Tietosuojavaltuutetun toimisto

Dnro 1164/401/08

16.1.2009

Finanssialan Keskusliitto
Rauno Lindahl
Eteläranta 10

00130 HELSINKI

sähköpostinne 1.6.2008
ja neuvottelu 8.1.2009

KÄYTÄNNESÄÄNTÖJEN TARKASTAMINEN

Olette lähettänyt *luottolaitosten henkilötietojen käsittelyä koskevat käytännesäännöt* (26.5.2008) tarkastettavaksi henkilötietolain 42 §:n perusteella.

Käytännesäännöt on tarkastettu seuraavilla huomiolla (H), täsmennyksillä (T), eriävillä käsityksillä (EK) ja kehityskohteilla (KK) sekä välittömillä toimilla (VT). Pahoittelemme tämän palautteen viipymistä varsinkin, kun käytännesääntöjen luonteeseen kuuluu niiden edelleen kehittäminen. Välittömiä toimia edellyttäväksi kysymykseksi on merkitty vain 4.3. kohta ja näiltä osin pyydän Finanssialan keskusliitolta luvanhakijoiden edustajana näkemystä ja ehdotusta.

Lainauksissa (heittomerkit) on pyritty tiivistämään käytännesääntötekstin ajatus; jossain tilanteissa teksti on sellaisenaan kirjattu.

2.1. Milloin henkilötietolakia ja käytännesääntöjä sovelletaan ?

1.k

"Käytännesäännöt koskevat asiakkaita koskevien henkilötietojen käsittelyä, ellei toisin ole mainittu."
Ulkopuolelle jäävät muun muassa työntekijää koskeva tiedonkäsittely työsuhteessa. H

4. k "Käytännesääntöjä sovelletaan luottolaitoksen toimialaan kuuluvien palveluihin ja niiden markkinointiin. "
Tarkempi henkilötietojen käsittelyn tarkastelu edellyttäisi palvelukohtaista tarkastelua. H

2.2. Henkilötietolain ja käytännesääntöjen keskeisten käsitteiden määritelmät

9. ja 10.k

"Luottolaitoksilla voi olla konsernisäännökseen perustuva yhteinen henkilörekisteri, vaikka tietoja pidetään teknisesti erillisissä osarekistereissä. Yhteisen rekisterin ja siellä olevien tietojen vaihdon osalta tulee huomioida myös luottolaitos-

lain
salassapitosäännökset."

Kehitys yhä laajempiin rekisterinpitäjä -yksikköihin on yksi keino vähentää tietojen siirron oikeudellisia hidasteita, joita perinteisessä yksittäistapauksellisessa luovutusharkinnassa on. Tämä koskee erityisesti toimialoja, jolla on erityiset salassapitosäännökset (kuten esim. terveydenhuolto). Kun luovutaan tällaisista sisäisistä organisatorisista tietosuojallisista rajoituksista, tulisi vastapainona kiinnittää huomiota yhteisten tietoresurssien käyttövaltuushallintaan (etukäteinen) ja käytönvalvontaan (jälkikäteinen). H ja KK, joka liittyy 10.luvun tiedonsuojaukseen.

4.1. Luottotiedot

1.k "Luottotietojen käyttämisestä säädetään luottotietolaissa."
Luottotiedolla tarkoitetaan tietoja, jotka koskevat luonnollisen henkilön tai yrityksen maksukykyä tai -halukkuutta tai jotka muulla tavalla kuvaavat henkilön tai yrityksen kykyä vastata sitoumuksistaan ja joita käytetään luottoa myönnettäessä tai luottoa valvottaessa. Määritelmä ei kata vain nimenomaista luottotietorekisteriä vaan myös pankin asiakastietoja, kun ne täyttävät em. tietosisältö- ja tarkoituskriteerit. Sovellettavaksi tulee näiltä osin lain 2 luvun säännökset. (T)

2.k
"Mikäli luottotiedot on tarkistettu rahanpesuepäilyn yhteydessä, siitä ei kuitenkaan saa ilmoittaa asiakkaalle."
Luottotietolakiin tehtiin rahanpesulain säätämisen yhteydessä näiltä osin poikkeus rekisteröidyn tarkastusoikeuteen (509/2008, luottotietolaki 30 §:n 3 momentti). Kun luottotietojen kyselijöistä on annettu yksilöidyt tiedot tarkastusoikeuden yhteydessä, on sillä ollut oma ennaltaehkäisevä ja kiinnijäämisriskiä lisäävä vaikutus. Tällainen "piilokysely" -mahdollisuus voi lisätä houkutusta luottotietojen luvattomiin kyselyihin. (H ja KK) KK liittyy tietosuojavaltuutetun tehtävään valvoa tällaisten kyselyiden lainmukaisuutta.

