintää on esimerkiksi yhteydenpito, jossa asiakkaalle annetaan tietoja palvelun tilanteesta, jatkuvuudesta tai muuttumisesta. Suoramarkkinointiin liittyvä erityisvelvoitteet eivät siten koske puhdasta asiakasviestintää. Jos viestintä sisältää sekä asiakasviestintää että suoramarkkinointia, viestintä katsotaan suoramarkkinoinniksi.

> Esim. ”Määräaikainen talletuksenne erääntyy ppkkvv” on asiakasviestintää kun taas ”Määräaikainen talletuksenne erääntyy ppkkvv. Tutustukaa uusiin rahastoihimme sijoitusvaihtoehtona!” on suoramarkkinointia.
>
> Esim. Määräaikainen vakuutuksenne erääntyy ppkkvv” on asiakasviestintää kun taas ”Määräaikainen vakuutuksenne erääntyy ppkkvv. Tutustukaa uusiin vaihtoehtoihin!” on suoramarkkinointia.

Käsittelyperusteet ja suoramarkkinointirekisteri

Suoramarkkinoinnin toteuttaminen edellyttää, että finanssiyrityksellä on asianmukainen käsittelyperuste tietojen käsittelylle suoramarkkinointitarkoituksiin. Tällainen käsittelyperuste syntyy, jos rekisteröity on joko antanut suostumuksensa suoramarkkinoinnille tai jos finanssiyrityksellä on oikeutettu etu käsitellä rekisteröidyn tietoja suoramarkkinointitarkoituksiin. Lisäksi sähköisen suoramarkkinoinnin

toteuttaminen edellyttää pääsääntöisesti aina rekisteröidyn suostumuksen olemassaoloa, kuten jäljempänä tarkemmin kuvataan.

Käytettäessä *suostumusta* perusteena suoramarkkinoinnille, on varmistettava, että annettava suostumus kattaa kaikki suunnitellut suoramarkkinoinnin toteutustavat, kuten että suostumusta ei ole hankittu vain puhelimitse tapahtuvaan suoramarkkinointiin, jos tarkoitus on toteuttaa suoramarkkinointia myös sähköisesti. Lisäksi itse suostumuksen tulee täyttää tietosuoja-asetuksen suostumukselle yleisesti asettamat vaatimukset (ks. tarkemmin suostumusta koskeva kappale 3.2.2).

Oikeutettu etu käyttää henkilötietoja suoramarkkinointitarkoituksiin on puolestaan käsillä ensinnäkin tilanteessa, jossa finanssiyrityksen ja rekisteröidyn välillä on merkityksellinen ja asianmukainen suhde kuten asiakassuhde tai siihen rinnastettava suhde (esimerkiksi vakuutus- tai korvauskäsittelyyn perustuva suhde). Finanssiyrityksen henkilörekisterissä, kuten asiakasrekisterissä, olevien tietojen käyttäminen suoramarkkinointitarkoituksiin edellyttää lisäksi, että näissä rekistereissä olevien tietojen yhdeksi käyttötarkoitukseksi on yksilöity tietojen käyttö suoramarkkinointitarkoituksiin.

Oikeutettu etu käyttää henkilötietoja suoramarkkinointitarkoituksiin katsotaan syntyvän asiakassuhteeseen rinnastuvan suhteen ohella myös tilanteessa, jossa finanssiyritys kerää ja käyttää henkilötietoja pelkästään suoramarkkinointitarkoituksiin ilman muuta käsittelyn tarkoitusta. Tietosuoja-asetuksessa todetuin tavoin henkilötietojen käsittelyä suoramarkkinointitarkoituksiin voidaan pitää oikeutetun edun toteuttamiseksi suoritettuna käsittelynä.

Yllä todettu mahdollistaa sen, että finanssiyritys voi käsitellä henkilötietoja suoramarkkinoinnin toteuttamiseksi, vaikka finanssiyrityksellä ei olisi asiakassuhdetta tai muuta siihen verrattavaa suhdetta henkilöön, jota tiedot koskevat. Lisäksi finanssiyritys voi ylläpitää myös erillistä suoramarkkinointirekisteriä (voidaan käyttää myös esimerkiksi nimeä "potentiaaliasiakkaiden rekisteri") sellaisista henkilöistä, joihin se tahtoo kohdentaa suoramarkkinointia, mutta jotka eivät enää ole tai jotka eivät koskaan ole olleet sen asiakkaita tai joihin sillä ei ole muuta asiallisen yhteyden perustavaa suhdetta. Suoramarkkinointirekisteri voi sisältää vanhojen asiakkaiden lisäksi tietoja esimerkiksi finanssiyrityksen internet-sivuilla käyneistä henkilöistä.

Suoramarkkinointirekisteri voi sisältää siihen rekisteröidyistä henkilöistä vain ne tiedot, jotka finanssiyritys perustellusti tarvitsee suoramarkkinoinnin toteuttamiseksi. Suoramarkkinointirekisteriin sisältyvien yksittäistä rekisteröityä koskevien tietojen määrää ei ole nimenomaisesti rajoitettu, mutta finanssiyrityksen on suoramarkkinointirekisterinsä sisältöä määritellessään huomioitava yleiset tietosuojalainsäädännön mukaiset periaatteet, kuten tietojen minimoinnin periaate.

Käyttäessään asiakasrekisterinsä tietoja suoramarkkinointitarkoituksiin finanssiyrityksen on puolestaan huomioitava, että sellaisia asiakkaan tuntemistietoja ja muita henkilötietoja, jotka on hankittu ainoastaan rahanpesulain tarkoittamiin käyttötarkoituksiin, ei saa käyttää näiden tarkoitusten kanssa yhteen sopimattomaan tarkoitukseen, kuten markkinointiin (ks. tarkemmin rahanpesusääntelyä koskeva kappale 4.4). Toisaalta sellaisia rahapesulainmukaisten velvoitteiden täyttämisen yhteydessä kerättyjä henkilötietoja, jotka voidaan kerätä myös muilla perusteilla,

kuten esimerkiksi luoton myöntämiseksi tai korvausasian ratkaisemiseksi, on mahdollista käyttää markkinointiin.

Suoramarkkinoinnin toteuttamisaika

Finanssiyritys voi hyödyntää asiakasrekisteriinsä sisältyviä tietoja suoramarkkinointitarkoituksiin niin kauan kuin finanssiyrityksellä on peruste säilyttää rekisteröityä koskevat tiedot suoramarkkinointitarkoituksissa asiakasrekisterissään ja edellyttäen, ettei rekisteröity missään vaiheessa ole vastustanut tietojensa käyttöä suoramarkkinointiin. Lisäksi siinä vaiheessa, kun finanssiyritykseltä poistuu peruste säilyttää rekisteröidyn tietoja osana asiakasrekisteriään, finanssiyrityksen on osittain mahdollista siirtää asiakasrekisteriinsä sisältyvät tiedot mahdollisesti ylläpitämäänsä erilliseen suoramarkkinointirekisteriin. Tällainen siirto voidaan tehdä, jos finanssiyritys on tiedottanut asianmukaisesti rekisteröityä tietojen siirtämisestä suoramarkkinointirekisteriin ja ilmoittanut tässä samassa yhteydessä rekisteröidyn käytössä olevasta vastustamisoikeudesta. Tiedottaminen voidaan toteuttaa esimerkiksi kertomalla siirtämisestä ja vastustamisoikeudesta asiakasrekisterin tietosuojaselosteessa.

Siirtäessään asiakasrekisterin tietoja suoramarkkinointirekisteriin finanssiyrityksen on myös huomioitava eroavaisuudet niissä tietoryhmissä, joita finanssiyrityksellä on oikeus kumpaakin näistä rekistereistä rekisteröityjä koskien tallettaa. Huomioiden etenkin tietojen minimoinnin periaatteen, todennäköistä on, että suoramarkkinointirekisteri voi sisältää vähemmän yksittäistä rekisteröityä koskevia tietoja kuin asiakasrekisteri. Suoramarkkinointirekisteriin voi siirtää vain tiedot, jotka ovat tarpeen suoramarkkinoinnin toteuttamiseksi.

Suoramarkkinointirekisteriin sisältyviä tietoja finanssiyritys voi puolestaan säilyttää niin kauan kuin finanssiyritys tarvitsee tietoja suoramarkkinoinnin toteuttamiseksi, ellei rekisteröity ole vastustanut henkilötietojensa käsittelyä suoramarkkinointiin. Jos finanssiyrityksellä on esimerkiksi toimintatapana lähestyä kaikkia aiemmin asiakkaanaan olleita henkilöitä pari kertaa vuodessa lähettävällä markkinointikirjeellä, on finanssiyrityksellä perusteltu tarve säilyttää näiden henkilöiden kyseisen markkinointikirjeen lähettämiseksi tarvittavia tietoja suoramarkkinointirekisterissään niin kauan kunnes henkilö joko käyttää oikeuttaan vastustaa suoramarkkinointia tai tulee uudelleen finanssiyrityksen asiakkaaksi, jolloin henkilön tiedot tulevat osaksi finanssiyrityksen asiakasrekisteriä.

Vastustamisoikeus

Rekisteröidyllä on oikeus milloin tahansa maksutta vastustaa häntä koskevien henkilötietojen käsittelyä suoramarkkinointia varten. Jos rekisteröity vastustaa henkilötietojen käsittelyä suoramarkkinointia varten, niitä ei saa enää käsitellä tähän tarkoitukseen. Suoramarkkinoinnin osalta finanssiyrityksellä ei ole vastaavaa harkintavaltaa kuin jos kyse olisi muusta oikeutettuun etuun perustuvasta käsittelystä, jolloin finanssiyritykselle on mahdollista jatkaa rekisteröidyn henkilötietojen käsittelyä vastustamisesta huolimatta, jos finanssiyritys voi osoittaa, että sillä on käsittelylle huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet. Rekisteröidyn vastustaessa suoramarkkinointia finanssiyrityksen tulee lopettaa myös rekisteröityyn kohdistuva profilointi niiltä osin kuin profilointi on suoritettu suoramarkkinointiin liittyen.

Rekisteröityä on tiedotettava vastustamisoikeudesta viimeistään siinä vaiheessa, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran eli käytännössä kohdennettaessa rekisteröityyn suoramarkkinointia. Tieto tulee esittää selkeästi ja muusta tiedotuksesta erillään, kuten ilmoittamalla vastustamisoikeudesta suoramarkkinointiviestin alareunassa. Lisäksi vastustamisoikeudesta on asiallista mainita sen henkilörekisterin tietosuojaselosteessa, jonka tietojen pohjalta suoramarkkinointi toteutetaan.

Rekisteröity voi halutessaan vastustaa kaikenlaista henkilötietojensa käyttöä suoramarkkinointiin, jolloin finanssiyrityksen ei tule kohdistaa rekisteröityyn mitään suoramarkkinointia. Vaihtoehtoisesti rekisteröity voi myös niin halutessaan vastustaa suoramarkkinointia vain osittain esimerkiksi rajaamalla halutulla tavalla erikseen puhelin-, postitus- tai sähköisiä markkinointitapoja. Jos finanssiyritykselle jää epäselväksi, miltä osin rekisteröity haluaa käyttää vastustamisoikeuttaan, asiaa tulee tarvittaessa tiedustella rekisteröidyltä itseltään.

Tiedonantovelvollisuus suoramarkkinoinnissa

Kuten muussakin henkilötietojen käsittelyssä myös suoramarkkinoinnin yhteydessä finanssiyrityksen on huolehdittava tietosuoja-asetuksen mukaisen tiedonantovelvollisuuden täyttämisestä. Tiedonantovelvollisuuden sisältö on kuvattu tarkemmin jäljempänä kohdassa 6 (Yleisölle ja rekisteröidylle tarkoitettu tiedotus). Finanssiyrityksen hankkiessa suoramarkkinoinnissa käytetyt tiedot muualta kuin rekisteröidyltä itseltään, finanssiyrityksen on erityisesti kiinnitettävä huomiota siihen, että tiedonantovelvollisuus tulee asianmukaisesti täytetyksi.

Käytännössä tiedonantovelvollisuus voidaan toteuttaa asettamalla tiedonantovelvollisuuden piiriin kuuluvat tiedot helposti rekisteröidyn saataville, kuten sisällyttämällä ne finanssiyrityksen internet-sivuilla olevaan tietosuojaselosteeseen, ja ilmoittamalla suoramarkkinointiviestissä, mistä rekisteröity voi nämä tiedot saada. Tiedonantovelvoitteen piiriin kuuluvia tietoja ei siis ole tarpeellista sisällyttää kokonaisuudessaan jokaiseen suoramarkkinointiviestiin vaan riittää, jos viestistä selkeästi ilmenee, mistä tiedot ovat helposti rekisteröidyn saatavissa.

Lisäksi täytettäessä tiedonantovelvollisuutta suoramarkkinoinnin yhteydessä huomiota tulee kiinnittää myös suoramarkkinointiin liittyvään erityisvelvoitteeseen informoida rekisteröityä selkeästi ja erillään muusta tiedotuksesta rekisteröidyn oikeudesta vastustaa suoramarkkinointia. Suositeltavana käytäntönä voidaan pitää, että vastustamisoikeuden olemassaolosta mainitaan jokaisen suoramarkkinointiviestin yhteydessä samalla kun kerrotaan, mistä rekisteröity voi saada tarkemmat tietosuoja-asetuksen mukaiset tiedot henkilötietojensa käsittelystä.

Tietojen luovuttaminen suoramarkkinointia varten

Luottolaitoksia sitoo luottolaitostoiminnasta annetun lainsäädännön mukainen ja vakuutusyhtiöitä vakuutusyhtiölain mukainen salassapito- ja vaitiolovelvollisuus. Tämän vuoksi finanssiyritykset eivät voi luovuttaa rekistereistään tietoja suoramarkkinointia varten muutoin kuin luottolaitostoiminnasta annettuna lainsäädännön ja vakuutusyhtiölain mahdollistamissa rajoissa samaan konserniin tai taloudelliseen yhteenliittymään kuuluvalle yritykselle.

Finanssiyritykset voivat kuitenkin ostaa, vastaanottaa ja liittää omiin suoramarkkinointirekistereihinsä tietoja ulkopuolisista lähteistä. Ulkopuolinen reksiterinpitäjä voi luovuttaa finanssiyritykselle henkilötietoja suoramarkkinointia varten, jollei rekisteröity ole kieltänyt tiedon luovuttamista ja jos on ilmeistä, että rekisteröity tietää tietojen luovuttamisesta tällaista tarkoitusta varten.

Finanssiyrityksen on hyvä sopimuksellisesti varmistua siitä, että taholla joka luovuttaa tiedot finanssiyritykselle, on oikeus luovuttaa tiedot suora markkinointitarkoituksiin ja että kyseinen taho on hankkinut tarvittavat suostumukset sekä täyttänyt tietosuojalainsäädännön asettamat informointi- ja muut velvoitteet suhteessa niihin rekisteröityihin, joiden tietoja ollaan luovuttamassa.

