Liikenne- ja viestintäministeriö

Vie palvelusi tietoturvallisesti verkkoon

Kansallisen tietoturvastrategian toimenpideohjelman hankkeen 2 ”Palveluntarjoajan vastuut, oikeudet ja velvollisuudet” loppuraportti

Julkaisuja 11/2011

Liikenne- ja viestintäministeriön

toiminta-ajatus
Liikenne- ja viestintäministeriö edistää yhteiskunnan toimivuutta ja väestön hyvinvointia huolehtimalla siitä, että kansalaisten ja elinkeinoelämän käytössä on laadukkaat, turvalliset ja edulliset liikenne- ja viestintäyhteydet sekä alan yrityksillä kilpailukykyiset toimintamahdollisuudet.

visio
Suomi on eturivin maa liikenteen ja viestinnän laadussa, tehokkuudessa ja kansainvälisessä osaamisessa.

arvot
Rohkeus
Oikeudenmukaisuus
Yhteistyö

Liikenne- ja viestintäministeriö

Julkaisun päivämäärä
11.2.2011

Julkaisun nimi
Vie palvelusi tietoturvallisesti verkkoon

Tekijät
Hankeryhmä 2, pj. lakimies Jaakko Turunen (Keskuskauppakamari), sihteeri kehityspäällikkö Jarkko Saarimäki (Viestintävirasto)

Toimeksiantaja ja asettamispäivämäärä
Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä 28.12.2009

Julkaisusarjan nimi ja numero
Liikenne- ja viestintäministeriön julkaisuja 11/2011

ISSN (verkkojulkaisu) 1798-4045
ISBN (verkkojulkaisu) 978-952-243-220-9
URN http://urn.fi/URN:ISBN:978-952-243-220-9
HARE-numero

Asiasanat
tietoturva, tietosuoja, sähköinen viestintä, tietoverkko, viestintäverkko, verkkopalvelu, palveluntarjoaja

Yhteyshenkilö
Neuvotteleva virkamies Timo Kievari, liikenne- ja viestintäministeriö

Muut tiedot

Tiivistelmä

Arjen tietoyhteiskunnan tietoturvallisuus -ryhmä asetti 28.12.2009 hankkeen, jonka tehtävänä oli selvittää tämän hetken tilanne palveluntarjoajien tietoturvaan liittyvistä vastuista, oikeuksista ja velvollisuuksista ja tehdä selvityksen pohjalta suositusluonteinen ehdotus parhaiksi käytännöiksi. Hankkeen työn tulokset on koottu tähän loppuraporttiin.

Aluksi selvitettiin kokonaiskuva palveluntarjoajan tietoturvavelvoitteita koskevan lainsäädännön nykytilasta, perustuslain ja EU-lainsäädännön asettamat velvoitteet, muu lainsäädäntö, alemmanasteinen normisto ja oikeuskäytäntö huomioiden.

Hankkeessa keskityttiin arvioimaan tietoturvan kannalta tilannetta, jossa pieni tai keskisuuri yritys (palveluntarjoaja) hankkii verkkosivuja tai muita verkkopalveluja toiselta yritykseltä. Hankkeen tulokset on laadittu siten, että ne palvelisivat ensisijaisesti pk-yritysten johdon tarpeita. Hanke suosittelee verkkopalvelujen suunnittelun, toteutuksen ja ylläpidon osalta seuraavaa:

1. Verkkopalvelua suunniteltaessa sen tietoturvavaatimukset määritetään siten, että palvelun tietoturva on asianmukaisella tasolla.
2. Tietoturvavaatimukset huomioidaan palvelua toteutettaessa.
3. Palvelun käyttöönoton jälkeen palvelua ja sen tietoturvaa ylläpidetään ja kehitetään jatkuvasti, jotta tietoturva säilyy asianmukaisella tasolla.

Palvelun tietoturvallinen toteuttaminen edellyttää, että tunnistetaan kaikki palvelun tietoturvaan vaikuttavat osatekijät ja vastuutetaan niistä huolehtiminen joko yrityksen omille työntekijöille tai ulkoisille kumppaneille. Palveluntarjoajan johdon on lisäksi valvottava, että palvelun toteuttamiseen osallistuvat tahot huolehtivat niille kuuluvien tehtävien hoitamisesta.

Kommunikations-
ministeriet

Publikationsdatum
11.2.2011

Publikation
Informationssäkerheten i nättjänster – rekommendationer om bästa praxis

Författare
Projektgrupp 2, ordförande jurist Jaakko Turunen (Centralhandelskammaren), sekreterare utvecklingschef Jarkko Saarimäki (Kommunikationsverket)

Tillsatt av och datum
Arbetsgruppen Informationssäkerheten i vardagens informationssamhälle 28.12.2009

Publikationsseriens namn och nummer
Kommunikationsministeriets publikationer 11/2011

ISSN (webbpublikation) 1798-4045
ISBN (webbpublikation) 978-952-243-220-9
URN http://urn.fi/URN:ISBN:978-952-243-220-9
HARE-nummer

Ämnesord
informationssäkerhet, dataskydd, elektronisk kommunikation, informationsnät, kommunikationsnät, nättjänst, tjänsteleverantör

Kontaktperson
Konsultativa tjänstemannen Timo Kievari, Kommunikationsministeriet

Övriga uppgifter
Rapporten är på finska.

Sammandrag
Informationssäkerheten i vardagens informationssamhälle är en arbetsgrupp som den 28.12.2009 startade ett projekt med uppgift att utreda tjänsteleverantörernas ansvar, rättigheter och skyldigheter i fråga om informationssäkerheten i nättjänster och att utgående från utredningen ge en rekommendation om bästa praxis. Resultaten av projektarbetet har sammanställts i denna rapport.

Till en början skisserades en helhetsbild av tjänsteleverantörernas skyldigheter i fråga om informationssäkerhet enligt gällande lagstiftning med beaktande av grundlagen, nationell lagstiftning, EU-lagstiftningen, normer på lägre nivå än lag och gällande rättspraxis.

Fokus i projektet låg på att utvärdera informationssäkerheten i en situation där ett litet eller medelstort företag (tjänsteleverantör) köper en webbplats eller andra nättjänster av ett annat företag. Projektresultaten är utarbetade så att de i första hand svarar mot ledningens behov i små och medelstora företag. Rekommendationerna för planering, genomförande och underhåll av nättjänster är följande:

1. Nättjänsten ska planeras så att kraven på dess informationssäkerhet definieras på adekvat nivå.
2. Kraven på informationssäkerhet ska beaktas när nättjänsten omsätts i praktiken.
3. När nättjänsten har tagits i bruk ska tjänsten och dess informationssäkerhet ständigt underhållas och utvecklas för att garantera en adekvat säkerhetsnivå.

För att tjänsten ska kunna genomföras på ett informationssäkert sätt måste alla faktorer som inverkar på tjänstens informationssäkerhet identifieras och ansvaret för dem läggas antingen på de anställda i företaget eller på utomstående parter. Ledningen i det företag som tillhandahåller nättjänster måste se till att de parter som deltar i att genomföra tjänsten sköter sina uppgifter.

Ministry of Transport and Communications

Date 11 February 2011	
Title of publication **Implementing online services in an information-secure way – recommendations for best practices**	
Author(s) Project group 2, Mr Jaakko Turunen, Legal Counsel, Finnish Central Chamber of Commerce (chair), Mr Jarkko Saarimäki, Development Manager, Finnish Communications Regulatory Authority (secretary)	
Commissioned by, date Information security group of the Ubiquitous Information Society Advisory Board, 28 December 2009	
Publication series and number **Publications of the Ministry of Transport and Communications 11/2011**	ISSN (online) 1798-4045 ISBN (online) 978-952-243-220-9 URN http://urn.fi/URN:ISBN:978-952-243-220-9 Reference number
Keywords information security, data protection, electronic communications, information network, communications network, network service, service provider	
Contact person Mr Timo Kievari, Ministerial Adviser, Ministry of Transport and Communications	
Other information The report is in Finnish.	

Abstract

The working group on information security, operating under the Ubiquitous Information Society Advisory Board, launched on 28 December 2009 a project to study the current situation of service providers' responsibilities, rights and obligations in the field of information security, and on the basis of the study, to draft a proposal for related best practices. This final report summarises the project's results.

At first, the current status of legislation concerning information security obligations of service providers was mapped out, paying due attention to the obligations arising from the Constitution of Finland and EU legislation, along with other legislation, subordinate rules and regulations, and case-law.

As its focus the project examined, in terms of information security, a situation in which a small or medium-sized enterprise (service provider) acquires websites or other online services from another company. The results of the project are presented in a form that primarily serves the needs of management in SMEs. As regards the design, implementation and maintenance of online services, the project puts forward the following recommendations:

1. When designing an online service, the associated information security requirements should be specified at an appropriate level.
2. Information security requirements should be taken into account in the implementation of the service.
3. After the service has been taken into use, continuous measures should be taken to maintain and develop the service and its information security in order to ensure an appropriate security level.

Implementing the service in an information-secure way requires that all factors affecting the information security of the service should be identified, and responsibility for addressing these issues should be assigned either to the company's own employees or to external partners. In addition, the management of the service provider organisation must supervise that all parties involved in the implementation of the service duly attend to the responsibilities they have been entrusted with.

Sisällysluettelo

Esipuhe

Kansallista tietoturvastrategiaa on toteutettu vuoden 2010 aikana toimenpideohjelmalla, jossa määriteltiin 9 kärkihanketta edistäämään tietoturvallisuutta Suomessa. Hanke 2:n puitteissa selvitettiin palveluntarjoajan vastuita, oikeuksia ja velvollisuuksia.

Liikenne- ja viestintäministeriö tilasi Asianajotoimisto Krogerus Oy:ltä selvityksen jossa pyydettiin antamaan kokonaiskuva palveluntarjoajan tietoturvavelvoitteita koskevan lainsäädännön nykytilasta, perustuslain ja EU-lainsäädännön asettamat velvoitteet, muu lainsäädäntö, alemmanasteinen normisto ja oikeuskäytäntö huomioiden. Lainsäädännön selvityksen jälkeen hankeryhmä ryhtyi laatimaan ehdotusta parhaiksi käytännöiksi pienten ja keskisuurten yritysten johdolle, näiden viedessään palveluitaan verkkoon. Sekä lainsäädännön tilan selvitys että hankeryhmän valmistelemat parhaat käytännöt ovat tämän hankeryhmän loppuraportin liitteinä.

Sähköisessä toimintaympäristössä palveluntarjoajana toimivan yrittäjän tietoturvallisuuteen liittyvien vastuiden, oikeuksien ja velvollisuuksien hahmottamiseksi on tärkeää ajatella tietoturvallisuutta erottamattomana osana yrityksen liiketoiminnan eri vaiheissa. Huomiota olisi kiinnitetttävä palvelun suunnitteluun, toteutukseen ja valvontaan. Palvelun tietoturvallisuus edellyttääkin ainakin, että palveluun kohdistuvat riskit on kartoitettu, palveluun liittyvät ulkoiset tietoturvavaatimukset (esim. pakottava lainsäädäntö tai toimialaa koskevat ohjeet) on huomioitu, palvelun tiedot säilyvät luottamuksellisina ja oikeellisina, palvelutasovaatimusten mukaisista ratkaisuista ja palveluista on huolehdittu, tietosuojanäkökohdat on huomioitu, palvelun käytöstä jää riittävät ”jäljet” (lokitiedot) jälkikäteen tapahtuvaa selvittämistä varten. Tietoturvallisuudesta huolehtimiseen ei tulisi suhtautua irrallisena projektina vaan pikemminkin jatkuvana prosessina, joka tulee suunnitella, jota tulee johtaa ja jota tulee valvoa liiketoiminnan yhteydessä.

Hankkeryhmän puheenjohtajana toimi Keskuskauppakamarin Jaakko Turunen ja sihteerinä Viestintäviraston Jarkko Saarimäki, joiden panos työssä on ollut korvaamaton. Kiitos kuuluu myös kaikille hankeryhmän jäsenille sekä selvityksen tekoon osallistuneille.

Timo Kievari
neuvotteleva virkamies

1. Johdanto

Valtioneuvoston hyväksyi 4.12.2008 periaatepäätöksen kansalliseksi tietoturvastrategiaksi ”Turvallinen arki tietoyhteiskunnassa – ei tuurilla vaan taidolla”. Strategia toimeenpannaan arjen tietoyhteiskunnan tietoturvallisuus -ryhmässä laaditulla toimenpideohjelmalla, johon sisältyvät strategian toteutuksen kannalta tarpeelliset toimenpiteet ja seuranta. Ohjelmaan koottiin tietoturvastrategian pohjalta yhdeksän kärkihanketta. Toimenpideohjelma julkaistiin ja siihen sisältyvät hankkeet asetettiin 28.12.2009.

Toimenpideohjelman hankkeen 2 ”Palveluntarjoajan vastuut, oikeudet ja velvollisuudet” tehtävänä oli selvittää tämän hetken tilanne palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista, sekä tehdä selvityksen pohjalta suositusluonteinen ehdotus parhaiksi käytännöiksi. Hankkeen tuli luovuttaa loppuraporttinsa 28.2.2011 mennessä.

Hankkeen päävastuulliseksi organisaatioksi nimettiin Keskuskauppakamari. Hankkeen vetäjäksi nimettiin Keskuskauppakamarista Jaakko Turunen, joka on toiminut myös hankeryhmän puheenjohtajana. Hankeryhmän sihteeriksi nimettiin Jarkko Saarimäki Viestintävirastosta. Hankeryhmän työskentelyyn ovat lisäksi osallistuneet Kimmo Bergius, Microsoft Oy; Antti Eskola, työ- ja elinkeinoministeriö; Kalevi Halonen, Fujitsu Services Oy; Erkki Heliö, Tieto Oyj; Antti Järvinen, Nokia Oyj; Mikael Kiviniemi, valtiovarainministeriö; Elina Kotilainen, Keskinäinen Vakuutusyhtiö Fennia/Finanssialan Keskusliitto ry; Arttu Lehmuskallio, TeliaSonera Finland Oyj; Timo Lehtimäki, Viestintävirasto; Timo Kievari, liikenne- ja viestintäministeriö; Pete Nieminen, Tietotekniikan liitto ry/Tietoturva ry; Miina Ojajärvi, Kuluttajavirasto; Heikki Partanen, Tietosuojavaltuutetun toimisto/oikeusministeriö; Antti Pietilä, Loyalistic Oy/Ohjelmistoyrittäjät ry; Jari Pirhonen, Oy Samlink Ab/Finanssialan Keskusliitto ry; Jyri Ryhänen, Verizon Business; Jarno Salonen, Teknologian tutkimuskeskus VTT; Heikki Sinervo, Elinkeinoelämän Keskusliitto ry; Ari Takanen, Codenomicon Oy; ja Esko Vainikka, Turun ammattikorkeakoulu.

Hankeryhmä on kokoontunut työnsä aikana kuusi kertaa. Asianajotoimisto Krogerus Oy laati hankkeen käyttöön oikeudellisen selvityksen palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista. Hanke on lisäksi saanut arvokasta apua Turun ammattikorkeakoulun opiskelijoilta, jotka hankkivat tietoa ja laativat tekstiluonnoksia hankkeen käyttöön.

Hankkeen puheenjohtaja osallistui tietoturvastrategian toimenpideohjelmaan sisältyvien hankkeiden seuraamiseksi ja ohjaamiseksi perustetun työvaliokunnan kokouksiin. Puheenjohtaja on lisäksi raportoinut hankkeen etenemisestä kahdesti arjen tietoyhteiskunnan tietoturvallisuus -ryhmälle.

Tähän loppuraporttiin on koottu hankkeen työn tulokset. Saatuaan työnsä päätökseen hanke luovuttaa loppuraporttinsa arjen tietoyhteiskunnan tietoturvallisuus -ryhmälle.

2. Hankkeen tulokset

2.1 Lähtökohdat ja tavoitteet

Kansallisen tietoturvastrategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona

on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa.

Strategiassa on todettu, että jokainen tietoyhteiskunnan toimija vaikuttaa teoillaan sekä omaan että muiden tietoturvallisuuteen. Siksi on tärkeää, että kaikilla on tietoturvallisuudesta riittävät perustiedot ja -taidot. Luottamus tietoyhteiskuntaa kohtaan syntyy, kun sekä palveluiden käyttäjät että tuottajat ymmärtävät vastuunsa, oikeutensa ja velvollisuutensa.

Palveluiden käyttäjien tulee kyetä tunnistamaan ja tiedostamaan turvallisen ja luotettavan palvelun lähtökohdat. Sähköisen asioinnin kansalaistaidot ja verkkolukutaito ovat edellytyksiä turvalliselle liikkumiselle verkossa. Riskien ennakointi, tunnistaminen ja niihin varautuminen säästää monelta ikävältä yllätykseltä. Erityisesti palveluntarjoajan tulee varmistaa palveluiden käytön turvallisuus sekä osaltaan huolehtia luottamuksellisten tietojen tunnistamisesta ja suojaamisesta. Palveluntarjoajalla on myös velvollisuus huolehtia palvelun turvallisuuden jatkuvasta ylläpitämisestä palvelu- ja toimintaympäristön muuttuessa.

Avoin ja selkeä viestintä palvelun turvallisuudesta ja mahdollisista riskeistä luo perustan sille luottamukselle, jota arjen tietoyhteiskunnassa toimimisessa tarvitaan. Palveluntarjoajan vastuuta ei voi ulkoistaa. Käytännössä palveluntarjoaja vastaa palvelun tuottamiseen osallistuvien toimijoiden kanssa palvelun tietoturvallisuudesta.

Tietoturvastrategian tehtävänä on integroida tietoturva kiinteäksi osaksi tietoyhteiskunnan perusrakenteita. Tämä edellyttää paitsi yleisen tietoturvatietoisuuden ja -osaamisen vahvistamista myös tietoturvanäkökohtien huomioon ottamista järjestelmähankinnoissa ja sopimusprosesseissa.

Kansallinen tietoturvastrategia toimeenpannaan arjen tietoyhteiskunnan tietoturvallisuus -ryhmässä laaditulla toimenpideohjelmalla. Toimenpideohjelman mukaan yhteiskunnan palvelut siirtyvät yhä voimakkaammin verkkoon, minkä vuoksi kansalaisten turvallinen siirtyminen palveluiden käyttäjiksi on varmistettava. Luottamuksen puute on yksi keskeisimmistä sähköisten palveluiden käyttöönoton esteistä. Kansalaisten on voitava luottaa siihen, että verkko- ja viestintäpalveluiden käyttö on turvallista.

Toimenpideohjelman mukaisesti hankkeen 2 tavoitteena oli:

- Lisätä palveluiden ja tuotteiden tietoturvaominaisuuksien vertailukelpoisuutta
- Tehdä tietoturvallisia palveluita näkyväksi
- Lisätä kansalaisten luottamusta.

Lisäksi hankkeen vaikuttavuustavoitteena oli:

- Selkiyttää palveluntarjoajan vastuita, oikeuksia ja velvollisuuksia
- Laajentaa luotettavien tietoturvaratkaisujen käyttöä
- Parantaa yritysten valveutuneisuutta tietoturva-asioista
- Edistää tietoturvan integroimista kiinteäksi osaksi tietoyhteiskunnan perusrakenteita.

2.2 Tehtävä, rajaukset ja kohderyhmä

Edellä mainitut lähtökohdat ja tavoitteet konkretisoidaan toimenpideohjelmassa eri hankkeille asetetuiksi tehtäviksi. Hankkeen 2 tehtävänä oli:

1. Selvittää tämän hetken tilanne palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista.
2. Tehdä selvityksen pohjalta suositusluonteinen ehdotus parhaiksi käytännöiksi.

Hankeryhmä totesi sille annetun tehtävän olevan laaja käytettävissä olevaan aikaan ja resursseihin nähden. Hankeryhmä on tehnyt työnsä aikana seuraavat rajaukset:

1. Hankkeessa on arvioitu palveluntarjoajan vastuita, oikeuksia ja velvollisuuksia nimenomaan tietoturvan[1] kannalta. Tietoturvaa on paikoin hankala erottaa tietosuojasta. Siksi tietoturvaa on käsitelty hankkeessa laajassa merkityksessä ottaen huomioon myös eräitä tietosuojan piiriin kuuluvia asioita. Arvioinnin ulkopuolelle on jätetty esimerkiksi verkkopalvelujen toteuttamiseen liittyvät viestinnälliset ja kaupalliset seikat. Hankkeessa ei ole myöskään arvioitu sopimusoikeudellista tai muuta yksityisoikeudellista taikka rikosoikeudellista vastuuta sen laajemmin kuin liitteenä 1 olevasta oikeudellisesta selvityksestä käy ilmi.

2. Hankkeessa täsmennettiin palveluntarjoajan käsitettä jättämällä sen ulkopuolelle yleisen viestintäpalvelun tarjoajat eli teleyritykset sekä julkishallinto, suuryritykset ja verkkopalveluja ammattimaisesti tarjoavat yritykset. Tällaisten toimijoiden tarpeet muun muassa suositusten yksityiskohtaisuuden osalta eroavat merkittävästi pk-yritysten tarpeista. Lisäksi hankkeessa laadittu oikeudellinen selvitys osoittaa, että näiden toimijoiden tarpeita varten on jo laadittu ohjeistusta.

Edellä mainittujen rajausten perusteella hankkeessa keskityttiin arvioimaan tietoturvan kannalta tilannetta, jossa pieni tai keskisuuri yritys (palveluntarjoaja) hankkii verkkosivuja tai muita verkkopalveluja toiselta yritykseltä. Hankkeen tulokset on laadittu siten, että ne palvelisivat ensisijaisesti tällaisten yritysten johdon tarpeita. Valittu kohderyhmä on syytä huomioida hankkeen tuloksia hyödynnettäessä.

2.3 Tulokset

2.3.1 Palveluntarjoajan vastuut, oikeudet ja velvollisuudet

Hanke selvitti aluksi tämän hetken tilanteen palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista. Kyseinen selvitys on liitteenä 1.

Selvityksessä on todettu muun muassa seuraavaa: ”- - *selvitystyössä on tullut esille tämän hetkisen tilanteen olevan palveluntarjoajien kannalta haasteellinen. Palveluntarjoajien on säännösten hajanaisesta luonteesta ja vaikeaselkoisista määritelmistä johtuen haasteellista olla tietoisia kaikista niiden liiketoimintaa koskevista laeista ja määräyksistä. Lisäksi eri kansallisten ja kansainvälisten viranomaisten palveluntarjoajien tietoturvaa koskevia ohjeita ja parhaita käytäntöjä on erittäin paljon.*”

Hankeryhmä ei havainnut työnsä aikana sääntelyssä merkittäviä puutteita tai olennaisia ristiriitaisuuksia. Tietoturva on tekninen ja alati muutoksessa oleva asia; verkkopalvelujen tietoturvavaatimukset muuttuvat jatkuvasti. Siten tietoturvan yksityiskohtainen sääntely lailla on ylipäätään vaikeaa. Hankeryhmä ei käsitellyt asiaa

[1] Tietoturvalla tarkoitetaan, että (1) palveluun tallennetut tiedot ovat vain niiden käyttöön oikeutettujen saatavilla (luottamuksellisuus); (2) tallennettuja tietoja ei voida muuttaa muiden kuin siihen oikeutettujen toimesta (eheys); ja (3) tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (käytettävyys).

enemmälti, koska hankkeen tehtäviin ei kuulunut lainsäädäntöä koskevien muutosehdotusten laatimien.

2.3.2 Suositusluonteinen ehdotus parhaiksi käytännöiksi

Hanke laati liitteenä 1 olevan selvityksen pohjalta suositusluonteiset ehdotuksensa parhaiksi käytännöiksi. Suositukset on koottu tähän loppuraporttiin ja sen liitteeseen 2.

Hanke suosittelee verkkopalvelujen suunnittelun, toteutuksen ja ylläpidon osalta yleisesti seuraavaa:

1. **Suunnittelu**. Verkkopalvelua suunniteltaessa sen tietoturvavaatimukset määritetään siten, että palvelun tietoturva on asianmukaisella tasolla.
2. **Toteutus**. Tietoturvavaatimukset huomioidaan palvelua toteutettaessa.
3. **Ylläpito**. Palvelun käyttöönoton jälkeen palvelua ja sen tietoturvaa ylläpidetään ja kehitetään jatkuvasti, jotta tietoturva säilyy asianmukaisella tasolla.

Palvelun tietoturvasta huolehtiminen on lähtökohtaisesti palveluntarjoajana olevan yrityksen johdon vastuulla. Palvelun tietoturvallinen toteuttaminen edellyttää, että tunnistetaan kaikki palvelun tietoturvaan vaikuttavat osatekijät ja vastuutetaan niistä huolehtiminen joko yrityksen omille työntekijöille tai ulkoisille kumppaneille. Johto voi hyödyntää liitteenä 2 olevaa tarkastuslistaa muistilistana vastuuttaessaan palvelun tietoturvan kannalta keskeisiä osatekijöitä eri osapuolille.

Vaikka palveluntarjoaja vastuuttaisi jonkin tehtävän alihankkijalleen, se on itse vastuussa alihankkijansa toiminnasta asiakkailleen tai muille sopimuskumppaneilleen. Riskejä arvioitaessa on hyvä huomioida, että vakuutukset eivät välttämättä kata tietoturvan pettämisestä aiheutuvia vahinkoja. Lisäksi palvelun tietoturvan pettämisestä aiheutuvat imagotappiot jäävät usein palveluntarjoajan itsensä kannettaviksi. Sen vuoksi palveluntarjoajan johdon on vastuuttamisen lisäksi valvottava, että palvelun toteuttamiseen osallistuvat tahot myös huolehtivat niille kuuluvien tehtävien hoitamisesta.

Täysin tietoturvallista palvelua ei ole olemassa. Tietoturvasta huolehdittaessa ratkaisevaksi muodostuu siten asianmukaisen tietoturvallisuuden tason määrittäminen. Ellei pakottava lainsäädäntö edellytä tiettyjä turvatoimia, on kysymys yrityksen omasta riskiarvioinnista. Arvioinnissa on otettava huomioon muun muassa verkkopalvelun tietoturvan pettämisen aiheuttamat vahingot palveluntarjoajalle itselleen, palvelun käyttäjille sekä muille sidosryhmille.

Palvelun tietoturvallisuus edellyttää ainakin seuraavaa:

1. Palveluun kohdistuvat riskit on kartoitettu
2. Palveluun liittyvät ulkoiset tietoturvavaatimukset (esim. pakottava lainsäädäntö tai toimialaa koskevat ohjeet) on huomioitu
3. Palvelun tiedot säilyvät luottamuksellisina ja oikeellisina
4. Palvelutasovaatimusten mukaisista ratkaisuista ja palveluista on huolehdittu
5. Tietosuojanäkökohdat on huomioitu
6. Palvelun käytöstä jää riittävät ”jäljet” (lokitiedot) jälkikäteen tapahtuvaa selvittämistä varten.

Tietoturvallisuus on prosessi, ei projekti. Tietoturvallisuus edellyttää jatkuvia toimenpiteitä sekä käytettävien järjestelmien teknisestä tietoturvallisuudesta huolehtimiseksi että palveluun kohdistuvien uusien riskien tunnistamiseksi.

Palveluntarjoajan on huomioitava henkilötietolaissa ja muussa sääntelyssä tietoturvalle asetetut vaatimukset (ks. liite 1). Jos palveluntarjoaja ulkoistaa verkkopalvelun suunnittelua, toteutusta, ylläpitoa tai kehittämistä, palveluntarjoajan on sovittava verkkopalvelun tietoturvavaatimuksista ulkoistuskumppanin kanssa. Tietoturvavaatimukset on tällöin suositeltavaa ottaa mukaan jo sopimusta edeltävään tarjouspyyntöön, jotta ne voidaan huomioida palvelun suunnitteluvaiheessa.