4.3. Luottolaitosten kannalta keskeisiä poikkeuksia arkaluoteisten tietojen käsittelykiellosta

2. k
Viimeisin tietosuojalautakunnan lupa on vuodelta 2004
ks. http://www.finlex.fi/fi/viranomaiset/ftie/2004/20040002

Päätöksessä tietosuojalautakunta ei ole antanut määräystä siitä, missä tilanteissa näitä arkaluonteisia tietoja voidaan käsitellä. Päätöksen yleisissä perusteluissa käsittelytilanteet yksilöidään seuraavasti : "....hakijoiden luoton- ja sitoumustenantoon liittyvien riskien pienentämiseksi ja väärinkäytösten estämiseksi."
Ottaen huomioon luottotietolain 19 §:n yksilöidyt käyttötilanteet näyttäisi tietojen suojaamisen kannalta tarpeelliselta yksilöidä tarkemmin missä 19 §:n mukaisissa luottolaitokselle luvallisessa tarkoituksessa myös väärinkäytöstiedot voidaan luottolaitosten kesken välittää. H + KK
Vaikka asia ei tähän yhteyteen kuulu, näyttäisi työelämän tietosuojalain 4 §:n 1 momentti aiheuttavan ongelman. Rikostietoja saa työnantaja hankkia suoraan laissa säädetyissä erityistapauksissa (kuten lasten kanssa työskentelevät). Ottaen huomioon työelämän tietosuojalain 5 a §:n säännöt ja nykyinen väärinkäytöstiedon jakelutapa, on ilmeinen riski, ettei väärinkäytöstiedon käsittelyssä saa-

tetaan päätyä lainvastaiseen tilanteeseen. Vaikka lupa perustuu lainsäädäntöön tulee luvan vastaavasti täyttää ne täsmällisyysvaatimukset, jotka lainsäädäntö asettaa varsinkin arkaluonteisten tietojen käsittelyn osalta. Näiltä osin pyydän luvanhakijoilta näkemystä tästä asiasta ja ratkaisuehdotuksista. VT

5. Henkilötietojen käsittely suoramarkkinoinnissa

3. k

Kielto-oikeus koskee suoramarkkinointia ja markkina- ja mielipidetutkimusta. Kun kielto-oikeus henkilötietolain perusteella koskee rekisterinpitäjää, on havaittu vaikeuksia tunnistaa, mikä on asiakassuhteeseen kuuluvaa jopa sen edellyttämää viestintää ja mikä on suoramarkkinointia. Toisaalta konsolidointiryhmässä tulisi olla käsitys siitä, mitä kielto-oikeus tarkoittaa tällaisessa ympäristössä. Yhteisen rekisterin osalta olisi perusteltua, että myös kielto-oikeus toteutetaan yhteisesti. H+ KK

5.4. Tietojen luovuttaminen suoramarkkinointia varten

1.k

Salassapitovelvollisuus rajoittaa henkilötietojen luovuttamista suoramarkkinointitarkoituksiin. Rajoitukset eivät koske konsolidointiryhmään kuuluvia yhtiöitä. Se, minkälaiset pelisäännöt koskevat tätä ristiinmarkkinointia, jää epäselväksi. Saattaa liittyä sellaista asiakastiedon käsittelyä, josta ei kilpailusyistä haluta yhteisiä pelisääntöjä H +KK

2. k jne

Muilta osin kappaleen teksti liittyy tiedonhankintaan uusasiakasmarkkinointia varten ja olisi luontevasti sijoitettavissa ennen 5.2 Suoramarkkinointirekisterit. Tiedonhankinnassa on ulkopuolisten lähteiden osalta selvitettävä tiedonhankinnan laillisuus (saanti luovutuksena tai kerääminen julkisista lähteistä). T

5.5. Televiestimien käyttö suoramarkkinoinnissa

2.k

Televiestinnästä osa kuuluu välinettä koskevaan kieltoon (opt-out) ja osa ennakollista suostumusta edellyttävään kohdeviestintään (opt-in). Tämä erottelu ei ole tekstin perusteella selvä tai se on harhaanjohtava. Tekstissä käsitellään automatisoituja soittojärjestelmiä, joita ei kai voi pitää kovin olennaisen välineenä luottolaitoksen palvelujen markkinoinnissa. Myös sähköposti ja tekstiviestit kuuluvat tähän suostumusta edellyttäviin viestintävälineisiin. Huomattavaa, että kyse on eri asiasta kuin henkilötietoihin kohdistuva markkinointikielto. H + EK