Huomionarvoista on, että mikäli finanssiyrityksen vastaanottamat tiedot sisältävät arkaluonteisia tietoja, joiden käsittelylle on asetettu tiukemmat vaatimukset, finanssiyrityksen on edellytettävä, että tiedot luovuttava taho on saanut näiden tietojen luovuttamiselle tietosuojalainsäädännössä edellytetyn suostumuksen.

Sähköinen suoramarkkinointi

Sähköinen suoramarkkinointi on sähköpostiviestien, tekstiviestien, automatisoitujen soittojärjestelmien sekä puhe-, ääni- ja kuvaviestin avulla toteutettua suoramarkkinointia. Jos sen sijaan yhteydenotto asiakkaaseen toteutetaan siten, että lopullinen yhteydenotto tapahtuu ihmistyöpanoksella – kuten esimerkiksi puhelinmyynnissä – ei kyseessä ole sähköinen suoramarkkinointi, vaan tavallinen suoramarkkinointi, joka voi perustua myös oikeutettuun etuun eikä tällöin edellytä ennakkosuostumusta.

Sähköistä suoramarkkinointia sääntelee yleisen tietosuojalainsäädännön lisäksi myös erityiset nimenomaan sähköistä suoramarkkinointia koskevat säännökset. Tämän ohjeen valmistuessa kyseiset säännökset sisältyvät kansalliseen tietoyhteiskuntakaareen (917/2014), jonka säännökset tulevat kuitenkin osittain korvautumaan uuden EU-tasolla valmisteltavana olevan ja suoraan sovellettavaksi tulevan sähköisen viestinnän tietosuoja-asetuksen (e-Privacy regulation) tullessa voimaan.

Sähköistä suoramarkkinointia saa pääsääntöisesti kohdistaa vain sellaisiin henkilöihin, jotka ovat antaneet siihen etukäteisen suostumuksensa. Suostumuksen tulee olla vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, minkä lisäksi sähköisessä suoramarkkinoinnissa korostuu vaatimus suostumuksen luonteesta aktiivisena toimenpiteenä. Suostumuksen antaminen edellyttää, että rekisteröity on nimenomaan aktiivisesti hyväksynyt sähköisen suoramarkkinoinnin vastaanottamisen. Näin ollen suostumusta ei voi hankkia esimerkiksi rastittamalla valmiiksi valintaruutuun suoramarkkinoinnin sallivan vaihtoehdon.

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

ennakkosuostumusta, mikäli asiakas on ostanut finanssiyritykseltä palvelun tekstiviestin välityksellä. Samoin finanssiyritys voi lähettää asiakkaalleen suoramarkkinointia sähköisten palveluidensa kautta ilman etukäteisen suostumuksen hankkimista.

Finanssiyritys voi myös muokata verkkopalvelunsa käyttöliittymää asiakaskohtaiseksi asiakkaan palvelujen ja palvelutottumusten mukaan ilman ennakkosuostumusta. Tällaista palvelun muokkaamista ei pidetä lähtökohtaisesti suoramarkkinointina, vaan kyse on asiakkaalle personoidun palvelun tuottamisesta. Kyseessä on kuitenkin asiakkaan profilointi, jolloin huomiotavaksi tulee profilointia koskevat säännökset. Lisäksi asiakkaasta evästeiden avulla kerättyjä tietoja voi käyttää suomarkkinointitarkoituksiin ilman erillisen suostumuksen hankkimista edellyttäen, että asiakas on sallinut evästeiden käyttämisen lainsäädännön edellyttämin tavoin eli asiakas ei ole käyttämänsä selaimen tai muun applikaation asetusten avulla estänyt evästeiden käyttämistä.

Sähköisen suoramarkkinoinnin toteuttamisen yhteydessä tulee huolehtia asianmukaisesti yleisen tiedonantovelvollisuuden noudattamisesta vastaavin tavoin kuin muun suoramarkkinoinnin osalta sekä vastustamisoikeuden tarjoamisesta rekisteröidylle. Erityisesti sähköisessä suoramarkkinoinnissa korostuu rekisteröidyn vastustamisoikeus, sillä rekisteröidylle tulee tarjota mahdollisuus ilman erillistä maksua ja helposti vastustaa yhteystietojensa käsittelyä suoramarkkinointitarkoituksiin jokaisen lähetetyn sähköisen suoramarkkinointiviestin yhteydessä.

Lisäksi luottolaitosten osalta huomionarvoista on, että e-laskupalvelussa laskuttaja saattaa kohdistaa asiakkaalle markkinointia osana e-laskun liitemateriaalia. Osa laskuttajista joutuu lain perusteella toimittamaan laskun ohessa myös tietoja laskun perusteesta liitteellä tai muulla vastaavalla tavalla (esimerkiksi sähköyhtiöt ja teleoperaattorit). Laskuttaja vastaa e-laskun ja liitemateriaalin sisällöstä sekä markkinoinnin lainmukaisuudesta kokonaisuudessaan. Luottolaitoksella ei ole mahdollisuutta vaikuttaa laskuttajan lähettämän liitemateriaalin sisältöön. Mikäli asiakas haluaa kieltää e-laskun liitemateriaaliin sisältyvän markkinoinnin, asiakkaan tulee ilmoittaa suoramarkkinointikielto suoraan laskuttajalle.

Suoramarkkinointihankkeiden yhteydessä on selvitettävä ja suunniteltava erityisesti

- soveltuvatko tiedot suoramarkkinoinnin lähdetietoina käytettäviksi (käsittelyperuste ja käyttötarkoitussidonnaisuus)
- ovatko suoramarkkinointia varten ulkopuoliselta saadut tiedot laillisesti luovutettuja
- onko aineistossa henkilöitä, jotka ovat käyttäneet oikeuttaan vastustaa suoramarkkinointia
- miten tietoa on annettava (tiedonantovelvollisuuden täyttäminen ja tiedottaminen vastustamisoikeudesta)

3.2.4 Profilointi ja automatisoitu päätöksenteko

Asiakkaiden profilointi

Finanssiyritys voi määritellä asiakkaitaan koskevien tietojen pohjalta kohderyhmiä muun muassa suoramarkkinoinnin tarkemmaksi kohdentamiseksi. Tämä on profilointia. Kun profiloinnissa hyödynnetään henkilöihin yhdistettävissä olevia tietoja, kuten nimen tai muun tunnisteen perusteella identifioidun kuluttajan käyttäytymiseen liittyviä tietoja, kysymys on henkilötietojen käsittelystä.

Profilointia varten finanssiyritys voi kerätä asiakkaita koskevia tietoja paitsi asiakkailta myös ulkopuolisista luotettavista 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 asiakasrekisterilleen. Profilointia ei voi suorittaa rekisterin käyttötarkoituksen vastaisesti. 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 teknisiä ja organisatorisia toimenpiteitä, jotta varmistetaan, että henkilötietojen virheellisyyteen johtavat tekijät korjataan ja virheriski minimoidaan. Lisäksi henkilötiedot on turvattava siten, että asiakkaiden etuihin ja oikeuksiin kohdistuvat mahdolliset riskit otetaan huomioon ja estetään syrjintä.

Automatisoitu päätöksenteko

Rekisteröidyllä on pääsääntöisesti oikeus olla joutumatta päätöksen kohteeksi, jossa arvioidaan hänen henkilökohtaisia ominaisuuksiaan ja joka aiheuttaa hänelle oikeusvaikutuksia tai vaikuttaa häneen muutoin vastaavalla tavalla merkittävästi ja joka on tehty ainoastaan automaattisen tietojenkäsittelyn avulla ilman ihmisen osallistumista (jäljempänä automatisoitu päätöksenteko). Näin ollen automatisoidusta päätöksenteosta ei ole kyse esimerkiksi silloin, kun järjestelmästä saatu kielteinen päätös menee aina toimihenkilön uudelleen harkittavaksi ennen päätöksen antamista asiakkaalle.

Automatisoidusta päätöksenteosta tietosuoja-asetuksen merkityksessä on kyse, mikäli päätös on vaikutuksiltaan merkittävä suhteessa rekisteröityyn, joka on päätöksen kohteena. Esimerkiksi kun finanssiyritys valitsee tiedostoistaan tietyt kriteerit täyttäviä henkilöasiakkaitaan kohteiksi suoramarkkinointiaineiston postitukseen, kyse ei ole automatisoidusta päätöksenteosta, koska tarjouksista ei aiheudu asiakkaalle merkittäviä vaikutuksia. Lisäksi esimerkiksi luotto- tai vakuutushakemuksen tai vakuutuskorvauksen täysin automatisoidussa myönnössä asiakkaan hakemuksen mukaisesti voidaan kyseenalaistaa asiakkaalle aiheutuneet

merkittävät oikeusvaikutukset ja näin ollen tietosuoja-asetuksessa säädetty oikeus olla joutumatta automatisoidun päätöksenteon kohteeksi. Tässä yhteydessä on myös huomioitava, että finanssialalla on useassa tilanteessa velvollisuus perustella päätökset ja pääsääntöisesti liittää päätöksiin muutoksenhakuohjeet. Päätöksentekoprosessia tulee siis arvioida kokonaisuudessaan.

Automatisoitu päätöksenteko on sallittua, kun

a) se on tarpeen rekisteröidyn ja finanssiyrityksen välisen sopimuksen tekemistä tai täytäntöönpanoa varten;

b) se on tarpeen finanssiyrityksen tarjoaman palvelun turvallisuuden ja luotettavuuden varmistamiseksi;

c) se on hyväksytty EU:n tai sen jäsenvaltion lainsäädännössä (tällaista sääntelyä liittyy finanssialalla muun muassa rahanpesun, petosten ja verovilpin torjuntaan); tai

d) päätös perustuu rekisteröidyn nimenomaiseen suostumukseen.

Sopimukseen ja suostumukseen liittyvässä automatisoidussa päätöksenteossa on aina sovellettava seuraavia suojatoimia: käsittelystä tiedottaminen ja rekisteröidyn oikeus vaatia ihmisen osallistumista tietojen käsittelemiseen, rekisteröidyn oikeus esittää kantansa, oikeus saada selvitys kyseisen arvioinnin jälkeen tehdystä päätöksestä ja oikeus riitauttaa päätös. Finanssiyritys voi myöntää esimerkiksi henkilöasiakkailleen tarkoitettuja luottoja tai vakuutuksia Internet-kotisivuillaan täysin automatisoidusti. Kun luotto tai vakuutus evätään tällaisessa prosessissa, on kyse automatisoidusta päätöksenteosta. Tällöin rekisteröidyllä on oltava mahdollisuus ottaa yhteyttä finanssiyrityksen asiakaspalveluun hakemuksen manuaalista käsittelyä varten. Näin rekisteröidylle järjestyy mahdollisuus esittää finanssiyritykselle kantansa ja sellaisia asiaan vaikuttavia tietoja, joita finanssiyrityksellä mahdollisesti ei ole. Tällöin rekisteröidyllä on myös mahdollisuus saada tietoja niistä perusteista, joita finanssiyritys on päätöksenteossaan käyttänyt. Tarkat luokitusperusteet kuuluvat finanssiyritysten liikesalaisuuden piiriin.

Automatisoitu päätöksenteko on kuitenkin ankarammin säänneltyä, kun kyse on tietosuoja-asetuksen 9 artiklan mukaisista erityisiin henkilötietoryhmiin perustuvista automatisoiduista päätöksistä. Tuolloin automatisoitu päätöksenteko on mahdollista, mikäli rekisteröity, johon automatisoitu päätöksenteko kohdistuu, on antanut nimenomaisen suostumuksensa tietojen käsitellylle taikka mikäli käsittely on tarpeen tärkeää yleistä etua koskevasta syystä EU:n tai sen jäsenvaltion lainsäädännön nojalla. Lisäksi edellytetään asianmukaisten suojatoimenpiteiden toteuttamista. Edellä mainituista vaatimuksista poiketen vakuutusyhtiöillä on yleisiä automatisoitua päätöksentekoa koskevia edellytyksiä noudattaen mahdollisuus tietosuojalain nojalla hyödyntää automatisoidussa päätöksenteossa vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, mikäli käsittely on tarpeen vakuutusyhtiön vastuun selvittämiseksi.

Automatisoitua päätöksentekoa voidaan kohdistaa lapseen sillä edellytyksellä, että täysin automatisoitu lapsiin kohdistuva päätöksentekoprosessi on finanssiyritykselle välttämätön. Tällöin tulee kuitenkin kiinnittää erityistä huomiota siihen, että käsittelyn

yhteydessä tarjotaan asianmukaiset ja kattavat suojatoimenpiteet, kuten mahdollisuus saada asian uudelleen käsitellyksi 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 jos päätöksellä ei ole suoria merkittäviä vaikutuksia lapseen. Automatisoitu päätöksenteko ei näin ollen kohdistu lapseen esimerkiksi silloin kun lapsi on vahinkovakuutuksen vakuutettu ja korvaus vakuutuksesta maksetaan vakuutussopimuksen osapuolena olevalle lapsen huoltajalle eikä lapselle itselleen. Tämä mahdollistaa esimerkiksi kertakorvausluontoisen lapsen lääkärikulun korvausta koskevan päätöksenteon automatisoinnin, kunhan automatisoidun päätöksenteon muut edellytykset täyttyvät.

Esimerkkejä

Kohdehenkilöiden valinta suoramarkkinoinnissa

Finanssiyritys valitsee tiedostoistaan tietyt kriteerit täyttäviä henkilöasiakkaitaan kohteiksi suoramarkkinointiaineiston postitukseen. Vaikka menettely olisi täysin automatisoitu, ei se ole asetuksen tarkoittamaan automatisoitua päätöksentekoa, koska tarjouksista ei aiheudu asiakkaalle oikeusvaikutuksia eikä se muuten vaikuta häneen vastaavalla tavalla merkittävästi.

Automatisoitu luoton myöntäminen ja vakuutuksen myynti

Luottolaitos myöntää henkilöasiakkailleen tarkoitettuja luottoja internet-kotisivuillaan tarjottavan palvelun välityksellä. Järjestelmä saattaa olla automatisoitu niin, että luotto myönnetään, jos luottolaitoksen tietokannoissa ei ole asiakkaasta sellaisia tietoja, esimerkiksi hänen maksukäyttäytymistään tai varallisuusasemaansa koskevia, jotka ovat perusteena luottohakemuksen hylkäämiselle. Jos tällaisia tietoja on, ei luottoa myönnetä tai se myönnetään hakemuksesta poikkeavin ehdoin.