2.4 Tulosten arviointi

Toimenpideohjelman mukaisesti siihen sisältyville hankkeille luodaan vetovastuullisten johdolla mittarit, joiden avulla hankkeen toteutumista seurataan. Hankkeen 2 osalta mittareiksi valittiin seuraavat:

1. Selvitys palveluntarjoajien vastuista, oikeuksista ja velvollisuuksista
2. Ehdotus parhaiksi käytännöiksi.

Hankkeen tulokset täyttävät hankkeelle asetetun tehtävän (ks. jakso 2.2) ja yllä mainitut mittarit.

Hanke otti huomioon sille asetetut tavoitteet (ks. jakso 2.1) ja pyrki toteuttamaan ne tehtävänsä puitteissa. Tavoitteiden saavuttamiseksi hanke pitää tarpeellisena jaksossa 3 mainittujen jatkotoimenpiteiden toteuttamista. Hankkeen tehtäväksi ei ollut määritelty tietoturvastrategiassa mainittua turvallisille palveluille myönnettävän erillisen sertifikaatin kehittämistä tai sertifioitujen tietoturva-ammattilaisten määrän lisäämistä Suomessa. Näiden toimenpiteiden toteuttaminen voisi kuitenkin osaltaan edistää hankkeen tavoitteiden toteuttamista.

3. Jatkotoimenpiteet

Hanke pitää tarpeellisena seuraavien jatko-toimenpiteiden toteuttamista:

1. **Tulosten julkaiseminen**. Hankkeen tulosten hyödyntäminen pk-yrityksissä edellyttää, että pk-yritykset ovat tietoisia hankkeen tuloksista ja tulokset ovat helposti pk-yritysten saatavilla. Hanke ehdottaa, että tulokset julkaistaan esimerkiksi liikenne- ja viestintäministeriön julkaisusarjassa ja verkkosivuilla.

2. **Tulosten saattaminen pk-yritysten tietoon**. Hanke ehdottaa, että tulokset saatetaan laajasti ja aktiivisesti pk-yritysten tietoon esimerkiksi toimenpideohjelman hankkeen 1 kautta.

3. **Tulosten ylläpito ja päivittäminen**. Verkkopalvelujen tietoturvavaatimukset muuttuvat alati. Sen vuoksi hankkeen tulosten ajantasaisuutta ja toimivuutta tulisi seurata ja ryhtyä tarvittaessa toimenpiteisiin tulosten päivittämiseksi.

4. Liitteet

1. Palveluntarjoajan vastuut, oikeudet ja velvollisuudet – oikeudellinen selvitys tietoturvan näkökulmasta

2. Vie palvelusi tietoturvallisesti verkkoon – johdon tarkastuslista

Krogerus

PALVELUNTARJOAJAN VASTUUT, OIKEUDET JA VELVOLLISUUDET – OIKEUDELLINEN SELVITYS TIETOTURVAN NÄKÖKULMASTA

Asianajotoimisto Attorneys Advokatbyrå

Asianajotoimisto Krogerus Oy, Jaakonkatu 3 A, P.O. Box 533, FI-00101 Helsinki, Finland
Phone +358 (0)29 000 6200, Fax +358 (0)29 000 6201, helsinki@krogerus.com
Registered Office: Helsinki, Business ID: 0919666-0

SISÄLLYSLUETTELO

1 JOHDANTO

1.1 Selvityksen tarkoitus ja keskeiset johtopäätökset

Liikenne- ja viestintäministeriön viestintäverkkoyksikkö on tilannut Asianajotoimisto Krogerus Oy:ltä (”Krogerus”) selvityksen aiheesta "Palveluntarjoajan vastuut, oikeudet ja velvollisuudet – Oikeudellinen selvitys tietoturvan näkökulmasta". Selvityksessä on pyydetty annettavan kokonaiskuva palveluntarjoajan tietoturvavelvoitteita koskevan lainsäädännön nykytilasta, perustuslain (11.6.1999/731; "PL") ja EU-lainsäädännön asettamat velvoitteet, muu lainsäädäntö, alemmanasteinen normisto ja oikeuskäytäntö huomioiden.

Selvitys liittyy valtioneuvoston periaatepäätökseen kansalliseksi tietoturvastrategiaksi, joka hyväksyttiin joulukuussa 2008. Kansallisen tietoturvastrategian tavoitteena on luoda suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Strategian pohjalta on laadittu toimenpideohjelma, joka sisältää yhdeksän kärkihanketta, joissa paneudutaan uusiin ajankohtaisiin tietoturva-asioihin, parannetaan jo olemassa olevia toimintoja sekä vältetään päällekkäisten toimintojen tekemistä.

Krogerukselta tilattu selvitys on esityö valtioneuvoston periaatepäätöksen hankkeelle 2: Palveluntarjoajan vastuut, oikeudet ja velvollisuudet. Krogeruksen selvityksen tarkoituksena on ollut koota hanketyöryhmälle keskeinen lainsäädäntö palveluntarjoajan vastuista, oikeuksista ja velvollisuuksista tietoturvan näkökulmasta.

Selvityksessä on arvioitu lainsäädäntöä, muuta sääntelyä ja ohjeistusta palveluntarjoajan näkökulmasta yleisellä tasolla, koska sovellettava lainsäädäntö riippuu palveluntarjoajan käsittelemistä tiedoista, ei palveluntarjoajan tyypistä tai tarjoamista palveluista. Palveluntarjoajan tietoturvan kannalta keskeiset säännökset ovat henkilötietolaissa (22.4.1999/523; "HetiL"), sähköisen viestinnän tietosuojalaissa (16.6.2004/516; "SVTSL") ja laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617; "VahvSTL"). Krogeruksen selvityksessä on keskitytty näiden lakien keskeisen sisällön kuvaamiseen palveluntarjoajan kannalta. Muu asiaan liittyvä kansallinen ja EU-sääntely ja ohjeistus on selvityksessä jätetty yleisen kuvauksen tasolle.

Krogeruksen selvitystyössä on tullut esille tämän hetkisen tilanteen olevan palveluntarjoajien kannalta haasteellinen. Palveluntarjoajien on säännösten hajanaisesta luonteesta ja vaikeaselkoisista määritelmistä johtuen haasteellista olla tietoisia kaikista niiden liiketoimintaa koskevista laeista ja määräyksistä. Lisäksi eri kansallisten ja kansainvälisten viranomaisten palveluntarjoajien tietoturvaa koskevia ohjeita ja parhaita käytäntöjä on erittäin paljon.

Selvityksen ovat laatineet Krogeruksen puolesta Katri Joenpolvi, Mikko Pirttilä, Mikko Äijälä, Matti Metsola, Christer Svartström ja Juho Kivi-Koskinen.

1.2 Tietoturva, tietosuoja ja tietoturvallisuus

Tietoturvalla tarkoitetaan kaikkia niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja järjestelmien käytettävyys. Tietojen *luottamuksellisuudella* tarkoitetaan, että tiedot ja tietojärjestelmät ovat vain niiden käytössä, joille on annettu niihin käyttöoikeus. *Eheydellä* tarkoitetaan, että tiedot ja tietojärjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muuttuneet tai muutettavissa. *Käytettävyydellä* tarkoitetaan, että tiedot ja tietojärjestelmien palvelut ovat niiden käyttöön oikeutettujen käytössä silloin, kun niitä tarvitaan.

Erilaisia tietoturvatoimia ovat esimerkiksi laitteille ja järjestelmiin pääsyn valvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta.

Tietoturvaan liittyvällä *tietosuojalla* tarkoitetaan henkilön yksityisyyden suojaamista henkilöön yhdistettävissä olevien tietojen käsittelyssä. Tietosuojalainsäädäntö luo henkilötietojaan luovuttaville henkilöille oikeuksia ja samanaikaisesti asettaa henkilötietoja käsitteleville yrityksille eli rekisterinpitäjille velvollisuuksia. Tietosuojalainsäädännössä suojan kohde on siten yksilö ja hänen oikeutensa tietoihinsa. Tietosuojalainsäädäntö suojaa yksilöä hänen henkilötietojensa vahingolliselta käytöltä.

Tietoturva on lainsäädännössä jäsennetty tarkemmin tietoliikenneturvallisuuteen, laitteisto- ja ohjelmistoturvallisuuteen ja tietoaineistoturvallisuuteen. *Tietoliikenneturvallisuudella* tarkoitetaan muun muassa sitä, että viestintäverkoissa välitettävät tunnistamiseen liittyvät viestit eivät paljastu asiaankuulumattomille ja asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä. *Laitteistoturvallisuudella ja ohjelmistoturvallisuudella* muun muassa sitä, että käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys. *Tietoaineistoturvallisuudella* tarkoitetaan muun muassa sitä, että järjestetään tietoaineistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti, järjestetään tietoaineistojen varmuuskopiointi ja turvallinen säilytys sekä suojataan tärkeät asiakirjat, tietovarastot ja yksittäiset tiedot.

1.3 Palveluntarjoajan kannalta keskeinen lainsäädäntö

1.3.1 Henkilötietolaki

<u>Lain tausta</u>

Henkilötietojen suojasta säädetään PL:n mukaan tarkemmin lailla. HetiL säätelee kaikkea tietyssä käyttötarkoituksessa tapahtuvaa henkilötietojen käsittelyä. Laki edellyttää henkilötietojen käsittelyn tarkoituksen määrittelyä. HetiL:n vaatimukset on huomioitava kattavasti kaikessa verkossa tapahtuvassa sähköisessä liiketoiminnassa, jonka yhteydessä henkilötietoja käsitellään. HetiL määrittelee ne ehdot, joiden puitteissa henkilötietoja voidaan käsitellä siten että rekisteröityjen oikeudet toteutuvat.

Yleiset periaatteet

Sähköistä liiketoimintaa harjoittava rekisterinpitovelvollinen palveluntarjoaja saa HetiL:n mukaan käsitellä asiakkaiden henkilötietoja lähinnä kolmella perusteella, jotka ovat kuluttajan eli rekisteröidyn suostumus, sopimuksen paneminen täytäntöön sekä kun tiedoilla on konkreettinen yhteys palveluntarjoajan toimintaan.

Henkilötietojen käsittelyyn vaadittavan rekisteröidyn suostumuksen tulee olla yksiselitteinen ja todistustaakka suostumuksen osalta on palvelun tarjoajalla. Suostumuksen nimenomaisuus ja asiakkaan riittävän tietoisuuden syntyminen edellyttää erityisesti asiakkaan informointia siitä mihin hän suostumuksensa antaa. Tietoisuuden vaatimus suostumuksesta edellyttää verkkopalvelussa käytännössä jotain asiakkaan toimenpidettä suostumuksen ilmaisemiseksi. Asiakkaalta saatu suostumus on syytä tallentaa siten, että tarvittaessa suostumuksen olemassaolo voidaan osoittaa.

Asiakassuhdeperuste

Asiakassuhdeperusteen osalta rekisterinpitovelvollisen palveluntarjoajan on määriteltävä, kuinka asiakassuhde syntyy ja kuinka se päättyy kyseisessä liiketoiminnassa.[1] Vaikkei varsinaista asiakkuutta syntyisi tai rekisteröidyn suostumusta saataisi, tietojen käsittely on tietyin ehdoin sallittua. Lähtökohtaisesti suoramarkkinointitarkoituksissa on luvallista käsitellä henkilötietoja. Tällöin tietojen laatu ja määrä tai niiden käytön aika on rajattu, ja kuluttajalla on oikeus kieltää tietojensa käyttäminen.

Sähköistä liiketoimintaa harjoittavan palveluntarjoajan oikeus käsitellä henkilötietoja perustuu käytännössä yleensä asiakassuhteeseen, jolloin tiedoilla on asiallinen yhteys palveluntarjoajan toimintaan.

Arkaluonteiset tiedot

Arkaluonteisia tietoja ei saa käsitellä, ellei rekisteröidyltä saada tähän nimenomaista suostumusta. Henkilötunnuksen käsittely on lisäksi sallittu tilanteissa, joissa palveluntarjoaja luotottaa ostajaa, esimerkiksi kun palvelu tai tavara toimitetaan ostajalle ennen maksun suorittamista.

Henkilötietojen käsittelyn yleiset edellytykset

Jotta henkilötietojen käsittely täyttää HetiL:n vaatimukset, rekisteripitovelvollisen palveluntarjoajan tulee noudattaa HetiL:ssa määriteltyjä yleisiä periaatteita. Huolellisuusvelvoite on tärkein HetiL:n periaate, jota tulee noudattaa koko henkilötietojen käsittelyn prosessin ajan.

HetiL:n suunnitteluvelvoitteen mukaan asiakastietojen käsittely tulee suunnitella etukäteen, eikä kerättyjä tietoja saa käyttää muihin tarkoituksiin kuin laillisiin,

[1] Suomen suoramarkkinointiliitto (”SSML”) on sähköisen kuluttajakaupan käytännesäännöissä ottanut kantaa asiakassuhteen syntymiseen verkkoympäristössä. SSML:n mukaan asiakassuhde syntyy, kun asiakas on tilannut tai ostanut yrityksen tuotteen tai palvelun. Myös vastikkeettoman palvelun käyttäjäksi rekisteröityminen voi SSML:n mukaan muodostaa asiakassuhteen. Sen sijaan kuluttajan vierailu yrityksen kotisivulla ilman rekisteröitymistä palvelun käyttäjäksi ei yleensä muodosta yrityksen ja kuluttajan välille asiakassuhdetta. Yrityksen tulee suunnitella verkko- tai muun palvelunsa käyttö siten, että kuluttaja on tietoinen asiakassuhteen syntymisestä yrityksen kanssa.

etukäteen määriteltyihin käyttötarkoituksiin. Käsiteltävien henkilötietojen tulee olla määritellyn käsittelyn tarkoituksen kannalta asianmukaisia ja tarpeellisia palvelun tarjoajan liiketoiminnan näkökulmasta.

Sähköistä liiketoimintaa harjoittavan palveluntarjoajan on kohtuullisessa määrin huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita tietoja käsitellä. Tarpeeton tai vanhentunut asiakasrekisteri on hävitettävä noudattaen erityistä huolellisuutta.

Henkilötietojen luovuttaminen

Henkilörekisterien ollessa haluttua kauppatavaraa, asiakasrekisterin tai sen osan luovuttaminen kolmannelle taholle on mahdollista ainoastaan HetiL:ssa määritellyistä erityisistä syistä, tai tapauksissa, joissa luovutuksensaajan toiminta tyypillisesti liittyy kiinteästi luovuttajan toimintaan. Henkilötietojen siirto saattaa perustua esimerkiksi saatavien myyntiin, liiketoimintakauppaan sekä henkilötietojen käsittelyyn konkurssissa.

Rekisteriseloste ja palveluntarjoajan informointivelvollisuus

Rekisteriseloste kuuluu sähköistä liiketoimintaa harjoittavan palveluntarjoajan informointivelvollisuuteen. Selosteen tulee sisältää HetiL:n edellyttämät tiedot muun muassa rekisterinpitäjästä, kerättävistä tiedoista, niiden käyttötarkoituksesta ja rekisterin suojaamisesta. Rekisteriselosteen tulee olla jokaisen saatavilla ja helposti löydettävissä. Selosteen tulee esimerkiksi olla saatavilla siinä verkkokaupassa, mistä tuote ostetaan.

Informointivelvollisuuden täysimittaisen täyttämisen avuksi tietosuojavaltuutettu on esitellyt niin sanotun tietosuojaselosteen, jossa sähköistä liiketoimintaa harjoittava palveluntarjoaja voi kootusti esittää rekisteriselosteen tietosisältöä vastaavat tiedot ja muut informointivelvollisuuteen kuuluvat tiedot. Tietosuojaselosteeseen voidaan lisäksi liittää tietoa esimerkiksi evästeiden käytöstä ja vastuuhenkilöistä.

Rekisteröidyn oikeudet

Sähköistä liiketoimintaa harjoittavan palveluntarjoajan velvollisuutena on toteuttaa HetiL:ssa säädetyt asiakkaan oikeudet, kuten oikeus tarkistaa tietonsa, korjauttaa väärät tiedot ja kieltää tietojensa käsittely. Näistä toimista palveluntarjoaja ei saa periä maksua. Asiakkaalla on tarkistusoikeus koskien hänestä asiakasrekisteriin tallennettuja tietoja. Tarkistusoikeuteen kuuluu myös sen tarkistaminen, ettei asiakkaasta ole tallennettu tietoja johonkin tiettyyn rekisteriin.

Sähköistä liiketoimintaa harjoittavan palveluntarjoajan on korjattava tai poistettava virheelliset, tarpeettomat, puutteelliset tai vanhentuneet henkilötiedot. Korjaukset on mahdollista tehdä joko oma-aloitteisesti tai asiakkaan pyynnöstä.

Rekisteröidyn kielto-oikeus

Sähköistä liiketoimintaa harjoittava palveluntarjoaja voi käyttää asiakasrekisterin tietoja myös suoramarkkinointiin. Asiakkaalla on kuitenkin oikeus kieltää tietojensa käyttäminen suoramarkkinointitarkoituksiin. Kieltoa voidaan käyttää jo siinä vaiheessa, kun kauppias kerää kuluttajan henkilötietoja eikä kieltoa tarvitse

perustella. Kielto-oikeudesta niin kuin muistakin oikeuksista tulee kertoa rekisteröitävälle kuluttajalle selkeästi.[2]

Tietoturvan taso ja palvelujen ulkoistaminen

Vaikka sähköistä liiketoimintaa harjoittavan palveluntarjoajan kauppapaikan tekninen toteutus ja ylläpito ostettaisiin ulkopuoliselta palvelun tarjoajalta, ei tämä vaikuta sähköistä liiketoimintaa harjoittavan palveluntarjoajan oikeuksiin käsitellä henkilötietoja rekisterinpitäjänä sekä viestejä ja tunnistamistietoja viestinnän osapuolena. Ulkoistetuissa palveluissa palvelun ylläpitäjä käsittelee henkilötietoja rekisterinpitäjän oikeuden perusteella.

Sähköistä liiketoimintaa harjoittavan palveluntarjoajan on huolehdittava riittävästä ja asianmukaisesta tietoturvasta muun muassa jotta henkilötiedot säilyvät luottamuksellisina ja ettei asiakkaiden yksityisyydensuojaa vaaranneta. Käsittelijöiden määrä on rajattava minimiin ja heitä koskee vaitiolovelvollisuus.

Varsinaisten henkilörekisterien lisäksi tulee suojata verkkopalvelu, lomakkeet ja yhteydet, joiden välityksellä tietoja kerätään. Tietoturvan tason tulee olla suhteutettu henkilötietojen luonteeseen.

Vaikka osa mainituista toiminnoista on yleensä ulkoistettu esimerkiksi teleyritykselle, rekisterinpitäjä on silti aina viime kädessä vastuussa rekisterinpitäjän oikeuden perusteella tapahtuvasta henkilötietojen käsittelystä. Tästä syystä osapuolten vastuut ja tehtävät on syytä määritellä yksityiskohtaisesti ulkoistamistilanteessa.

Seuraamukset

HetiL:ssa on säädetty henkilötietojen lainvastaisesta käsittelystä seuraavasta vahingonkorvausvelvollisuudesta. HetiL:ssa ja rikoslaissa (19.12.1889/39; "RL") on sanktiot HetiL:n vastaisesta menettelystä. HetiL:n säännösten noudattamista Suomessa valvoo tietosuojavaltuutettu.

Rekisteröityjen oikeuksien turvaaminen päätavoitteena

HetiL:n haasteena on sovittaa yhteen rekisteröityjen oikeuksien turvaaminen ja liiketaloudellisesti kestävän elinkeinotoiminnan harjoittamisen mahdollisuus. Rekisteröityjen oikeusturva vaatii, että ei-havaittavaa ja kuluttajalle haitallista henkilötietojen käsittelyä ei tapahdu. Tämä puolestaan vaatii, että rekisterinpitäjät ja palveluntarjoajat sitoutuvat yhteisiin pelisääntöihin, jossa tavoitteena on rekisteröityjen yksityisyyden suojaaminen.

Rekisterinpitovelvolliselle palveluntarjoajalle paras kannustin tietoturva-asioiden mallikkaaseen hoitoon lienee laadultaan liiketaloudellinen. Rekisteröidyn kannalta on olennaista, että yksityisyyttä suojaavien teknologioiden käyttö olisi helppoa.

[2] SVTSL 26 §:ssä puolestaan vaaditaan markkinoinnin kohdentamiseksi luonnollisen henkilön suostumus, kun markkinointia toteutetaan automatisoitujen soittojärjestelmien, sekä telekopiolaitteiden, sähköpostiviestien, tekstiviestien, puheviestien, ääniviestien tai kuvaviestien avulla. SVTSL:n 26.2 §:n perusteella sallitaan suoramarkkinointi muiden kuin sähköisten viestimien avulla, mikäli henkilö ei ole tätä nimenomaisesti kieltänyt. SVTSL:n 26.3 § sisältää kuitenkin myös poikkeuksen suostumusvaatimukseen. Mikäli palvelun tarjoaja tai tuotteen myyjä saa asiakkaana olevalta luonnolliselta henkilöltä sähköiseen viestiin liittyvän yhteystiedon tuotteen tai palvelun myynnin yhteydessä, sama palvelun tarjoaja tai tuotteen myyjä voi käyttää tätä yhteystietoa omien samaan tuoteryhmään kuuluvien tai muuten vastaavien tuotteiden ja palveluiden suoramarkkinoinnissa.

Viranomaiset ovat kansalaisten teknisen osaamisen edistämisessä vähintään yhtä merkittävässä roolissa kuin kaupalliset tahot.

1.3.2 Sähköisen viestinnän tietosuojalaki

SVTSL kattaa sähköisen viestinnän tietosuojan tunnistamistietojen, paikkatietojen, tietoturvan, evästeiden käytön ja sähköisen suoramarkkinoinnin osalta. Laki koskee kaikkia luonnollisia henkilöitä ja oikeushenkilöitä viestinnän osapuolena, teleyrityksiä, yhteisötilaajia ja lisäarvopalvelun tarjoajia. Se sisältää velvoitteitteita teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille silloin, kun ne eivät ole viestinnän osapuolena. Laki on tärkeä viestinnän siirtyessä enenevissä määrin sähköiseen muotoon. SVTSL:n säännökset täydentävät PL:n takaamaa yksityisyyden suojaa sähköisen viestinnän osalta.

SVTSL:n tarkoituksena on turvata sähköisten viestintäpalvelujen käyttäjille yksityisyyden suojan yhdenmukainen taso riippumatta käytetystä tekniikasta ja sovelluksista. Tämä toteutuu määrittelemällä käyttäjien yksityisyyden suojan, viestinnän luottamuksellisuuden ja tietoturvan osalta riittävä perustaso. Lain avulla pyritään lisäämään käyttäjien luottamusta sähköiseen viestintään mahdollistaen näin uusien viestintäpalvelujen menestymisen ja yleistymisen. Selvityksen osalta keskeisimmät SVTSL:n palveluntarjoajia koskevat velvoitteet koskevat lain 3. luvun mukaista tunnistamistietojen käsittelyä ja 5. luvun mukaista viestinnän tietoturvaa.

On oleellista, että käsitellessään tunnistamistietoja teleyritykset, yhteisötilaajat ja lisäarvopalvelun tarjoajat ovat tietoisia niistä säännöksistä, jotka sääntelevät näiden tietojen käsittelyä. Tunnistustietojen käsittely on lähtökohtaisesti sallittua vain siinä määrin, kuin on tarpeellista käsittelyn tarkoitukseen nähden. Teleyrityksen, yhteisötilaajan ja lisäarvopalvelun tarjoajan on oltava tietoinen niistä SVTSL:n mukaisista tarkoituksista, joihin tunnistamistietoja saa käsitellä.

Tunnistamistietoja saa käsitellä ainoastaan palveluntarjoajan palveluksessa tai tämän lukuun toimiva luonnollinen henkilö, jonka tehtäväksi käsittely on osoitettava. SVTSL velvoittaa palveluntarjoajaa järjestämään toimintansa siten, että tietoturvanäkökohdat on otettu huomioon. Laissa painotetaan kustannustehokkaan ratkaisun käyttämistä tietoturvasta huolehtimiseen. Tämä tarkoittaa sitä, ettei palveluntarjoajalta voida edellyttää kohtuuttomia panostuksia velvollisuuden täyttämiseksi. Oleellista on, ettei käyttäjien tunnistamistietojen ja paikkatietojen yksityisyys vaarannu palveluntarjoajan puutteellisen tietoturvan johdosta.

Palveluntarjoaja vastaa siitä vahingosta, joka aiheutuu tietoturvan laiminlyönnistä. On tärkeää, että SVTSL:n tietoturvasäännöksiä sekä niitä täydentäviä Viestintäviraston määräyksiä noudatetaan palveluntarjoajan toiminnassa, jotta vältetään tietoturvauhkat sekä ylläpidetään käyttäjien luottamus sähköiseen viestintään.

SVTSL:ssa on erikseen mainittu toimet, joihin palveluntarjoaja voi ryhtyä tietoturvan toteuttamiseksi. Palveluntarjoajalle sallitaan viestien automaattinen käsittely ja suodattaminen puuttumatta kuitenkaan käyttäjän yksityisyyteen. Laki rajaa sen, missä määrin viestiä voidaan uhkien torjumiseksi käsitellä. Palveluntarjoajan on toiminnassaan huolehdittava lain mukaisesta tietoturvailmoituksesta, mikäli palvelun tietoturvaan kohdistuu erityinen uhka. Tällä edesautetaan käyttäjien mahdollisuutta ennaltaehkäistä näitä uhkia ja suojautua niitä vastaan, ja pyritään mahdollisimman häiriöttömään palveluiden käyttöön.

1.3.3 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista

VahvSTL sisältää perustason sääntelyn vahvan sähköisen tunnistamisen palveluiden tarjonnalle Suomessa. Lain tarkoituksena on edistää vahvan sähköisen tunnistamisen palveluiden tarjontaa ja luoda markkinoille perussäännökset palveluiden tarjontaan. Samalla pyritään varmistamaan, että palveluiden tarjonnassa otetaan huomioon tietoturvan ja tietosuojan vaatimukset.

VahvSTL sisältää säännökset siitä, *mitä edellytyksiä tunnistusmenetelmän tulee täyttää ollakseen vahvaa*. Lisäksi laki sisältää säännökset vahvan sähköisen tunnistuspalvelun tarjoajaan ja sen tarjoamaan palveluun kohdistuvista vaatimuksista.

Laissa tarkoitetaan *vahvalla sähköisellä tunnistamisella* henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttämällä perustuen *vähintään kahteen seuraavista kolmesta* vaihtoehdosta: a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää; b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen.

Käytössä olevista vahvan sähköisen tunnistamisen menetelmistä selvästi yleisimpiä ovat pankkitunnisteet. Lisäksi käytössä on julkisen avaimen järjestelmään perustuvia varmenteita. Niitä on tarjonnut viime vuosina lähinnä Väestörekisterikeskus.

Tunnistusmenetelmän on oltava *riittävän turvallinen ja luotettava ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat.* Esimerkiksi, jos tarjottava tunnistusmenetelmä perustuu *varmenteisiin*, palveluntarjoajan on varmistettava, että käytettävä algoritmi on riittävän vahva ja avainparin pituus riittävä.