Tietolaatikko s.12

Tietolaatikossa on hyvin tiivistetty suoramarkkinointirekisterien muodostamiseen liittyvät kysymykset. Tietolähteen osalta kiinnitän myös huomiota siihen, mikä rekisteri ilmoitetaan tietolähteeksi. Jos julkisista osakasluetteloista kerätään tietoja suoramarkkinointirekisteriä varten, tulisi tietolähteenä ilmoittaa kerääjän muodostama oma suoramarkkinointirekisteri sekä ne tietolähteet, joita on käytetty suoramarkkinointirekisterin muodostamiseen. T

6. Henkilötietojen luovuttaminen ja siirto

6.1. Henkilötietojen luovuttaminen

1.-3. k

Nämä luovuttamisen ja siirron käsitteet ovat hyvinkin haasteellisia. Luottolaitostoiminnassa tämä näyttää erityisesti korostuvan salassapitovelvollisuuden ja sen poikkeusten johdosta. Luovutukselle näyttäisi olevan luonteenomaista, että rekisterinpitäjällä on luovutuksen osalta harkintavaltaa. Jos jollekin on säädetty tiedonsaantioikeus, ei voida puhua luovutusharkinnasta. Myös salassapitovelvollisuus poistaa tällaisen harkintavallan itse asiassa sitä voidaan pitää erityisenä luovutuskieltona. Kun salassapitovelvollisuudesta on säädetty poikkeus, on perusteltua ajatella, että poikkeus on rajattu tiettyihin tarkoituksiin, jolloin ollaan luovutusharkinnan puolella, ei kuitenkaan vielä tiedonantovelvollisuuden piirissä. Konsolidointiryhmän sisällä tietoja voidaan siis luovuttaa, mutta miten konsolidointiryhmän sisällä yksittäinen rekisterinpitäjä tämän tekee. Jos tämä tapahtuu käyttöoikeuksien myöntämisellä konsolidointiryhmän sisällä yksittäisen rekisterinpitäjän rajat ylittäen ei varsinaisesti ole kyse luovutusharkinnan käytöstä vaan sen delegoinnista yksittäisille käyttäjille. Mitkä periaatteet tätä delegointia koskee ilmenee käyttövaltuushallinnosta (kenelle annetaan ja minkä tason käyttöoikeuksia)?
H + KK

Luottolaitoksissa erityinen henkilötietojen siirtotilanne syntyy silloin kun luottolaitos päättää velkojana myydä saatavia. Tällaista tilannetta ei myöskään ole pidetty puhtaana henkilötietojen luovutuksena vaan itse käsittelyperusteen siirtona (velkakirja), jolloin rekisterinpitäjä vaihtuu ja itseasiassa myyjä menettää henkilötietoihin käsittelyoikeuden. Tällaisessa tilanteessa on rekisterinpitäjän vaihdoksesta ilmoitettava rekisteröidylle. T

6.2 Henkilötietojen siirto Euroopan unionin ulkopuolelle

Viimeisen virkkeen muistutus on hyvä. Poikkeusperusteen olemassaolo ei poista rekisterinpitäjän velvollisuutta selvittää vastaanottajamaan tietosuojan tasoa. Tämä on pääsääntö ja se tulisi nähdä velvollisuutena perehtyä ko. maan tietosuojan tasoon. Suhteellisuusperiaatteen mukaisesti arvioinnissa on otettava huomioon käsittelyn tietosuojallinen merkitys huomioiden myös taloudelliset väärinkäytön mahdollisuudet suhteessa kolmannen maan edellytyksiin vastata näihin rekisterinpitäjän tietosuoja- ja tietoturvavaatimuksiin. Tämän selvityksen perusteella voidaan myös tarkentaa sopimusehtoja, jos katsotaan riskien olevan hallittavissa tällaisin keinoin. Vakiosopimusehtojen täsmentäminen on tällaisista syistä kannatettavaa eikä tällaiset lisäykset laukaise ilmoitusvelvollisuutta tietosuojavaltuutetulle. T

7 ja 8 luvut

Nämä kaksi lukua liittyvät rekisterinpidon avoimuuteen, yleiseen ja erityiseen. Rekisteriseloste on yleinen avoimuussäännös. Jokaisella on oikeus saada. Informointi on tulevasta tai jatkuvasti tapahtuvasta käsittelystä tiedottamista ja tarkastusoikeus tietyn henkilön oikeus itseään koskeviin tietoihin. H