Kyseessä on automatisoitu päätös, josta aiheutuu oikeusvaikutuksia asiakkaalle. Järjestelmä on varustettava ominaisuuksilla, joiden avulla varmistetaan rekisteröidyn oikeuksien suojaaminen. Hylkäys- tai osahylkäystapauksessa asiakkaalla on oltava mahdollisuus ottaa yhteyttä luottolaitoksen asiakaspalvelupisteeseen luottohakemuksen manuaalista käsittelyä varten. Näin asiakkaalle järjestyy mahdollisuus esittää luottolaitokselle kantansa ja sellaisia asiaan vaikuttavia tietoja, joita yhtiöllä mahdollisesti ei ole. Tällöin asiakkaalla on myös mahdollisuus saada tietoja niistä perusteista, joita luottolaitos on päätöksenteossaan käyttänyt.

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

Vakuutusyhtiö myy henkilöasiakkailleen tarkoitettuja vakuutuksia internet-kotisivuillaan tarjottavan palvelun välityksellä. Järjestelmä on täysin automatisoitu niin, että vakuutus myönnetään, jos vakuutusyhtiön tietokannoissa ei ole asiakkaasta sellaisia tietoja, esimerkiksi hänen maksukäyttäytymistään tai terveydentilaansa

koskevia, jotka ovat perusteena vakuutushakemuksen hylkäämiselle. Jos tällaisia tietoja on, ei vakuutusta myönnetä tai se myönnetään hakemuksesta poikkeavin ehdoin.

Kyseessä on automatisoitu päätös, josta aiheutuu oikeusvaikutuksia asiakkaalle. Järjestelmä on varustettava ominaisuuksilla, joiden avulla varmistetaan rekisteröidyn oikeuksien suojaaminen. Hylkäys- tai osahylkäystapauksessa asiakkaalle ilmoitetaan hylkäyksen peruste ja hänet ohjataan ottamaan yhteyttä vakuutusyhtiön asiakaspalvelupisteeseen vakuutushakemuksen manuaalikäsittelyä varten. Näin asiakkaalle järjestyy mahdollisuus esittää vakuutusyhtiölle kantansa ja sellaisia asiaan vaikuttavia tietoja, joita yhtiöllä mahdollisesti ei ole.

4 Henkilötietojen käsittelyä koskevia erityissäännöksiä

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.

Finanssialalla tällaisten arkaluonteisten tietojen käsittely on kuitenkin mahdollista liiketoiminnan luonteesta johtuen. Käsittelylle on olemassa aina jokin erityisperuste ja niistä kerrotaan tarkemmin seuraavissa kappaleissa.

Finanssiyrityksen ja asiakkaan välisessä suhteessa voi esiintyä muitakin luottamuksellisia tietoa, joiden käsittelyn asiakas kokee yksityisyyteensä liittyväksi. Nämä tiedot eivät kuitenkaan ole asetuksen tarkoittamia arkaluonteisia tietoja.

4.2 Finanssiyritysten kannalta keskeisiä poikkeuksia erityisiä henkilöryhmiä koskevaan käsittelykieltoon

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

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. Suostumuksena voidaan myös pitää esimerkiksi arkaluonteisen tiedon sisältävää maksutoimeksiannon antamista.

Käsittely on tarpeen sosiaaliturvan alalla

Erityisiä henkilötietoryhmiä on mahdollista käsitellä myös silloin, kun käsittely on tarpeen vakuutusyhtiön tai asiakkaan velvoitteiden ja erityisten oikeuksien noudattamiseksi sosiaaliturvan alalla tai jos käsittely on tarpeen erityislainsäädännön

nojalla. Sosiaaliturvaan katsotaan kuuluviksi lakisääteinen työtapaturma- ja ammattitautivakuutus sekä työeläkevakuutus.

Ammattiliittoon kuuluminen

Finanssiyritykset voivat käsitellä tietoa asiakkaansa kuulumisesta ammattiliittoon, jos tällainen tieto ammattiliittoon kuulumisesta kuuluu ammattiliittotoiminnan laillisen toiminnan piiriin, kuten ammattiliittojen jäsenilleen ottamiin ryhmävakuutuksiin tai ammattiliittojen 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 että jäsenet ovat antaneet suostumuksensa tietojen luovuttamiseen. Finanssiyritykset voivat käsitellä tietoa ammattiliittoon kuulumisesta vain siinä määrin, kuin se on välttämätöntä.

Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittely oikeusvaateiden yhteydessä sekä vakuutusyhtiön vastuun selvittämiseksi

Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja saa käsitellä oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi oikeudellisessa menettelyssä tai hallinnollisessa tai tuomioistuimen ulkopuolisessa menettelyssä. Suomessa tällaisia tuomioistuimen ulkopuolisia menettelyjä ovat lautakuntamenettelyt, kuten FINE:n pankki-, vakuutus- ja arvopaperilautakunnat sekä kuluttajariitalautakunta. Oikeusvaateeseen katsotaan lautakuntakäsittelyssäkin kuuluvan asian selvittämiseen kuuluva henkilötietojen käsittely.

> Luottolaitoksella on oikeus käsitellä rikostietoja silloin, kun luottolaitos pyrkii selvittämään sitä vastaan suunnattua rikosta.
>
> 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 sitä vastaan suunnattua rikosta. Vakuutusyhtiölain säännösten mukaan vakuutuslaitoksilla on oikeus luovuttaa toisille vakuutuslaitoksille vaitiolovelvollisuuden piiriin kuuluvia tietoja niihin kohdistuneista rikoksista sekä niille ilmoitetuista vahingoista.

Lisäksi valmisteilla olevaan tietosuojalakiin on ehdotettu voimassa olevaa henkilötietolakia vastaavaa säännöstä, jonka perusteella vakuutusyhtiöillä on oikeus käsitellä rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja, jos ne ovat tarpeen vakuutusyhtiön vastuun selvittämiseksi.

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 liikennerikoksista. 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 eli osaksi korvaustoiminnan rekisteriä.

Finanssiyrityksellä on velvollisuus laatia tietosuojaa koskeva vaikutustenarviointi tietojenkäsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin. Vaikutusten arviointia käsitellään tarkemmin kohdassa 5.4.

Rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittely asiakashäiriö- ja väärinkäytösrekistereissä

Tietosuojalautakunta on voimassa olevan 43 §:n mukaisesti myöntänyt finanssialan toimijoille luvat rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelyyn. Tällainen lupa on myönnetty luottolaitoksille asiakashäiriörekisterin ja vakuutusyhtiöille väärinkäytösrekisterin osalta. Tietosuojalautakunnan luvat sisältävät yksityiskohtaisia lupamääräyksiä henkilötietojen käsittelystä, jotka koskevat muun muassa henkilötietojen tallennusajankohtaa, tietojen poistamista sekä rekisteröidyn informoimista.

Uutta tietosuojalakia valmistelleen oikeusministeriön työryhmän näkemyksen mukaan olisi perusteltua, että mainittujen tietosuojalautakunnan lupien mukainen henkilötietojen käsittely voisi jatkua yleisen tietosuoja-asetuksenkin tullessa sovellettavaksi. Koska sääntelyltä edellytetään tarkkarajaisuutta ja erityisiä suojatoimia, ei tällaisesta käsittelystä ole työryhmän mielestä mielekästä säätää tietosuojaa koskevassa yleislaissa. Näin ollen tältäkin osin olisi tarvetta säätää asiasta sektorilainsäädännössä, kuten luottolaitosten osalta esimerkiksi luottolaitostoiminnasta annetussa laissa ja vakuutusyhtiöiden osalta vakuutusyhtiölaissa. Mahdollisen sektorikohtaisen lainsäädännön tarkempi sisältö varmistuu myöhemmin.

4.3 Eräät vakuutustoiminnassa saadut tiedot

Tietosuojalaki antaa vakuutusyhtiöille mahdollisuuden käsitellä arkaluontoisiksi katsottavia tietoja 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 henkilövakuutusten riskinvalinnassa ja korvaustoiminnassa.

4.4 Rahanpesun ja terrorismin rahoituksen torjunta, kansainväliset finanssipakotteet ja kansalliset jäädyttämispäätökset sekä näihin liittyvä henkilötietojen luovuttaminen

Rahanpesun ja terrorismin rahoituksen torjunta

Finanssiyritysten velvollisuus tuntea asiakkaansa perustuu luottolaitoslain 15 luvun 18 §:ään ja vakuutusyhtiölain 6 luvun 13 §:ään. Asiakkaan tuntemista koskevat aineelliset vaatimukset sisältyvät rahanpesulakiin (L rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017).

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

Rahanpesun ja terrorismin rahoituksen torjunta on yleisen tietosuoja-asetuksen 23 artiklassa tarkoitettua rikosten ennalta estämistä, tutkintaa ja torjuntaa. Rahanpesulain 3 luvun 3 § 4 momentin mukaisesti finanssiyrityksen on ilmoitettava asiakkaalle, että asiakkaan tuntemistietoja ja muita henkilötietoja voidaan käyttää rahanpesun ja terrorismin rahoittamisen estämiseen, paljastamiseen ja selvittämiseen sekä muihin lainkohdassa mainittuihin tarkoituksiin.

Rahanpesulain vaatimusten täyttäminen voi edellyttää finanssiyritykseltä henkilötietojen käsittelyä myös ilman asiakkuussuhdetta siitä riippumatta, onko kyse asiakkaan tuntemiseen vai nimenomaisesti rahanpesun ja terrorismin rahoituksen torjuntaan liittyvistä velvoitteista.

Esimerkkeinä tiedoista, joita on hankittu ainoastaan rahanpesun ja terrorismin rahoittamisen estämiseksi ja paljastamiseksi voidaan pitää rahanpesulain 4 luvun 3 §:n ilmoitusvelvollisuuden täyttämiseksi hankittuja tietoja, jotka on pidettävä erillään asiakasrekisteristä eikä niitä saa käyttää muuhun kuin rahanpesulaissa säädettyyn tarkoitukseen. Muitakaan henkilötietoja, jotka on hankittu ainoastaan rahanpesun ja terrorismin rahoittamisen estämiseksi ja paljastamiseksi, ei saa käyttää tarkoitukseen, joka on yhteen sopimaton näiden tarkoitusten kanssa, kuten finanssiyrityksen tuotteiden tai palvelujen markkinointiin.

Laki ei määrittele tietolähteitä, joita finanssiyrityksen tulee tai on sallittua hyödyntää asiakkaan tuntemista tai muita rahanpesulain mukaisia velvoitteita täyttäessään. Lähtökohtana on, että tiedot saadaan asiakkaalta tai julkisista rekistereistä. Muiden tietolähteiden tarve ja käyttökelpoisuus on harkittava osana asiakkaaseen liittyvien rahanpesun ja terrorismin rahoituksen riskien arviointia.

Rahanpesuilmoituksen tekemistä tai selvittelyä ei saa paljastaa epäilyn kohteelle tai muulle henkilölle. Rajoituksen piiriin kuuluvat muun muassa sovellettuja riskienhallintatoimenpiteitä, asiakkaan riskiluokitusta tai asiakkaan luottotietojen tarkistamista rahanpesuepäilyn yhteydessä koskevat tiedot. Finanssiyritys saa kuitenkin salassapitovelvoitteen estämättä luovuttaa tiedon rahanpesulassa säädetyin rajoituksin muun muassa samaan rahoitus- ja vakuutusryhmittymään kuuluvalle toimiluvan saaneelle yhteisölle.

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.

Kansainväliset finanssipakotteet ja kansalliset jäädyttämispäätökset

Kansainvälisillä finanssipakotteilla 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. Suomea sitovat kansainväliset finanssipakotteet perustuvat YK:n turvallisuusneuvoston tai 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.

Kansalliset jäädyttämispäätökset ovat Keskusrikospoliisin tekemiä, lakiin varojen jäädyttämisestä terrorismin torjumiseksi (325/2013) perustuvia päätöksiä varojen jäädyttämisestä.

YK:n ja EU:n asettamien finanssipakotteiden lisäksi useilla valtioilla ja viranomaisilla on omia kansallisia pakotteita, esimerkiksi Yhdysvaltojen Office of Foreign Assets Control (OFAC) -nimisen viranomaisen listaukset henkilöistä ja yhteisöistä, joiden varat tulee OFACin mukaan jäädyttää. Finanssivalvonta on katsonut, että OFAC-listojen seuraaminen on perustellusti rahanpesulain 3 luvun 4 §:ssä säädetyn selonottovelvollisuuden piiriin kuuluva tilanne. Finanssiyrityksillä voidaan siten katsoa olevan velvollisuus seurata eri valtioiden kansallisia pakotelistoja kansainvälisen maksuliikenteen tai muiden rajat ylittävien finanssipalveluiden toimivuuden turvaamiseksi sekä rahanpesulakiin perustuvien ja kansainvälisten velvoitteidensa täyttämiseksi. Listoja saa hyödyntää vain näihin käyttötarkoituksiin ja niitä käytettäessä on huolehdittava, ettei listalla olevien henkilöiden tietosuoja aiheettomasti vaarannu. Tämä tarkoittaa muun muassa sitä, ettei listoille sisältyviä henkilötietoja tallenneta finanssiyrityksen asiakasrekistereihin.

Finanssiyritykset ovat velvollisia seuraamaan pakotteiden ja jäädyttämispäätösten 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 lakisääteiseen velvoitteen noudattamiseksi.

Henkilötietojen luovutus viranomaisille

Finanssiyrityksellä on velvollisuus antaa muutoin salassa pidettäväksi säädettyjä tietoja syyttäjä- ja esitutkintaviranomaiselle rikoksen selvittämiseksi sekä muulle viranomaiselle, jolla on lain mukaan oikeus saada sellaisia tietoja (esimerkiksi Finanssivalvonta, rahanpesun selvittelykeskus sekä ulosotto-, vero- ja sosiaaliviranomaiset).

Viranomaisen oikeus saada tietoja perustuu sen lakisääteisiin tehtäviin. Tietojenluovutukseen voi liittyä erityislakiin tai viranomaisen toimivaltuuksiensa puitteissa antama ilmaisukielto. Ellei tällaista kieltoa ole tai sen voimassaolo on päättynyt, tietojen luovutus kuuluu asiakkaan tarkastusoikeuden piiriin.

4.5 Luottotiedot

Luottotietojen käyttämistä säännellään luottotietolaissa. Sen mukaan luottotietoja saa käyttää se, joka tarvitsee tietoa luoton myöntämistä tai luoton valvontaa varten tai muuhun luottotietolaissa yksilöityyn tarkoitukseen. Luottotietolaki koskee sekä yksityishenkilöiden että yritysten luottotietoja. Finanssiyrityksen toimihenkilö saa tehdä luottotietokyselyn ja tutkia asiakkaiden tietoja luottolaitoksen rekistereistä ainoastaan työtehtäviin liittyvissä tilanteissa.