Tunnistuspalvelun tarjoajan on huolehdittava siitä, että sen palveluksessa olevalla henkilöstöllä on harjoitetun toiminnan laajuuteen nähden riittävä teknillinen ja oikeudellinen asiantuntemus, kokemus ja pätevyys. Tunnistuspalvelun tarjoajan yleisiä velvollisuuksia koskevan säännöksen mukaan tunnistamispalvelun tarjoajan on huolehdittava palvelujensa HetiL:n mukaisesta *tietojen suojaamisesta sekä riittävästä tietoturvasta*. Näitä koskevat toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Tunnistuspalvelun tarjoajan on ilmoitettava ilman aiheetonta viivästystä tunnistuspalvelua käyttäville palveluntarjoajille, tunnistusvälineiden haltijoille ja Viestintävirastolle palvelun tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä. Uhkan tai häiriön kohdistuessa HetiL:ssa tarkoitettuun tietojen suojaamiseen, tunnistuspalvelun tarjoajan on ilmoitettava asiasta myös tietosuojavaltuutetulle.

1.3.4 Muu lainsäädäntö

Tietosuojan ja yksityisyyden suojaamisen taustalla vaikuttaa vahvasti perusoikeudet. Asiakastietojen käsittelyn ja yksityisyyden suoja perustuu perusoikeuksiin, kuten PL 6 §:n yhdenvertaisuuteen, PL 7 §:n koskemattomuuteen ja PL 10 §:n yksityiselämän suojaan.

Viestintämarkkinalain (23.5.2003/393; "VML") 128 § (viestintäverkon ja viestintäpalvelun laatuvaatimukset) sisältää teleyrityksiin kohdistuvia yleisiä, tietoturvaa koskevia vaatimuksia.

Laissa tietoyhteiskunnan palvelun tarjoamisesta (458/2002) säädetään sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti ja sähköisen tiedon välitys- tai tallennuspalveluita tarjoavien palveluntarjoajien vastuusta välittämänsä tai tallentamansa tiedon lainvastaisesta sisällöstä. Tietoyhteiskunnan palvelujen tarjoajien on lain mukaan pidettävä palvelujen vastaanottajien saatavilla myös määrätyt tiedot itsestään ja toiminnastaan. Lisäksi palveluntarjoajien on ennen sähköisen tilauksen tekemistä annettava kuluttajille ohjeita ja tietoja sekä järjestettävä kuluttajien käyttöön menettelyt, joiden avulla mahdolliset virheet tilauksissa voidaan etukäteen havaita ja korjata.

Viestintään ja tietojenkäsittelyyn liittyvät pakkokeinot oikeuttavat poikkeamaan yksityisyyden ja sananvapauden suojaksi säädetyistä säännöksistä. Pakkokeinoja koskevia säännöksiä löytyy pakkokeinolaista (30.4.1987/450, ”PKL”), laista tietoyhteiskunnan palvelujen tarjoamisesta, poliisilaista (7.4.1995/493) ja laista sananvapauden käyttämisestä joukkoviestinnässä (13.6.2003/460, ”sananvapauslaki”). Pakkokeinoilla on liittymä tietoon, sen suojaamiseen tai tietoturvallisuuteen kahdella tavalla. Ensinnäkin laissa määrätyillä perusteilla viranomaisella on oikeus saada tieto muuten yksityisyyden piiriin kuuluvasta tiedosta. Toisaalta viranomaisilla on oikeus estää laissa määrätyissä tapauksissa tiedon levittäminen viestinnän keinoin verkossa tai muualla tiedonvälityksessä.

RL tulee sovellettavaksi yksityisyyden suojaa loukattaessa esimerkiksi RL 38:9 henkilörekisteririkoksen, RL 38:8 tietomurron tai RL 38:1 salassapitorikoksen yhteydessä.

Laissa yksityisyyden suojasta työelämässä (759/2004) säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta.

1.3.5 Muut määräykset ja ohjeistukset

Tietoturvan ollessa teknisesti kompleksi ja laaja-alainen kenttä, on siitä olemassa runsaasti muita määräyksiä, suosituksia ja ohjeita. Lainsäädännöllä on miltei mahdoton kuvailla kaikkia niitä tekijöitä, jotka vaikuttavat huolellisesti toteutettuun tietoturvaan.

Suomessa tärkeimpiä lain ulkopuolisia säännöksiä ovat Viestintäviraston määräykset. Viestintäviraston määräykset ovat palveluntarjoajia sitovia ja ne täydentävät pääasiassa SVTSL:a. Määräysten soveltamisohjeet tarjoavat kattavat vaatimukset tietoturvan toteuttamiselle sähköisessä liiketoiminnassa. Palveluntarjoajan on oleellista olla tietoinen relevanteista Viestintäviraston määräyksistä toiminnassaan.

Tietosuojavaltuutetun HetiL:n soveltamisohjeet, VAHTI-ohjeet sekä muut ohjeet eivät sido palveluntarjoajia. Ne antavat kuitenkin tarkkoja ja yksityiskohtaisia ratkaisuja ja parhaita käytäntöjä tietoturvan toteuttamiseksi. Ohjeistusta voidaan pitää tietoturvan vähimmäistasoa korkeampana suositeltuna tasona. Ohjeistusta

voidaan käyttää mittapuuna arvioitaessa sitä, vastaako palveluntarjoajan tietoturva lain vaatimuksia niiltä osin, kun se ei laista tai sen perusteluista suoraan ilmene.

2 LAINSÄÄDÄNTÖ JA OIKEUSKÄYTÄNTÖ

2.1 Henkilötietolaki (22.4.1999/523)

2.1.1 Lain tausta, tarkoitus ja soveltamisala

Tietoturvallisuusasioiden parissa työskentelevältä henkilöltä edellytetään käytännön henkilötietojen käsittelyn toimintojen ja HetiL:n yleisten periaatteiden ja erityisten vaatimusten ymmärtämistä.

HetiL:n tarkoituksena on toteuttaa yksityisyydensuojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä ja edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. HetiL jättää tavoitteiden toteutuksessa rekisterinpitäjälle valinnanvapauden teknologioiden suhteen. Teknologian ja termistön kehittyessä HetiL:n on mahdollista välttää tästä seuraava uudistumispaine yleisiin periaatteisiin nojautuvana sekä järjestelmätietoja ja teknologisia termejä erikseen yksilöimättömänä lakina. Tällaisessa lainsäädännöllisessä ratkaisussa tosin saattaa varjopuolena piillä tulkinnanvaraisuuden riski.[3]

HetiL voidaan jakaa karkeasti kolmeen osaan: rekisterinpitäjän velvollisuuksiin, rekisteröidyn oikeuksiin ja viranomaismääräyksiin. HetiL:n yleisiä periaatteita ovat rekisterinpidon avoimuus ja rekisteröidyn itsemääräämisoikeus.[4]

On huomattava, että HetiL:n soveltuvuuden edellytyksenä ei ole se, että henkilötiedoista muodostuisi henkilörekisteri, vaan ainoastaan se, että tietoja käsitellään automaattisen tietojenkäsittelyn avulla. Muulla tavoin kuin automaattisen tietojenkäsittelyn avulla tapahtuvaan tietojenkäsittelyyn laki soveltuu ainoastaan, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa.

HetiL:n tarkasteleminen voidaan aloittaa käymällä läpi lain määritelmät. Tämän jälkeen luodaan puitteet arvioinnille, soveltuuko HetiL: (i) yrityksen harjoittamaan henkilötietojen käsittelyyn, (ii) yritykseen rekisterinpitäjänä, ja (iii) yrityksen henkilörekistereihin näiden laatu huomioon ottaen. Lisäksi tässä jaksossa tarkastellaan lain yleisiä periaatteita sekä arvioidaan näiden liityntöjä henkilötietojen käsittelyyn käytännön tasolla.

2.1.2 Keskeiset määritelmät

<u>Henkilötieto</u>

Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään koskeviksi.[5] Yrityksen toiminnassa henkilötiedoksi voidaan siten lukea laajasti katsottuna kaikki tieto, jonka perusteella yksittäinen

[3] Ibid.

[4] Viemerö 2009, s. 86.

[5] HetiL 3 § 1-kohta.

henkilö on mahdollista yksilöidä. On huomattava, että henkilötieto koskee ainoastaan luonnollisia henkilöitä, jolloin oikeushenkilöt rajautuvat kokonaan henkilötietokäsitteen ulkopuolelle. Henkilötiedoiksi voidaan mieltää muun muassa henkilön osoitetiedot, puhelinnumero ja sähköpostiosoite.

Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallentamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista ja muita henkilötietoihin kohdistuvia toimenpiteitä.[6] Luettelo ei ole tyhjentävä. Tarkoituksena on ollut kaikenlaisen yrityksen toiminnassa tapahtuvan henkilötietojen käsittelyn sisältyvän lain määritelmään.

Henkilörekisteri

Henkilörekisterillä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuullisin kustannuksin.[7] Käytännössä ollakseen henkilörekisteri, tämän tulee siten sisältää luonnollisen henkilön henkilötietoja ja henkilötietojen tulee kuulua saman käyttötarkoituksensa perusteella samaan joukkoon.[8,,] Tyypillisiä henkilörekistereitä ovat työnantajan rekisteri työsuhteiden hoitamista varten sekä yrityksen asiakasrekisteri.

Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. HetiL:n asettamien vaatimusten toteutuminen on rekisterinpitäjän vastuulla. HetiL:ssa tarkoitettu rekisterinpitäjä ei koskaan ole työntekijä vaan yritys.[9] Ratkaisevaa rekisterinpitäjätahon määrittelyssä on tosiasiallinen valta määrätä koko rekisterin käytöstä.[10]

Rekisteröity

Rekisteröidyllä tarkoitetaan henkilöä, jonka henkilötietoja käsitellään.[11] Vaikka rekisteröity antaisi suostumuksensa, ei henkilötietojen käsittelytarkoituksen kannalta tarpeettomia tietoja saa kerätä.[12]

Sivullinen

[6] HetiL 3 § 2-kohta.

[7] HetiL 3 § 3-kohta.

[8] Laaksonen – Nevasalo – Tomula 2006, s. 33.

[9] Laaksonen – Nevasalo – Tomula 2006, s. 34.

[10] Viemerö 2009, s. 49.

[11] HetiL 3 § 5-kohta.

[12] Laaksonen – Nevasalo – Tomula 2006, s. 37.

Sivullisella tarkoitetaan muuta henkilöä, yhteisöä, laitosta tai säätiötä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää.[13]

Suostumus

Suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.[14]

Suostumus voi olla suullinen, kunhan se täyttää lain määritelmässä mainitut edellytykset. Suostumukselle asetettujen edellytysten täyttyminen määräytyy viimekädessä tapauskohtaisesti. Suostumus on voimassa toistaiseksi, jollei suostumuksesta muuta ilmene. Rekisteröidyllä on oikeus milloin tahansa peruuttaa suostumuksensa.[15]

2.1.3 Henkilötietojen käsittelyn yleiset periaatteet

HetiL 2 luvussa on määritelty henkilötietojen käsittelyn yleiset periaatteet, joita rekisterinpitäjän on noudatettava rekisterinpidossa, jotta henkilötietojen kerääminen olisi ylipäätään sallittua. Periaatteissa voidaan erottaa rekisterinpitäjään kohdennetut velvoitteet (huolellisuus- ja suunnitteluvelvollisuus sekä käyttötarkoitussidonnaisuus) ja toisaalta tietojen laadulle vaatimuksia asettavat periaatteet (tarpeellisuus- ja virheettömyysvaatimus).

Huolellisuusvelvollisuus

Rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa ja toimia niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Sama velvollisuus on sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun.[16]

Huolellisuusvelvoite on yleisluonteinen velvoite, joka tulee ottaa kaikessa lain tarkoittamassa henkilötiedon käsittelyssä huomioon. Rekisterinpitovelvollisen palveluntarjoajan on huomattava, että velvoitteesta on katsottu johtuvan niin sanottu itseohjautuvuuden ajatus, jonka mukaisesti rekisterinpitäjän on oma-aloitteisesti toimittava tietosuojan parantamiseksi.[17] Lain huolellisuusvelvoitteen noudattamispyrkimyksessä hyvänä apuna toimivat yleisesti tunnetut standardit ja käytänteet.[18]

Suunnitteluvelvollisuus

Henkilötietojen käsittelyn tulee olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta. Rekisterinpitäjän on suunniteltava ennen henkilötietojen keräämistä tai

[13] HetiL 3 § 6-kohta.

[14] HetiL 3 § 7-kohta.

[15] HE 96/1998 vp., 3 § 7-kohta.

[16] HetiL 5 §.

[17] Viemerö 2009, s. 54.

[18] Standardeista ja toimintamalleista lisää tämän selvityksen jaksoissa 3.7 ja 3.8. Ks. myös Laaksonen – Nevasalo – Tomula 2006, s. 83–114.

muodostamista henkilörekisteriksi se, mistä henkilötiedot hankitaan (esimerkiksi rekisteröidyltä itseltään vai toisesta henkilörekisteristä) ja mihin niitä luovutetaan (sekä millä perusteella luovuttaminen voisi tapahtua). Henkilötietojen käsittelyn tarkoituksesta tulee ilmetä, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.[19]

Suunnittelun on tarkoitus johtaa kirjalliseen suunnitelmaan, joka sisältää tietoja tietoturvan hoitamiseen liittyvistä toimenpiteistä. Suunnitelman tulee kattaa käsiteltävien henkilötietojen koko elinkaari. Suunnitelmassa on yksilöitävä prosessissa kerättävät tiedot, sen yhteydessä syntyvät tiedot sekä se, miten nämä tiedot lopulta tuhotaan. Suunnittelussa pitää kuvata, miten henkilötietojen käsittely on järjestetty hallinnollisesta näkökulmasta.[20]

Käyttötarkoitussidonnaisuusperiaate

Henkilötietojen käsittelyn käyttötarkoitussidonnaisuus tarkoittaa sitä, että henkilötietoja saa käsitellä vain niihin käyttötarkoituksiin, jotka eivät ole yhteensopimattomia rekisterinpitäjän toiminnan tai sen perustehtävään kuuluvien henkilötietojen käyttötarkoitusten kanssa. Henkilötietojen käsittelyn tulee olla rekisterinpitäjän toiminnan kannalta asiallisesti perusteltua eikä niiden käsittely ole sallittua muihin kuin ennalta määriteltyihin käyttötarkoituksiin.[21]

Henkilötietojen laatua koskevat periaatteet

Tarpeellisuusvaatimuksen mukaisesti käsiteltävien henkilötietojen tulee olla määritellyn käsittelyn tarkoituksen kannalta tarpeellisia.[22] Lain esityöt korostavat tässä yhteydessä suoritettavassa harkinnassa tarkoitussidonnaisuutta, toisin sanoen mitään sellaista tietoa, vaikka sen keräämiseen olisi mahdollisuus, ei tule kerätä, jos se ei ole käsittelyn tarkoituksen kannalta olennaista.[23]

V*irheettömyysvaatimuksen* mukaan rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä. Rekisterinpitäjän velvollisuutta arvioitaessa on otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle.

Palveluntarjoajan rekistereissä saattaa helposti olla virheellisiä tietoja, koska rekisteröityjen elämäntilanne muuttuu ajan kuluessa. Vähäisiksi katsottavat virheet eivät kuitenkaan pääsääntöisesti johda oikeudellisiin toimenpiteisiin rekisterinpitäjää kohtaan. Toisaalta, toiminnan laatu sekä olosuhteet saattavat asettaa erittäin tiukatkin reunaehdot tietojen oikeellisuudelle, kuten esimerkiksi vakuutus- ja luototustoiminnassa.[24]

Rekisteriseloste

[19] HetiL 6 §.

[20] Laaksonen – Nevasalo – Tomula 2006, s. 39.

[21] HetiL 7 §. Ks. myös Salminen 2009, s. 59.

[22] HetiL 9 §.

[23] Viemerö 2009, s. 57. Tarpeellisuusarvioinnista, ks. HE 49/1986 vp., s. 28.

[24] Viemerö 2009, s. 60.

Rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee: i) rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot; ii) henkilötietojen käsittelyn tarkoitus; iii) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä; iv) mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; ja v) kuvaus rekisterin suojauksen periaatteista.[25]

Rekisterinpitäjän on pidettävä rekisteriseloste jokaisen saatavilla. Velvollisuudesta voidaan poiketa, jos se on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi.

Säännöksen tarkoitus on varmistaa henkilötietojen käsittelyn avoimuus. Tarkoituksena on lisäksi se, että rekisteröityjä informoidaan siitä, että heidän tietoja käsitellään, mitä tietoja käsitellään, ja mihin tarkoituksiin niitä käytetään. Rekisteriselosteen laatimisvelvollisuus koskee sekä automaattisen tietojenkäsittelyn avulla muodostettua että manuaalista rekisteriä. Rekisteröidyn tulee voida minä hetkenä hyvänsä ottaa selvää rekisteriselosteen sisällöstä (esimerkiksi jos rekisteri on Internetissä, myös selosteen tulee olla saatavilla siellä).[26]

Usein ne tahot, joille henkilötietoja tullaan luovuttamaan, eivät vielä rekisteriselostetta laadittaessa ole edes rekisterinpitäjänkään tiedossa. Tässä yhteydessä on olennaista huomata, että rekisteröidyn tulee edellä mainitusta huolimatta kyetä tekemään rekisteripitäjän antaman informaation perusteella ratkaisu omien tietojensa käytöstä.[27]

Arkaluonteisten tietojen käsittely

Arkaluonteisten henkilötietojen käsittely on kielletty.[28] HetiL 12 §:ssä säädetään arkaluonteisten henkilötietojen käsittelykiellon poikkeuksista. Koska viranomaisten rekistereissä olevat arkaluonteiset henkilötiedot ovat usein salassapidettäviä, näiden tietojen luovuttamisessa on otettava lisäksi huomioon lainsäädäntöön sisältyvät salassapitoa ja salassapidon poikkeuksia koskevat säännökset[29].

Henkilötunnuksen käsittely

Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisesti antaman suostumuksen perusteella taikka muissa lain tarkemmin määrittelemissä tilanteissa. Lisäksi laissa

[25] HetiL 6 §.

[26] Viemerö 2009, s. 60–61.

[27] Viemerö 2009, s. 61–62.

[28] HetiL 11 §:n mukaan arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:

1. rotua tai etnistä alkuperää; 2. henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista; 3. rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta; 4. henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia; 5. henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka 6. henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

[29] HE 96/1998 vp., 12 §.

luetellaan ne tilanteet, joissa henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää.[30]

2.1.4 Henkilötietojen käsittelyn yleiset edellytykset

HetiL:ssa määritetään ne edellytykset, joilla henkilötietojen käsittely ja henkilörekisterin perustaminen ylipäätään on mahdollista. Lain tarkoittamat edellytykset voidaan jakaa systematisointiperustein kahteen ryhmään siten, että käsittelylle on oltava rekisteröidyn suostumus tai käsittelyn peruste on löydyttävä laista.[31]

Henkilötietojen käsittely rekisteröidyn suostumuksella, toimeksiannosta tai pyynnöstä

Henkilötietoja saa käsitellä rekisteröidyn yksiselitteisesti antamalla suostumuksella tai rekisteröidyn toimeksiannosta tai sellaisen sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osallisena, taikka sopimusta edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.[32]

Henkilötietojen käsittelyn tulee perustua rekisteröidyn yksiselitteiseen suostumukseen, jolloin esimerkiksi rekisteröidyn passiivisuutta ei voida katsoa lainkohdan tarkoittamaksi suostumukseksi.[33] Laissa tarkoitetun suostumuksen voi lain esitöiden mukaan antaa joissakin tapauksissa myös konkludenttisesti.[34] Jos suostumuksen olemassaolosta syntyisi kiistaa, kuten usein saattaa tapahtua esimerkiksi suoramarkkinointiliitännäisissä asioissa, todistustaakka suostumuksen olemassaolosta on rekisterinpitäjällä.[35]

Rekisteripitovelvollisen palveluntarjoajan tulee huolehtia siitä, että rekisteröity on tietoinen siitä mihin suostumuksensa antaa. Lisäksi tulee huolehtia siitä, että rekisteröity on tietoinen kaikista niistä käsittelytarkoituksista, joita varten rekisterinpitäjän on määrä henkilötietoja käsitellä. Etenkin sähköisessä kaupassa palvelun toteuttaminen edellyttää usein, että kuluttaja suostuu antamaan henkilötietonsa rekisterinpitäjän ylläpitämään rekisteriin. Edellä mainituista huolellisuusperiaatteesta ja tietojen virheettömyysvelvoitteesta seuraa, että rekisterinpitovelvollisen palveluntarjoajan on riittävissä määrin varmistuttava rekisteröityvän henkilön antamien tietojen oikeellisuudesta. Tämä on haastavaa ottaen jo sen huomioon, että useimmiten rekisterinpitäjä ja rekisteröityvä henkilö eivät ole samassa fyysisessä tilassa, jolloin muiden varmentamistekniikoiden merkitys kasvaa. Siten on suositeltavaa, että rekisteripitovelvollinen palveluntarjoaja hankkii suostumuksen tavalla, jolla vaaditunkaltaisen suostumuksenannon voidaan jälkikäteen todistaa tapahtuneen.[36]

---

[30] HetiL 13 §.

[31] HetiL 8 §. Ks. myös Viemerö 2009, s. 65.

[32] HetiL 8 § 1–2 -kohdat.

[33] HetiL 8 § 1-kohta.

[34] HetiL 3 § 7-kohta.

[35] HE 96/1998 vp., 8 §.

[36] Viemerö 2009, s. 65–68.

HetiL 8 §:n 2-kohdan tarkoittama henkilötietojen käsittelyn salliminen tapauksessa, jossa tämä on välttämätöntä sopimuksen täytäntöönpanemiseksi, on varsin tavanomaista esimerkiksi Internetissä tapahtuvassa kuluttajakaupassa, jossa rekisterivelvollinen palveluntarjoaja tarvitsee erinäisiä tietoja kuluttajasta liiketoimen loppuunsaattamiseksi.

Henkilötietojen käsittely ilman rekisteröidyn nimenomaista suostumusta

HetiL:ssa säädetään niistä edellytyksistä, jolloin henkilötietojen käsittely on sallittua ilman rekisteröidyn antamaa nimenomaista suostumusta. Henkilötietoja saa käsitellä muissa kuin HetiL 8 §:n 1- ja 2-kohdissa tarkoitetuissa tapauksissa ainoastaan:

(i) jos käsittely yksittäistapauksessa on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi;
(ii) jos käsittelystä säädetään laissa tai jos käsittely johtuu rekisterinpitäjälle laissa säädetystä tai sen nojalla määrätystä tehtävästä tai velvoitteesta;
(iii) jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan (*yhteysvaatimus*);
(iv) jos kysymys on konsernin tai muun taloudellisen yhteenliittymän asiakkaita tai työntekijöitä koskevista tiedoista ja näitä tietoja käsitellään kyseisen yhteenliittymän sisällä;
(v) jos käsittely on tarpeen rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai muita niihin verrattavia tehtäviä varten;
(vi) jos kysymys on henkilön asemaa, tehtäviä ja niiden hoitoa julkisyhteisössä tai elinkeinoelämässä kuvaavista yleisesti saatavilla olevista tiedoista ja näitä tietoja käsitellään rekisterinpitäjän tai tiedot saavan sivullisen oikeuksien ja etujen turvaamiseksi; tai
(vii) jos tietosuojalautakunta on antanut käsittelyyn HetiL 43 §:n 1 momentissa tarkoitetun luvan.[37]

Ilman suostumusta tapahtuvan henkilötietojen käsittelyn sallimisen merkitys on erityisen suuri viranomaistoiminnassa (esimerkiksi verottajalla on velvollisuus ylläpitää rekisteriä verosubjekteista). Viranomaisten tietojen luovuttamisesta säädetään myös laissa viranomaisten toiminnan julkisuudesta (621/1999).

HetiL:n esitöissä selvennetään yhteysvaatimuksen täyttymistä siten, että HetiL 8 § 5-kohta sallii henkilötietojen käsittelyn, jos se on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn suojaa tarvitsevat intressit ja perusoikeudet ja -vapaudet.[38] Rekisterinpitovelvollisen palveluntarjoajan kannalta kyseinen lainkohta on kuluttajasopimusten solmimisen kannalta väistämätön, sillä asiakkaista kertyy asiakkuuden aikana väistämättä tietoja riippumatta siitä, mihin käyttöön niitä on jatkossa tarkoitus käyttää.[39]

[37] HetiL 8 § 3–9 -kohdat.

[38] HE 96/1998 vp., 8 § 5-kohta.

[39] Viemerö 2009, s. 69–71.

2.1.5 Rekisteröidyn oikeudet

Rekisteröidyn oikeuksia koskevalla sääntelyllä on tärkeä merkitys läpi HetiL:n kulkevien rekisterinpidon avoimuus- ja rekisteröidyn itsemääräämisoikeusperiaatteiden toteutumisessa. Oikeuksien toteutumista valvoo tietosuojavaltuutettu.[40]

Informointi tietojen käsittelystä

Rekisterinpitäjän on kerätessään henkilötietoja huolehdittava siitä, että rekisteröity voi saada tiedon rekisterinpitäjästä ja tarvittaessa tämän edustajasta, henkilötietojen käsittelyn tarkoituksesta sekä siitä, mihin tietoja säännönmukaisesti luovutetaan.[41]

Tietosuojaseloste

Tietosuojaseloste on tietosuojavaltuutetun HetiL 24 §:n mukaisen informointivelvollisuuden ja 10 §:ssä tarkoitetun rekisteriselosteen saatavillapitovelvoitteen täyttämiseksi kehittämä käsite. Käsitettä ei suoranaisesti mainita HetiL:ssa, mutta konsepti on epäsuorasti johdettu informointivelvollisuuden täyttämisen luomasta tarpeesta koota tiedot yhteen loogiseen kokonaisuuteen. Käytännössä sen on tarkoitettu olevan apuväline, jota noudattamalla rekisterinpitäjä voi varmistua lain määräyksien noudattamisesta. Tietosuojaselosteelle ei ole mitään tiettyä määrämuotoa, joten se voi olla vapaamuotoinen, kunhan se sisältää em. pykälissä edellytetyn informaation.

Tietosuojaselosteen tulee sisältää ainakin seuraavat tiedot:

- tiedot rekisterinpitäjästä ja tarvittaessa hänen edustajasta;
- tiedot henkilötietojen käsittelyn tarkoituksesta;
- tiedot säännönmukaisista tiedonluovutuksista; ja
- ne tiedot, jotka ovat tarpeen rekisteröidyn oikeuksien käyttämiseksi henkilötietojen käsittelyssä. Näihin sisältyvät muun muassa 26 §:n tarkastusoikeus, 29 §:n tiedonkorjaamisoikeus ja 30 §:n suoramarkkinointiin liittyvä kielto-oikeus.

Rekisteröidyn tarkastusoikeus

Rekisterinpidon avoimuuden ja tiedollisen itsemääräämisoikeuden kannalta on ensisijaisen tärkeää, että rekisteröidyllä on a) tieto siitä, missä rekistereissä hänestä on tietoja ja b) oikeus saada tieto siitä, mitä tietoja hänestä on rekisteröity. Näiden oikeuksien turvaamisessa rekisteröidyn tarkastusoikeudella on ratkaiseva asema. Jokaisella on salassapitosäännösten estämättä oikeus saada tietää, mitä häntä koskevia tietoja on tallennettu, mutta myös se, että hänestä ei ole tallennettu tietoja tiettyyn rekisteriin. Samalla rekisteröidylle on ilmoitettava rekisterin säännön mukaiset tietolähteet ja mihin rekisteröityjä tietoja käytetään ja säännönmukaisesti luovutetaan.[42]

---

[40] Viemerö 2009, s. 86.