7.2 Luottoluokittelua koskevien periaatteiden informointi

Aina kun ihmisiä arvioidaan ja luokitellaan liittyy toimintaa ja luokittelun perusteisiin sekä lopputuloksiin yleistä ja erityistä mielenkiintoa. Yleinen mielenkiinto purkautuu varmaan kysymyksissä onko tällainen jatkuva luokittelu lainmukaista. Tähän olisi hyvä saada lisäperusteita, miksi pankki luokittelee, onko sen velvollisuus jopa tehdä näin ? Basel II ja asuntoluottokriisi uhkakuvana ??? (H)
Erityinen mielenkiinto kohdistuu tietysti lopputulokseen ja siihen, onko sen generoinnissa käytetty tieto riittävää, virheetöntä tai muuten laillista (esim. ei kiellettyjä syrjintäperusteita). H
Kun ja jos luottoluokitus kirjataan asiakkaan tiedoksi on hänellä tarkastusoikeuden nojalla oikeus saada nämä tiedot. Kun tiedot on annettava ymmärrettävässä muodossa, mikä olisi luokitustiedon osalta tällainen riittävä ymmärrettävyyden muodostava konteksti, joka tulisi myös ilmaista (esim. mihin asiakasryhmään kuuluu) T+KK

8.2. Rekisteröidyn tarkastusoikeus

Viimeisessä virkkeessä on huomautus, jonka perusteella tarkastusoikeuden merkitys jää vähäiseksi. Normaalissa asiakassuhteessa tiedonsaanti kuuluu sopimusperusteiseen järjestelyyn (esim. tilitiedot verkkopankissa). Tarkastusoikeutta sovelletaan jos rekisteröity osaa siihen nimenomaan vedota. Kun tarkastusoikeus on tietyin edellytyksin maksutonta, on ymmärrettävää, ettei sitä tarjota aktiivisesti. Joissakin tapauksissa on tullut esille tuntilaskutustyyppiset maksut kun asiakirjoja on pyydetty. Takauslain 14 §:n 2 momentti antaa tähän maksullisuuden ensisijaisuuteen oikeusperusteen. Jos käytäntö johtaa siihen, että saman tyyppisissä tapauksissa ne asiakkaat, jotka osaavat vedota tarkastusoikeuteen saavat maksutta tietonsa ja ne, jotka eivät osaa tähän vedota maksavat vastaavista tiedoista, ei käytäntöä voida pitää yleisesti hyväksyttävänä eikä sopimussuhteessa lojaliteettivelvoitteen mukaisena. H+KK

8.3 Tarkastusoikeuden toteuttaminen

Tarkastusoikeuteen liittyy myös kysymys sen laajuudesta. Jos asiakas yksilöi pyyntönsä eikä pyydä kaikkia tietoja, ei tällaista asiakaslähtöistä rajausta voida pitää lainvastaisena. Jos sitten pyydetään kaikki tiedot, mitä nämä tiedot luottolaitostoiminnassa oikein ovat ? KHO:n päätöksessä 27.2.2007 taltionumero 457 on käsitelty takaajan oikeutta tiedonsaantiin tarkastusoikeuden nojalla. Linkissä lehtijuttu tapauksesta http://www.rakennuslehti.fi/uutiset/lehtiarkisto/8917.html
Puhelutallenteiden tarkastamisesta olisi hyvä olla jonkinlainen näkemys. Onko kaikki puhelutallenteet tällaisia vai tulisiko niiden olla järjestetty asiakaskohtaisesti ? Miten niihin perehtyminen järjestetään, onko asiakkaalla oikeus saada ne "tulostettuna" ? T+KK

9.1. Tietojen säilyttäminen

"Luottolaitoksen ei tarvitse tuhota tietoja asiakasrekisteristään, mikäli niiden säilyttäminen on edelleen tarpeen."
Joskus säilyttämisajat vaikuttavat liian pitkiltä ja jossain tapauksessa liian lyhyiltä. Kummatkin tilanteet tulisi ottaa huomioon. Meille tulevien valitusten mukaan yleisimmät kysymykset liittyvät päättyneen velkajärjestelytiedon säilyttämiseen ja hylättyjen (ei ole syntynyt asiakassuhdetta) luottohakemustietojen säilyttämi-

seen. Tietojen liian aikaiseen hävittämiseen olemme törmänneet näissä takaajatapauksissa, joissa takaaja haluaisi tietää mistä nostoista ja niiden perusteista perittävä luotto on muodostuu. Jos tositteisiin sovelletaan yksioikoisesti kirjapitolain vaatimuksia, voidaan takaajien tiedollista oikeutta rajoittua tahattomasti. T + KK