Kun henkilöluottotiedot tarkastetaan ulkopuolisesta luottotietorekisteristä, asiakkaalle tulee ilmoittaa henkilöluottotietojen käytöstä sekä siitä, mistä rekisteristä luottotiedot hankitaan tai on hankittu. Mikäli luottotiedot on tarkistettu rahanpesuepäilyn yhteydessä, siitä ei kuitenkaan 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 luottohakemuksen ulkopuolisesta luottotietorekisteristä saatujen henkilöluottotietojen perusteella, tulee myös huomioida se, että luottolaitoksen on välittömästi päätöksen jälkeen ilmoitettava luotonhakijalle 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 (esimerkiksi Suomen Asiakastieto Oy).

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

4.6 Henkilötunnuksen käsittely

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

Henkilötunnuksen käsittely finanssiyrityksissä

Finanssiyritysten toiminnassa on tärkeää, että toimintaan liittyvät henkilöt (kuten tallettajat, maksajat, takaajat, käyttöoikeudenhaltijat, vakuutuksenottajat, vakuutetut, edunsaajat, vahingonkärsineet) voidaan yksilöidä täysin yksiselitteisesti. Tämän vuoksi tietosuojalakiin on otettu nimenomainen maininta siitä, että henkilötunnuksen käsittely on finanssiyritysten toiminnassa sallittua.

Lain nojalla vakuutusyhtiö voi esimerkiksi tallettaa henkivakuutuksen yhteyteen tiedon edunsaajan henkilötunnuksesta.

Vakuutusyhtiö voi myös esimerkiksi pyytää vakuutuksen hakijaa ilmoittamaan henkilötunnuksensa ennen kuin yhtiö tekee itseään sitovan vakuutustarjouksen.

Yksiselitteinen suostumus

Henkilötunnusta voidaan käsitellä myös rekisteröidyn yksiselitteisesti antamalla suostumuksella. Suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

Finanssiyritysten toiminnassa ei yleensä tarvita erillisiä suostumuksia, koska lakiin sisältyy edellä kerrottu nimenomainen maininta siitä, että henkilötunnuksen käsittely on sallittua finanssiyritysten toiminnassa.

Henkilötunnuksen luovuttaminen osoitetietojen päivitystä varten

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

Henkilötunnuksen merkitseminen tulosteisiin

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

4.7 Turvakielto

Turvakielto on väestötietojärjestelmästä annetun lain 36 ja 37 §:n mukainen tietojenluovutuskielto, jolla rajoitetaan henkilön yhteystietojen luovuttamista väestötietojärjestelmästä. Turvakielto koskee usein koko perhettä. Mikäli asiakkaalla on turvakielto, Väestörekisterikeskus ei välitä asiakkaan osoitetietoja luottolaitokselle, eikä edes syytä, miksi asiakkaan tietojenvälitys on loppunut. Turvakieltoasiakkaan tulee itse ilmoittaa finanssiyritykselle turvakiellosta ja osoitteessaan tapahtuvista muutoksista.

Esimerkiksi luottolaitoksen järjestelmissä oleva tieto asiakkaan turvakiellosta ei estä asiakkaan yhteystietojen välittymistä

luottolaitoksen asiakastietojärjestelmästä niille tahoille (esim. korttimaksunsaajat, viranomaiset), joille luottolaitos voi lainsäädännön ja sopimusehtojen mukaan välittää asiakkaan tietoja. Turvakieltoasiakkaan tulee ilmoittaa luottolaitokselle 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 turvakieltoasiakas antaa luottolaitokselle myös varsinaisen osoitteensa, joka asiakasrekisteriin tallennettuna tietona on pankkisalaisuuden alainen tieto.

5 Rekisterinpitäjän velvollisuudet

5.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

Henkilötietojen käsittelyä koskevat periaatteet otetaan huomioon alkaen henkilötietojen keräämisestä ja päättyen niiden hävittämiseen. Ne huomioidaan aikaisessa vaiheessa muun muassa

- järjestelmä- ja sovelluskehityksessä,
- tuotteiden ja palveluiden kehityksessä ja
- hankinnoissa ja projekteissa.

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.

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 muun muassa tehtävien ja vastuiden määrittely, sisäiset ohjeet ja koulutus sekä esimiesvalvonta.

Rekisterinpitäjän on lisäksi toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että se käsittelee oletusarvoisesti vain kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä koskee

- kerättyjen henkilötietojen määriä
- käsittelyn laajuutta
- säilytysaikaa ja
- saatavilla oloa.

5.2 Osoitusvelvollisuus

Rekisterinpitäjän on huolehdittava siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjää koskevan osoitusvelvollisuuden johdosta rekisterinpitäjän on pystyttävä myös osoittamaan, että periaatteita noudatetaan. Rekisterinpitäjän on siis arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa. Periaatteiden noudattamisen osoittaminen edellyttää rekisterinpitäjältä muun muassa henkilötietojen käsittelyn aiempaa tarkempaa suunnittelua ja dokumentointia.

Kuten sisäänrakennetun ja oletusarvoisen tietosuojanperiaatteiden myös osoitusvelvollisuuden ja rekisterinpitäjän vastuun toteuttamiseksi rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että asetusta noudatetaan. Tällä voidaan tietyissä tilanteissa tarkoittaa myös sitä, että rekisterinpitäjän on pantava täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.

Tietosuoja-asetuksen mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on ylläpidettävä selostetta sen vastuulla olevista käsittelytoimista, jotta voidaan osoittaa, että ne ovat asetuksen mukaisia. Selosteen on asetuksen mukaan oltava kirjallisessa muodossa ja se on pyydettäessä toimitettava viranomaiselle.

5.3 Tietosuojavastaavan nimittäminen

Tietosuoja-asetuksen mukaan tietosuojavastaava on nimitettävä organisaatioon, kun:

- on kyse julkisen sektorin toimijasta, joka ei ole tuomioistuin
- organisaation ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- organisaation ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Tietosuoja-asetus sisältää yksityiskohtaiset säännökset tietosuojavastaavan asemasta ja tehtävistä. Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni voi tietyin edellytyksin nimittää vain yhden tietosuojavastaavan. Finanssialalla on hyvin erikokoisia ja erilailla organisoituneita yrityksiä. Kukin arvioi tietosuojavastaavan nimittämistarpeen ja aseman organisaatiossa omista lähtökohdistaan.

Nimitettäessä tietosuojavastaavaa tulee ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä. Tietosuojavastaavan on oltava asetuksen tarkoittamalla tavalla riippumaton eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Hän ei saa esimerkiksi määritellä henkilötietojen käsittelyn tarkoituksia. Tietosuojavastaavan tehtävänä on muun muassa seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Tietosuojavastaavan tehtävänä on myös toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tästä johtuen organisaation on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle. Tietosuojavastaava ei kuitenkaan ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta, vaan vastuu kuuluu edelleen organisaation johdolle.

Tietosuojavastaava voidaan nimittää, vaikkei tietosuoja-asetus tähän nimenomaisesti velvoita. Niissä tilanteissa, joissa tietosuojavastaavan nimittäminen ei ole nimenomaisesti velvollisuus, tietosuojavaltuutetun toimiston ohjeistuksen mukaisesti on organisaatiossa kuitenkin syytä määritellä henkilö, jonka tehtävänä on tietosuojaa koskevien asioiden huomioiminen organisaation toiminnassa ja joka voi toimia yhteyshenkilönä rekisteröidyn oikeuksiin ja viranomaisvalvontaan liittyvissä kysymyksissä.

5.4 Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

Vaikutustenarviointi

Kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi.

Riskin tasoa arvioitaessa on otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Vaikutuksenarviointi on tehtävä erityisesti silloin, kun

- otetaan käyttöön uutta teknologiaa
- käsitellään laajamittaisesti rikostuomioita tai rikkomuksia
- käsitellään laajamittaisesti erityisiin henkilöryhmiin kuuluvia tietoja
- kyse on järjestelmällisestä ja kattavasta automatisoituun päätöksentekoon perustuvasta arvioinnista
- kyse on yleisölle avoimen alueen järjestelmällisestä ja laajamittaisesta valvonnasta
- Vaikutustenarviointi soveltuu laajoihin käsittelytoimiin, joissa on tarkoitus käsitellä huomattavia määriä henkilötietoja tai jotka voivat vaikuttaa suureen määrään rekisteröityjä.

Yhtä arviota voidaan käyttää samankaltaisiin vastaavia riskejä aiheuttaviin käsittelytoimiin.

Vaikutustenarvioinnin on sisällettävä vähintään

- järjestelmällinen kuvaus suunnitelluista käsittelytoimista
- tiedot käsittelyn tarkoituksista sekä tarvittaessa kuvaus rekisterinpitäjän oikeutetuista eduista
- arvio käsittelytoimien tarpeellisuudesta
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä

- tiedot suojatoimista ja mekanismeista, joiden avulla voidaan lievittää käsittelyyn kohdistuvaa riskiä ja varmistaa henkilötietojen suoja sekä asetuksen vaatimusten toteutuminen rekisterinpitäjän toiminnassa.

Rekisterinpitäjän on tarvittaessa varmistettava, että henkilötietojen käsittely tosiasiallisesti tapahtuu vaikutustenarvioinnin mukaisesti ja etenkin silloin, jos käsittelytoimien sisältämä riski muuttuu.

Vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta, jos sellainen on nimitetty.

Ennakkokuulemisvelvoite

Ennakkokuulemisvelvoite tarkoittaa riskiperusteista ilmoitusvelvollisuutta.

Jos vaikutustenarvioinnin perusteella riskin taso on korkea, eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi, on rekisterinpitäjän kuultava valvontaviranomista ennen käsittelyn aloittamista.

Rekisterinpitäjän on toimitettava valvontaviranomaiselle kuulemista varten tiedot

- tarvittaessa rekisterinpitäjän, yhteisrekisterinpitäjien ja käsittelyyn osallistuneiden henkilötietojen käsittelijöiden vastuualueet erityisesti konsernin sisällä suoritettavaa käsittelyä varten
- suunnitellun käsittelyn tarkoituksesta ja keinoista
- suojatoimista
- tietosuojaa koskeva vaikutustenarviointi
- tietosuojavastaavan yhteystiedot
- muut valvontaviranomaisen pyytämät tiedot

Valvontaviranomaisten on laadittava ja julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan vaikutustenarviointia. Valvontaviranomainen voi myös laatia luettelon käsittelytyypeistä, joiden osalta ei vaadita vaikutustenarviointia. Jos kyse on rajat ylittävästä henkilötietojen käsittelystä, vahvistetaan luettelo tietosuojaneuvostossa.

5.5 Tietoturva: käsittelyn turvallisuus, henkilötietojen suojaaminen ja hävittäminen

5.5.1 Tietojen suojaaminen on järjestettävä

Finanssiyrityksen on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta henkilötietojen käsittely on turvattua. Henkilötiedot tulee suojata siirron, tallennuksen ja käsittelyn aikana tapahtuvalta oikeudettomalta tai vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai tietoihin pääsyltä. Tietojen suojaamisesta on huolehdittava käsittelyn kaikissa vaiheissa alkaen tietojen keräämisestä ja päättyen niiden tuhoamiseen. Sekä manuaalisesti että automaattisesti käsiteltävät henkilötiedot on suojattava.

Käsittelyn turvallisuus voi edellyttää muun muassa

- henkilötietojen pseudonymisointia ja salausta
- kykyä taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- kykyä palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin vikatilanteissa
- menettelyä, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi

Luottotietolaki määrittelee erikseen hyvän luottotietotavan, jonka perusteella luottotietojen käyttäjän on noudatettava toiminnassaan huolellisuutta ja varmistuttava siitä, että luottotietojen laadusta, rekisteröityjen oikeuksien toteutumisesta, tietoturvallisuudesta ja luottotietojen käytön valvonnasta huolehditaan.

5.5.2 Suojaamistarpeen ja -tason arviointi

Valtaosa henkilöasiakkaita koskevista tiedoista on sellaisia, jotka on suojattava sivullisille paljastumiselta.

Tietojen paljastuminen sivullisille torjutaan yleensä huolehtimalla seuraavista suojauskäytännöistä:

- tietojen tehtäväkohtainen käyttövaltuusvalvonta
- henkilötietojen käyttöä koskeva ohjeistus
- toimitilojen kulunvalvonta
- tietojen asianmukainen hävittäminen
- tietojen suojaaminen niitä siirrettäessä

Asianmukainen suojan taso voidaan arvioida riskiperusteisesti ottaen huomioon tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Mitä suurempi riski rekisteröidylle voi aiheutua tietojen paljastumisesta sivulliselle, sitä parempi suojauksen taso tiedolla tulee olla.

Lähtökohdaksi voidaan ottaa se, että kaikki henkilötiedot suojataan saman tasoisella suojauskäytännöllä. Näin saatua suojauksen perustasoa voidaan parantaa tarpeen mukaan parempaa tietosuojaa vaativien tietoryhmien kohdalla. Näitä parannustoimenpiteitä voidaan suorittaa kaikilla suojaamistoiminnan alueilla. Hyvää suojaa vaativat tiedot voidaan käyttövaltuustoimintojen avulla asettaa vain harvojen henkilöiden saataville, niitä sisältävät asiakirjat voidaan määrätä säilytettäväksi vain hyvin suojatuissa tiloissa, asiakirjoille voidaan perustaa suojattu hävityskäytäntö ja tiedot voidaan salata niitä tietoliikenneverkossa siirrettäessä.

Parempaa suojaa vaativien tietojen yksityiskohtainen luettelointi ei ole mahdollista, mutta on syytä kiinnittää huomioita varsinkin erityisiin henkilötietoryhmiin. Lisäksi on

tarpeen harkita parannettua tietojen suojaa sellaisten tietojen osalta, joiden paljastuminen sivullisille voisi lisätä asianomaisen henkilön riskiä joutua rikoksen kohteeksi. Tällaisia tietoja voivat olla esimerkiksi tiedot huomattavan arvokkaasta koti-irtaimistosta, osoite, ammatti taikka tili- tai korttitiedot.

5.5.3 Suojaamisen keinoja

Vastuiden määrittely

Suojaamistehtävien menetyksellinen suorittaminen edellyttää, että nimetään suojattavista tiedoista vastuussa oleva organisaation osa ja kytketään se mukaan suojaamisen suunnitteluun ja käyttöönottoon. Ensisijainen vastuu suojaamisesta on useimmiten tarkoituksenmukaista sijoittaa siihen osaan organisaatiota, jonka käyttöä varten tiedot ensi sijassa on kerätty ja jolla on mahdollisuus määrätä niiden käytöstä. Jos tietojen yksikäsitteistä omistajaa ei kyetä määrittelemään, voidaan sopia siitä, kuka toimii tietojen haltijana muiden omistajien lukuun.

Asiakkaan luotettava tunnistaminen

Finanssiyrityksen ja asiakkaan välisessä yhteydenpidossa finanssiyritys usein antaa asiakkaalle häntä koskevia henkilötietoja. Finanssiyrityksen tulee varmistua riittävällä tavalla pyynnön esittäjän henkilöllisyydestä. Esimerkiksi verkon kautta asioidessa tämä voi tarkoittaa sitä että rekisteröidyllä tulee olla käytössä sähköiset tunnistusvälineet.