[41] HetiL 24 §.

[42] Viemerö 2009, s. 92.

Tiedot tulee antaa rekisteröidylle hänelle ymmärrettävässä muodossa. Rekisteröidyllä on oikeus saada nämä tiedot maksutta kerran vuodessa. Mikäli edellisestä tarkastuspyynnöstä on kulunut aikaa alle vuosi, rekisterinpitäjä saa veloittaa rekisteröidyltä kohtuullisen korvauksen, joka ei saa kuitenkaan ylittää tiedon antamisesta koituvia välittömiä kuluja.

Tarkastusoikeuden rajoitukset

Rekisteröidyn tarkastusoikeutta on rajattu HetiL 27 §:ssä. Sen mukaan tarkastusoikeutta ei ole, jos esimerkiksi valtion turvallisuus tai valvontatehtävät vaarantuisivat.

Tarkastusoikeuden toteuttaminen

Tarkastusoikeutta käytetään rekisteröidyn omakätisesti allekirjoittamalla tai sitä vastaavalla tavalla varmennetulla asiakirjalla tai vaihtoehtoisesti henkilökohtaisesti rekisterinpitäjän luona. HetiL:n mukaan kyseinen asiakirja voidaan varmentaa myös sähköisesti.

Rekisterinpitäjän on ilman aiheetonta viivästystä varattava rekisteröidylle tilaisuus tutustua HetiL 26 §:ssä mainittuihin tietoihin. Tiedot on annettava rekisteröidylle ymmärrettävässä muodossa ja pyydettäessä kirjallisesti. Jos rekisterinpitäjä kieltäytyy antamasta tietoja, tästä on annettava kirjallinen todistus. Todistuksessa tulee mainita ne syyt joihin vedoten tietojen antamisesta on kieltäydytty.[43] Rekisterinpitäjän passiivisuus tarkastuspyyntöä kohtaan voidaan katsoa tiedonannosta kieltäytymiseksi. Rekisterinpitäjän kieltäytyessä tarkastusoikeuden toteuttamisesta, rekisteröity voi saattaa asian tietosuojavaltuutetun käsiteltäväksi.

Tiedon korjaaminen

Rekisterinpidon virheettömyysvaatimus edellyttää, ettei virheellisiä, epätäydellisiä tai vanhentuneita tietoja käsitellä. Rekisterinpitäjän on ilman aiheetonta viivytystä oma-aloitteisesti tai rekisteröidyn vaatimuksesta oikaistava, poistettava tai täydennettävä rekisterissä oleva, käsittelyn tarkoituksen kannalta virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto.[44]

Rekisteröidyllä on oikeus pyytää jotain yksittäistä itseään koskevaa tietoa mutta myös kaikkia itseään koskevia tietoja poistettavaksi rekisteristä, käsittelyn tarkoituksen kannalta virheellisinä tietoina. Poistopyyntöä ei tarvitse perustella. Mikäli peruste henkilötietojen käsittelylle on kuitenkin edelleen olemassa, palveluntarjoajalla ei ole velvollisuutta poistaa kyseisiä tietoja rekisteristä.[45]

Rekisterinpitäjän on estettävä virheellisen, tarpeettoman, puutteellisen tai vanhentuneen tiedon leviäminen, jos tieto voi vaarantaa rekisteröidyn yksityisyydensuojaa tai hänen oikeuksiaan.[46]

---

[43] HetiL 28 §.

[44] HetiL 29.1 §.

[45] HE 96/1998 vp., 29 §.

[46] HetiL 29.1 §.

Kun tieto on syystä tai toisesta korjattu, on tästä ilmoitettava sille, jolta rekisterinpitäjä on alun perin saanut henkilötiedot. Samoin tulee informoida niitä tahoja, joille rekisterinpitäjä on luovuttanut tietoja.[47]

2.1.6 Rekisteröidyn kielto-oikeus

Jos rekisteröity haluaa, ettei rekisterinpitäjä enää käsittele rekisteröidyn antamia tietoja, on tämän yleensä pyydettävä itseään koskevien tietojen poistamista henkilörekisteristä.[48]

Rekisteröidyllä on oikeus kieltää rekisterinpitäjää käsittelemästä itseään koskevia tietoja suoramainontaa, etämyyntiä ja muuta suoramarkkinointia varten.[49] Rekisteröityä tulee informoida kielto-oikeudestaan jo liittymis- eli tietojenantovaiheessa[50], sillä kielto-oikeutta tulee voida käyttää jo tietojenantovaiheessa.

Käsittelykiellosta seuraa, että suoramarkkinointirekisterin kyseessä ollessa kielto-oikeuttaan harjoittaneen tiedot on poistettava oma-aloitteisesti rekisteristä henkilötietojen käsittelyn tarkoituksen kannalta virheellisinä. Rekisteröidyn ei tarvitse perustella kieltoansa. Rekisterinpitäjä ei saa periä kiellon asettamisesta kuluja.

2.1.7 Henkilörekisterin hävittäminen

Tietojen tarpeellisuusvaatimuksen mukaan käsiteltävien henkilötietojen tulee olla määritellyn käsittelyn tarkoituksen kannalta tarpeellisia. Rekisterinpitäjän toiminnan kannalta tarpeettomat henkilötietorekisterit on hävitettävä.[51]

Rekisteriä ei saa säilyttää ainoastaan sillä perusteella, että sillä saattaa tulevaisuudessa olla käyttöarvoa.

Suunnitteluvelvoite koskee myös henkilörekisterin hävittämistä, joten käytettävä prosessi on suunniteltava jo ennakkoon rekisteriä perustettaessa. Hävittämisen tulee tapahtua siten, että pääsy tietoihin ei ole mahdollista enää kenellekään ulkopuoliselle.

2.1.8 Tietoturvaperiaatteet ja vaadittava tietoturvan taso

Rekisterinpitäjän tulee toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon:

- käytettävissä olevat tekniset mahdollisuudet;
- toimenpiteiden aiheuttamat kustannukset;

---

[47] HetiL 29.3 §.

[48] HetiL 29 §.

[49] HetiL 30 §.

[50] HetiL 24 §.

[51] HetiL 34 §.

- käsiteltävien tietojen laatu, määrä ja ikä; sekä
- käsittelyn merkitys yksityisyyden suojan kannalta.[52]

Rekisteri on suojattava niin, että laittomat yritykset päästä tunkeutumaan jo siihen laitteistoon, jossa henkilötietoja talletetaan, ja erityisesti yritykset päästä käsittelemään rekisterin tietoja, aiheuttavat ilman viiveitä hälytyksen rekisterinpitäjälle. Suojaus on tehtävä niin, että se antaa mahdollisuuksien mukaan tietoa laittoman yrityksen alkuperästä. Tietojen siirto on varmistettava erityisin toimenpitein, esimerkiksi siten, että siirto ei aiheuta muutoksia tietojen sisällössä ja että tietoja ei häviä siirron yhteydessä.[53] Käytännössä edellä mainittu vaatimus tarkoittaa tietoturvan suunnittelua, toteutusta ja ylläpitoa niin, että se antaa mahdollisuuksien mukaan tietoa laittomasta yrityksestä päästä tietojärjestelmään ja tietoa yrityksen alkuperästä. Tämä edellyttää vähintään palomuuri- ja järjestelmälokien käytön määrittämistä, lokitietojen tallentamista ja prosessia tai automaattista sovellusta lokien seuraamiseksi.[54]

HetiL:n lähtökohtana on se, että ensisijaisesti riittävän tietoturvatason määrittelee rekisterinpitäjä itse. Mikäli joku taho vaatii selvästi korkeampaa tietoturvan tasoa kuin henkilötiedot normaalisti edellyttäisivät, on tällaista vaativan tahon vastattava niistä kustannuksista, joita tietoturvan parantamisesta aiheutuu. On huomattava, että osa yhteisöistä ja yrityksistä saa tietoturvan tasosta erityismääräyksiä, jotka vaikuttavat myös henkilötietojen suojauksen tasoon.[55]

Riittävää tietoturvan tasoa ei ole kattavasti määritelty määrällisesti tai laadullisesti lain tasolla tai oikeustapausten perusteella. Lähtökohtana on, että rekisterinpitäjä itse arvioi tietoturvan tason riittävyyden. Käytännössä lienee niin, että mikäli olisi epäilystä tietoturvan tason riittävyydestä, vertailtaisiin yrityksen tietoturvaa saman toimialan yrityksiin, joilla on olemassa vastaavanlaisia henkilörekistereitä ja pyrittäisiin asiantuntijalausunnoin saamaan vertailuaineistoa analyysin perustaksi. Mikäli havaittaisiin olennaisia poikkeamia tietoturvan tasossa vertailuryhmään nähden, olisi mahdollista, että yritys joutuu vastuuseen tietoturvan hoitamisen laiminlyönnistä HetiL:n perusteella. Samanlainen arviointi voidaan suorittaa lain asettamien tietoturvavelvoitteiden osalta. Tällainen tilanne voisi realisoitua esimerkiksi tietomurron yhteydessä, jossa henkilötietoja on joutunut ulkopuolisille ja jossa joudutaan arvioimaan tietoturvan riittävyyttä.[56]

2.1.9 Tietoturvavelvoitteet ulkoistamistilanteissa

Sillä taholla, joka toimii rekisterinpitäjän lukuun itsenäisenä elinkeinonharjoittajana on velvollisuus antaa rekisterinpitäjälle ennen tietojen käsittelyyn ryhtymistä asianmukaiset sitoumukset ja muutoin riittävät takeet henkilötietojen

---

[52] HetiL 32 §. Ks. myös HE 96/1998 vp., 32 §.

[53] Ibid.

[54] Laaksonen – Nevasalo – Tomula 2006, s. 42.

[55] Finanssivalvonta (FIVA) antaa luottolaitoksille tarkempia määräyksiä pankkisalaisuuden piiriin kuuluvien tietojen suojaamisesta. Viestintävirasto antaa teleyrityksille määräyksiä tietoturvavelvoitteiden toteuttamisesta. Kaikki edellä mainittujen tahojen antamat ohjeet vaikuttavat vähintään välillisesti myös henkilörekisterien suojan tasoon.

[56] Laaksonen – Nevasalo – Tomula 2006, s. 45.

suojaamisesta.[57] Käytännössä tämä tarkoittaa erillisen sopimuksen laatimista osapuolten välille. Sopimuksessa on todettava henkilötietojen käsittelijän toimivan ainoastaan rekisterinpitäjän ohjeiden mukaisesti ja olevan velvollinen noudattamaan rekisterinpitäjälle säädettyjä rekisterin ja sen tietojen suojaamisvelvoitteita.[58]

Henkilörekisterin sisältävää tietojärjestelmää tai pelkkää henkilörekisteriä ulkoistettaessa, ulkoistajan tulee sopimusjärjestelyin varmistaa henkilötietojen käsittelyn lainmukaisuus ja tietoturva siten, että ulkoistuspalvelun tarjoaja sitoutuu noudattamaan vähintään HetiL 32.1 §:n vaatimuksia ulkoistuspalvelun toimituksessa. Ulkoistajan kannattaa jättää sopimuksessa itselleen mahdollisuus auditoida tai muulla tavoin varmistaa, että sopimusvelvoitteet muun muassa tietoturvan osalta on täytetty sopimuksen mukaisesti.[59]

Samat tietoturvavelvoitteet koskevat rekisterinpitäjän lukuun toimivaa tahoa eli esimerkiksi ulkoistamispalvelun tarjoajaa, joka hoitaa yrityksen tietojärjestelmien ylläpidon osapuolten välisen sopimuksen perusteella. Lopullinen vastuu tietoturvavelvoitteista on aina kuitenkin palvelun ostajalla (rekisterinpitäjällä) eikä rekisterinpitäjä voi siten ulkoistaa tietoturvaan liittyviä vastuita.[60]

2.1.10 Seuraamukset

HetiL:n määräysten vastaisesta menettelystä seuraamuksena voi olla rikosoikeudellinen rangaistus. Lisäksi lainvastaiseen menettelyyn syyllistynyt voi joutua vahingonkorvausoikeudelliseen vastuuseen.

HetiL:n 48.1 § sisältää viittaussäännöksen RL 38 ja 40 luvun säännöksiin, joissa säädetään rangaistus henkilörekisteririkoksesta, henkilörekisteriin sisältyvästä tietomurrosta ja HetiL:n 33 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta.

HetiL:n määräysten rikkomisesta on aina vastuussa rekisterinpitäjä.

Henkilörekisteririkoksia ovat muun muassa:

- henkilötietojen käsittely vastoin käyttötarkoitusta;
- käsittely vastoin yleisiä käsittelyedellytyksiä;
- tarpeettomien tai virheellisten tietojen käsittely;
- henkilötietojen siirto EU:n/ETA:n ulkopuolelle vastoin HetiL:n säännöksiä; ja
- rekisteröidyn tarkastusoikeuden laiminlyönti.

Henkilörekisteririkoksesta voidaan tuomita sakkoon tai vankeusrangaistukseen enintään vuodeksi.[61]

---

[57] HetiL 32.2 §.

[58] HE 96/1998 vp., 32 §.

[59] Laaksonen – Nevasalo – Tomula 2006, s. 46.

[60] Laaksonen – Nevasalo – Tomula 2006, s. 47.

[61] RL 38.9 §.

Rangaistavuuden edellytyksenä henkilörekisteririkoksen osalta on, että teko loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa.[62]

Salassapitorangaistuksesta eli vaitiolovelvollisuuden rikkomisesta voidaan RL 38.1 §:n mukaan tuomita henkilö sakkoon tai vankeuteen enintään yhdeksi vuodeksi, ellei muualla rikoslaissa säädetä ankarammasta rangaistuksesta. Salassapitorikkomuksesta voidaan tuomita sakkoihin.[63]

Lievemmistä teoista ja niiden seuraamuksista säädetään HetiL 48.2 §:ssä. Henkilörekisteririkkomuksesta voidaan tuomita sakkoihin, ellei muualla ole säädetty ankarammasta rangaistuksesta, henkilö joka tahallaan tai törkeästä huolimattomuudesta:

- laiminlyö noudattaa, mitä henkilötietojen käsittelyn tarkoitusten määrittelystä, rekisteriselosteen laatimisesta, tietojen käsittelystä, informoimisesta, henkilörekisterissä olevan tiedon korjaamisesta, rekisteröidyn kielto-oikeudesta tai ilmoituksen tekemisestä tietosuojavaltuutetulle säädetään;
- antaa tietosuojaviranomaiselle henkilötietojen käsittelyä koskevassa asiassa väärän tai harhaanjohtavan tiedon;
- rikkoo henkilötietojen suojaamisesta ja henkilörekisterin hävittämisestä annettuja säännöksiä ja määräyksiä; taikka
- rikkoo tietosuojalautakunnan HetiL 43.3 §:n nojalla antamaa lainvoimaista määräystä.

Rangaistavuuden lisäedellytyksenä on, että teko vaarantaa rekisteröidyn yksityisyydensuojaa tai hänen oikeuksiaan.

2.1.11 Vahingonkorvausvastuu

Nykyiseen lainsäädäntöön sisältyy huomattava määrä vahingonkorvaussäännöksiä, joiden mukainen vastuu on niin sanottua ankaraa vastuuta. Lainsäätäjä on päätynyt ankaran vastuun malliin myös HetiL:n kohdalla, ja lain vahingonkorvaussäännöksessä on säilytetty kumottuun henkilörekisterilakiin (30.4.1987/471) ja sen 42 §:ään sisältyvä rekisterinpitäjän tuottamuksesta riippumaton vahingonkorvausvastuu. Voimassaolevan sääntelyn perusteella muun muassa sellainen taloudellinen vahinko on korvattava, joka rekisteröidylle on aiheutunut virheellisen tiedon käytöstä tai luovutuksesta taikka siitä, että henkilötietojen käyttö tai luovutus on ollut lainvastaista. Vastuu on laissa ulotettu koskemaan myös kaikesta muusta laittomasta henkilötietojen käsittelystä aiheutuvaa taloudellista ja muuta vahinkoa. Vastuu kattaisi tällöin lain tarkoittamana muuna vahinkona myös henkilölle laittomasta käsittelystä aiheutuneen kärsimyksen.[64] Vahingonkorvauslain (31.5.1974/412) 5:6:n mukaan oikeus korvaukseen loukkauksen aiheuttamasta kärsimyksestä on muun muassa sillä, jonka kunniaa tai yksityiselämää on rangaistavaksi säädetyllä teolla loukattu.

---

[62] Ibid.

[63] RL 38.2 §.

[64] HE 96/1998 vp., 47 § sekä HetiL 47 §.

2.1.12 Olennainen oikeuskäytäntö

KHO 8.1.2010, taltionumero 15, Diaarinumero 1568/1/09

Korkeimman hallinto-oikeuden päätös niin sanotussa pikavippiasiassa.

Tapauksessa on kysymys X Oy:n käyttämän luotonhakijoiden tunnistamistavan henkilötietolain mukaisuudesta. Hyväksyttävät luotonhakijan tunnistamismenettelyt voivat vaihdella palvelualojen mukaan.

HetiL 1 §, 2 §, 5 §, 6 §, 9.2 §, 44 § 2-kohta

KHO 2009:82 / KHO 2007:9

Yhtiö julkaisi vuosittain yli miljoonan suomalaisen verotustiedot alueellisissa lehdissä ja luovutti tiedot edelleen toiselle yhtiölle tekstiviestipalvelun toteuttamista varten. Lehdissä julkaistuja tietoja luovutettiin maksua vastaan tekstiviestipalveluna. Korkeimman hallinto-oikeuden ratkaistavana oli kysymys siitä, oliko yhtiöiden toimintaa pidettävä yksityisyyden suojaa turvaavien henkilötietojen käsittelyä koskevien säännösten vastaisena. Korkeimman hallinto-oikeuden ratkaistavana ei ollut kysymys siitä, olivatko verotusta koskevat tiedot julkisia. Kysymys ei myöskään ollut oikeudesta julkaista näitä tietoja.

KHO 2007:9 välipäätös yllä mainittuun päätökseen KHO 2009:82 liittyen

Korkein hallinto-oikeus päätti tällä välipäätöksellä lykätä asian käsittelyä ja pyytää Euroopan yhteisöjen tuomioistuimelta Euroopan yhteisön perustamissopimuksen 234 artiklan nojalla ennakkoratkaisun henkilötietodirektiivin 95/46/EY tulkinnasta.

Tietosuojavaltuutetun valitettua korkeimmalle hallinto-oikeudelle hallinto-oikeuden päätöksestä, korkein hallinto-oikeus päätti esittää yhteisöjen tuomioistuimelle seuraavan EY 234 artiklassa tarkoitetun ennakkoratkaisupyynnön:

1. Onko direktiivin 95/46/EY 3 artiklan 1 kohdan tarkoittamana henkilötietojen käsittelynä pidettävä toimintaa, jossa luonnollisten henkilöiden ansio- ja pääomatulo- sekä varallisuustietoja:

a) kerätään veroviranomaisten julkisista asiakirjoista ja niitä käsitellään julkaisemista varten,

b) julkaistaan aakkosjärjestyksessä tuloluokittain laajoina kuntakohtaisina luetteloina painotuotteessa,

c) luovutetaan edelleen CD-ROM -levykkeellä käytettäväksi kaupallisessa tarkoituksessa,

d) käsitellään tekstiviestipalvelussa, jossa matkapuhelimen käyttäjät voivat ilmoittamalla henkilön nimen ja kotikunnan ja lähettämällä tekstiviestin määrättyyn numeroon saada paluuviestinä ilmoitetun henkilön ansio- ja pääomatulo- sekä varallisuustiedot.

2. Onko direktiiviä 95/46/EY tulkittava niin, että edellä 1 a - 1 d kohdissa mainittuja eri toimintoja voidaan pitää direktiivin 9 artiklan tarkoittamana ainoastaan journalistiseen tarkoitukseen toteutettavana henkilötietojen käsittelynä, kun otetaan huomioon, että tietoja on kerätty yli miljoonan verovelvollisen osalta kansallisen

julkisuuslainsäädännön nojalla julkisista tiedoista ja että toiminnan pääasiallisena tarkoituksena on mainittujen tietojen julkaiseminen?

3. Onko direktiiviä 95/46/EY tulkittava siten, että jäsenvaltion kansallisessa lainsäädännössä voidaan rajata kaikki direktiivin 9 artiklassa mainitut direktiivin määräykset ja erityisesti direktiivin II luvun tiedon laatua koskevat vaatimukset kokonaan sovellettavien säännösten ulkopuolelle direktiivin artiklan tarkoittamien journalististen henkilörekisterien osalta?

4. Voidaanko direktiiviä 95/46/EY tulkita siten, että sen soveltamisalan ulkopuolelle jäävät kokonaan sellaiset henkilörekisterit, jotka sisältävät vain tiedotusvälineissä julkaistua aineistoa sellaisenaan?

Saatuaan Euroopan yhteisöjen tuomioistuimelta ennakkoratkaisun tietosuojadirektiivin tulkinnasta korkein hallinto-oikeus katsoi päätöksellään KHO 2009:82, ettei HetiL 2.4 §:a voitu tulkita siten, että kertaalleen julkaistuja henkilötietoja voitaisiin yksin julkaisemisen perusteella yleisesti käsitellä uudelleen, eri yhteyksissä ja eri tarkoituksessa henkilötietojen käsittelyä koskevien säännösten millään tavoin toimintaa rajoittamatta. Edelleen yhteisöjen tuomioistuimen ennakkoratkaisu huomioon ottaen korkein hallinto-oikeus katsoi, ettei henkilötietojen käsittely yhtiöiden toiminnassa ollut tapahtunut HetiL 2.5 §:n tarkoittamalla tavalla toimituksellisessa tarkoituksessa. Tietosuojavaltuutetun valituksesta korkein hallinto-oikeus kumosi hallinto-oikeuden ja tietosuojalautakunnan päätökset ja palautti asian tietosuojalautakuntaan uudelleen käsiteltäväksi HetiL 44 §:ssä tarkoitettujen määräysten antamiseksi yhtiöille.

HetiL 1 §, 2.4-5 §, 3 §, 17 §, 32 §, 44 §
PL 10.1 § ja 12.1 §
Henkilötietodirektiivi 95/46/EY

2.2 Sähköisen viestinnän tietosuojalaki (16.6.2004/516)

2.2.1 Lain tausta, tarkoitus ja soveltamisala

SVTSL:n tarkoituksena on turvata PL:ssa säädettyjen luottamuksellisen viestin ja yksityisyyden suojan toteutuminen sähköisessä viestinnässä sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.[65]

SVTSL:lla on pyritty selkeyttämään luottamuksellisten tunnistamistietojen käsittelysääntöjä ja ne ulotetaan yhteisötilaajaan. Lisäksi lain tavoitteena on selkeyttää tietoturvan toteuttamismahdollisuuksia ja antaa pelisäännöt evästeiden käytölle sekä paikkatietojen käsittelylle. Lailla halutaan lisätä sähköisen viestinnän tietoturvaa ja tietosuojaa sekä lisätä käyttäjien luottamusta siihen. Lain ja sen nojalla annettujen määräysten noudattamista valvoo pääasiassa Viestintävirasto kun taas muun muassa paikkatietojen käsittelyä ja automatisoitujen järjestelmien avulla tapahtuvaa suoramarkkinointia koskevien säädösten noudattamista valvoo tietosuojavaltuutettu.[66]

---

[65] HE 125/2003 vp.

[66] Tietoturvaopas sähköisen palvelun tarjoajalle, Luoti-julkaisuja 8/2006, s. 15. Verkkojulkaisu saatavilla osoitteessa URL: <http://www.lvm.fi/fileserver/8_2006.pdf>

Valtaosa SVTSL:n säännöksistä kohdistuu viestinnän välittäjiin, joita ovat teleyritykset ja yhteisötilaajat. Nämä tahot ovat sivullisia suhteessa viestinnän osapuoliin, jolla tarkoitetaan käytännössä viestin lähettäjää ja vastaanottajaa. SVTSL koskettaa lähes kaikkia yrityksiä, koska lähtökohtaisesti jokainen yritys käsittelee viestintäverkossaan (esimerkiksi puhelin- tai tietoverkossa) työntekijöidensä (käyttäjien) tunnistamistietoja tai luottamuksellisia viestejä. Erityisesti laki koskettaa teleyrityksiä sekä yrityksiä silloin, kun ne eivät ole viestinnän osapuolena vaan yhteisötilaajana.[67] Esimerkki tällaisesta tilanteesta on työntekijän lähettämä yksityinen viesti, joka välitetään yrityksen tietojärjestelmien kautta vastaanottajalle.

SVTSL:ää sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin ja palveluihin, joissa käsitellään palvelun käyttöä kuvaavia tietoja.[68] Lisäksi lakia sovelletaan suoramarkkinointiin yleisissä viestintäverkoissa sekä tilaajaluettelopalveluihin ja numerotiedotuspalveluihin. Hallituksen esityksen mukaan näin ilmaistaan soveltamisalan pääsääntö, jonka mukaan soveltamisala rajoittuu yleisiin viestintäverkkoihin, joita tarjotaan etukäteen rajaamattomalle käyttäjäpiirille. Verkkopalvelulla ja viestintäpalvelulla tarkoitetaan samaa kuin vastaavilla käsitteillä VML:ssa.[69] Laissa tarkoitettuihin lisäarvopalveluihin kuuluvat pääasiassa paikkatietoihin perustuvat palvelut.[70] Tältä osin soveltamisala vastaa sähköisen viestinnän tietosuojadirektiiviä.

SVTSL:ia ei sovelleta sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, ellei näitä verkkoja ole liitetty yleiseen viestintäverkkoon.[71] Viestin, tunnistamistietojen ja paikkatietojen luottamuksellisuutta, vaitiolovelvollisuutta ja hyväksikäyttövelvollisuutta sovelletaan kuitenkin myös sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, vaikka näitä verkkoja ei ole liitetty yleiseen viestintäverkkoon.[72]

Henkilötietojen käsittelyyn sovelletaan, mitä HetiL:ssa säädetään, jollei laista muuta johdu.[73] Toisin sanoen SVTSL on luonnolliseen henkilöön yhdistettävien tietojen osalta erityislaki suhteessa HetiL:iin. Tämä tarkoittaa sitä, että sen lisäksi, mitä SVTSL:ssä, lain soveltamisalaan kuuluvilla toimijoilla on henkilötietojen käsittelyssä ne velvollisuudet, jotka rekisterinpitäjälle säädetään HetiL:ssa. HetiL tulee

---

[67] Yhteistötilaajan käsite on SVTSL:ssa käytetty käsite, joka määritellään SVTSL 2:1.11:ssä viestintäpalvelun tai lisäarvopalvelun tilaajana olevaksi yritykseksi tai yhteisöksi, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja.

[68] SVTSL 3.1 §.

[69] SVTSL 2.1 §:n 5–6 -kohtien määritelmän mukaan *verkkopalvelulla* teleyrityksen toteuttamaa viestintäverkon tarjoamista käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon etukäteen rajoittamattomalle käyttäjäpiirille ja *viestintäpalvelulla* sellaista teleyrityksen toteuttamaa viestien siirtämistä, jakelemista tai tarjolla pitämistä viestintäverkossa, jota tarjotaan etukäteen rajoittamattomalle käyttäjäpiirille. *Viestintäverkon* ja *yleisen viestintäverkon* käsitteet on määritelty SVTSL 2.1 §:ien 2–3 -kohdissa VML:a vastaavalla tavalla. SVTSL 2.1 §:n 1-kohdassa on VML:sta poiketen määritelty myös *viestin* käsite.