10. Henkilötietojen suojaaminen ja hävittäminen

Henkilötietolain 32 § velvoittaa rekisterinpitäjää suojaamaan henkilötiedollisen järjestelmän asiattomalta pääsyltä tietoihin, vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Rekisterinpitäjän vastuuta suojauksen osalta voidaan arvioida henkilörekisteririkoksena, jos suojauksen laiminlyönti on tahallista tai vähintään törkeän huolimatonta. Arvioitaessa laiminlyönnin moitittavuutta käytetään apuna yleensä viranomaismääräyksiä ja hyviä käytäntöjä (esim. kunkin hetkinen hyvä hoito). Henkilötietolain 40 §:n 3 momentin mukaan tietosuojavaltuutettu voi antaa ohjeita siitä, miten henkilötietoja on suojattava henkilötietojen laittomalta käsittelyltä. Tämän perusteella tietosuojavaltuutettu ei ole antanut yhtään ohjetta. Tästä syystä arviointi tapahtuu toimialan omaksuman hyvän käytännön perusteella, joka voisi olla esitettynä käytännesäännöissä. T

Tästä näkökulmasta tarkasteltuna suojausta koskeva luku antaa aiheen seuraaviin huomioihin. Jotta suojaustoimet olisivat kohdennettuja ja tehokkaita tulisi tarkemmin yksilöidä mitä uhkia pyritään torjumaan. Henkilötietolain 32 §:n tarkoittamat uhkat on ymmärrettävissä hyvin laajasti. Ensinnäkin säännöksessä erotellaan tietoihin pääsy niiden muuttamisesta. Toisaalta säännöksessä tarkoitetaan täysin ulkopuolta tulevia uhkia mutta myös sisältäpäin tulevaa luvatonta käsittelyä. Kolmanneksi se koskee myös käyttöoikeusjärjestelmiä (tunnuksineen), oli ne tehty työntekijöiden tai asiakkaiden tunnistamiseksi. Tällainen tietojärjestelmän suojaamiseksi rakennettu tietojärjestelmä ja sen turvallisuus on myös otettava huomioon. H+KK

Verkkopankkitoiminnassa on huomiota kiinnitettävä pankin asiakkaisiin kohdistuvaan laittomaan tiedonhankintaa (phishing, spyware). Vaikka tekijöillä ei ole mitä ilmeisimmin tarkoitus loukata yksityisyyttä vaan ottaa rahat pois, voidaan katsoa, että pääsyoikeustunnisteet ovat myös henkilötietoja ja siten kyseessä on laittomasta henkilötietojen käsittelystä. Olemme yhdessä KRP ja Viestintäviraston kanssa miettimässä viranomaisyhteistyötä tällaisen laittoman usein vielä ulkomailta tapahtuvan henkilötietojen käsittelyn torjumiseksi ja tässä toiminnassa tulisi tietysti rekisterinpitäjien olla mukana. T

Kun konsolidointiryhmän sisäiset organisaatiorajat eivät muodosta relevanttia oikeudellista rajapintaa, jossa sovellettaisiin tapauskohtaisesti luovutussäännöksiä, tulee myös käyttöoikeuksien valvonta järjestää konsolidointiryhmän sisällä riittävällä tavalla. T

11. Automatisoitu päätös

11.4. Esimerkkejä

3. k

"Automatisoitu päätöstekojärjestelmä on varustettava ominaisuuksilla, joiden avulla varmistetaan rekisteröidyn oikeuksien suojaaminen."
Yhteydenottomahdollisuutta ei yksistään voida pitää riittävänä vaan kyse on kyseisen järjestelmän luotettavasta toiminnasta ottaen huomioon asiakkaan riittävä tunnistaminen, käytetyt tiedot ja tietolähteet ja niiden laatu sekä se, että arvioinnissa käytetyt tiedot ovat relevantteja eikä niitä voida pitää kiellettynä syrjintänä.
T

12. Ilmoitusvelvollisuus tietosuojavaltuutetulle

3. k

Ilmoitusvelvollisuutta ei ole silloin kun käytetään komission hyväksymiä mallisopimuslausekkeita. Ihan vaan turhien ilmoitusten välttämiseksi. T

Muita kysymyksiä

Toimialan yhteisenä kysymyksenä voidaan pitää terrorismin ja rahanpesun estämiseksi kansainvälisesti levitettäviä sulkulistoja. Esim. USA:n Office of Foreign Assets (OFAC) tuottaa tällaisia sulkulistoja.
Ruotsissa näiden listojen ylläpitämiseen on haettu ja saatu lupa ks.
http://www.datainspektionen.se/Documents/beslut/2006-02-24-bankforeningen.pdf

Tietosuojavaltuutettu Reijo Aarnio

Ylitarkastaja Heikki Partanen