Varmuuskopiointi

Periaatteena on, että henkilötietoja sisältävät tiedot kopioidaan systemaattisesti tietovälineille, jotka säilytetään turvallisessa säilytyspaikassa. Voidaan myös toimia niin, että varmistettavat tiedot siirretään tietoliikenteen avulla muualla sijaitsevaan toiseen tietojärjestelmään. Varmuuskopioiden tulee sijaita eri palo-osastossa – mieluiten eri kiinteistössä – kuin missä käytössä olevat tiedostot sijaitsevat. Säilytyspaikka on suojattava erityyppisiltä fyysisiltä vahingoilta, kuten palo- ja nestevahingoilta, taltioita vahingoittavalta ilman lämpötilalta ja kosteudelta sekä tunkeutumiselta ja vahingonteolta.

Henkilötietojen käyttövaltuushallinta

Käyttövaltuushallinnan perustehtävä on pitää huolta siitä, että henkilötietoja voivat käsitellä vain ne, joilla on siihen oikeus. Tietojen käsittelyoikeus perustuu siihen, että henkilö tarvitsee tietoja suorittaakseen finanssiyrityksen antamia tehtäviä.

Käyttövaltuushallinnan järjestelmiä voidaan käyttää monin eri tavoin, mutta pääsäännöksi on aiheellista ottaa se, että tietojen käyttövaltuudet annetaan henkilölle, ei ryhmille tai muille yhteisöille. Käytännössä tämä merkitsee, että tietojärjestelmien käyttäjätunnukset ovat henkilökohtaiset riippumatta siitä, että oikeus tietojen käsittelyyn perustuu usein siihen, mihin ryhmään henkilö kuuluu. Vaatimus johtuu siitä, että finanssiyrityksen on tiedettävä, kuka käsittelee henkilötietoja, jotta se voisi varmistua siitä, että tietojen saajalla on oikeus niiden käyttöön. Myös mahdollisessa jälkikäteen suoritettavassa virhe- tai muussa selvitystyössä on usein tärkeä tietää, kuka on käsitellyt tietoja. Tämä tieto saadaan tietojärjestelmien lokitiedostoista, jos käyttäjätunnukset ovat henkilökohtaiset.

Tietojen käyttövaltuushallinnasta on pidettävä huolta myös manuaalisesti hoidettujen rekisterien ja arkistojen ollessa kyseessä.

Tietojen suojaaminen tiedonsiirrossa

Tiedonsiirrossa tietosuojaa uhkaava keskeinen riski on sanomien joutuminen väärille vastaanottajille. On myös pidettävä mielessä se, että siirrettävät viestit voivat paljastua sivullisille siirtoverkon palvelinlaitteista ja suoraan tiedonsiirtolinjoiltakin. On myös syytä tiedostaa finanssiyrityksen oman henkilöstön aiheuttamat riskit.

Peruskeinot tiedonsiirron suojaamisessa ovat

- suljettujen tiedonsiirtoverkkojen käyttäminen tai sellaisten muodostaminen julkiseen verkkoon,
- salaus- ja tunnistustekniikoiden käyttö ja
- siirrettävän aineiston suojaaminen ennen sen lähetystä verkkoon ja sen saavuttua verkosta.

Finanssiyrityksen on aiheellista ottaa käyttöön mahdollisuuksien mukaan sellaista tiedonsiirtotekniikkaa, joka yhtiön sisäisen tiedonsiirron lisäksi tarjoaa myös asiakkaille turvallisen yhteydenpidon yhtiöönsä. Turvallisessa yhteydenpidossa asiakkaalla on mahdollisuus salata julkisessa verkossa siirrettävät tiedot ja hän voi luottaa siihen, että asioi oikean yhtiön kanssa. Näitä mahdollisuuksia tarjoavat esimerkiksi internetissä laajasti käytetyt selainohjelmat.

Henkilötietojen poistaminen

Tarpeettomaksi käyneet henkilötietoja sisältävät aineistot on poistettava tietoturvallisesti. Jos henkilötietoja käsittelee finanssiyrityksen ulkopuolinen taho, finanssiyrityksen on huolehdittava, että henkilötietojen turvallisesta poistamisesta sovitaan finanssiyrityksen ja käsittelijän välisessä sopimuksessa.

Sisäinen ohjeistus

Finanssiyrityksen on toteutettava toimenpiteet sen varmistamiseksi, että sen henkilökunta käsittelee henkilötietoja ainoastaan finanssiyrityksen ohjeiden mukaisesti.

Erityisen tärkeää kattavan ja selkeän ohjeistuksen saatavilla olo on tilanteissa, joissa henkilötietojen käsittelyä ei ole mahdollista suojata käyttövaltuushallinnalla. 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.

6 Tiedonantovelvollisuus yleisölle ja rekisteröidylle

6.1 Tietojen toimittamista koskevat periaatteet

Finanssiyrityksen tulee toimittaa rekisteröidylle jäljempänä tässä kohdassa kuvatut tiedot.

Läpinäkyvyyden periaatteen mukaisesti annettavat tiedot tulee olla helposti ymmärrettävässä ja ne on ilmaistava selkeällä ja yksinkertaisella kielellä. Tarvittaessa tietoja on havainnollistettava.

Tiedot voidaan toimittaa rekisteröidylle asettamalla ne tämän saataville sähköisessä muodossa esim. internet-sivuston kautta. Tiedot voidaan antaa rekisteröidylle myös kirjallisesti tai muussa pysyvässä muodossa.

6.2 Tietojen käsittelyä ja käsittelyn tarkoitusta koskevat tiedot

Rekisteröidylle toimitettavien tietojen sisältö vaihtelee sen mukaan, mistä henkilötietoja kerätään – kerätäänkö niitä rekisteröidyltä itseltään vai kolmannelta taholta.

A. Kun henkilötietoja kerätään rekisteröidyltä itseltään

Finanssiyrityksen on toimitettava rekisteröidylle kaikki seuraavat tiedot:

1. finanssiyrityksen ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot;
2. tietosuojavastaavan yhteystiedot;
3. henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;
4. finanssiyrityksen tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu siihen, että käsittely on tarpeen oikeutettujen etujen toteuttamiseksi;
5. henkilötietojen vastaanottajat tai vastaanottajaryhmät;
6. tapauksen mukaan tieto siitä, että finanssiyritys aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja
   - tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai
   - tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville, silloin kun kyseessä on
     - siirto asiamukaisia suojatoimia soveltaen tai
     - yritystä koskevien sitovien sääntöjen perusteella tai
     - kyseessä on ei-toistuva siirto, joka koskee rajallista määrää rekisteröityjä ja on tarpeen finanssiyrityksen sellaisten pakottavien ja oikeutettujen etujen toteuttamiseksi, joita rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä.
7. henkilötietojen säilytysaika tai jos se ei ole mahdollista, tieto miten säilytysaika määritellään;

8. rekisteröidyn oikeus pyytää finanssiyritykseltä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;

9. oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu rekisteröidyn antamaan suostumukseen tai nimenomaiseen suostumukseen;

10. oikeus tehdä valitus valvontaviranomaiselle;

11. onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;

12. automaattisen päätöksenteon tai sellaisen profiloinnin olemassaolo, mikäli mainittu profilointi perustuu pelkästään automaattiseen käsittelyyn ja sillä on rekisteröityä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi tai erityisiin henkilötietoryhmiin kuuluvia tietoja käsitellään rekisteröidyn nimenomaiset suostumuksen perusteella. Rekisteröidylle on annettava merkitykselliset tiedot käsittelyyn liittyvästä logiikasta, käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Jos finanssiyritys aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, sen on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava kohtien 7-12 mukaiset tiedot.

B. Kun henkilötietoja ei ole saatu rekisteröidyltä itseltään

Kun tietoja ei ole saatu rekisteröidyltä itseltään, finanssiyrityksen on toimitettava rekisteröidylle edellisessä kohdassa mainittujen tietojen lisäksi seuraavat tiedot:

13. kyseessä olevat henkilötietoryhmät (kuten esimerkiksi suoramarkkinointia varten hankittu asiakasdata); ja

14. mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä.

Jos finanssiyritys aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, sen on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava kohtien 7-14 mukaiset tiedot.

Milloin kohtien A ja B mukaisesta tiedonantovelvollisuudesta voidaan poiketa?

Sellaisia tietoja ei tarvitse toimittaa, jotka rekisteröity on jo saanut. Silloin kun tietoja kerätään kolmannelta taholta, tietoja ei tarvitse toimittaa myöskään seuraavissa tilanteissa:

- tietojen hankinnasta tai luovuttamisesta säädetään nimenomaisesti finanssiyritykseen sovellettavassa lainsäädännössä, tai

- tiedot on pidettävä luottamuksellisina, koska niitä koskee unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuva vaitiolovelvollisuus, kuten lakisääteinen salassapitovelvollisuus.

6.3 Rekisteröidyn oikeuksien käyttämistä koskevat tiedot

Finanssiyritys toteuttaa asianmukaiset toimenpiteet toimittaakseen rekisteröidylle hänen oikeuksien käyttöä varten seuraavat tiedot:

- Rekisteröidyllä on oikeus saada finanssiyritykseltä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Jos näitä henkilötietoja käsitellään, rekisteröidyllä oikeus saada pääsy henkilötietoihin;

- Rekisteröidyllä on oikeus vaatia, että finanssiyritys oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot;

- Rekisteröidyllä on oikeus saada finanssiyritys poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä;

- Rekisteröidyllä on oikeus siihen, että finanssiyritys rajoittaa käsittelyä;

- Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella vastustaa häntä koskevien henkilötietojen käsittelyä;

- Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut finanssiyritykselle, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle; ja

- Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

6.4 Milloin tiedot täytyy toimittaa?

Kun tiedot kerätään rekisteröidyltä itseltään, tiedot on toimitettava niitä kerättäessä.

Kun tietoja ei saada rekisteröidyltä, kohtien A ja B tiedot toimitetaan rekisteröidylle:

- kohtuullisessa ajassa niiden keräämisestä, kuitenkin viimeistään kuukauden kuluessa tietojen saamisesta;

- käytettäessä henkilötietoja viestintään rekisteröidyn kanssa, tiedot on toimitettava viimeistään, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran; tai

- jos henkilötietoja on tarkoitus luovuttaa kolmannelle, viimeistään silloin kun tietoja luovutetaan ensimmäisen kerran.

7 Rekisterinpitäjän informointivelvollisuudet valvontaviranomaista kohtaan

7.1 Seloste käsittelytoimista

Rekisterinpitäjänä toimivan finanssiyrityksen on ylläpidettävä selostetta vastuullaan olevista henkilötietojen käsittelytoimista. Tämä seloste on pyydettäessä saatettava valvontaviranomaisen saataville.

Selosteen tulee sisältää kaikki seuraavat tiedot:

- rekisterinpitäjän sekä tietosuojavastaavan, mikäli sellainen on nimitetty, nimi ja yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ja käsiteltävien henkilötietojen ryhmistä
- ne henkilötietoja vastaanottavat ryhmät, joille tietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa olevat vastaanottajat
- tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan, kyseinen maa yksilöiden, sekä suojatoimia koskevat asiakirjat silloin kun on kysymys poikkeuksellisesta, kertaluonteisesta tiedonsiirrosta pakottavien ja oikeutettujen etujen perusteella
- yleinen kuvaus eri tietoryhmien poistamisen suunnitelluista määräajoista
- yleinen kuvaus henkilötietojen turvallisuutta varmistavista teknisistä ja organisatorisista turvatoimista

Käsittelijänä toimivan finanssiyrityksen on ylläpidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista. Selosteen tulee sisältää seuraavat tiedot:

- henkilötietojen käsittelijän ja kunkin rekisterinpitäjän, jonka lukuun käsittelijä toimii, sekä tietosuojavastaavan nimi ja yhteystiedot
- kunkin rekisterinpitäjän lukuun suoritettavien käsittelyiden ryhmät
- tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan, kyseinen maa yksilöiden, sekä suojatoimia koskevat asiakirjat silloin kun on kysymys poikkeuksellisesta, kertaluonteisesta tiedonsiirrosta pakottavien ja oikeutettujen etujen perusteella
- yleinen kuvaus henkilötietojen turvallisuutta varmistavista teknisistä ja organisatorisista turvatoimista

Finanssiyrityksen niin rekisterinpitäjänä kuin henkilötietojen käsittelijänäkin ylläpitämän selosteen tulee olla kirjallinen. Sähköinen muoto täyttää kirjallisuusvaatimuksen.

7.2 Valvontaviranomaisen ennakkokuuleminen

Rekisterinpitäjänä toimivan finanssiyrityksen on ennen käsittelyn aloittamista kuultava valvontaviranomaista, jos toteutettu tietosuojan vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi.

Rekisterinpitäjän kuullessa valvontaviranomaista sen on toimitettava viranomaiselle seuraavat tiedot:

- rekisterinpitäjän ja käsittelyyn osallistuvien henkilötietojen käsittelijöiden vastuualueet, erityisesti konsernin sisällä suoritettavan käsittelyn osalta
- suunnitellun käsittelyn tarkoitus ja keinot
- rekisteröityjen oikeuksien suojaamiseksi toteutetut toimenpiteet ja suojatoimet
- tarvittaessa tietosuojavastaavan yhteystiedot
- toteutettu tietosuojan vaikutustenarviointi
- muut valvontaviranomaisen pyytämät tiedot

Jos valvontaviranomainen katsoo, että suunnittelu käsittely rikkoisi tietosuoja-asetusta, viranomaisen on kahdeksan viikon kuluessa kuulemispyynnöstä annettava kirjalliset ohjeet rekisterinpitäjälle tai, tapauksen mukaan, käsittelijälle, ja valvontaviranomainen voi käyttää tietosuoja-asetuksen sille suomia valvontavaltuuksia. Valvontaviranomaisen käytettävissä olevaa määräaikaa voidaan jatkaa kuudella viikolla suunnitellun käsittelyn monimutkaisuus huomioon ottaen.

7.3 Tietosuojavastaavasta ilmoittaminen

Rekisterinpitäjänä tai henkilötietojen käsittelijänä toimivan finanssiyrityksen on ilmoitettava mahdollisesti nimittämänsä tietosuojavastaavan yhteystiedot valvontaviranomaiselle.

8 Tietoturvaloukkauksista ilmoittaminen

8.1 Tietoturvaloukkaukset

Tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin.