[70] SVTSL 2.1 § 7-kohdan määritelmän mukaan *lisäarvopalvelulla* tarkoitetaan palvelua, joka perustuu tunnistamistietojen tai paikkatietojen käsittelyyn muuta tarkoitusta kuin verkkopalvelun tai viestintäpalvelun toteuttamista varten.

[71] SVTSL 3.2 §.

[72] SVTSL 4–5 § sekä SVTSL 3.3 §.

[73] SVTSL 3.4 §.

sovellettavaksi luonnollisiin henkilöihin liitettävien tietojen osalta erityisesti yleisistä viestintäverkoista erillään olevissa sisäisissä viestintäverkoissa, joihin SVTSL:a sovelletaan vain hyvin rajoitetusti.[74]

Työnantajan ja työntekijän välisessä suhteessa sovelletaan lisäksi, mitä säädetään yksityisyyden suojasta työelämässä annetussa laissa.[75] SVTSL:ia ei sovelleta joukkoviestintäverkossa välitettävään viestiin, jos viestiä ei voi yksittäisessä tapauksessa yhdistää sitä vastaanottavaan tilaajaan tai käyttäjään.[76] Digitaalisten tv-lähetysten aikakaudella, kun käyttäjä voi esimerkiksi Internet-yhteyden kautta vaikuttaa lähetettäviin (kuluttajan näkökulmasta tilattaviin) ohjelmisto- tai muihin sisältöihin saattaa palveluntarjoajalle jäädä tällöin tunnistamistietoja, jotka ovat yksittäistapauksissa yhdistettävissä käyttäjään. Tällöin SVTSL:n säännökset soveltuvat.[77]

Lakia ei sovelleta viranomaistoimintaan VML:ssa tarkoitetussa viranomaisverkossa tai muussa yleiseen järjestykseen ja turvallisuuteen, maanpuolustukseen, pelastustehtäviin, väestönsuojeluun tai maaliikenteen, meriliikenteen, raideliikenteen taikka ilmaliikenteen turvallisuuteen liittyvien tarpeiden vuoksi rakennetussa viestintäverkossa. Lakia ei sovelleta myöskään, jos laista rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008) muuta johtuu.[78]

2.2.2 Yksityisyyden ja luottamuksellisen viestin suoja

Viesti, tunnistamistiedot ja paikkatiedot ovat luottamuksellisia, jollei SVTSL:ssa tai muussa laissa toisin säädetä.[79] Luottamuksellisuus koskee myös verkkosivustojen selaamisesta kertyviä tunnistamistietoja.[80] Viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi.[81] Viestiin liittyvät tunnistamistiedot ovat kuitenkin tällöinkin luottamuksellisia.

Luottamuksellisuus tarkoittaa sitä, että viestejä, tunnistamistietoja ja paikkatietoja saa käsitellä vain erikseen laissa säädettyihin tarkoituksiin. Säännös antaa suojaa kaikille viesteille, jotka viestintäverkoissa liikkuvat. Luottamuksellisuutta ei ole rajattu tiettyjen osapuolten väliseen viestintään, joten myös koneiden välinen viestintä on luottamuksellista. Etukäteen maksettujen puheaikakorttien liittymät eli niin sanotut prepaid-liittymät saavat myös sekä viestin että tunnistamistietojen luottamuksellisuuden suojan. Vaikka prepaid-liittymästä ei välttämättä voidakaan tunnistaa sen käyttäjää, on tällaisella liittymällä aina tilaaja, johon liittymä voidaan yhdistää.[82]

---

[74] Helopuro – Perttula – Ristola 2009, s. 8.

[75] SVTSL 3.5 §.

[76] SVTSL 3.6 §.

[77] Viemerö 2009, s. 129.

[78] SVTSL 3.7–8 §.

[79] SVTSL 4.1 §.

[80] SVTSL 4.3 §.

[81] SVTSL 4.2 §.

[82] HE 125/2003 vp.

Arvioitaessa viestin luottamuksellisuutta keskeistä on se, onko viestin lähettäjä saattanut viestin yleisesti vastaanotettavaksi, esimerkiksi keskustelupalstalle tai mielipidepalstalle. Jos lähettäjä ei ole saattanut viestiä yleisesti vastaanotettavaksi, viestin oletetaan olevan luottamuksellinen, ja samalla myös siihen liittyvät tunnistamistiedot ovat luottamuksellisia. Vastaanottajien lukumäärällä ei ole merkitystä tarkasteltaessa viestin luottamuksellisuutta. Esimerkiksi useammalle henkilölle lähetettyä sähköpostia voidaan pitää luottamuksellisena, jos sitä ei ole saatettu yleisesti vastaanotettavaksi. Esimerkiksi viesti, joka lähetetään Internetin uutisryhmiin, on saatettu kenen tahansa ulottuville. Erilaisten uutisryhmien ja keskustelupalstojen pitäjille jää mahdollisuus julkaista myös viestin tunnistamistiedot tai jättää ne julkaisematta, kuten perinteisessä muodossa lehtien keskustelupalstoilla tapahtuvassa joukkoviestinnässä. Sen sijaan esimerkiksi neuvottelupuhelut, videokonferenssit ja Internetissä käytävät kahdenkeskiset keskustelut ovat luottamuksellisia, jos viestintään osallistumista on rajoitettu.[83]

Se, joka on ottanut vastaan tai muutoin saanut tiedon luottamuksellisesta viestistä tai tunnistamistiedosta, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä, tunnistamistietoa tai tietoa viestin olemassaolosta, ellei laissa toisin säädetä.[84] Kyseessä on tilanne, jossa luottamuksellisen viestin on saanut muu kuin vastaanottajaksi tarkoitettu henkilö, mutta hän ei ole sitä itse aktiivisesti toimien saanut ja hänen tarkoituksenaan ei ole ollut hankkia tietoa viestistä, sen olemassaolosta tai siihen liittyvistä tunnistamistiedoista. Kyseessä voi siten olla esimerkiksi erehdyksissä saatu viesti. Tällöin viestin saaneelle syntyy vaitiolovelvollisuus viestistä ja tunnistamistiedoista.[85]

SVTSL sisältää erityisen vaitiolovelvollisuuden sellaisille toimijoille, joiden katsotaan käsittelevän siinä määrin luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja, että näiden tietojen joutuminen vääriin käsiin olisi yksityisyyden suojan ja luottamuksellisen viestinnän kannalta merkittävä uhka.[86] Erityinen vaitiolovelvollisuus koskee niitä, jotka ovat teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai VML:n 137 §:ssä tarkoitetun teleurakoitsijan palveluksessa tehtäviään hoitaessaan saaneet tietoja viesteistä ja tunnistamistiedoista sekä paikkatiedoista.[87] Edellä tarkoitettu vaitiolovelvollisuus on myös sillä, joka toimii tai on toiminut teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan tai teleurakoitsijan lukuun.[88]

2.2.3 Velvollisuus huolehtia tietoturvasta

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa

[83] HE 125/2003 vp.

[84] SVTSL 5.1 §.

[85] HE 125/2003 vp.

[86] SVTSL 5.3 §.

[87] HE 125/2003 vp.

[88] SVTSL 5.4 §.

muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.[89]

Määritelmä tarkoittaa tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamista hallinnollisin ja teknisin toimin. Näitä tietoturvatoimia ovat esimerkiksi laitteille ja järjestelmiin pääsynvalvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta.

Tietoturvatoimia ovat tietoliikenteen häirinnän valvonta ja sen estäminen. Kyseinen yleinen määrittely vastaa siten tarkoitukseltaan HetiL:n 32 §:n tarkoitusta. Tietoturvatoimenpiteillä tulee suojata sekä viestinnän luottamuksellisuutta että kansalaisten yksityisyyden suojaa että sananvapautta.

Teleyrityksen ja lisäarvopalvelun tarjoajalla on velvollisuus huolehtia palvelujensa tietoturvasta.[90] Yhteisötilaajan on huolehdittava käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Palvelun ja käsittelyn tietoturvasta huolehtiminen tarkoittaa toimia toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Tätä tietoturvasta huolehtimisen sisällöllistä jaottelua edellytti eduskunnan perustuslakivaliokunta sähköisen viestinnän tietosuojalakiesityksestä antamassaan lausunnossa (PeVL 9/2004 vp.). Nämä toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Toiminnan turvallisuudella tarkoitetaan muun muassa sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan.[91] Lisäksi toiminnan turvallisuudella tarkoitetaan sitä, että pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan.

Tietoliikenneturvallisuudella tarkoitetaan muun muassa sitä, että viestintäverkkojen avulla välitettävät viestit ja tunnistamistiedot eivät paljastu asiaankuulumattomille ja asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä. Lisäksi tietoliikenneturvallisuudella tarkoitetaan sitä, että viestintäverkoissa on toiminnan kannalta riittävät todentamismenettelyt, pääsynvalvontamenettelyt ja kiistämättömyysmenettelyt, ja että asiaankuulumattomat eivät pääse tunnistamistietoihin tai käsittelyä koskeviin tietoihin.

Laitteistoturvallisuudella ja ohjelmistoturvallisuudella tarkoitetaan muun muassa sitä, että käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen sekä järjestetään toiminnan kannalta tärkeiden

[89] SVTSL 2.1 § 13-kohta.

[90] SVTSL 19 §.

[91] HE 125/2003 vp.

ohjelmistojen varmuuskopiointi ja turvallinen säilytys. *Tietoaineistoturvallisuudella* tarkoitetaan muun muassa sitä, että järjestetään tietoaineistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti, järjestetään tietoaineistojen varmuuskopiointi ja turvallinen säilytys sekä suojataan tärkeät asiakirjat, tietovarastot ja yksittäiset tiedot.

Toimet tietoturvasta huolehtimiseksi on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.[92] Vaatimus tarkoittaa sitä, että tiedossa oleviin uhkiin tulee varautua uskottavin tietoturvatoimin, mutta toisaalta myös sitä, ettei normaalin toiminnan kannalta kohtuuttomia kustannuksia edellytetä käytettäväksi toimien toteuttamisessa.[93]

SVTSL:n 19 §:n avulla on implementoitu sähköisen viestinnän tietosuojadirektiivin 4 artiklan 1 kohta, jonka mukaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen tarjoamiensa palvelujen turvallisuuden, verkon turvallisuuden osalta tarvittaessa yhdessä yleisen viestintäverkon tarjoajan kanssa. Näillä toimenpiteillä on voitava varmistaa riskiin suhteutettu turvallisuustaso ottaen huomioon uusin tekniikka ja toimenpiteiden käyttöönottokustannukset. Teknisten turvatoimenpiteiden tulee olla ajan ja teknologian tasolla sekä henkilökunnan tulee olla koulutettu käyttämään tätä teknologiaa.[94]

Teleyritys ja lisäarvopalvelun tarjoaja vastaa tilaajille ja käyttäjille tarkoitetusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun.[95] Ulkoistettu riski on hoitamattomana vähintään yhtä suuri kuin oma riski, joten on pystyttävä seuraamaan myös mahdollisen alihankkijan toimintaa ja varmistumaan sen tietoturvallisuuden riittävästä tasosta. Sama koskee tilanteita, joissa palvelu toteutetaan monen eri yrityksen yhteistyönä.[96]

2.2.4 Toimenpiteet tietoturvan toteuttamiseksi

Toimenpiteitä tietoturvan toteuttamiseksi koskevan SVTSL 20 §:n muutokset tulivat voimaan 13. maaliskuuta 2009. Pykälässä säädetään teleyritysten, lisäarvopalvelun tarjoajien ja yhteisötilaajien oikeuksista toimenpiteisiin tietoturvasta huolehtimiseksi. Säännös mahdollistaa viestintäverkkojen sekä niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemisen, estämisen, selvittämisen ja esitutkintaan saattamisen.[97]

Teleyrityksellä, lisäarvopalvelun tarjoajalla ja yhteisötilaajalla sekä niiden lukuun toimivalla on oikeus ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi: 1) viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi; 2) viestin lähettäjän tai viestin vastaanottajan

[92] SVTSL 19 §.

[93] Helopuro – Perttula – Ristola 2009, s. 195.

[94] Viemerö 2009, s. 182.

[95] SVTSL 19.2 §.

[96] Viemerö 2009, s. 183 ja Hakala – Vainio – Vuorinen 2006, s. 90.

[97] HE 48/2008 vp.

viestintämahdollisuuksien turvaamiseksi; tai 3) viestintäpalvelujen kautta laajamittaisesti toteutettavien RL:n 37:11:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.[98]

Tietoturvalle haittaa aiheuttavia häiriöitä ovat esimerkiksi tahallisten haittaohjelmien laaja levittäminen ja käyttö. Kohdassa tarkoitettuja häiriöitä ovat myös viestintäverkon käyttö ei-toivottujen suoramarkkinointiviestien lähettämiseen tai tällaisten viestien laajamittainen saapuminen viestintäverkkoon taikka muiden viestien käyttö tietoliikenteen tai tietojärjestelmien lamauttamiseen taikka muut viestintäverkon tai siihen liitetyn palvelun toimintakyvyn kannalta hyvin vakavat häiriöt. Myös tilanteet, joissa viestintäverkon normaali toiminta häiriintyy muilla tavoin, taikka joissa luvatta tuhotaan tai muutetaan koneisiin tallennettuja tietoja, voivat olla tällaisia haittaa aiheuttavia häiriöitä.[99]

Viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamisella on haluttu turvata myös yksittäisen käyttäjän asema ja viestintämahdollisuudet, koska ei-toivottujen suoramarkkinointiviestien ja muiden vastaavien viestien loppukäyttäjälle tuleva määrä voi nousta niin korkeaksi, että hänen viestintämahdollisuutensa estyvät kokonaan, vaikka tällaisten viestien määrä ei vaikuttaisikaan koko viestintäverkon tai -palvelun toimintaan. Viittauksessa RL:iin on kyse niin sanotusta "phishingistä", eli suurelle käyttäjäjoukolle toimitettavista viesteistä, joilla pyritään urkkimaan käyttäjien identiteetti- ja maksuvälinetietojen hankkimista laittomiin käyttötarkoituksiin.[100]

Toimenpiteet, joilla tietoturvasta huolehtimiseen pyritään, voivat käsittää: 1) viestin automaattisen sisällöllisen analyysin; 2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen; 3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä; sekä 4) muut näihin rinnastettavat *teknisluonteiset toimenpiteet*.[101] Toimet voivat kohdistua itse viestien lisäksi myös niiden mahdollisiin liitteisiin.[102]

Uudistettu SVTSL antaa teleyritykselle, yhteisötilaajalle ja lisäarvopalvelun tarjoajalle oikeuden käsitellä yksittäisen viestin sisältöä myös manuaalisesti, jos on ilmeistä, ettei automaattisen tietojenkäsittelyn avulla pystytä turvaamaan edellä mainittujen tavoitteiden toteutumista.[103] Laki oikeuttaa viestin sisällön manuaaliseen tarkastamiseen vakavissa uhkatilanteissa, joissa viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn, eikä automaattinen sisällöllinen analyysi riitä tietoturvan takaamiseen.[104] Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, ellei ilmoittamisella todennäköisesti vaaranneta edellä mainittujen tavoitteiden toteutumista.

---

[98] SVTSL 20.1 §.

[99] HE 48/2008 vp.

[100] HE 48/2008 vp.

[101] SVTSL 20 §.

[102] HE 48/2008 vp.

[103] SVTSL 20.3 §.

[104] SVTSL 20.3 §.

Toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole edellytyksiä.

Tietoturvailmoitus

Teleyrityksen ja lisäarvopalvelun tarjoajan on ilmoitettava tietoturvauhkasta viipymättä tilaajalle ja kerrottava samalla tilaajan ja käyttäjän käytettävissä olevista toimenpiteistä uhkan torjumiseksi sekä niiden todennäköisistä kustannuksista.[105] Kuluttajansuojalain (20.1.1978/38; "KSL") mukaan palveluntarjoajan täytyy informoida kuluttajia palvelujensa vaarallisuudesta, eli käytännössä tietoturvan kannalta teleyrityksen ja lisäarvopalvelun tarjoajan olisi annettava kuluttajalle tietoa esimerkiksi asianmukaisen tietoturvan toteuttamisesta sekä palvelun käyttöön liittyvistä tietoturvariskeistä. Palveluntarjoaja saa viivyttää ilmoitusta, mikäli uhka on vakava ja on olemassa riski siitä, että tietoturva-aukkoa pyrittäisiin hyväksikäyttämään. Näissä tilanteissa on pyrittävä ensisijaisesti tietoturva-aukon korjaamiseen ennen ilmoitusta käyttäjille.

Teleyritykset ovat velvollisia ilmoittamaan havaitsemistaan vakavista tietoturvaloukkauksista ja tietoturvauhkista myös Viestintävirastolle. Viestintävirastolle on niin ikään ilmoitettava niistä toimenpiteistä, joilla tietoturvaloukkausten ja niiden uhkien toistuminen pyritään estämään. Viestintäviraston määräyksessä 9 D/2009 M on tarkemmin määritelty tietoturvailmoituksen vaadittu sisältö.

2.2.5 Tunnistamistietojen käsittely

Tunnistamistiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.[106] Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat muun muassa viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Tiedot voivat myös koskea muotoa, jossa viesti välitetään verkossa. Olennaista on, että näiden tietojen tulee olla yhdistettävissä tilaajaan tai käyttäjään. Tunnistamistiedon käsitteen kannalta on huomattava, että tilaaja, johon tunnistamistieto voidaan yhdistää, voi olla luonnollisen henkilön lisäksi myös oikeushenkilö, kuten yritys.[107]

Viestin lähettäjä tai se, jolle viesti on tarkoitettu, voi käsitellä omia viestejään ja niihin liittyviä tunnistamistietoja, jollei toisin ole säädetty.[108] Viestin osapuoli voi olla sekä luonnollinen henkilö että oikeushenkilö. SVTSL:n 9-14 § sisältää ne perusteet, joilla tunnistamistietojen käsittely on laillista viestinnän osapuoliin nähden sivullisille. Tunnistamistietojen käsittelyn on oltava luvallista, jotta viestintäpalveluita on

[105] SVTSL 21 §.

[106] SVTSL 21.8 §.

[107] HE 125/2003 vp.

[108] SVTSL 8 §.

ylipäätään mahdollista toteuttaa. Tunnistamistietojen käsittelyn täydellisellä kieltämisellä rajoitettaisiin liian raskaasti palveluntarjoajien elinkeinonharjoittamisvapautta, joskin yksityisyys- ja tietosuojanäkökohdat huomioon ottaen tunnistamistietojen käsittelyn on oltava myös säänneltyä. [109]

Tunnistamistietojen käsittely, esimerkiksi tietojen luovutus, on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa sekä pelkästään sen ajan, joka tarvitaan tietyn tarkoituksen toteuttamiseen. Tunnistamistietojen käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voida yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä. Laskutustietoja tulee poikkeuksellisesti säilyttää pidempään, vähintään kolme kuukautta eräpäivästä tai tunnistamistiedon tallennuspäivästä riippuen siitä, kumpi on myöhempi. Tunnistamistietoja on sallittua luovuttaa ainoastaan niille tahoille, joilla on oikeus käsitellä tietoja sekä ainoastaan käyttötarkoituksen sallimassa laajuudessa.[110]

Käsittely palvelun toteuttamiseksi ja käyttämiseksi

Tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä näiden tietoturvasta huolehtimiseksi.[111] Laki antaa myös yleisen käsittelyoikeuden verkkopalvelun, viestintäpalvelun ja lisäarvopalvelun tietoturvasta huolehtimiseksi. Esimerkiksi lokitietojen säilyttäminen voidaan katsoa olevan välttämätöntä järjestelmän toiminnan varmistamiseksi.[112] Tiedot on tuhottava tai muutettava anonyymeiksi niiden muuttuessa tarpeettomiksi.

Tunnistamistietoja saa käsitellä vain teleyrityksen, lisäarvopalvelun tarjoajan ja yhteisötilaajan palveluksessa oleva sekä näiden lukuun toimiva luonnollinen henkilö, jonka tehtävänä on käsitellä tietoja lain 9-14 §:ssä erikseen säädettyjen tarkoitusten toteuttamiseksi. Käsittely tulee rajata vain tiettyyn henkilöpiiriin, jotta voidaan varmistua viestinnän luottamuksellisuudesta ja yksityisyyden suojasta. Käsittely on lisäksi rajattava tietojen käyttötarkoituksen toteuttamiseen. Organisaatiossa on tämän lisäksi osoitettava vastuuhenkilö, joka vastaa palvelun toteuttamisesta ja tunnistamistietojen käsittelystä, vaikka tietojenkäsittely suoritettaisiin koneellisesti. [113]

Käsittely laskutusta varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä keskinäisten maksujensa määrittämistä ja laskutusta varten tarvittavia tunnistamistietoja.[114] Lisäksi voidaan käsitellä palveluista perittävien maksujen määrittämiseksi tai laskujen perimiseksi välttämättömiä tunnistamistietoja. Yhteisötilaaja voi käsitellä sisäistä laskutusta varten välttämättömiä tunnistamistietoja. Tilaajalle tai käyttäjällä on näissä tilanteissa kuitenkin ilmoitettava, millaisia tunnistamistietoja käsitellään ja kuinka kauan käsittely kestää.

---

[109] Viemerö 2009, s. 140.

[110] Viemerö 2009, s. 140.

[111] SVTSL 9 §.

[112] Lokitiedoista ks. VAHTI 3/2009 – Lokiohje.

[113] SVTSL 9 §.

[114] SVTSL 10 §.

Tietoyhteiskunnan palvelun tarjoaja voi käsitellä teleyrityksen hallinnoiman viestintäverkon välityksellä tarjottavien kuvatallenteiden, äänitallenteiden ja muiden maksullisten palvelujensa laskutusta varten välttämättömiä tunnistamistietoja ja muita laskutuksen kannalta välttämättömiä tietoja, jos tilaaja tai käyttäjä, jota tiedot koskevat, on antanut siihen suostumuksensa. Tällaisia palveluja ovat esimerkiksi matkapuhelimeen tilattu musiikki, soittoäänet ja videot. Mainitunlainen palveluntarjoaja saa toteuttaa laskutuksen itsenäiseksi tunnistustietoja käsittelemällä.[115] Tietojen luovutukseen on kuitenkin saatava tilaajan tai käyttäjän suostumus, jota tiedot koskevat.

Vaikka tunnistamistietoja ei yleisesti saa säilyttää yli sen ajan, joka on välttämätöntä palvelun tarjoamiseksi, on laskun määräytymiseen liittyviä tietoja säilytettävä vähintään kolme kuukautta laskun eräpäivästä tai tunnistamistiedon tallentumisesta riippuen siitä, kumpi näistä ajankohdista on myöhäisempi. Tietoja ei saa säilyttää enää sen jälkeen, kun saatava on velan vanhentumisesta annetun lain mukaan vanhentunut. Lisäksi mikäli laskusta syntyy erimielisyys, tulee sitä koskevat tiedot säilyttää siihen saakka, kunnes asia on sovittu tai ratkaistu.[116]

Käsittely markkinointia varten

Teleyritys voi viestintäpalvelujen tai lisäarvopalvelujen markkinoimiseksi käsitellä tunnistamistietoja siinä määrin ja niin kauan kuin tällainen markkinointi sitä edellyttää, mikäli tilaaja tai käyttäjä on antanut siihen nimenomaisen suostumuksensa. Palveluntarjoajan on ilmoitettava ennen suostumuksen pyytämistä millaisia ja kuinka kauan tunnistamistietoja markkinoinnissa käsitellään. Käyttäjälle tai tilaajalle on lisäksi annettava mahdollisuus perua käsittelyä koskeva suostumuksensa missä tahansa vaiheessa.[117]

Käsittely teknistä kehittämistä varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun teknistä kehittämistä varten. Yhteisötilaaja voi käsitellä tunnistamistietoja oman viestintäverkkonsa ja siihen liitetyn oman palvelunsa teknistä kehittämistä varten.[118] Teknisellä kehittämisellä voidaan tarkoittaa esimerkiksi suorituskyvyn parantamista tai käytettävyyden lisäämistä. Käsittely on sallittua ainoastaan toimien vaatimassa laajuudessa ja se on toteutettava luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta.[119]

Tunnistamistietojen käsittelyä teknistä kehittämistä varten on käyttäjälle tai tilaajalle ilmoitettava ennen käsittelyn aloittamista, millaisia tunnistamistietoja käsitellään ja kuinka kauan käsittely kestää. Ilmoitus voidaan antaa joko tilaajalle tai käyttäjällä, esimerkiksi liittymäsopimuksessa tai palveluntarjoajan kotisivuilla.[120]

---

[115] SVTSL 10 §.

[116] SVTSL 10.5 §.

[117] SVTSL 11 §.

[118] SVTSL 12 §.

[119] HE 125/2003 vp.

[120] SVTSL 12 §.

Informointivelvollisuus koskee ainoastaan teleyrityksiä ja lisäarvopalvelun tarjoajia, eikä sitä voida katsoa erityisen vahvaksi.

Käsittely tilastollista analyysiä varten

Teleyritys, yhteisötilaaja ja lisäarvopalvelun tarjoaja voi käsitellä viestintäverkkonsa tai siihen liitetyn palvelunsa tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten, jos analyysiä ei voida muuten tuottaa ilman kohtuutonta vaivaa eikä analyysistä voida tunnistaa yksittäistä luonnollista henkilöä. Tilastollista analyysiä varten saa käsitellä myös tietoja, joista tilaaja tai käyttäjä voidaan tunnistaa. On kuitenkin huolehdittava siitä, ettei lopullisesta analyysistä voida yksittäistä luonnollista henkilöä tunnistaa. Analyysi on lisäksi suoritettava automaattisen tietojenkäsittelyn avulla, ei manuaalisesti.[121]

Käsittely väärinkäytöstapauksissa

Teleyritys, yhteisötilaaja ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun maksullisen palvelun käyttöä maksutta tai muiden siihen rinnastuvien käyttöä koskevien väärinkäytösten havaitsemiseksi, estämiseksi, selvittämiseksi sekä esitutkintaan saattamiseksi.[122]

Esimerkkejä väärinkäytöstilanteista ovat tilanteet, joilla pyritään luvatta käyttämään tietoverkoissa olevia resursseja, häiritään tietoverkon normaalia toimintaa tai luvatta tuhotaan tai muutetaan koneisiin talletettuja tietoja.[123] Palveluntarjoaja voi näissä tilanteissa tunnistamistietojen avulla selvittää, mitkä tahot väärinkäytöksiin syyllistyvät.

Käsittely teknisen vian tai virheen havaitsemiseksi

Teleyritys, lisäarvopalvelun tarjoaja ja yhteisötilaaja voi käsitellä tunnistamistietoja, jos se on tarpeen viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi.[124] Tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen jonka jälkeen ne on hävitettävä. Koska palvelun toteuttamisessa on usein osallisena useampi taho, edellyttää vian tai virheen selvittäminen ja korjaaminen näiden tahojen yhteistyötä. Tunnistamistietojen luovutus tulisi tämän johdosta olla mahdollista tahojen kesken. Tietojen luovutus on tehtävä siten, ettei luottamuksellisen viestin tai yksityisyyden suoja tarpeettomasti vaarannu. Lisäksi tietojen luovutus voi tapahtua ainoastaan niille tahoille, joilla on oikeus käsitellä tunnistamistietoja kyseisessä tilanteessa.[125]

Käsittelyä koskevien tietojen tallentaminen

Käsittelytietojen tallentamisvelvollisuus koskee ainoastaan teleyrityksiä. Teleyrityksen on tallennettava tunnistamistietojen käsittelystä yksityiskohtaiset

[121] SVTSL 12a §.

[122] SVTSL 13 §.

[123] HE 125/2003 vp.

[124] SVTSL 14 §.

[125] HE 125/2003 vp.

tapahtumatiedot, joista käy ilmi käsittelyn ajankohta, kesto ja käsittelijä. Tiedot on säilytettävä kaksi vuotta niiden tallentamisesta.[126]

2.2.6 Paikkatietojen käsittely

Paikkatiedon käsite

Paikkatiedolla tarkoitetaan tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun tarkoitukseen kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen.[127] Paikkatiedoilla voidaan ilmaista liittymän tai päätelaitteen sijainti, paikkatiedon tarkkuus, se osa verkkoa, jossa liittymä tai päätelaite paikannetaan tietyllä hetkellä, ja paikkatiedon tallentamisen ajankohta.

Käyttötarkoitus ratkaisee, pidetäänkö tietoa tunnistamistietona vai paikkatietona. Jos sijainnin ilmaisevaa tietoa käytetään viestintäpalvelun toteuttamisessa, kysymyksessä on tunnistamistieto. Esimerkiksi matkaviestinverkossa tieto siitä, minkä tukiaseman alueella päällä oleva matkaviestin on kulloisellakin hetkellä, on tunnistamistieto. Tällöin liittymän tai päätelaitteen sijainnin ilmaiseva tieto on välttämätön viestintäpalvelun toteuttamiseksi. Jos sijaintia ilmaisevaa tietoa käytetään muuhun tarkoitukseen kuin viestintäpalvelun toteuttamiseen, kyseessä on paikkatieto.[128]

Käsittely ja luovutus

Teleyritys, yhteisötilaaja ja lisäarvopalvelun tarjoaja saa käsitellä paikkatietoja tietyin edellytyksin lisäarvopalvelun tarjoamiseksi. Paikkatietojen käsittely on vapaata, mikäli ne ovat tehty sellaisiksi, ettei niitä pysty missään tilanteessa yhdistämään käyttäjään tai tilaajaan.[129] Käsittely on rajattava palveluntarjoajan palveluksessa sekä näiden lukuun toimiviin henkilöihin. Rajoitukset ovat ankaruudessa verrattavissa HetiL:n vastaaviin.

Kuten tunnistamistietojen osalta, paikkatietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen edellyttämässä laajuudessa eikä sillä saa vaarantaa yksityisyyden suojaa enemmän kuin on palvelun toteuttamiseksi välttämätöntä. Tiedot on käsittelyn jälkeen hävitettävä tai tehtävä sellaisiksi, ettei niitä voida yhdistää tilaajaan tai käyttäjään. Huomattavaa on lisäksi palvelua suunniteltaessa, että alle 15-vuotiaiden sekä holhouksen alaisten paikantamisen suostumuksesta päättää tämän huoltaja tai edunvalvoja.[130]

Oikeus kieltää paikkatietojen käsittely

Paikkatietoja saa käsitellä, jollei tilaaja ole sitä kieltänyt. Teleyrityksellä on velvollisuus huolehtia siitä, että tilaajalla on mahdollisuus kieltää paikkatietojen käsittely sekä liittymäsopimusta tehtäessä että koska tahansa palvelun käytön alettua. Teleyrityksen on lisäksi huolehdittava, että tilaajan saatavilla on helposti ja

[126] SVTSL 15 §.

[127] SVTSL 2.1 § 9-kohta.

[128] HE 125/2003 vp.

[129] SVTSL 16.1 §.

[130] SVTSL 16 §.

jatkuvasti tietoa käsiteltävien paikkatietojen tarkkuudesta ja käsittelyn tarkoituksesta sekä siitä, voidaanko paikkatiedot luovuttaa kolmannelle osapuolelle lisäarvopalvelun tarjoamista varten.[131]

Palvelukohtainen suostumus

Lisäarvopalvelun tarjoajan ja yhteisötilaajan on pyydettävä paikannettavalta palvelukohtainen suostumus ennen kuin se aloittaa paikkatietojen käsittelyn, jollei suostumus ilmene yksiselitteisesti asiayhteydestä, esimerkiksi liittymissopimuksesta, palvelun tilauksen yhteydessä tai muusta.[132] Mikäli teleyrityksenä toimiva yhtiö käsittelee tietoja tarjotakseen sellaista palvelua, jossa paikkatietoja käsitellään ensisijaisesti muuhun tarkoitukseen kuin viestintäpalvelun toteuttamiseen, yhtiötä pidetään siltä osin lisäarvopalvelun tarjoajana.[133] Paikannettavalla tarkoitetaan sitä luonnollista henkilöä, jonka hallussa paikannettava laite tai päätelaite on. Näin ollen paikannettava voi olla muukin henkilö, kuin palvelun tilaaja, jonka palvelukohtainen suostumus edellytetään paikkatietojen käsittelemistä varten. Käsittelyssä on korostettu paikannettavan oikeutta päättää itse paikkatiedoistaan siten, ettei tietoja käsitellä käyttäjän tietämättä tai tahdon vastaisesti.[134]

Suostumuksen tulee olla yksiselitteinen ja kyseistä yksittäistä palvelutapahtumaa varten annettu. Yhtäjaksoisen paikantamisen osalta suostumus tulee pyytää aina ennen paikantamisen aloittamista, lyhyttä paikantamista varten jokaista paikannustapahtumaa kohden. Suostumus on voitava peruuttaa milloin tahansa helposti ja ilman erillistä maksua.[135]

2.2.7 Evästeiden käyttö

Evästeellä (engl. cookie) tarkoitetaan palvelun käyttöä kuvaavaa tietoa, joka tallennetaan käyttäjän päätelaitteelle ja jonka palveluntarjoajan palvelin voi myöhemmin hakea takaisin.[136] Laki itsessään ei erityisesti avaa evästeiden käyttöä koskevia säännöksiä. Hallituksen esitys täydentää tarkemmin SVTSL:n 7 §:n sisältöä ja tarkoitusta. Kuten siinä todetaan, voidaan lähes kaikissa Internet-selaimissa estää evästeiden ja muiden päätelaitteille tallennettavien tietojen tallennus käyttäjän itsensä toimesta. Pykälä koskeekin niitä tilanteita, joissa palvelun käyttö edellyttää toimiakseen evästeiden käytön sallimisen. Evästeitä käytetään muun muassa käyttäjän tunnistamiseksi verkkopalvelussa koko istunnon ajaksi tai niitä tilanteita varten, jossa käyttäjä palaa uudelleen palveluun. Evästeitä voidaan myös käyttää kohdistettua markkinointia varten, sillä eväste voi sisältää tietoa käyttäjän kiinnostuksen kohteista, tai se voi yksilöidä käyttäjän siten, että palveluntarjoajan palvelimelle tallennetut tiedot voidaan yhdistää tähän käyttäjään.

SVTSL:ssa sallitaan evästeiden käyttö siten ehdollisena, että käyttäjälle on annettava ymmärrettävät ja kattavat tiedot tallentamisen tai käytön tarkoituksesta. Lisäksi käyttäjälle on annettava mahdollisuus kieltää evästeiden tallentaminen tai

[131] SVTSL 17 §.

[132] SVTSL 18 §.

[133] HE 125/2003 vp.

[134] HE 125/2003 vp.

[135] HE 125/2003 vp.

[136] HE 125/2003 vp.

käyttö. Kuten aikaisemmin todettu, evästeiden tallennus on mahdollista estää käyttäjän päätelaitteen asetuksilla. Kun tämä otetaan huomioon sen ohessa, että monet palvelut edellyttävät evästeiden käyttöä teknisesti toimiakseen, jää kyseisen lain funktio kyseenalaiseksi.

Palveluntarjoajan tietojen antamisvelvollisuus ja käyttäjän kielto-oikeus eivät koske sellaista tietojen tallentamista ja käyttöä, joiden ainoana tarkoituksena on toteuttaa tai helpottaa viestin välittämistä viestintäverkoissa tai jotka ovat välttämättömiä tilaajan tai käyttäjän nimenomaisesti pyytämien palvelujen tarjoamiseksi.

2.2.8 Seuraamukset

SVTSL:n 31 § ja 32 § antaa Viestintävirastolle ja tietosuojavaltuutetulle valtuudet valvoa lain noudattamista. Mikäli teleyritys, yhteisötilaaja tai lisäarvopalvelun tarjoaja rikkoo laista johtuvia velvoitteitaan, voi Viestintävirasto tai tietosuojavaltuutettu määrätä tätä korjaamaan menettelyään kohtuullisessa ajassa. Kohtuullinen aika määräytyy sen mukaan, kuinka vakavana rikkomusta voidaan pitää. Mikäli käyttäjien yksityisyyden tai luottamuksellisen viestin suoja voi vakavasti loukkaantua menettelyn seurauksena voidaan palveluntarjoajaa kehottaa oikaisemaan menettelynsä välittömästi.[137] Noudattamisen tehosteeksi voidaan määrätä uhkasakko, tai rikkomuksen ollessa vakava voidaan toiminta määrätä keskeytettäväksi osaksi tai kokonaan. Uhkasakkoa on kuitenkin pidettävä ensisijaisena keinona rikkomusten varalle.[138] Viestintävirasto tai tietosuojavaltuutettu voi myös saattaa asian esitutkinnan kohteeksi tarpeen vaatiessa.

SVTSL:n 42 §:ssä on myös rangaistussäännökset sähköisen viestinnän tietosuojarikkomuksesta. Rangaistussäännökset täydentävät RL:n vastaavia säännöksiä. 42 §:n mukaan joka tahallaan laiminlyö 7 §:n evästeitä koskevia määräyksiä, 19 §:n velvollisuuden huolehtia tietoturvasta tai käsittelee tunnistamis- ja paikkatietoja säädetyn vastaisesti voidaan tuomita sakkoon, ellei muualla laissa säädetä teosta ankarampaa rangaistusta. Rangaistusta ei määrätä vähäisten rikkomusten osalta.[139]

Rangaistavuus ulottuu myös lisäarvopalveluiden tarjoajiin, sillä niitä koskevat myös lain tietoturvavelvoitteet ja ne joutuvat toiminnassaan käsittelemään luottamuksellisia tunnistamis- ja paikkatietoja.

2.2.9 Luonnos hallituksen esitykseksi laeiksi viestintämarkkinalain, radiotaajuuksista ja telelaitteista annetun lain ja sähköisen viestinnän tietosuojalain muuttamisesta

Esitysluonnoksen pääasiallinen sisältö

Luonnoksella hallituksen esitykseksi laeiksi VML:n, radiotaajuuksista ja telelaitteista annetun lain (16.11.2001/1015) ja SVTSL:n muuttamisesta ("esitysluonnos") on tarkoitus panna kansallisesti täytäntöön ne sähköisen viestinnän direktiiveihin kohdistuvat muutokset, jotka on hyväksytty joulukuussa 2009 voimaan tulleilla direktiiveillä 2009/140/EY ja 2009/136/EY.

---

[137] HE 125/2003 vp.

[138] HE 125/2003 vp.

[139] SVTSL 42 §.

Selvityksen kannalta keskeisin esitysluonnoksessa muutettavaksi ehdotettu sääntely koskee SVTSL:n 7 §:ä, 21 §:ä, 21 a §:ä, 21 b §:ä ja 28 §:ä. Esitysluonnoksen lakimuutokset voimaantullessaan edellyttäisivät, että palveluntarjoajan tulisi jatkossa: (i) hankkia käyttäjän suostumus evästeiden, myös viestintäverkon välityksellä latautumattomien vakoiluohjelmien avulla saatujen, hyödyntämiseen sekä käyttäjä- ja käyttäytymistietojen tallentamiseen; (ii) ilmoittaa Viestintävirastolle ilman aiheetonta viivästystä vika- ja häiriötilanteissa myös niistä toimenpiteistä, joilla kyseisten tilanteiden toistuminen pyritään estämään; (iii) ilmoittaa Viestintävirastolle myös tietoturvaloukkauksista, eikä vain niiden uhkista, kuten nykyisin (ja mikäli kyseessä on teleyritys tai lisäarvopalveluntarjoaja, niin tällöin myös tiedot kyseisistä ilmoituksista on tallennettava); (iv) jo käytännössä vallitsevan tilanteen mukaisesti ja vastaisuudessa myös laintasoisen velvoitteen johdosta pitää huoli siitä, että Viestintävirastolla tai sen lukuun toimivalla on turvallisuustarkastuksen yhteydessä pääsy teleyrityksen laitetiloihin ja muihin tiloihin sekä mahdollisuus saada tutkittavakseen valvontatehtävän kannalta tarpeelliset tiedot viestinnän tietoturvaa koskevassa luvussa asetettujen velvoitteiden valvomiseksi; sekä (v) olla ohjaamatta vastaanottajat KSL:n 2 luvussa tarkoitetun hyvän tavan vastaista markkinointia sisältäville verkkosivustoille.[140]

Esitysluonnoksen olennaiset muutokset

Esitysluonnoksessa ehdotetut selvitykseen liittyen huomioitavat muutokset rajautuvat yllä mainittuihin SVTSL:n alla tarkemmin esitettyihin lainkohtiin. Jäljempänä otsikoissa mainitut lainkohdat noudattavat esitysluonnoksessa käytettyä systematisointia.

7 § Palvelun käyttöä kuvaavien tietojen tallentaminen käyttäjän päätelaitteelle ja näiden tietojen käyttö

Käyttäjälle tulee antaa kielto-oikeus, jotta palvelun käyttöä kuvaavien tietojen tallentaminen käyttäjän päätelaitteelle ja näiden tietojen käyttö olisi sallittua.[141] Esitysluonnoksessa ehdotetaan, että palveluntarjoajalla tulisi olla evästeiden hyödyntämiseen sekä käyttäjä- ja käyttäytymistietojen tallentamiseen käyttäjän suostumus. Tämä voisi tapahtua esimerkiksi selaimen tai muun sovelluksen asetusten avulla.[142]

21 § Tietoturvailmoitukset Viestintävirastolle

Esitysluonnoksessa ehdotetaan poistettavaksi SVTSL:stä merkittäviä vika- ja häiriötilanteita koskeva ilmoitusvelvollisuus, koska vastaava säännös on jo VML 128 §:ssä. Uudistuksen myötä palveluntarjoajan tulisi ilmoittaa myös niistä toimenpiteistä, joilla vika- ja häiriötilanteiden toistuminen pyritään estämään. Sääntelyyn esitetään tarkennusta myös siltä osin, että ilmoitus on annettava ilman aiheetonta viivästystä. Viestintävirasto voi määrätä teleyrityksen tiedottamaan tietoturvaloukkauksesta, jos tämä katsotaan yleisen edun mukaiseksi.[143]

21 a § Tietoturvailmoitukset tilaajalle ja käyttäjälle

[140] Esitysluonnos, s. 1.

[141] SVTSL 7 §.

[142] Esitysluonnos, s. 117–119.

[143] Ibid. s. 119–120.

Ehdotettuun uuteen 21 a §:ään on koottu säännökset, joiden mukaan teleyritys on velvollinen ilmoittamaan tilaajalle tai käyttäjälle tietoturvaloukkauksista tai tietoturvauhkista. Ehdotettu pykälä on siten uusi, mutta sen sisältö vastaa osittain voimassa olevan lain säännöksiä. Säännökseen ehdotetaan lisättäväksi velvollisuus ilmoittaa myös tietoturvaloukkauksista, eikä voimassa olevan sääntelyn mukaisesti vain niiden uhkista. Teleyrityksen ja lisäarvopalvelun tarjoajan on säilytettävä tiedot ilmoituksista. Säännöksestä on poistettu johdonmukaisuuden vuoksi häiriöstä tiedottaminen ja siirretty säännös VML 128.4 §:iin. Ehdotetussa 4 momentissa Viestintävirastolle annetaan oikeus antaa tarkempia määräyksiä esitysluonnoksen kyseessä olevan lainkohdan 1 ja 2 momentissa tarkoitettujen ilmoitusten sisällöstä, muodosta ja Viestintävirastolle toimittamisesta tai 3 momentissa tarkoitetun tiedottamisen sisällöstä ja muodosta.[144]

21 b § Turvallisuustarkastus

Viestintävirastolla on oikeus tehdä teleyrityksessä turvallisuustarkastus viestinnän tietoturvaa koskevassa luvussa asetettujen velvoitteiden valvomiseksi. Viestintävirastolla on jo VML 124 §:n mukaan oikeus tehdä teleyrityksessä tekninen tarkastus. Käytännössä Viestintävirasto on jo suorittaessaan teknistä tarkastusta samalla pyytänyt tietoturvaa koskevan valvontatehtävänsä suorittamiseksi teleyrityksiltä tietoja siitä, kuinka teleyritykset ovat toteuttaneet lain edellyttämät velvoitteet. Säännöksellä annettaisiin virastolle nimenomainen toimivalta tietoturvatarkastusten tekemiseen.[145]

Viestintävirastolla on oikeus teettää turvallisuustarkastus riippumattomalla asiantuntijalla. Viestintävirastolla ja sen lukuun toimivalla on turvallisuustarkastuksen yhteydessä oikeus päästä teleyrityksen laitetiloihin ja muihin tiloihin sekä saada tutkittavakseen valvontatehtävän kannalta tarpeelliset tiedot. Esitetyllä säännöksellä lähinnä todettaisiin jo käytännössä vallitseva tilanne.[146]

Turvallisuustarkastusta ei saa suorittaa kotirauhan piiriin kuuluvissa tiloissa. Turvallisuustarkastuksen kustannukset katettaisiin SVTSL 10 luvun mukaisella tietoturvamaksulla.[147]

28 § Suoramarkkinoinnin tunnistaminen

Kyseisen pykälän 2 momenttiin ehdotetaan lisättäväksi uusi 3-kohta, jonka mukaan esitetään kielletyksi pyrkiä ohjaamaan vastaanottajat KSL:n 2 luvun säännösten[148] vastaisille verkkosivustoille.[149]

42 § Rangaistusäännökset

Sisällöllisesti säännöksessä ei tapahdu muutosta.[150]

---

[144] Ibid. s. 120.

[145] Ibid. s. 120–121.

[146] Ibid. s. 121.

[147] Ibid. s. 121.

[148] Tarkoitettu lainkohta sisältää markkinoinnin hyvän tavan vastaisuutta koskevan säännöstelyn yms.

[149] Esitysluonnos, s. 121–122.

[150] Ibid. s. 122.

2.3 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617)

2.3.1 Lain tausta, tarkoitus ja soveltamisala

Suurin osa sähköisistä palveluista ei edellytä sähköistä tunnistamista tai sähköisiä allekirjoituksia. Osassa sähköisiä palveluita voidaan kuitenkin muun muassa tehdä erilaisia oikeustoimia. Tällaiset sähköiset palvelut edellyttävät osapuolten välisen luottamussuhteen olemassa oloa. Palvelun käyttäjän on voitava luottaa siihen, että palveluntarjoaja on palveluansa rakentaessaan ottanut huomioon tietoturvan ja yksityisyyden suojan vaatimukset. Palveluntarjoajan on puolestaan voitava luottaa siihen, että etäyhteyden päässä oleva palvelunkäyttäjä on se, joka väittää olevansa. Sähköisten palveluiden ja sähköisen asioinnin kehittyminen edellyttää siten hyvin toimivia sähköisen tunnistamisen palveluita.

VahvSTL sisältää perustason sääntelyn niin sanotun vahvan sähköisen tunnistamisen palveluiden tarjonnalle Suomessa. Lain tarkoituksena on edistää vahvan sähköisen tunnistamisen palveluiden tarjontaa ja luoda markkinoille perussäännökset palveluiden tarjontaan. Samalla pyritään varmistamaan, että palveluiden tarjonnassa otetaan huomioon tietoturvan ja tietosuojan vaatimukset. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sisältää säännökset siitä, mitä edellytyksiä tunnistusmenetelmän tulee täyttää ollakseen vahvaa. Lisäksi laki sisältää säännökset vahvan sähköisen tunnistuspalvelun tarjoajaan ja sen tarjoamaan palveluun kohdistuvista vaatimuksista. Lain sähköistä allekirjoitusta koskevat säännökset vastaavat aiemmin voimassa ollutta lakia sähköisistä allekirjoituksista.[151]

Olemassa ei ole yleistä sääntelyä siitä, missä tapauksissa palvelu edellyttää vahvaa sähköistä tunnistamista. Yksittäisissä laeissa saattaa olla tällaisia säännöksiä, ja tällaisten säännösten määrän on puheena olevaa lakia koskevassa hallituksen esityksessä todettu olevan kasvussa. Liikenne- ja viestintäministeriön kaksivuotisen LUOTI-ohjelman (luottamus ja tietoturva sähköisissä palveluissa) yhteydessä vahvan sähköisen tunnistamisen käyttötilanteiksi katsottiin yleisesti ottaen taloudellisia tai oikeudellisia sitoumuksia ja luottamuksellisten tietojen, kuten HetiL:n mukaisten arkaluonteisten henkilötietojen tai organisaation salassa pidettävien tietojen käsittelyä edellyttävät sähköiset palvelut. Julkisen sektorin osalta valtiovarainministeriön ohjeessa 12/2006 on todettu, että vahvaa tunnistamista tarvitaan luottamuksellisissa vuorovaikutteisissa asiointipalveluissa sekä tietojärjestelmien välisessä tietojenvaihdossa eli sovellus-sovellus-asioinnissa.[152]

VahvSTL:ssa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle. Lakia ei sen 1 §:n mukaan sovelleta yhteisön sisäiseen tunnistamiseen käytettävien palveluiden tai yhteisön sisäiseen sähköiseen allekirjoittamiseen käytettävien palveluiden tarjontaan. Lakia ei sovelleta myöskään, jos yhteisö käyttää omaa tunnistusmenetelmäänsä omien asiakkaidensa tunnistamiseen omissa palveluissaan, eikä tunnistusvälineiden tai sähköisen allekirjoittamisen välineiden valmistamiseen, maahantuontiin tai myyntiin.

---

[151] HE 36/2009 vp.

[152] HE 36/2009 vp.

Lailla säännellään ainoastaan vahvan sähköisen tunnistamisen palvelujen tarjoamista. Heikko tunnistaminen on siten täysin sääntelyn ulkopuolelle. Heikon tunnistamisen menetelmät ovat nykyään yleisimmin käytettyjä tunnistamismenetelmiä. Käytännössä tämä tarkoittaa käyttäjätunnusten ja salasanojen yhdistelmiä.[153]

2.3.2 Keskeiset määritelmät

VahvSTL:ssa tarkoitetaan *vahvalla sähköisellä tunnistamisella* henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttämällä perustuen *vähintään kahteen seuraavista kolmesta* vaihtoehdosta: a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää; b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen.[154]

Vaatimus siitä, että kahden näistä on toteuduttava, jotta sähköisen tunnistamisen menetelmää voidaan pitää vahvana, vastaavat yleisesti esitettyä kansainvälistä vahvan sähköisen tunnistamisen määritelmää. Kohta a tarkoittaa salasanaa tai salalausetta, jonka käyttäjä joutuu antamaan käyttäjätunnuksensa yhteydessä. Kohta b puolestaan tarkoittaa tunnistusvälinettä, jonka sisältämän tiedon perusteella käyttäjäidentiteetti pystytään määrittämään. Esimerkkejä ovat sirukortti ja tietyllä SIM-kortilla varustettu matkapuhelin. Kohta c tarkoittaa käytännössä jotain käyttäjän biometristä ominaisuutta, kuten sormenjälkeä, kasvojen muotoa tai silmän iiristä. Vahvan sähköisen tunnistamisen määritelmä pitää aina sisällään myös todentamisen, jolla varmistetaan tunnisteen aitous ja oikeellisuus. Tunnisteella tarkoitetaan tunnistamiseen käytettävää tietoa.[155]

Käytössä olevista vahvan sähköisen tunnistamisen menetelmistä selvästi yleisimpiä ovat pankkitunnisteet. Lisäksi käytössä on julkisen avaimen järjestelmään perustuvia varmenteita. Niitä on tarjonnut viime vuosina lähinnä Väestörekisterikeskus, mutta on odotettavissa, että teleyritykset aloittaisivat mobiilivarmenteiden tarjoamisen jo tänä vuonna.[156]

Laissa tarkoitetaan *sähköisellä allekirjoituksella* sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. *Kehittyneellä sähköisellä allekirjoituksella* tarkoitetaan sähköistä allekirjoitusta: a) joka liittyy yksiselitteisesti sen allekirjoittajaan; b) jolla voidaan yksilöidä allekirjoittaja; c) joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja d) joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita.

---

[153] HE 36/2009 vp.

[154] VahvSTL 2.1 § 1-kohta.

[155] HE 36/2009 vp.

[156] HE 36/2009 vp., www.tietokone.fi (15.4.2010): "Mobiilivarmenne tulee tänä vuonna".

2.3.3 Tietoturvaa koskevat velvoitteet laissa

Tunnistusmenetelmälle asetettavia vaatimuksia koskevan, VahvSTL:n mukaan tunnistusmenetelmän on oltava *riittävän turvallinen ja luotettava ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat.*[157] Esimerkiksi, jos tarjottava tunnistusmenetelmä perustuu *varmenteisiin*, palveluntarjoajan on varmistettava, että käytettävä algoritmi on riittävän vahva ja avainparin pituus riittävä.[158] Varmenteella tarkoitetaan lain määritelmäsäännöksen mukaan sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa sekä sähköisessä allekirjoituksessa.[159]

Tunnistuspalvelun tarjoajan yleisiä velvollisuuksia koskeva VahvSTL 13 § on tietoturvan kannalta keskeinen. Tunnistuspalvelun tarjoajan on huolehdittava siitä, että sen palveluksessa olevalla henkilöstöllä on harjoitetun toiminnan laajuuteen nähden riittävä asiantuntemus, kokemus ja pätevyys.[160] Asiantuntemuksella tarkoitetaan sekä teknistä että oikeudellista asiantuntemusta.[161] Esimerkiksi henkilötietojen käsittelyyn liittyvät voimassa olevan lainsäädännön asettamat vaatimukset ovat huomattavat. Asiantuntemuksen, tarvittavan kokemuksen ja pätevyyden, kuten esimerkiksi koulutuksen vaatimukset määräytyvät kunkin henkilön kohdalla hänen hoitamiensa tehtävien mukaan. Suoraan sähköisen tunnistamisen kanssa tekemisissä olevilla on oltava riittävä asiantuntemus esimerkiksi sähköiseen tunnistamiseen liittyvistä teknisistä seikoista sekä *tietoturvasta*.

Tunnistamispalvelun tarjoajan on huolehdittava palvelujensa HetiL:n 32 §:ssä tarkoitetusta *tietojen suojaamisesta sekä riittävästä tietoturvasta*.[162] Palvelujen tietoturvalla käsitetään hallituksen esityksen mukaan tässä samaa kuin SVTSL:n 19 §:n 1 momentissa. Toiminnan turvallisuudella tarkoitetaan siten muun muassa sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan. Lisäksi toiminnan turvallisuudella tarkoitetaan sitä, että pidetään rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan.

Näiden toimien on oltava riittäviä eli ne on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. Tällä tarkoitetaan sitä, että täydellistä tietoturvaa ei yleisesti ottaen ole mahdollista saada aikaan ainakaan ilman

---

[157] VahvSTL 8.1 § 4-kohta.