Finanssiyrityksen on rekisterinpitäjänä ilmoitettava tietoturvaloukkauksista tietosuojaviranomaiselle ja jossain tapauksissa myös rekisteröidylle. Finanssiyrityksen pitää suunnitella, miten mahdollinen tietoturvaloukkaus tunnistetaan, ilmoitetaan, selvitetään ja dokumentoidaan, jotta se pystyy toimimaan vahingon minimoimiseksi ja toimintakyvyn palauttamiseksi.

8.2 Ilmoitus viranomaiselle

Rekisterinpitäjänä toimivan finanssiyrityksen on ilmoitettava henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja, mahdollisuuksien mukaan, 72 tunnin kuluessa loukkauksen ilmitulosta toimivaltaiselle valvontaviranomaiselle. Ilmoitusta ei tarvitse tehdä, jos rekisterinpitäjä pystyy osoittamaan tilivelvollisuusperiaatteen mukaisesti että henkilötietojen tietoturvaloukkauksesta 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
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteydenottopiste lisätiedon saamiseksi
- kuvaus tietoturvaloukkauksen todennäköisistä seurauksista
- kuvaus toimenpiteistä, joita 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.

Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, niihin liittyvät seikat, niiden vaikutukset sekä toteutetut korjaavat toimenpiteet. Dokumentoinnin on oltava sellainen, että valvontaviranomainen voi sen avulla varmistaa että asetuksen vaatimuksia on noudatettu.

Henkilötietojen käsittelijänä toimivan finanssiyrityksen on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan loukkauksen tietoonsa.

8.3 Ilmoitus rekisteröidylle

Mikäli henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjänä toimivan finanssiyrityksen on ilmoitettava tietoturvaloukkauksesta valvontaviranomaisen lisäksi rekisteröidylle, jota loukkaus koskee, ilman aiheetonta viivytystä. 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, joita

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 muutettu muotoon, jossa ne eivät ole ulkopuolisen ymmärrettävissä, esim. salaamalla tiedot

- rekisterinpitäjä on toteuttanut toimenpiteet sen varmistamiseksi, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuvan korkean riskin toteutumistodennäköisyyttä on pienennetty

- 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.

8.4 Muut ilmoitukset tietoturvaloukkauksista

Tietoturvaloukkaus tai sen uhka voi aiheuttaa finanssiyritykselle muitakin ilmoitusvelvoitteita. Esimerkiksi luottolaitokset raportoivat tietoturvaloukkaukset myös Finanssivalvonnalle ja vahvan sähköisen tunnistuspalvelujen tarjoajat raportoivat tietoturvaan tai sähköisen henkilöllisyyden käyttöön kohdistuvista merkittävistä uhkista tai häiriöistä Viestintävirastolle.

9 Rekisteröidyn oikeudet

9.1 Oikeuksien toteuttamista koskevat periaatteet

Tietosuoja on ihmisten yksityiselämän suojaamista. Siihen kuuluu kunkin oikeus omiin henkilötietoihinsa.

Finanssiyrityksen yhtenä päävelvollisuutena on toteuttaa asiakkaan oikeuksia. Asiakkaan oikeuksien perusperiaatteena on henkilötietojen suojaaminen oikeudettomalta ja henkilöä vahingoittavalta tietojen käytöltä. Finanssiyritysten on varmistettava, että prosessit ja tietojärjestelmät taipuvat asiakkaan oikeuksien toteuttamiseen. Asiakkaan oikeudet on otettava huomioon henkilötietojen käsittelyyn liittyvien prosessien ja tietojärjestelmien suunnittelussa.

Tietosuojalainsäädännön pääperiaatteena on tiedonsaantioikeus. Tämä oikeus ei kuitenkaan saa vaikuttaa epäedullisesti muiden oikeuksiin tai vapauksiin, esimerkiksi luottolaitoksen/vakuutusyhtiön liikesalaisuuden piiriin kuuluvat asiat voivat aiheuttaa rajoituksia oikeuksiin, esimerkiksi oikeuteen saada pääsy tietoihin.

Henkilötietojen käsittelyn on perustuttava tietosuoja-asetukseen tai Euroopan unionin tai jäsenvaltion lainsäädäntöön. Käsittelyperuste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeus siirtää tiedot järjestelmästä toiseen ja oikeus

vastustaa tietojen käsittelyssä ovat mahdollisia vain, jos tietoja käsitellään tietyllä perusteella. Finanssiyritys voi käsitellä tietoja yhdellä tai useammalla perusteella. Finanssiyrityksen onkin oltava tietoinen, millä perusteella se käsittelee tietoja ja mitä oikeuksia käytössä oleviin käsittelyn perusteisiin liittyy.

Finanssiyrityksen on toimitettava käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Finanssiyrityksen on annettava tiedot omalla palvelukielellä. Tietojen selkeyteen, ymmärrettävyyteen ja yksinkertaiseen kieleen on kiinnitettävä erityistä huomiota, jos tiedot on tarkoitettu lapselle. Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa. Jos henkilö sitä pyytää, tiedot voidaan antaa suullisesti. Jos henkilö esittää pyynnön sähköisesti, tiedot on toimitettava sähköisesti mahdollisuuksien mukaan, paitsi jos rekisteröity toisin pyytää.

Finanssiyrityksen on helpotettava oikeuksien käyttämistä. Henkilökunta on koulutettava niin, että se pystyy auttamaan ja neuvomaan asiakasta oikeuksien toteuttamisessa. Asiakkaan on saatava tietoa oikeuksien toteuttamisesta helposti, niin sähköisesti kuin kirjallisesti. Finanssiyrityksen on toimittava oma-aloitteisesti helpottaakseen oikeuksien käyttämistä.

Ilmoitettava toimenpiteistä kuukaudessa

Finanssiyrityksen on ilmoitettava asiakkaalle toimenpiteistä, joihin se pyynnön johdosta on ryhtynyt. Toimenpiteistä on kerrottava ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella, jos pyyntöjen määrä ja monimutkaisuus sitä edellyttävä. Määräajan jatkamisesta ja viivästymisen syystä on ilmoitettava asiakkaalle kuukauden kuluessa pyynnön vastaanottamisesta.

Jos asiakas on pyytänyt tietojen oikaisua, poistamista tai käsittelyn rajoittamista, on finanssiyrityksen ilmoitettava toimenpiteistä myös niille tahoille, joille henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Finanssiyrityksen on ilmoitettava asiakkaalle näistä vastaanottajista, jos henkilö sitä pyytää.

Kieltäytyminen toimenpiteistä

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

Maksuttomuus

Oikeuksien käyttämisen ja toteuttamisen lähtökohtana on maksuttomuus. Jos henkilön pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti, voi tietojen toimittamisesta ja muista toimenpiteistä periä kohtuullisen maksun ottaen huomioon tietojen tai viestien toimittamisesta tai pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset tai kokonaan kieltäytyä suorittamasta pyydettyä toimea. Näissä tapauksissa finanssiyrityksen on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

Pyynnön esittäjän tunnistaminen

Pyynnön esittäjän henkilöllisyys on varmistettava. Näin vältytään tilanteilta, joissa muiden henkilöiden oikeuksia tai vapauksia loukattaisiin. Finanssiyrityksen tulee varmistua riittävällä tavalla pyynnön esittäjän henkilöllisyydestä, joten verkon kautta asioitaessa tämä voi tarkoittaa sitä, että rekisteröidyllä tulee olla käytössä sähköiset tunnistusvälineet.

Jos finanssiyrityksellä on perusteltua syytä epäillä pyynnön tehneen luonnollisen henkilön henkilöllisyyttä, finanssiyritys voi pyytää toimittamaan lisätiedot, jotka ovat tarpeen henkilöllisyyden vahvistamiseksi. Jos finanssiyritys ei pysty tunnistamaan henkilöä ja pystyy tämän osoittamaan, voi finanssiyritys kieltäytyä toimimasta henkilön oikeuksien käyttämiseksi

9.2 Oikeus saada pääsy tietoihin

Jokaisella henkilöllä on oikeus saada finanssiyritykseltä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Oikeuttaan käyttävän henkilön on annettava ja esitettävä finanssiyrityksellä tietojen etsimiseksi tarpeelliset seikat. Finanssiyrityksen tulee varmistua riittävällä tavalla pyynnön esittäjän henkilöllisyydestä. Esimerkiksi verkon kautta asioidessa tämä voi tarkoittaa sitä että pyynnön esittäjällä tulee olla käytössä sähköiset tunnistusvälineet.

Jos finanssiyritys käsittelee henkilötietoja, rekisteröidyllä on oikeus saada pääsy henkilötietoihin. Oikeus saada pääsy tietoihin tarkoittaa pääsääntöisesti sitä, että finanssiyritys toimittaa tiedot rekisteröidylle käytössään olevilla menetelmillä sähköisesti. Tiettyihin tietoihin pääsy voi tarkoittaa rekisteröidyn oikeutta päästä tietoon vain finanssiyrityksen toimipisteessä tai saada tiedot kirjepostitse.

Edellä mainitun oikeuteen perustuen finanssiyrityksen tulee antaa lisäksi seuraavat 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 tietosuojavirastolle;
- 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.

Jos rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti, finanssiyritys voi joko a) periä kohtuullisen maksun ottaen huomioon tietojen tai viestien toimittamisesta tai pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset; tai b) kieltäytyä suorittamasta pyydettyä toimea. Näissä tapauksissa finanssiyrityksen on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Rekisteröidyllä on oikeus tehdä valitus kieltäytymisestä tietosuojavirastolle, finanssiyrityksen on kieltäytyessään ilmoitettava tästä oikeudesta rekisteröidylle.

Finanssiyrityksen tulee vastata rekisteröidyn pyyntöön kuukaudessa. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Finanssiyrityksen on ilmoitettava rekisteröidylle tällaisesta mahdollisesta jatkamisesta kuukausi pyynnön vastaanottamisesta sekä viivästymisen syyt.

Tietosuojalainsäädännön pääperiaatteena on rekisteröidyn oikeus saada pääsy rekisteröityä itseään koskeviin tietoihin ja näiden tietojen tiedonsaantioikeus. Tämä oikeus ei saa vaikuttaa epäedullisesti muiden oikeuksiin ja vapauksiin. Esimerkiksi finanssiyrityksen liikesalaisuuden piiriin tai muiden rekisteröityjen salassapidettäviin tietoihin kuuluvat asiat voivat aiheuttaa rajoituksia rekisteröidyn oikeuteen saada pääsy tietoihin.

9.3 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). Velvollisuutta ja oikeutta arvioitaessa on otettava huomioon esimerkiksi erityislaissa säädetyt tietojen säilytysajat. Esimerkkejä tietojen säilytysajoista on koottu näiden käytännesääntöjen liitteeseen.

9.4 Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)

Finanssialan sääntelystä johtuen finanssiyritys on lähtökohtaisesti velvoitettu säilyttämään rekisteröidyn tietoja koko asiakassuhteen voimassaolonajan ja vielä asiakassuhteen päättymisen jälkeenkin. Oikeutta omien tietojen poistamiseen ei ole, jos käsittely on tarpeen finanssiyrityksiin sovellettavaan lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen velvoitteen 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 käsittelyä profilointi tarkoituksessa 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;
- alaikäisten henkilötiedot, mikäli näitä on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

Velvollisuus poistaa vanhentunut tieto saattaa joissakin tapauksissa johtaa siihen, ettei finanssiyrityksestä löydy enää tietoa tai asiakirjaa, jonka rekisteröity esim. pääsyoikeutensa nojalla haluaisi nähtäväkseen.

9.5 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on 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 olisi 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 (käyttöperuste hävinnyt ja finanssiyritys haluaa hävittää tiedot), mutta asiakas tarvitsee tietoja oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
- Jos asiakas on vastustanut henkilötietojen käsittelyä henkilökohtaiseen erityiseen tilanteeseen liittyvän perusteen nojalla ja odottaa sen todentamista, syrjäyttävätkö finanssiyrityksen oikeutetut perusteet asiakkaan perusteet.

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 finanssiyrityksen ilmoitettava jokaiselle luovutuksensaajalle kaikista rajoittamista koskevista toimenpiteistä paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa. Finanssiyrityksen on myös ilmoitettava rekisteröidylle luovutuksensaajista, jos rekisteröity sitä pyytää.

Käsittelyä koskevan rajoituksen poistamisesta on tehtävä asiakkaalle ilmoitus ennen kuin rajoitus poistetaan.

9.6 Oikeus vastustaa käsittelyä

Käsittelyperusteen merkitys

Rekisteröity voi tietyissä tilanteissa vastustaa tietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella. Rekisteröidyllä on oikeus vastustaa tietojensa käsittelyä vain, jos tietojen käsittely perustuu julkisen vallan käyttöön tai finanssiyrityksen tai kolmannen oikeutetun edun toteuttamiseen. Finanssiyrityksen oikeus käsitellä tietoja perustuu monesti muihin käsittelyperusteisiin. Tämä tarkoittaa, että rekisteröidyllä on vain poikkeuksellisesti oikeus vastustaa tietojensa käsittelyä eikä rekisteröidyn pyyntö käsittelyn vastustamisesta aiheuta toimenpiteitä finanssiyrityksessä.

Rekisteröidyllä voi olla oikeus vastustaa tietojensa käsittelyä esimerkiksi,

- kun käsittely perustuu julkisen vallan käyttöön eli lakisääteisessä tapaturmavakuuttamisessa tai lakisääteisen liikennevakuutuksen liikennevahingoissa vahingonkärsineen tietojen käsittelyn osalta.

- kun käsittely perustuu kolmannen edun toteuttamiseen eli vastuuvakuutuksessa vahingonkärsineen tietojen käsittelyssä.

Jos asiakkaalla on oikeus vastustaa tietojensa käsittelyä, ei tietoja saa enää käsitellä. Finanssiyritys saa kuitenkin käsitellä tietoja, jos se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää asiakkaan edut, oikeudet ja vapaudet tai jos käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

9.7 Oikeus siirtää tiedot järjestelmästä toiseen

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

Tämä siirto-oikeus koskee nimenomaisesti vain tietoja, joiden käsittelyperusteena on joko asiakkaan antama suostumus tietojen käsittelylle tai joiden käsittely on tarpeen finanssiyrityksen ja asiakkaan välisen sopimuksen täytäntöön panemiseksi. Näin ollen, mikäli käsittelyperusteena on esimerkiksi oikeutettu etu, velvoitetta tietojen siirtämiseen ei ole. Halutessaan finanssiyritykset voivat kuitenkin vapaaehtoisesti tarjota siirtomahdollisuuden asiakkaalle 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 asiakkaalle vahvistaa asiakkaan kontrollointimahdollisuuksia omiin tietoihinsa ja samalla asiakkaan asemaa suhteessa finanssiyritykseen.