[158] HE 36/2009 vp.

[159] VahvSTL 2.1 § 7-kohta.

[160] VahvSTL 13.1 §.

[161] HE 36/2009 vp.

[162] VahvSTL 13.3 §.

kohtuuttomia kustannuksia. Tietoturvan tasoon kohdistuvat vaatimukset saattavat vaihdella tarjottavista palveluista johtuen. Jos palveluntarjoaja esimerkiksi tarjoaa biometristen tunnisteiden käyttöön perustuvaa vahvaa sähköistä tunnistuspalvelua, kohdistuu tällaiseen toimintaan korostettu turvallisuusvaatimus. Samoin eroa saattaa olla siinä, tarjoaako palveluntarjoaja tunnistuspalvelua sitä käyttäville palveluntarjoajille vai laskeeko se ainoastaan liikkeelle tunnistusvälineitä.[163]

2.3.4 Uhkat ja häiriöt

Tunnistuspalvelun tarjoajalla on *velvollisuus ilmoittaa tietoturvaan ja tietojen suojaamiseen kohdistuvista uhkista tai häiriöistä.*[164] SVTSL:n 21 § sisältää vastaavanlaisen säännöksen, joka kuitenkin on huomattavasti yksityiskohtaisempi. Pykälässä tarkoitettu velvollisuus ilmoittaa tietoturvaan ja tietojen suojaamiseen kohdistuvista uhkista ja häiriöistä kohdistuu sopimuksen voimassaoloaikaan. Tunnistuspalvelun tarjoajan on ilmoitettava ilman aiheetonta viivästystä tunnistuspalvelua käyttäville palveluntarjoajille, tunnistusvälineiden haltijoille sekä Viestintävirastolle palvelun tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä.[165]

Jos uhka tai häiriö kohdistuu HetiL:n 32 §:ssä tarkoitettuun tietojen suojaamiseen, tunnistuspalvelun tarjoajan on ilmoitettava asiasta lisäksi tietosuojavaltuutetulle.[166] Ilmoituksessa on samalla kerrottava niistä toimista, joita eri tahoilla on käytettävissään uhkien tai häiriöiden torjumiseksi sekä näistä toimenpiteistä aiheutuvista arvioiduista kustannuksista.[167]

Ilmoittamisella tunnistuspalvelua käyttäville palveluntarjoajille ja tunnistusvälineiden haltijoille pyritään hallituksen esityksen mukaan estämään vahinkojen syntyminen tai paheneminen. Esimerkiksi erilaisissa huijausyrityksissä saattaa olla tärkeää, että olemassa on yleinen tietoisuus meneillään olevasta huijauspyrkimyksestä. Mikäli kyse on teknisestä tietoturvasta, välineiden haltijat voivat pidättyä välineen käytöstä, kunnes vika on korjattu. Kaiken kaikkiaan pyrkimyksenä on estää tai minimoida mahdollisesti aiheutuvat vahingot.[168]

VahvSTL 16 § ei sisällä yksityiskohtaisia ohjeita ilmoittamisesta tai esimerkiksi niistä tavoista, joilla ilmoittaminen voidaan tehdä. Tämä tarkoittaa sitä, että palveluntarjoajan tehtävänä on harkita kulloinkin tehokas ilmoittamistapa. Tapauksesta riippuen ilmoitus voidaan antaa esimerkiksi Internetin kautta tai tiedotusvälineiden välityksellä. Joskus myös henkilökohtainen yhteydenotto voi olla tehokkain. Säännös lähtee siitä, että palveluntarjoajan oman edun mukaista on estää tai minimoida vahingot.[169]

VahvSTL 16 § ei sisällä myöskään vaatimusta välittömästä ilmoittamisesta, koska toisinaan voi olla parempi ensin pyrkiä korjaamaan esimerkiksi palveluntarjoajan

---

[163] HE 36/2009 vp.

[164] VahvSTL 16 §.

[165] VahvSTL 16.1 §.

[166] VahvSTL 16.2 §.

[167] VahvSTL 16.3 §.

[168] HE 36/2009 vp.

[169] HE 36/2009 vp.

tiedossa oleva vaan ei yleisesti tiedossa oleva tietoturva-aukko. Harkinta tiedottamisen ajankohdasta jää siis tunnistuspalvelun tarjoajan tehtäväksi. Viestintävirastolle ja henkilötietojen kyseessä ollen tietosuojavaltuutetulle tehtävien ilmoitusten tarkoituksena on, että valvovat viranomaiset olisivat tietoisia säännöksessä tarkoitetuista uhista ja häiriöistä. Viranomaiset voivat muun muassa tarvittaessa osallistua tiedottamiseen, jotta tieto leviäisi mahdollisimman nopeasti silloin, kun tämänkaltainen toiminta estäisi vahinkoja syntymästä.[170]

2.4 Muu lainsäädäntö

2.4.1 Perustuslaki (11.6.1999/731)

2.4.1.1 Oikeus yksityiselämään

Keskeisimpänä perusoikeutena tietoturvallisuuden kannalta voidaan pitää oikeutta yksityiselämään. PL 10 §:n mukaan jokaisen yksityiselämän kunnia ja kotirauha on turvattu, ja että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Perusoikeusuudistuksen esitöiden mukaan käsite 'yksityiselämä' voidaan ymmärtää henkilön yksityisyyden piiriä koskevaksi yleiskäsitteeksi. Tähän yksityisyyden suojaan kuuluu siis henkilötietojen suoja sekä luottamuksellisen viestin suoja.

2.4.1.2 Lakisidonnaisuusperiaate

Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin kuuluvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

2.4.1.3 Oikeus elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen

PL 7.1 §:n takaa jokaiselle oikeuden elämään, henkilökohtaiseen vapauteen ja turvallisuuteen. Henkilökohtaista turvallisuutta ei ollut mainittu hallitusmuodossa, mutta se vastaa kansainvälisiä ihmisoikeussopimuksia sillä sekä Euroopan ihmisoikeussopimuksen 5 artiklassa että kansalais- ja poliittisia oikeuksia koskevan yleissopimuksen 9 artiklassa on henkilökohtainen turvallisuus suojattu henkilökohtaisen vapauden yhteydessä. Vaikka kansainväliset sopimukset eivät olekaan alun perin pitäneet tietoturvallisuutta tavoitteenaan, voi Suomen PL:n säännös saada itsenäisen tulkinnan tässä suhteessa.

2.4.1.4 Sananvapaus ja julkisuus

PL 12 § sisältää sananvapautta ja julkisuutta koskevat lainsäädännön perusperiaatteet. Niiden mukaan jokaisella on sananvapaus. Sananvapauteen liittyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Tarkempia säännöksiä sananvapaudesta annetaan lailla. Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat

[170] HE 36/2009 vp.

julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.

Käytännössä PL:n määrittelemä suojan laajuus edellyttää moninaisia toimia, jotta määriteltyä oikeushyvää voitaisiin tietoturvalla suojata. Kaikki tietoturvatoimenpiteet pyrkivät suojaamaan PL:ssa suojattuja oikeuksia.

2.4.2 Viestintämarkkinalaki (23.5.2003/393)

VML koskee lähinnä teleyrityksille asetettavia yleisiä tietoturvavelvoitteita. Teleyrityksen tulee huolehtia siitä, että telepalveluja sekä viestintäverkkojen tietosuojan ja tietoturvan taso on asianmukaisesti hoidettu. Tämän selvityksen puitteissa ei VML:n tietoturvaa koskevia määräyksiä ole syytä selvittää tarkemmin.

2.4.3 Laki tietoyhteiskunnan palvelujen tarjoamisesta (5.6.2002/458)

2.4.3.1 Lain soveltaminen

Laki soveltuu palvelun vastaanottajan pyynnöstä tapahtuvaan tietoyhteiskunnan palvelun tarjoamiseen eli etäpalveluiden tarjoamiseen sähköisesti, joka yleensä toimitetaan vastiketta vastaan.[171]

2.4.3.2 Määritelmät

Tietoyhteiskunnan palveluilla tarkoitetaan sähköisiä etäpalveluja, jotka toimitetaan vastaanottajan pyynnöstä ja tavallisesti vastiketta vastaan. Lain mukaan Suomen viranomaiset valvovat, että Suomeen sijoittautuneet tietoyhteiskunnan palvelujen tarjoajat noudattavat yhteen sovitettuun alaan kuuluvissa asioissa Suomen lakia. [172]

2.4.3.3 Palveluntarjoajan velvollisuudet

Tietoyhteiskunnan palveluntarjoajien on pidettävä palvelujen vastaanottajien saatavilla määrätyt tiedot itsestään ja toiminnastaan.[173] Palveluntarjoajien on ennen sähköisen tilauksen tekemistä annettava kuluttajille ohjeita ja tietoja sekä järjestettävä kuluttajien käyttöön menettelyt, joiden avulla mahdolliset virheet tilauksissa voidaan etukäteen havaita ja korjata.

Palveluntarjoajan on viivytyksettä sähköisesti ilmoitettava palvelun vastaanottajalle tilauksen vastaanottamisesta, ellei tilattua hyödykettä toimiteta viivytyksettä sähköisesti.[174] Palvelun sopimusehdot on toimitettava palvelun vastaanottajan saataville siten, että palvelun vastaanottaja voi tallentaa ja toisintaa ne.[175] Sopimuksissa, jotka tehdään käyttäen yksinomaan sähköpostia tai muuta henkilökohtaista viestintätapaa, on palvelun tarjoajan tiedonantovelvollisuutta hieman lievennetty.[176]

---

[171] Laki tietoyhteiskunnan palvelujen tarjoamisesta 2 §. Ks. myös HE 194/2001 vp., 2 §.

[172] Ibid.

[173] Laki tietoyhteiskunnan palvelujen tarjoamisesta 7 §. Ks. myös HE 194/2001 vp., 7 §.

[174] Laki tietoyhteiskunnan palvelujen tarjoamisesta 8 §. Ks. myös HE 194/2001 vp., 8 §.

[175] Laki tietoyhteiskunnan palvelujen tarjoamisesta 9 §. Ks. myös HE 194/2001 vp., 9 §.

[176] Laki tietoyhteiskunnan palvelujen tarjoamisesta 12 §. Ks. myös HE 194/2001 vp., 12 §.

2.4.3.4 Vastuuvapaus

Laissa säädetään myös sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä sähköisen tiedon välitys- tai tallennuspalveluita tarjoavien palveluntarjoajien vastuusta välittämänsä tai tallentamansa tiedon lainvastaisesta sisällöstä. Vastuuvapauden perusedellytys on, että palveluntarjoajan toiminta on luonteeltaan teknistä eikä palveluntarjoaja itse osallistu lainvastaisen sisällön tuottamiseen.[177] Palveluntarjoajan tulee noudattaa tiettyjä laissa säädettyjä menettelytapoja saatuaan tiedon lainvastaisesta tiedosta.[178]

2.4.4 Laki potilaan asemasta ja oikeuksista (17.8.1992/785)

Erityinen tietosuojasäännös on lain 13 §:ssä, jossa säädetään potilasasiakirjojen salassapidosta, minkä lisäksi laissa säädetään rikosoikeudellisesta seuraamuksesta potilassalaisuuden rikkomistapauksissa.

2.4.5 Poliisilaki (7.4.1995/493)

Poliisilain 36 §:n perusteella poliisilla on oikeus saada teleyritykseltä ja yhteisötilaajalta tai teknisellä laitteella yhteystiedot sellaisesta teleliittymästä, jota ei mainita julkisessa luettelossa, tai teleliittymän, sähköpostiosoitteen, muun teleosoitteen tai telepääte- laitteen yksilöivät tiedot, jos tietoja yksittäistapauksessa tarvitaan poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja. Poliisi saa käyttää tietojen hankkimiseksi ainoastaan sellaista teknistä laitetta, jota voidaan käyttää vain teleliittymän ja telepäätelaitteen yksilöimiseen. Viestintävirasto tarkastaa teknisen laitteen vaatimustenmukaisuuden sekä sen, ettei tekninen laite ominaisuuksiensa vuoksi aiheuta haitallista häiriötä yleisen viestintäverkon laitteille tai palveluille.

Poliisilla on lisäksi SVTSL 36 §:n perusteella oikeus saada teleyritykseltä tarvittavia tunnistamistietoja eräiden rikosten selvittämiseksi.

2.4.6 Pakkokeinolaki (30.4.1987/450)

Rikostorjunnan tiedonsaantioikeuksista tietoverkossa säädellään sekä PKL:n telepakkokeinopykälissä[179] että erityislainsäädännössä. Lähtökohtaisesti tunnistamistietojen hankkimisesta päättää tuomioistuin pidättämiseen oikeutetun virkamiehen vaatimuksesta tutkittaessa vakavaa rikosta eräin poikkeuksin[180].

Rikoksesta epäillyn lähettämä tai vastaanottama postilähetys tai sähkösanoma voidaan pysäyttää PKL 4:4:n perusteella ja ottaa haltuun PKL 4.3:n mukaisesti pidättämiseen oikeutetun virkamiehen toimesta.

Nykyinen PKL koetaan ongelmalliseksi syystä, että laissa ei säännellä verkkorikosten selvittämiseksi tarvittavia pakkokeinoja. Poliisin keinovalikoimaa säätelevää PKL:a ollaan kuitenkin parhaillaan uudistamassa juuri tästä syystä. Esimerkiksi rikoksesta epäillyn viestintäsalaisuutta saatetaan suojata vahvemmin

---

[177] Laki tietoyhteiskunnan palvelujen tarjoamisesta 13–15 §. Ks. myös HE 194/2001 vp., 13–15 §.

[178] Laki tietoyhteiskunnan palvelujen tarjoamisesta 16 §. Ks. myös HE 194/2001 vp.,16 §.

[179] PKL 5a luku.

[180] PKL 5a:3.

kuin uhrin. Vaikkapa jos sähköpostin ylläpitäjä on käynyt lukemassa jonkun käyttäjän viestejä ilman lupaa, poliisi ei saa selvittää rikosta katsomalla lokitiedoista, mistä sähköpostiin on kirjauduttu. Se loukkaisi epäillyn viestintäsalaisuutta.[181]

2.4.7 Laki sananvapauden käyttämisestä joukkoviestinnässä (13.6.2003/460)

Sananvapauslain 17 § tarjoaa mahdollisuuden tunnistamistietojen hankkimiseksi verkkoviestistä, jonka asettaminen julkisesti saataville on säädetty rangaistavaksi. Toimenpiteestä päättää tuomioistuin pidättämiseen oikeutetun virkamiehen vaatimuksesta.

2.4.8 Rikoslaki (19.12.1889/39)

HetiL:ssa on viittaussäännökset RL:in.

2.4.8.1 Vaaran aiheuttaminen tietojenkäsittelylle

RL 34:9a:ään on lisätty erilliskriminalisointi, jonka rikosnimike on ’vaaran aiheuttaminen tietojenkäsittelylle’. Tällä rikossäännöksellä on kriminalisoitu muun muassa tietokoneviruksen valmistaminen ja levittäminen. RL 35:1.2:iin sisältyy säännös niin sanotun tietovahingon aiheuttamisesta. Säännöksen mukaan voidaan tuomita rangaistukseen vahingonteosta se, joka toista vahingoittaakseen oikeudettomasti 1) hävittää, 2) turmelee, 3) kätkee tai 4) salaa tietovälineelle tallennetun tiedon tai muun tallennuksen.

2.4.8.2 Salassapitovelvoitteiden rikkomisen rangaistavuus

Salassapitovelvoitteiden rikkomisen rangaistavuudesta säädetään RL 38:1:ssä (salassapitorikos) ja 2 §:ssä (salassapitorikkomus, kun teko on kokonaisuutena arvostellen vähäinen). RL 38:3:ssä on säädetty rangaistavaksi viestintäsalaisuuden loukkaaminen. Rangaistavaa on muun muassa oikeudeton tiedon hankkiminen televerkossa välitettävänä olevasta viestistä sekä sähköisesti tallennetusta, ulkopuoliselta suojatusta viestistä murtamalla sen suojaus.

2.4.8.3 Tietomurron rangaistavuus

Tietomurron rangaistavuudesta säädetään RL 38:8:ssä. Sen mukaan henkilö, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta oikeudettomasti tunkeutuu tietojärjestelmään, tuomitaan tietomurrosta sakkoon tai enintään vuoden vankeuteen.

2.4.8.4 Henkilörekisteririkos

Henkilörekisteririkoksesta säädetään RL 38:9:ssä. Rangaistavuus edellyttää tahallisuutta tai törkeää huolimattomuutta. Henkilörekisteririkoksen tunnusmerkkinä on muun muassa henkilötietojen käsittely vastoin käyttötarkoitussidonnaisuutta tai käsittelyn yleisiä edellytyksiä ja siten rekisteröidyn yksityisyyden suojan loukkaaminen. Lisäksi HetiL:ssa säädetään sakkorangaistuksesta tahallisesti tai törkeästä huolimattomuudesta tehdystä henkilörekisteririkkomuksesta, esimerkiksi

---

[181] YLE 16.7.2010. URL: <http://yle.fi/uutiset/kotimaa/2010/07/laki_estaa_poliisia_selvittamasta_verkkorikoksia_1834845.html?origin=rss>

rekisteröidyn yksityisyyden suojaa vaarantavasta henkilötietojen lainvastaisesta käsittelystä.

2.4.8.5 Lakia koskeva olennainen oikeuskäytäntö

KKO 2003:36

Porttiskannaus on toimenpide, jolla on mahdollista selvittää tietojärjestelmän tietoturva-aukkoja ja muita heikkouksia sekä saada kohdejärjestelmästä sellaisia tietoja, joiden avulla järjestelmään voidaan murtautua. Nuori turkulainen opiskelija etsi marraskuussa 1998 porttiskannausohjelman avulla Osuuspankkikeskuksen tietojärjestelmästä avoimia välityspalvelimia. Korkein oikeus pysytti Turun hovioikeuden tuomion, jossa tekijä tuomittiin tietomurron yrityksestä. Korkein oikeus totesi tuomiolauselmassaan: ”Ottaen huomioon tietoturvallisuuden tärkeyden, teon tahallisuuden ja laadun sekä sen, että A:n teon tehdessään on kyennyt ymmärtämään siitä aiheutuvan vahingonvaaran, Korkein oikeus katsoo, ettei vahingonkorvauksia ole perusteltua tässä tapauksessa sovitella.”

RL 38:8

2.4.9 Laki yksityisyyden suojasta työelämässä (13.8.2004/759)

Lain yksityisyyden suojasta työelämässä tarkoituksena on turvata yksityisyyden suojaa sekä sitä turvaavia perusoikeuksia työelämässä.

Työnantaja saa käsitellä vain tehtävän kannalta tarpeellisia henkilötietoja. Tiedot voivat liittyä ”työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta”.[182]

Työnantaja voi kerätä henkilötietoja muualta kuin työntekijältä itseltään, mutta tällöin työntekijältä on saatava suostumus tietojen keräämiseen. Suostumus ei ole tarpeellista viranomaisilta tai henkilöluottotiedoista saaduista tiedoista. Mikäli työntekijän luotettavuuden selvittämiseksi etsitään tietoa muualta kuin työntekijältä itseltään, on työntekijälle ilmoitettava tiedoista ennen niiden käyttöä työntekijää koskevassa päätöksenteossa.[183]

Työntekijän terveystietoja saavat käsitellä vain niiden pohjalta päätöksiä tai toimeenpanoja tekevät henkilöt.[184] Työnantajalla on oikeus saada työntekijän luottotietoja, mikäli työntekijän tehtävät edellyttävät erityistä luotettavuutta. Lisäksi työtehtävien pitää olla käytännössä myös sellaisia, joissa pääsee käsiksi esimerkiksi omaisuuteen, käyttöoikeustietoihin tai työtehtävässä on ”merkittäviä taloudellisia sitoumuksia”.[185] Henkilöluottotietojen hankinnan kustannukset maksaa työnantaja.[186]

---

[182] Laki yksityisyyden suojasta työelämässä 3 §.

[183] Laki yksityisyyden suojasta työelämässä 4 §.

[184] Laki yksityisyyden suojasta työelämässä 5 §.

[185] Laki yksityisyyden suojasta työelämässä 5 a §.

[186] Laki yksityisyyden suojasta työelämässä 5 § ja 5 a §.

Työnantajan on huolehdittava työntekijän sähköpostin käytön perusedellytyksistä joita ovat sähköpostin edelleen lähettäminen, lomavastaaja sekä mahdollisuus ohjata työntekijän viestit hänen poissa ollessaan työnantajan hyväksymälle toiselle henkilölle.[187]

Näiden toimenpiteiden jälkeen työnantajalla on oikeus hakea viestin tunnistetietoja selvittääkseen, onko työntekijä vastaanottanut työnantajalle kuuluvia viestejä työntekijän poissa ollessa. Tämä on mahdollista vain, mikäli se on yritystoiminnan kannalta välttämätöntä; asiantilaa ei saada muuten selville; työtehtävästä johtuen on ilmeistä, että työntekijä on vastaanottanut työnantajalle kuuluvia viestejä; työntekijä on tilapäisesti estynyt työtehtäviensä suorittamisesta tai työntekijältä ei voida kohtuullisessa ajassa saada suostumusta. Näissäkin tapauksissa tunnistetietojen käsittely on sallittu vain työnantajalle välttämättömissä viesteissä.[188]

Mikäli viestin tunnistetietojen perusteella on selvää, että viesti on työnantajalle kuuluva ja se on työtehtävien kannalta välttämätön, eikä lähettäjältä tai vastaanottajalta saada selvyyttä viestin sisällöstä, saa työnantaja avata viestin.[189]

Mikäli viestin tunnistetietoja tai itse viestiä avataan, on siitä tehtävä työntekijälle allekirjoitettu kirjallinen selvitys, josta käy ilmi miksi tietoja on käsitelty, kuka tietoja on käsitellyt sekä koska tietoja on käsitelty. Lisäksi viestin avaamisen yhteydessä selvitykseen on kirjattava kenelle tieto avatusta viestistä on annettu. Selvitys on toimitettava ilman aiheetonta viivästystä työntekijälle.[190]

2.4.10 Kuluttajansuojalaki (20.1.1978/38)

KSL:n 6 luvussa on sähköistä kuluttajakauppaa (laissa käytetään käsitettä etämyynti) koskevat säännökset, jotka ovat kuluttajien hyväksi pakottavia. KSL:n 6 luvun soveltamisen edellytyksenä on, että palveluntarjoaja tarjoaa kulutushyödykkeitä kuluttajille palveluntarjoajan järjestämän sellaisen etätarjontamenetelmän avulla, jossa sopimuksen tekemiseen ja sitä edeltävään markkinointiin käytetään yksinomaan yhtä tai useampaa etäviestintä. Etätarjontamenetelmiä ovat esimerkiksi sähköposti, tekstiviesti, television interaktiiviset ostoskanavat sekä Internet-pohjaiset järjestelmät.

Kulutushyödykkeet ovat tavaroita tai palveluja. KSL:n 6 lukua sovelletaan lähtökohtaisesti kaikkien tavaroiden ja palvelujen sähköiseen kauppaan. Tärkeimmät poikkeukset ovat kiinteää omaisuutta koskevat sopimukset vuokraoikeutta lukuun ottamatta, arvopaperia koskevat sopimukset ja talletusta, luottoa, vakuutusta tai muita rahoituspalveluja koskevat sopimukset. KSL:n 6 luvussa ei ole asetettu euromääräistä alarajaa niiden palvelujen ja tavaroiden hinnalle, joiden kauppaan lakia sovelletaan.

Etätarjontamenetelmällä tarkoitetaan markkinointi- ja myyntitapaa, joiden tarkoituksena on kaupankäynti etäviestimen avulla.

---

[187] Laki yksityisyyden suojasta työelämässä 18 §.

[188] Laki yksityisyyden suojasta työelämässä 19 §.

[189] Laki yksityisyyden suojasta työelämässä 20 §.

[190] Laki yksityisyyden suojasta työelämässä 19 § ja 20 §.

KSL:n 6 luvun soveltaminen edellyttää, että palveluntarjoaja markkinoi tavaraa tai palvelua kuluttajalle jollakin etäviestimellä (esim. sanomalehti, suoramarkkinointikirje, verkkosivu ja tekstiviesti). KSL:n 6 lukua sovelletaan, vaikka markkinointi ja ostaminen tapahtuisivat eri etäviestimillä ja siitä riippumatta, millä tavalla tavaraa tai palvelua on markkinoitu kuluttajalle.

KSL:n 6 luvun soveltamisen kannalta ei ole merkitystä sillä, ottaako palveluntarjoaja yhteyttä kuluttajaan vai päinvastoin. Palveluntarjoajan tulee ottaa huomioon, että verkkomarkkinointiin sovelletaan myös KSL:n 2 luvun säännöksiä markkinoinnista ja menettelyistä asiakassuhteessa.

KLS:n 6a luvussa säädetään myyjän tiedonantovelvollisuudesta kuluttaja-asiakkaille ja sopimuksen peruuttamismahdollisuudesta, kun kyseessä on rahoituspalvelun etämyynti. Rahoituspalveluja ovat lähes kaikki pankki- ja rahastoyhtiöpalvelut, kuten tilit, luotot sijoituspalvelut ja rahastot. Etämyynti tarkoittaa sitä, että uusi rahoituspalvelua koskeva sopimus tehdään alusta loppuun verkkopankissa tai puhelinpalvelussa. Etämyynnistä on kyse, kun asiakas ei henkilökohtaisesti tapaa myyjän edustajaa sopimuksen tekemisen yhteydessä.

Kuluttajansuojalain 6a luvun rahoituspalveluiden ja rahoitusvälineiden etämyyntisäännöksen[191] keskeinen tarkoitus on, että ennakkotiedot ja sopimusehdot toimitetaan kuluttajalle hyvissä ajoin ennen sopimuksen tekemistä henkilökohtaisesti, kirjallisesti tai sähköisesti siten, että kuluttaja voi tallentaa ja toisintaa ne muuttumattomina. Kuluttajan tulee voida säilyttää tiedot pysyvällä tavalla ja tarvittaessa vedota niihin.

KSL 7:9a:ssä puolestaan viitataan vahvasta sähköisestä tunnistamisesta annettuun lakiin. Säännöksen mukaan ennen kulutusluottosopimuksen päättämistä luotonantajan on todennettava luottoa hakevan henkilöllisyys huolellisesti. Jos henkilöllisyys todennetaan sähköisesti, luotonantajan on käytettävä tunnistusmenetelmää, joka täyttää VahvSTL:n 8 §:ssä säädetyt vaatimukset.

Kuluttajaviraston ja kuluttaja-asiamiehen kannanottoja palveluntarjoajan velvollisuuksista sisältyy mm. alaikäisten palvelun käyttäjien osalta kuluttajaoikeuden linjaukseen Alaikäinen, markkinointi ja ostokset (henkilötiedot, tunnistaminen,)[192] sekä mobiilipalveluiden osalta Mobiilisisältöpalveluiden myynti ja markkinointi[193] (mm. mobiilimaksaminen, alaikäiset, tunnistaminen). Pohjoismaisten kuluttaja-asiamiesten ohje verkkokaupasta sisältää myös monia erilaisia palveluntarjoajien vastuuta koskevia kohtia (mm. maksaminen)[194].