Siirto-oikeus takaa asiakkaalle käytännössä kaksi oikeutta: (i) oikeuden saada tiedot itselleen sähköisessä muodossa ja (ii) oikeuden siirtää tiedot kolmannelle taholle. Varsinkin näistä ensimmäinen on hyvin läheisessä yhteydessä asiakkaan oikeuteen saada pääsy itseään koskeviin tietoihin. Merkittävimmät erot siirto-oikeuden ja pääsyoikeuden välillä on kuvattu alla olevassa taulukossa:

	Oikeus saada pääsy tietoihin	Siirto-oikeus
Mitä tietoja koskee	Kaikki finanssiyrityksellä olevat asiakasta koskevat henkilötiedot	Asiakkaan finanssiyritykselle toimittamat tiedot
Käsittelyperusteen vaikutus	Soveltuu kaikki tietoihin riippumatta käsittelyperusteesta	Soveltuu vain niihin tietoihin, joiden käsittelyperusteena joko suostumus tai sopimuksen täytäntöönpano
Miten tiedot voidaan toimittaa asiakkaalle	Voidaan toimittaa asiakkaalle myös muutoin kuin sähköisessä muodossa tai tietyissä tilanteissa asiakkaalle voidaan järjestää pääsy tietoihin esimerkiksi finanssiyrityksen toimipisteessä	Toimitettava sähköisessä ja koneellisesti luettavassa muodossa

Finanssiyrityksen tulee tiedottaa asiakkaita siirto-oikeuden olemassaolosta osana yleistä tiedonantovelvollisuuttaan.

Siirto-oikeuden kohteena olevat tiedot

Siirto-oikeuden kohteena ovat tiedot, jotka (i) koskevat asiakasta itseään ja (ii) jotka asiakas on toimittanut finanssiyritykselle.

i. Tietojen tulee koskea asiakasta, joten siirto-oikeus ei koske enää tietoja, jotka ovat anonymisoitu. Lisäksi siirto-oikeus koskee lähtökohtaisesti vain asiakasta itseään koskevia tietoja. Mikäli asiakasta koskevat tiedot kuitenkin läheisesti linkittyvät tiettyihin kolmansia henkilöitä koskeviin tietoihin, voi tietojen siirto edellyttää käytännössä myös näiden kolmansien henkilöiden tietojen siirtämistä. Tällöin tulee kuitenkin huolehtia siitä, ettei siirto vaikuta haitallisesti kolmansien henkilöiden oikeuksiin ja että siirto ei estä heitä käyttämästä oikeuksiaan, kuten oikeutta saada pääsy henkilötietoihinsa. Yhtenä esimerkkinä, jossa kolmansien tietojen siirtäminen voi olla tarpeen, on tilanne, kun asiakas vaihtaa pankkipalvelujen tarjoajaansa ja pyytää siirtämään tiedot tilitapahtumistaan palveluntarjoaja pankilta toiselle. Tässä yhteydessä tietoja voi olla vaikea siirtää ilman, että samalla siirtyy tietoja myös sellaisista kolmansista henkilöistä, joille asiakas on joko tehnyt maksusuorituksia tai joilta asiakas on vastaanottanut masusuorituksia. Mikäli vastaanottava pankki käyttää vastaanottamiaan tilitietoja samoihin tarkoituksiin kuin tiedot siirtänyt pankki, ei ole todennäköistä, että siirto asettaisi kolmannet henkilöt aikaisempaa epäedullisempaan asemaan ja vaikuttaisi haitallisesti heidän oikeuksiinsa ja vapauksiinsa.

ii. Asiakkaan toimittamiksi tiedoiksi katsotaan sekä tiedot, jotka asiakas on aktiivisesti ja tietoisesti toimittanut finanssiyritykselle (esimerkiksi asiakkaan luotto- tai vakuutushakemuksessa antamat tiedot) sekä tiedot, jotka finanssiyritys on havainnoinut tai kerännyt asiakkaasta asiakkaan käyttäessä finanssiyrityksen tarjoamia palveluja (esimerkiksi erilaisten mittarien avulla asiakkaasta kerätyt tiedot kuten ajotietokoneen avulla kerätyt tiedot asiakkaan liikkumisesta). Siirto-oikeus ei sovellu kuitenkaan enää sellaisiin tietoihin, jotka finanssiyritys on itse luonut tai johtanut sellaisen tiedon pohjalta, jonka asiakas on toimittanut. Tällaisia siirtovelvoitteen ulkopuolelle jääviä johdettuja tietoja ovat esimerkiksi finanssiyrityksen asiakkaan toimittamien tietojen pohjalta tekemä luottoluokitus tai arvio asiakkaan terveydentilasta.

Siirto-oikeus koskee vain automaattisen käsittelyn kohteena olevia tietoja. Näin ollen siirto-oikeus ei sisällä velvoitetta siirtää esimerkiksi paperisessa muodossa arkistoituja tietoja, mikrofilmauksen avulla tallennettuja tietoja tai sellaisessa sähköisessä muodossa tallennettuja tietoja (esim. pdf tai word), joita ei pystytä hakemaan ja tunnistamaan tietojärjestelmän avulla.

Siirto-oikeuden suhde muuhun henkilötietojen käsittelyyn

Asiakas voi käyttää siirto-oikeutta milloin vain asiakassuhteen aikana ilman että siirto-oikeuden käyttäminen itsessään aiheuttaa mitään muutosta asiakassuhteeseen tai asiakkaan mahdollisuuksiin hyödyntää muita henkilötietoihin liittyviä oikeuksiaan, kuten oikeutta saada pääsy tietoihin. Vastaavasti se, että asiakkaalle on oikeus saada tietonsa siirrettyä, ei itsessään luo myöskään finanssiyritykselle velvoitetta poistaa niitä tietoja, jotka asiakas on pyytänyt siirrettäväksi toiselle palveluntarjoajalle. Mikäli finanssiyrityksellä senkin jälkeen, kun asiakas on siirtänyt tietonsa uudelle palveluntarjoajalle, on esimerkiksi edelleen asiakassuhde asiakkaaseen tai lakiin perustuva velvoite arkistoida tiedot taikka vireillä oleva valitusprosessi, jonka yhteydessä tietoja tullaan tarvitsemaan, finanssiyrityksellä on oikeus säilyttää tiedot.

Toisaalta siirto-oikeuden olemassaolo sinänsä ei luo finanssiyritykselle myöskään velvollisuutta taikka oikeutta säilyttää tietoja kauemmin kuin mitä finanssiyritys muutoin on velvollinen niitä säilyttämään. Käsittelyperusteen päättyessä finanssiyritys on velvollinen poistamaan tiedot riippumatta siitä, onko asiakas käyttänyt siirto-oikeutta. Lisäksi viranomainen on suosittanut, että asiakassuhteen päättymisen yhteydessä finanssiyritys tarjoaisi asiakkaalle mahdollisuuden siirtää tarvittavat tietonsa joko itselleen tai uudelle palveluntarjoajalle ennen tietojen lopullista poistamista järjestelmistään. Tämän voidaan kuitenkin katsoa edellyttävän, että siirtomahdollisuuden oma-aloitteinen tarjoaminen on olosuhteet huomioon ottaen kussakin tilanteessa tarkoituksenmukaista ja kohtuullisin keinoin järjestettävissä. Mikäli tiedot kuitenkin poistetaan lakisääteisten arkistointivelvoitteiden johdosta vasta useamman vuoden kuluttua asiakassuhteen päättymisestä, ei tietojen poistoajankohtana tietojen käsittelyperusteena ole enää suostumus taikka sopimuksen täytäntöönpano, vaan lakisääteisen velvoitteen toteuttaminen, jolloin siirtomahdollisuuden tarjoamista ei enää edellytetä.

Siirto-oikeuden käyttäminen

Finanssiyritys voi tarvittaessa pyytää asiakasta täsmentämään asiakkaan finanssiyritykselle osoittamaa tietojen siirtopyyntöä, mikäli pyynnöstä ei yksiselitteisesti ilmene, mitä tietoja siirtopyyntö koskee. Finanssiyritys voi esimerkiksi pyytää asiakasta yksilöimään tietoluokat, jotka ovat pyynnön kohteena, tai tietojärjestelmän, josta löytyvät tiedot asiakas pyytää saada siirrettyä.

Finanssiyrityksen vastaanotettua asiakkaan pyynnön tietojensa siirtämistä, finanssiyrityksen on varmistettava riittävällä tavalla pyynnön esittäjän henkilöllisyys ennen siirron toteuttamista. Finanssiyrityksen on toteutettava siirto ilman aiheetonta viivytystä ja lähtökohtaisesti yhden kuukauden kuluessa pyynnön vastaanottamisesta. Vaikeammin toteutettavien siirtopyyntöjen kohdalla tiedot voidaan kuitenkin toimittaa kolmen kuukauden kuluessa pyynnön vastaanottamisesta edellyttäen, että asiakasta on tiedotettu viiveestä ja siihen johtaneista syistä kuukauden sisällä pyynnön vastaanottamisesta. Finanssiyrityksellä on kuukausi aikaa tiedottaa asiakasta myös silloin, jos finanssiyritys kieltäytyy toteuttamasta pyydettyä siirtoa. Tällöin sen on samalla ilmoitettava asiakkaalle perusteet kieltäytymiselle ja asiakkaan käytettävissä oleva valitusmahdollisuus.

Asiakkaan käyttäessä siirto-oikeuttaan tiedot luovuttavan finanssiyrityksen vastuu tietojen käsittelystä päättyy, kun se on asiakkaan pyynnön mukaisesti siirtänyt tiedot joko asiakkaalle itselleen tai toiselle palveluntarjoajalle. Jos finanssiyritys puolestaan on tiedot vastaanottavana tahona, tulee sen varmistua siitä, että finanssiyrityksen siirto-oikeuden nojalla saamat tiedot ovat olennaisia ja tarpeellisia sen käyttötarkoituksen kannalta, johon finanssiyritys tietoja käsittelee. Näin ollen mikäli finanssiyritys saa asiakkaan vanhalta palveluntarjoajalta tietoja, joita finanssiyritys ei tarvitse oman palvelunsa tarjoamiseksi asiakkaalle eikä finanssiyrityksellä ole muutakaan perustetta käsitellä näitä tietoja, tulee finanssiyrityksen poistaa tiedot.

Finanssiyrityksen tulee toimittaa tiedot asiakkaalle tai asiakkaan osoittamalle kolmannelle taholle jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Toimitusmuodon tulisi sallia mahdollisuuksien mukaan tietojen siirron järjestelmästä toiseen. Siirto-oikeus ei kuitenkaan luo finanssiyritykselle velvoitetta ylläpitää sellaisia tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia

toisten palveluntarjoajien kanssa eikä velvoitetta hankkia lisälaitteita pelkästään siirto-oikeuden toteutumisen turvaamiseksi. Tietojen siirto voitaisiin siis toteuttaa finanssiyrityksellä jo käytettävissä olevien teknisten laitteiden mahdollistamalla tavalla. Käytännössä tietojen siirto voitaisiin toteuttaa esimerkiksi API-rajapintoja hyödyntäen, tarjoamalla asiakkaalle mahdollisuus ladata tiedot internet-yhteyden välityksellä valitsemalleen tallennusalustalle tai toimittamalla tiedot asiakkaalle muistitikulla tai muulla ulkoisella tallennusvälineellä.

Tietojen toimitusmuodon tulisi olla myös sellainen, että se mahdollisuuksien mukaan tukisi tietojen uudelleen käyttöä ja mahdollistaisi yksittäisten tietojen tunnistamisen ja poimimisen aineistosta. Myös tietoihin liittyvät metadatat tulisi pyrkiä säilyttämään osana siirrettäviä tietoja, mikäli tämä on finanssiyritykselle tarkoituksenmukaisella tavalla järjestettävissä olemassa olevien tietojärjestelmien ja laitteiden avulla.

10 Henkilötietojen luovuttaminen ja siirto

Finanssiyritys voi siirtää asiakkaitaan koskevia henkilötietoja esimerkiksi tietotekniikka-palveluja tarjoavaan yritykseen 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 yleisen tietosuoja-asetuksen tarkoittamaa henkilötietojen luovutusta, koska luovutukselle on olennaista se, että vastaanottajalla on oikeus määrittää tietojen käyttötarkoitus ja käsitellä saamiaan tietoja omassa toiminnassaan. Toisin ilmaistuna luovutuksessa rekisterinpitäjä vaihtuu. Luovutuksen ja siirron suhdetta voi lyhyesti kuvailla niin, että tietoja voidaan siirtää vastaanottajalle niitä luovuttamatta ja toisaalta luovuttaminen ei välttämättä edellytä tietojen siirtoa.

Henkilötietoja käsiteltäessä on oltava selkeä käsitys tietojen luovutuksen ja siirron suhteista, koska ne ovat lainsäädännön soveltamisen kannalta eri asioita. Tällainen erityinen henkilötietojen siirtotilanne voi finanssiyrityksissä syntyä esimerkiksi silloin, kun finanssiyritys päättää velkojana myydä saatavia. Tällaista tilannetta ei ole pidetty puhtaana henkilötietojen luovutuksena, sillä luovutuksen jälkeen myyjällä on edelleen oikeus käsitellä saatavaa koskevia tietoja myyntiä edeltävältä ajalta.

10.1 Henkilötietojen luovuttaminen

Tietosuoja-asetuksen mukaan luovutus on yksi henkilötietojen käsittelyn muoto, joten luovutusta sääntelee mm. asetuksen käsittelyn lainmukaisuutta koskeva 6 artikla ja erityisiä henkilötietoryhmiä koskevien (arkaluonteisten) tietojen osalta asetuksen 9 ja 10 artiklat. Luottolaitos- ja vakuutustoimintaa harjoittavat finanssiyritykset ovat toimialakohtaisen sääntelyn nojalla salassapitovelvollisia ja voivat luovuttaa 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 vastaanottajaakoskevat muut säännökset. Tärkeimmät näistä ovat:

- Tietojen vastaanottajalla on oltava oikeus saamiensa henkilötietojen käsittelyyn asetuksen 6, 9 tai 10 artiklan perusteella;

- Tietojen vastaanottajan on noudatettava henkilötietojen käsittelyä koskevia periaatteita (5 artikla):

- Tietojen luovuttajan on informoitava rekisteröityä tietojen luovutuksesta, paitsi jos tietosuoja-asetuksen 14 artiklan 5 kohdan mukaan tiedonantovelvollisuudesta voidaan poiketa.

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 kuuluvalle yhteisölle asiakaspalvelua, ja muuta asiakassuhteen hoitamista, markkinointia sekä 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 viitatut poikkeukset eivät kuitenkaan mahdollista arkaluontoisten henkilötietojen tai maksutapahtumatietojen luovuttamista.

10.2 Henkilötietojen siirto Euroopan talousalueen ulkopuolelle

Yleisessä tietosuoja-asetuksessa on erityisesti säännelty henkilötietojen siirto 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 laske siirrettäessä tietoja rajojen yli.

Siirroksi on tässä yhteydessä lähtökohtaisesti katsottava kaikki sellainen toiminta, jonka yhteydessä henkilötietoja siirtyy rajojen yli kolmansiin maihin. Kyseessä voi olla esimerkiksi henkilötietoja sisältävän kortiston tai tietokoneen kuljetus rajan yli, tiedoston siirto tai rajan yli tapahtuva henkilötietojen päätekäsittely. On huomattava, että julkisessa tietoliikenneverkossa, kuten esimerkiksi internetissä, viestinnän osapuolilla ei ole varmaa tietoa toistensa maantieteellisestä sijainnista eikä siitä, mitä kautta sanomien kuljetus reititetään.

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 riittävyyttä koskevan päätöksen. Vaihtoehtoisesti siirto on mahdollista toteuttaa asetuksessa määritettyjä asianmukaisia suojatoimia soveltaen tai jos sellaisia ei ole, jollakin asetuksessa säädetyllä erityistilanteita koskevalla poikkeusperusteella. Viitatut vaatimukset, siirron oikeusperusteet, koskevat myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle.

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

10.2.1 Siirto tietosuojan riittävyyttä 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. Tällaiselle siirrolle rekisterinpitäjä ei tarvita erityistä lupaa.

Komissio voi suojan riittävyyttä arvioituaan päättää, että kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö tarjoaa tietosuoja-asetuksessa määritetyn riittävän tietosuojan tason (45 artikla, 2 kohta). Komission täytäntöönpanosäädöksessä on säädettävä vähintään joka neljäs vuosi tehtävästä määräaikaistarkastelusta, jossa on otettava huomioon kaikki asiaan liittyvä kehitys kyseisessä kolmannessa maassa tai kansainvälisessä järjestössä. Komissio seuraa myös jatkuvasti kolmansissa maissa ja kansainvälisissä järjestöissä tapahtuvaa kehitystä ja tarvittaessa kumoaa tietosuojan riittävyyttä koskevan päätöksensä.

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.

10.2.2 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 käytännesäännöt (40 artikla) yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, tai
- 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.

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.

10.2.3 Erityistilanteita koskevat poikkeukset

Mikäli komissio ei ole tehnyt edellä kuvattua tietosuojan tason riittävyyttä koskevaa päätöstä eikä edellä kuvattuja asianmukaisia suojatoimia ole toteutettu, henkilötietojen siirto kolmanteen maahan tai kansainväliselle järjestölle voidaan suorittaa tietosuoja-asetuksen 49 artiklassa kuvatulla poikkeuksella. Finanssiyrityksen toiminnan kannalta kyseeseen yleisimmin 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 täytäntöön panemiseksi 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 täytäntöön panemiseksi, kuten vakuutuksen hankinta ETA:n ulkopuoliselta palveluntarjoajalta rekisteröidyn eduksi;

- siirto on tarpeen tärkeää yleistä etua koskevien syiden vuoksi, kuten rahanpesun estämiseksi; ja

- siirto on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi

Mikäli siirto ei voi perustua komission päätökseen, yritystä koskeviin sitoviin sääntöihin eikä mikään edellä kuvatuista erityistilanteita 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. Edellytyksenä on myös, että rekisterinpitäjä on arvioinut kaikkia tiedonsiirtoon liittyviä seikkoja ja toteuttanut tämän arvioinnin perusteella henkilötietojen suojaa koskevat asianmukaiset suojatoimet.

Rekisterinpitäjän tai henkilötietojen käsittelijän on dokumentoitava edellisessä kappaleessa viitattu arviointi ja asianmukaiset suojatoimet käsittelytoimia koskevaan

selosteeseensa. Rekisterinpitäjän on myös ilmoitettava mainitusta siirrosta valvontaviranomaiselle ja annettava rekisteröidylle tiedot siirrosta sekä viitatuista pakottavista ja oikeutetuista eduista.

10.3 Luovutus viranomaisille

Finanssiyrityksellä ja sen kanssa samaan konserniin tai konsolidointiryhmään kuuluvalla yrityksellä on velvollisuus antaa muutoin salassa pidettäväksi säädettyjä tietoja syyttäjä- ja esitutkintaviranomaiselle rikoksen selvittämiseksi sekä muulle viranomaiselle, jolla on lain mukaan oikeus saada sellaisia tietoja (esim. vero- ja sosiaaliviranomaiset).

Rahanpesun estämisestä ja selvittämisestä annetun lain perusteella rahanpesun selvittelykeskuksella on oikeus saada finanssiyritykseltä rahanpesun selvittämisessä tarvittavia tietoja salassapitovelvollisuuden estämättä.

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.

10.4 Esimerkkejä

Palveluyrityksen käyttö (siirto)

Finanssiyritys siirtää asiakkaidensa nimi- ja osoitetietoja sisältävän tiedoston tietoliikenneverkon välityksellä tietotekniikka-palveluyritykseen. Tarkoitus on, että palveluyritys tulostaa nimi- ja osoitetiedot kirjekuorille finanssiyrityksen markkinointiaineiston postitusta varten. Kyseessä on tiedon siirto, mutta ei luovutus. Palveluyritys voi käsitellä saamiaan tietoja siinä määrin kuin palvelun toimittaminen vaatii, mutta ei saa käyttää tietoja omassa toiminnassaan, esimerkiksi sijoittamalla omaa toimintaansa koskevaa mainosaineistoa kirjekuoriin.

Henkilötietojen käsittely kolmannessa maassa

Finanssiyrityksen tavanmukaisessa toiminnassa sen asiakkaita koskevia henkilötietoja saattaa siirtyä Euroopan talousalueen rajojen yli lähinnä silloin kun

- finanssiyrityksen palveluksessa oleva työskentelee ETA:n ulkopuolella ja käsittelee työssään yhtiönsä asiakkaita koskevia henkilötietoja,
- finanssiyrityksen asiakaspalvelupiste sijaitsee ETA:n ulkopuolella ja siinä annetaan asiakkaille henkilötietojen käsittelyä edellyttäviä palveluja tai
- finanssiyrityksen toimeksiannosta ETA:n ulkopuolella oleva yritys käsittelee luottolaitoksen asiakkaan henkilötietoja (poikkeusperusteet ks. edellä).

Näissä tilanteissa finanssiyrityksen tulee varmistaa siirtoa koskevien tietosuoja-asetuksen mukaisten edellytysten täyttyminen. Yleensä se on asiakkaan ja finanssiyritysten välisen sopimuksen tai toimeksiannon täytäntöönpano.

11 Tietojen säilyttäminen, virheen oikaisu ja poistaminen

11.1 Tietojen säilyttäminen

Finanssialan sääntelystä johtuen finanssiyritys on lähtökohtaisesti velvoitettu säilyttämään rekisteröidyn tietoja koko asiakassuhteen voimassaoloajan ja vielä sen päättymisen jälkeenkin. Asiaa on käsitelty tarkemmin kohdissa 9.2 ja 9.3 sekä esimerkkejä tietojen säilytysajoista sisältävässä liitteessä.

11.2 Tietojen oikaiseminen ja poistaminen

Tietosuoja-asetus takaa rekisteröidylle tietyin poikkeuksin oikeuden tietojen oikaisemiseen sekä oikeuden tietojen poistamiseen eli niin kutsutun oikeuden tulla unohdetuksi. Asiaa on käsitelty tarkemmin kohdissa 9.2 ja 9.3.

11.3 Erityisiä henkilötietoryhmiä koskevien tietojen poistaminen rekisteristä

Erityisiä henkilötietoryhmiä koskevat tiedot on poistettava rekisteristä ilman aiheetonta viivytystä sen jälkeen kun käsittelylle ei enää ole laillista perustetta. Talletettuja asiakirjoja on yleensä mahdotonta käydä läpi systemaattisesti. Suositeltava käytäntö on, että esim. manuaalisessa käsittelyssä korvauskäsittelyn yhteydessä säilytettäviin asiakirjakansioihin merkitään hävitysvuosi silloin, kun sen arvioiminen on mahdollista. Kriittisten automatisoitujen tuotantojärjestelmien osalta suositeltava käytäntö on esimerkiksi se, että henkilötietoja poistetaan säännöllisin määräajoin tiettyjen sääntöjen perusteella eräajoina.

Vakuutusyhtiöissä käsiteltäviä arkaluonteisiakin tietoja on säilytettävä vähintään niin kauan kuin yhtiöllä on vastuu mahdollisista vakuutustapahtumista. Tämän vuoksi esimerkiksi vakuutus- ja korvaushakemuksissa olevien terveydentilatietojen poistaminen rekistereistä ei ole mahdollista edes vakuutuksen voimassaolon päättymisen jälkeen. Esimerkiksi lapselle liikennevahingon seurauksena syntyneen vamman hoito voi jatkua vuosia tai jopa vuosikymmeniä liikenneonnettomuuden sattumisen ja liikennevakuutuksen päättymisen jälkeen. Kuitenkin vain niitä tietoja, jotka ovat kyseessä olevan vakuutustapahtuman käsittelyn kannalta relevantteja, voidaan säilyttää.

12 Tietosuojaviranomaiset

12.1 Riippumattomat valvontaviranomaiset

Jokaisessa jäsenvaltiossa on valvontaviranomainen, jolle on myönnetty valtuudet hoitaa tehtävänsä ja käyttää toimivaltansa täysin riippumattomasti. Suomessa tietosuojavirasto toimii valvontaviranomaisena ja edustaa Suomea Euroopan tietosuojaneuvostossa, jonka tehtävänä on varmistaa, että tietosuoja-asetusta sovelletaan yhdenmukaisesti jäsenvaltioissa. Tietosuojavirastossa toimii tietosuojavaltuutettu ja apulaistietosuojavaltuutettu(ja), joiden tehtävien jaosta määritetään tietosuojaviraston työjärjestyksessä. Tietosuojavirastossa toimii myös seuraamuslautakunta, johon kuuluu puheenjohtajan ja varapuheenjohtajan lisäksi kolme muuta jäsentä.

12.2 Valvontaviranomaisen toimivalta

Jokaisella valvontaviranomaisella on sille tietosuoja-asetuksen mukaisesti annettujen tehtävien hoitoa ja valtuuksien käyttöä koskeva toimivalta oman jäsenvaltionsa alueella. Mikäli organisaatio toimii useassa EU:n jäsenvaltiossa, rekisterinpitäjän on selvitettävä minkä jäsenvaltion valvontaviranomaisen kanssa se asetuksen mukaan asioi, eikä rekisterinpitäjä tarvitse asioida kuin yhden valvontaviranomaisen kanssa. Tarvetta asioida usean jäsenvaltion valvontaviranomaisen kanssa ei ole.

Valvontaviranomainen määräytyy rekisterinpitäjän tai henkilötietojen käsittelijän ainoan toimipaikan tai päätoimipaikan mukaan, ja toimii ainoana yhteyspisteenä kaikissa henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tätä kutsutaan yhden luukun periaatteeksi – *one stop shop* -mekanismiksi.

Unioniin sijoittautuneen rekisterinpitäjän päätoimipaikan on sen keskushallinnon sijaintipaikka unionissa, paitsi jos päätökset henkilötietojen käsittelyn tarkoituksista ja keinoista tehdään jossakin toisessa unioniin sijoittautuneen rekisterinpitäjän toimipaikassa. Tässä tapauksessa tämä toinen toimipaikka olisi katsottava päätoimipaikaksi. Rekisterinpitäjän tai henkilötietojen käsittelijän päätoimipaikan tai ainoan toimipaikan valvontaviranomaisella on toimivalta toimia johtavana valvontaviranomaisena kyseisen rekisterinpitäjän tai henkilötietojen käsittelijän toteuttaman rajat ylittävän käsittelyn osalta.

12.3 Tietosuojaviraston tehtävä ja sisäinen työnjako

Tietosuojaviraston tehtävä on alueellaan seurata tietosuoja-asetuksen säännösten soveltamista ja edistettävä sen yhdenmukaista soveltamista koko unionissa luonnollisten henkilöiden suojaamiseksi henkilötietojen käsittelyssä ja henkilötietojen vapaan liikkuvuuden varmistamiseksi sisämarkkinoilla. Näihin tehtäviin sisältyy tehtäviä, kuten asetuksen soveltamisen valvontaa, ohjausta, neuvontaa, luettelon laadintaa siitä, milloin vaaditaan tietosuojan vaikutustenarviointi, sekä sen ylläpitoa. Tarkemmin tehtävistä on säädetty tietosuoja-asetuksen 57 artiklassa sekä tietosuojalain 13 §:ssä.

Seuraamuslautakunnan toimivaltaan kuuluu tehdä tietosuojavaltuutetun tai apulaistietosuojavaltuutetun esityksestä päätöksiä merkittävimmissä yleisen tietosuoja-asetuksen mukaisissa seuraamusasioissa. Seuraamuslautakunta kokoontuu tarvittaessa tietosuojavaltuutetun koollekutsumana.

12.4 Valvontaviranomaisen valtuudet

Valvontaviranomaisen valtuuksista on säädetty tietosuoja-asetuksen 58 artiklassa sekä tietosuojalain 13 § 4 momentissa sekä 14 §:ssä. Jokaisella valvontaviranomaisella on tutkintavaltuuksia, korjaavia toimivaltuuksia, hyväksymis- ja neuvontavaltuuksia, valtuudet määrätä seuraamuksia sekä oikeus tarvittaessa ilmoittaa asia syytteeseenpanoa varten.

Tietosuojavaltuutettu voi asettaa henkilötietojen käsittelylle väliaikaisen rajoituksen tai kiellon. Tietosuojavaltuutetun on saatettava väliaikaista rajoitusta tai kieltoa koskeva asia ilman aiheetonta viivästystä seuraamuslautakunnan ratkaistavaksi.

Tietosuojavirastolla on tietosuojalain 17 §:ssä säädetty tiedonsaanti- ja tarkastusoikeus ja valtuus määrätä rekisterinpitäjää ja henkilötietojen käsittelijää sekä tarvittaessa näiden edustajaa antamaan kaikki tehtäviensä suorittamiseksi tarvittavat tiedot. Tietosuojavirastolla myös valtuus saada rekisterinpitäjältä ja henkilötietojen käsittelijältä pääsy kaikkiin henkilötietoihin, jotka ovat tarpeen sen tehtävien suorittamista varten sekä valtuus toteuttaa tutkimuksia tietosuojaa koskevien tarkastusten muodossa.

Seuraamuslautakunnalla on toimivalta määrätä hallinnollinen sakko tietosuojavaltuutetun esittelystä. Määräämisestä on tarkemmin säädetty tietosuojalain 15 §:ssä.

12.5 Muutoksenhaku

Tietosuoja-asetuksen VIII luvussa ja tietosuojalain 22 §:ssä on säännökset muutoksenhausta, sekä 23 § rekisteröidyn oikeusturvakeinoista tilanteissa, joissa hänen tietosuojavirastossa vireille saattamansa asian käsittely on viivästynyt, ns. passiivisuuskanne.