2.5 Euroopan unionin oikeus

EU on antanut kaksi tietosuojaan liittyvää direktiiviä. Ensimmäinen on Euroopan parlamentin ja neuvoston vuonna 1995 antama henkilötietodirektiivi ja toinen on vuonna 2002 annettu sähköisen viestinnän tietosuojadirektiivi. Molempien direktiivien velvoitteet on saatettu voimaan osaksi Suomen kansallista

[191] KSL 6a:11.1

[192] Kuluttajaoikeuden linjauksia, Alaikäiset, markkinointi ja ostokset

[193] Kuluttajaoikeuden linjauksia, Mobiilisisältöpalveluiden myynti ja markkinointi (2008)

[194] Kuluttajaoikeuden linjauksia Pohjoismaiden kuluttaja-asiamiesten yhteinen kannanotto, Verkkokauppa ja markkinointi (2009)

lainsäädäntöä. Selvitykseen liittyen huomionarvoinen on myös sähköisiä allekirjoituksia koskeva direktiivi vuodelta 1999. Alla esitellään edellä mainittujen lisäksi henkilötietojen suojaa koskevat perussopimustasoiset määräykset, joihin Lissabonin sopimuksen myötä kuuluu myös EU:n perusoikeuskirja. Direktiivejä koskeva EU-tuomioistuinten ratkaisukäytäntö esitellään alla direktiivien käsittelyn yhteydessä.

2.5.1 Euroopan unionin perusoikeuskirja ja EU:n perussopimukset

Henkilötietojen suoja turvataan EU:n lainsäädännössä perusoikeutena. EU:n perusoikeuskirjan mukaan jokaisella unionin kansalaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan (7 artikla) ja jokaisella on oikeus henkilötietojensa suojaan (8 artikla).

EU:n perusoikeuskirjan oikeudellinen merkitys on entisestään kasvanut Lissabonin sopimuksella hyväksytyn EU:sta tehdyn sopimuksen myötä. Sen 6 artiklan mukaan EU tunnustaa oikeudet, vapaudet ja periaatteet, jotka esitetään EU:n perusoikeuskirjassa, jolla on sama oikeudellinen arvo kuin perussopimuksilla.

Lisäksi periaatteellisesti merkittävä on Lissabonin sopimuksella muutettu EU:n toiminnasta tehdyn sopimuksen 16 artikla (entinen EY 286 artikla), jonka 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan. Ennen Lissabonin sopimusta henkilötietojen suojaa ei ollut kirjoitettu perussopimuksiin subjektiivisen oikeuden muotoon.

2.5.2 Henkilötietodirektiivi 95/46/EY

Eurooppalaisella tasolla direktiivi 95/46/EY, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta ("henkilötietodirektiivi") muodostaa henkilötietojen suojan perustan. Sen tarkoituksena on luoda tasapaino korkeatasoisen yksityisyyden suojan ja henkilötietojen vapaan liikkuvuuden välillä EU:ssa. Tämän vuoksi direktiivissä vahvistetaan tiukat rajat henkilötietojen keruulle ja käytölle sekä kehotetaan perustamaan kuhunkin jäsenvaltioon riippumaton kansallinen elin, joka vastaa henkilötietojen suojasta.

Kyseistä direktiiviä sovelletaan automatisoituun tietojenkäsittelyyn (esimerkiksi tietokoneella oleviin asiakasrekistereihin) sekä sellaisten tietojen manuaaliseen käsittelyyn, jotka sisältyvät tai joiden on tarkoitus sisältyä paperiasiakirjoihin. Direktiivillä on tarkoitus suojella yksilöiden henkilötietojen käsittelyyn liittyviä oikeuksia ja vapauksia vahvistamalla pääperiaatteet, joita noudatetaan näiden käsittelyjen laillisuuden määrittämisessä. Henkilötietodirektiivin velvoitteet on tuotu Suomen oikeusjärjestyksessä osaksi HetiL:a vuonna 1999.

<u>Direktiiviä koskeva olennainen oikeuskäytäntö</u>

Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy, C-73/07, EYT 16.12.2008

Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY 3 artiklan 1 kohtaa on tulkittava siten, että toimintaa, jossa 1) luonnollisten henkilöiden ansio- ja pääomatulo- sekä varallisuustietoja kerätään veroviranomaisten julkisista asiakirjoista ja niitä käsitellään julkaisemista varten; 2)

julkaistaan aakkosjärjestyksessä tuloluokittain laajoina kuntakohtaisina luetteloina painotuotteessa; 3) luovutetaan edelleen CD-ROM -levykkeellä käytettäväksi kaupallisessa tarkoituksessa; ja 4) käsitellään tekstiviestipalvelussa, jossa matkapuhelimen käyttäjät voivat ilmoittamalla henkilön nimen ja kotikunnan ja lähettämällä tekstiviestin määrättyyn numeroon saada paluuviestinä ilmoitetun henkilön ansio- ja pääomatulo- sekä varallisuustiedot, on pidettävä kyseisessä säännöksessä tarkoitettuna "henkilötietojen käsittelynä".

Bodil Lindqvist, C-101/01, EYT 6.11.2003

Sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumeronsa tai antamalla tietoja heidän työsuhteestaan ja harrastuksistaan, on pidettävä yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä. Tällainen henkilötietojen käsittely ei kuulu minkään direktiivin 95/46/EY 3 artiklan 2 kohdassa säädetyn poikkeuksen alaan. Mainintaa siitä, että henkilö on loukannut jalkansa ja on osa-aikaisella sairaslomalla, on pidettävä direktiivin 95/46/EY 8 artiklan 1 kohdassa tarkoitettuna terveyteen liittyvänä henkilötietona.

2.5.3 Sähköisen viestinnän tietosuojadirektiivi 2002/58/EY

Samaan aikaan niin sanotun sähköisen viestinnän sääntelypaketin kanssa vuonna 2002 hyväksyttiin sähköisen viestinnän tietosuojadirektiivinä tunnettu direktiivi 2002/58/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla. Siinä säädetään eräistä varsin arkaluonteisista aiheista, kuten yhteystietojen säilyttämisestä jäsenvaltioiden poliisivalvontatarkoituksiin, ei-toivottujen sähköpostiviestien lähettämisestä, evästeiden (cookies) käytöstä ja henkilökohtaisten tietojen sisällyttämisestä julkisiin luetteloihin. Sähköisen viestinnän tietosuojadirektiivin velvoitteet on saatettu voimaan osaksi SVTSL:a vuonna 2004.

<u>Direktiiviä koskeva olennainen oikeuskäytäntö</u>

LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH, C 557/07, EYT 19.2.2009

Yhteisön oikeus eikä etenkään teollis- ja tekijänoikeuksien noudattamisen varmistamisesta 29.4.2004 annetun Euroopan parlamentin ja neuvoston direktiivin 2004/48/EY 8 artiklan 3 kohta, kun sitä tulkitaan yhdessä henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 22.5.2001 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) 15 artiklan 1 kohdan kanssa, ei ole esteenä sille, että jäsenvaltiot säätävät velvollisuudesta luovuttaa yksityisille kolmansille osapuolille liikennettä koskevia henkilötietoja, jotta siviilituomioistuimissa voidaan panna vireille menettely tekijänoikeuksien loukkauksia vastaan.

Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, EYT 29.1.2008

Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetussa direktiivissä 2002/58 (sähköisen viestinnän tietosuojadirektiivi)

jäsenvaltioita ei edellytetä säätämään velvollisuudesta luovuttaa henkilötietoja tekijänoikeuden tehokkaan suojan varmistamiseksi siviiliprosessin yhteydessä tilanteessa, jossa voittoa tavoittelematon yhdistys, jonka jäsenet ovat musiikkitallenteiden ja audiovisuaalisten tallenteiden tuottajia ja julkaisijoita, on esittänyt vaatimuksen siitä, että Internet-yhteyspalvelun tarjoaja määrätään paljastamaan sille tiettyjen tilaajaliittymien haltijoiden henkilöllisyys ja kotiosoite, jotta se voisi panna vireille siviiliprosessit tekijäoikeuksien loukkaamisen johdosta.

Yhteisön oikeuden mukaan jäsenvaltioiden on kuitenkin pannessaan täytäntöön kyseisiä direktiivejä huolehdittava siitä, että ne nojautuvat sellaiseen kyseisten direktiivien tulkintaan, jolla voidaan varmistaa yhteisön oikeusjärjestyksessä suojattujen eri perusoikeuksien välinen asianmukainen tasapaino. Jäsenvaltioiden viranomaisten ja tuomioistuinten on pannessaan täytäntöön mainittujen direktiivien noudattamisen edellyttämiä toimenpiteitä tulkittava kansallista oikeuttaan näiden samojen direktiivien mukaisesti, ja tämän lisäksi ne eivät myöskään saa nojautua sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan mainittujen perusoikeuksien kanssa tai muiden yhteisön oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa.

2.5.4 Sähköisiä allekirjoituksia koskeva direktiivi 1999/93/EY

Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY sähköisiä allekirjoituksia koskevista yhteisön puitteista vahvistaa oikeudelliset puitteet sähköisille allekirjoituksille ja tietyille varmennepalveluille sisämarkkinoiden moitteettoman toiminnan varmistamiseksi. Direktiivin 8 artiklan sisältämien tietosuojasäännösten mukaan jäsenvaltioiden on varmistettava, että varmentajat, akkreditointijärjestelmät ja valvovat viranomaiset noudattavat sähköisen viestinnän tietosuojadirektiivissä säädettyjä vaatimuksia.

3 VIRANOMAISMÄÄRÄYKSET JA MUU SÄÄNTELY

3.1 Viestintäviraston määräykset

Sekä SVTSL:ssa että VahvSTL:ssa on usean pykälän osalta maininta siitä, että Viestintävirastolla on oikeus antaa tarkempia määräyksiä itse lain ja sen soveltamisen kannalta. Palveluntarjoajan on tunnettava määräysten sisältö soveltaakseen SVTSL:n ja VahvSTL:n määräyksiä.

Viestintäviraston määräykset on jaettu itse määräysteksteihin ja niitä täydentäviin ohjeisiin, jotka täydentävät määräyksiä sekä ohjeistavat niiden soveltamista.

3.1.1 7 B/2009 M: Määräys tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle

Määräystä sovelletaan tunnistuspalvelun tarjoajiin sekä varmentajiin, jotka tarjoavat sähköisiin allekirjoituksiin liittyviä laatuvarmenteita yleisölle. Tunnistuspalvelun tarjoajia ovat esimerkiksi pankit ja laatuvarmenteita yleisölle tarjoaa Suomessa lähinnä Väestörekisterikeskus.

Määräyksen mukaan tunnistuspalvelun tarjoajan on tehtävä Viestintävirastolle kirjallinen ilmoitus ennen toiminnan aloittamista. Ilmoituksen tarkoituksena on toiminnan luotettavuuden arviointi. Ilmoituksesta on käytävä ilmi tietoturvaan liittyviä

tekijöitä, muun muassa tunnistusperiaatteet, tietoturvallisuuden periaatteet ynnä muut. Lisäksi määräyksessä säädetään laatuvarmenteita yleisölle tarjoavan varmentajan toiminnan aloitusilmoituksesta, joka vastaa sisällöltään pitkälti tunnistuspalvelun tarjoajan ilmoitusta.

Määräyksessä säädetään näiden ohessa muun muassa muista edellä mainittujen palveluiden tarjoajien ilmoitusvelvollisuuksista, joilla valvotaan tietoturvan tasoa. Näitä ovat toiminnan muutosilmoitus, vuosiraportti, toiminnan lopettamis- ja siirtymisilmoitus sekä muut, kuten tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä, annetut ilmoitukset.

3.1.2 8 B/2009 M: Määräys tunnistamispalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien toiminnan luotettavuusvaatimuksista

Määräystä sovelletaan 7 B/2009:n tavoin tunnistamispalvelun tarjoajiin sekä yleisölle laatuvarmenteita tarjoaviin varmentajiin.

Määräys sekä sen sovellusohjeet kattavat määräyksessä tarkoitetun palveluntarjoajan vähimmäistietoturvan vaatimukset. Määräys sisältää tietoturvallisuuden hallintaa koskevaa sääntelyä, joka on jaettu hallinnolliseen turvallisuuteen ja henkilöturvallisuuteen. Määräys sisältää myös tarkempaa sääntelyä teknisestä vaatimustasosta sekä palveluntarjoajan tietoturvasta yleisesti että erityisesti laatuvarmenteiden osalta.

Määräys täydentää VahvSTL:a soveltuvin osin. Määräystä ollaan muuttamassa, ja uuden määräysluonnoksen lausuntopyyntö on päättynyt 31.7.2010.

3.1.3 11 A/2008 M: Määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta

Viestintäviraston määräys koskee yleisissä viestintäverkoissa sähköpostipalveluita tarjoavia palveluntarjoajia riippumatta siitä, missä muodossa toimintaa harjoitetaan. Määräystä ei kuitenkaan sovelleta rajatulle käyttäjäpiirille tarjottuihin sähköpostipalveluihin, esimerkiksi yrityksen sisäiseen sähköpostiin.

Määräyksessä täydennetään SVTSL:n säännöksiä. Määräys sisältää teknistä sääntelyä koskien sähköpostipalvelinten toimintaa sekä sähköpostiliikenteen käsittelyä. Lisäksi säännellään vaatimuksista sähköpostipalveluiden toimintaa ja laatua koskien.

3.1.4 57/2009 M: Määräys viestintäverkkojen ja -palvelujen ylläpidosta sekä menettelystä vika- ja häiriötilanteissa

Määräystä sovelletaan yleisiin viestintäverkkoihin ja viestintäpalveluihin sekä viranomaisverkkoihin. Se koskee viestintäverkkojen ja -palvelujen hallintaa ja ylläpitoa, vika- ja häiriötilanteiden hallintaa ja tilastointia sekä viankorjauksen seurantaa. Määräyksessä määrätään vikojen ja häiriöiden vakavuusluokittelusta sekä vioista ja häiriöistä Viestintävirastolle tehtävistä ilmoituksista. Edelleen määräyksessä määrätään asiakkaiden vikailmoitusten vastaanottamisesta. Määräys kattaa puhelin-, Internet-yhteys-, sähköposti-, joukkoviestintä- ja muut viestintäpalvelut.

3.1.5 9 D/2009 M: Määräys tietoturvaloukkausten ilmoitusvelvollisuudesta yleisessä teletoiminnassa

Määräys koskee ainoastaan teleyrityksiä. Siinä säännellään SVTSL:n mukaisesta teleyrityksen tietoturvaloukkauksen ilmoitusvelvollisuudesta sekä ilmoituksen sisällöllisistä vaatimuksista.

3.1.6 13 A/2008 M: Määräys Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta

Määräystä sovelletaan lähinnä teleyrityksiin, sillä ne ovat pääasiallisia Internet-yhteyspalveluiden tarjoajia. Määräys käsittää Internet-yhteyden teknisen tietoturvan toteuttamisen vähimmäisvaatimukset sekä sähköpostiliikenteen ohjaukseen ja reititykseen liittyvän tietoturvan. Määräys myös täydentää SVTSL:a haittaliikenteen suodattamisen osalta.

3.1.7 47 C/2009 M: Määräys teleyritysten tietoturvallisuuden hallinnasta

Määräystä sovelletaan verkko- ja viestintäpalveluihin, joita tarjotaan yleisessä viestintäverkossa, esimerkiksi Internetissä. Määräys koskee lähinnä teleyrityksiä. Se määrittää vaadittavat tietoturva-asiakirjat tietoturvan eri osa-alueiden osalta, riskien hallinnan, tietoturvasuunnitelman sekä tietoturvan seurannan.

3.1.8 53/2008 M: Määräys tunnistamistietojen tallennusvelvollisuudesta

Määräys täydentää SVTSL:n tunnistamistietojen käsittelyä koskevaa normistoa. Määräyksessä säännellään puhelinpalveluiden lisäksi Internet- sekä sähköpostipalveluiden toteuttamisessa kertyneiden tunnistamistietojen tallennusvelvollisuudesta.

3.1.9 58/2009 M: Määräys viestintäverkkojen ja -palvelujen laadusta ja yleispalvelusta

Viestintäviraston määräyksessä säädetään yleisten viestintäverkkojen sekä niissä tarjottavien viestintäpalvelujen suorituskyvystä ja laadusta, viestintäpalvelun asiakaspalvelun laadun tekijöiden seurannasta ja yleispalveluvelvoitteeseen kuuluvan tarkoituksenmukaisen Internet-yhteyden vähimmäisnopeuden teknisestä määrittelystä ja mittaamisesta. Määräys koskee lähinnä teleyrityksiä, joskin soveltuvin osin myös muita palveluntarjoajia.

3.2 Tietosuojavaltuutetun ohjeet

Tietosuojavaltuutettu käsittelee ja ratkaisee henkilötietojen käsittelyä koskevia asioita HetiL:n mukaan. Valtuutetun toimintaa sääntelee laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (27.5.1994/389).

Tietosuojavaltuutettu antaa ohjeistusta HetiL:n sovelluksesta vaikuttaen ennakkoon rekisterinpidon lainmukaisuuteen, kehittäen hyvää tietojenkäsittelytapaa ja ehkäisten tietosuojaloukkauksia. Tietosuojavaltuutettu tekee myös pyynnöstä sitovia ratkaisuja ja antaa kannanottoja HetiL:n soveltamisesta yksittäistapauksissa.

Seuraavat ohjeet ovat tietoturvan ja -suojan kannalta olennaisia tietosuojavaltuutetun julkaisemia ohjeita sekä rekisterinpitäjänä toimiville palveluntarjoajille että kuluttajille, jotka käyttävät mainittuja palveluja. Ohjeet eivät itsessään ole sitovia, joskin ne antavat pohjan sille, miten palveluntarjoajan tulisi toimia edistääkseen parhaiten tietosuojaa sekä toimiakseen HetiL:n edellyttämällä tavalla.

3.2.1 2/1999: Henkilötietolain mukainen yleinen informointivelvollisuus (Henkilötietolaki selitettynä rekisterinpitäjälle)

3.2.2 2/2001: Toimialakohtaisten käytännesääntöjen laatiminen

3.2.3 1/2002: Tarkistuslista henkilötietojen luovutusmenettelyä suunniteltaessa huomioon otettavista asioista

3.2.4 1/2003: Käyttäjälokin tietojen käsittely henkilötietolain mukaan

3.2.5 1/2004: Henkilötunnuksen käsittely henkilötietolain mukaan

3.2.6 2/2004: Henkilötietolain mukainen ilmoitusvelvollisuus

3.2.7 3/2005: Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset

3.2.8 2/2007: Portaalitoiminnan suunnittelu ja toteutus

3.2.9 1/2009: Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa

3.2.10 12/2009: Rekisteröidyn oikeudet - Oikeus kieltää henkilötietojen käsittely

3.2.11 Opas rekisterinpitäjälle

3.2.12 Opas rekisteröidylle

3.3 VAHTI-ohjeistukset

Valtiohallinnon tietoturvallisuuden johtoryhmä ("VAHTI") on Valtiovarainministeriön asettama elin, jonka tehtävä on hallinnon tietoturvallisuuden yhteistyö, ohjaus ja kehittäminen.

VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toimialaan kuuluvat kaikki valtionhallinnon tietoturvallisuuden osa-alueet: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.

Iso osa VAHTIn ohjeistuksista on sovellettavissa ja myös sovelletaan muussakin toiminnassa, kuin valtionhallinnossa. Ohjeistukset tarjoavat myös muille palveluntarjoajille hyvät tietoturvan vähimmäisvaatimukset ja parhaat käytännöt.

3.3.1 VAHTI 3/2000 – Valtiohallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus

Ohje vaatimuksista ja parhaista käytännöistä tietoturvallisuuden toteuttamiseksi järjestelmän elinkaaren aikana.

3.3.2 VAHTI 4/2001 – Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Ohje tietoturvan toteuttamiseen ja riskien sekä niihin varautumiseen liittyen sähköisiin palveluihin ja niiden toteutukseen. Ohje on jaettu sähköisiin palveluihin liittyviin vaatimuksiin, niiden tietoturvalliseen toteutukseen sekä riskienhallintaan. Lisäksi ohjeessa on otettu huomioon sähköinen tunnistaminen.

3.3.3 VAHTI 1/2002 – Tietoteknisten laitetilojen turvallisuussuositus

Tarkka tekninen ohjeistus siitä, miten palveluntarjoajan tulisi toteuttaa teknisten laitetilojensa fyysinen tietoturvallisuus.

3.3.4 VAHTI 1/2003 – Valtion tietohallinnon Internet-tietoturvallisuusohje

Ohje Internet-käytön ja Internetissä tarjottavien palveluiden tietoturvallisen toteutuksen ohjaukseen, suunnitteluun, valvontaan, toteutukseen sekä hankintoihin.

3.3.5 VAHTI 7/2003 – Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa

Yleisohje erilaisten tietoturvariskien määrittelemiseksi, tunnistamiseksi ja arvioimiseksi. Ohje sisältää yksityiskohtaisen osion riskien tunnistamiseksi tietoturvallisuuden eri osa-alueilla.

3.3.6 VAHTI 3/2004 – Haittaohjelmilta suojautumisen yleisohje

Ohje sisältää yleisluontoisen kuvauksen erilaisista haittaohjelmista. Ohjeen painotus on haittaohjelmilta suojautumisen tehokkaassa organisoinnissa sekä asetusten, haavoittuvuuksien ja torjuntaohjelmiston läpikäynnissä

3.3.7 VAHTI 5/2004 – Valtiohallinnon keskeisten tietojärjestelmien turvaaminen

VAHTI 5/2004 on tarkemman tason erityisohje keskeisimpien tietojärjestelmien vaativan tietoturvallisuuden järjestämiseksi

3.3.8 VAHTI 2/2005 – Valtiohallinnon sähköpostien käsittelyohje

Ohjeessa käsitellään sähköpostin erityiskysymyksiä tietoturvallisuuden kannalta. Ohjeen suositukset on tarkoitettu organisaation sähköpostipolitiikan perusteiksi sekä käytännön toiminnan ja sen ohjeistuksen pohjaksi.

3.3.9 VAHTI 3/2005 – Tietoturvapoikkeamatilanteiden hallinta

Ohje sisältää keskeistä tietoa tietoturvapoikkeamatilanteissa ja niihin varautumisessa sovellettavasta lainsäädännöstä, ennaltaehkäisevistä toimenpiteistä, tietoturvapoikkeamiin varautumisesta sekä niistä toipumisesta.

3.3.10 VAHTI 9/2006 – Käyttövaltuushallinnon periaatteet ja hyvät käytännöt

Ohjeessa kuvataan hyvän käyttövaltuushallinnon edellytykset ja hyvää hallintokäytäntöä tukevan käyttövaltuuksien hallintaympäristön arkkitehtuuri. Ohje on tarkoitettu organisaation johdolle, tietoturvavastaaville, henkilöstö- ja tietohallinnosta vastaaville sekä tietojärjestelmien omistajille ja niiden toiminnasta vastaaville.

3.3.11 VAHTI 10/2006 – Henkilöstön tietoturvaohje

Ohjeen tarkoitus on toimia henkilöstön tietoturvatyötä koskevana yleisohjeena. Ohjeessa on kuvattu tietoturvallisuuden perusasiat ja siinä annetaan käytännön neuvoja tietoturvallisuuden toteuttamiseen.

3.3.12 VAHTI 12/2006 – Tunnistaminen julkishallinnon verkkopalveluissa

Ohje käyttäjien tunnistamisen järjestämiseen viranomaisen verkkopalveluissa -ohjeessa otetaan huomioon muun muassa tunnistamisen eri tasot ja luotettavuus sekä sähköpostiasioinnin soveltuvuus.

3.3.13 VAHTI 3/2007 – Tietoturvallisuudella tuloksia

Tarkkajakoinen yleisohje tietoturvan eri osa-alueiden kattavaksi organisoimiseksi

3.3.14 VAHTI 2/2008 – Henkilöstöturvallisuus

VAHTI 2/2008 on johdolle suunnattu ohje erilaisten henkilöstöstä aiheutuvien tietoturvariskien hallintaan, missä on kysymys on salassapidon ja käytettävyyden oikeanlaisen kohtaamisen toteuttamisesta. Ohje käsittelee myös henkilöstöriskien tunnistamista, tietojen kategorisointia, pääsyoikeuksien hallintaa ja tähän liittyviä väliaikaisjärjestelyjä.

3.3.15 VAHTI 6/2008 – Tietoturvallisuus on asenne

Ohje kohdistuu kattavan ja toimivan tietoturvakoulutuksen järjestämiseen organisaatiossa. Huomioon otetaan muun muassa erilaisten henkilöstöryhmien eroava koulutustarve, koulutuksen mielekkyys ja henkilöstön oikeanlainen asennoituminen tietoturvaan.

3.3.16 VAHTI 3/2009 – Lokiohje

Yleisohje lokijärjestelyiden suunnitteluun sekä erityyppisten lokien keräämiseen analysointiin, säilyttämiseen, luovuttamiseen, arkistointiin ja poistamiseen (koko lokin elinkaari)

3.3.17 VAHTI 6/2009 - Kohdistetut hyökkäykset

Ohje sisältää selvityksen kohdistetuista hyökkäyksistä, niiden tekotavoista, suojautumisvalmistelujen kohdistamisesta oikein sekä hyökkäyksen havaitsemisesta. Ohjeen kohderyhmänä ovat tietoturvallisuuden ja järjestelmänvalvonnan piirin henkilöt.

3.3.18 Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus

3.4 JHS-suositukset

Julkishallinnon suositukset ("JHS") ovat julkisen hallinnon tietohallinnon neuvottelukunnan ("JUHTA") hyväksymiä valtion- ja kunnallishallinnon tietohallintoa koskevia yhtenäisiä menettelytapoja, määrittelyjä ja ohjeita. Vaikka JHS-järjestelmän mukaiset suositukset ovat tarkoitettuja julkishallintoa varten, ovat ne pitkälti myös sovellettavissa yksityisiin palveluntarjoajiin.

3.4.1 JHS 129: Julkishallinnon verkkopalvelun suunnittelun ja toteuttamisen periaatteet

Suositus opastaa viranomaisia verkkopalveluiden suunnittelussa, toteutuksessa ja hankinnassa. Suositus kuvaa verkkopalvelun tuottamisprosessin ja päähuomio on erityisesti loppukäyttäjälle tarkoitetun käyttöliittymän toteutuksessa ja hyvän palvelun tuottamisessa. Erityistä huomiota on kiinnitetty verkkopalvelun käytettävyyden ja saavutettavuuden varmistamiseen.

3.4.2 JHS 146: Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus

Suosituksen tarkoituksena on yhdenmukaistaa julkisuuslain edellyttämän tietojärjestelmäselosteen laadintaa sekä helpottaa julkisuuslain toteuttamista.

3.4.3 JHS 165: Tietojärjestelmän vaatimusten määrittely osana järjestelmän hankintaa

Tämän suosituksen tarkoituksena on opastaa tietojärjestelmiä hankkivia organisaatioita järjestelmän hankinnassa antamalla ohjeita ja malleja järjestelmän vaatimusten määrittelemiseksi. Suosituksessa kuvataan tietojärjestelmän vaatimusten määrittelyn periaatteet ja vaatimusten määrittelyssä tuotettavat dokumentit.

3.5 Arjen tietoyhteiskunnan neuvottelukunta – Ohjeet ja suositukset

Arjen tietoyhteiskunnan neuvottelukunta pyrkii varmistamaan kansallisen tietoyhteiskuntastrategian käytännön toteutumisen. Neuvottelukuntaan kuuluu seitsemän työryhmää joiden vastuualueina ovat julkisen tiedon saatavuus, tietoturva, sähköinen tunnistaminen, sähköinen laskutus, lapset ja media, ICT - opetuksessa sekä viestinnän elinkeinopolitiikka. Neuvottelukunta on julkaissut käsillä olevan selvityksen kannalta seuraavat relevantit selvitykset, linjaukset ja ohjeet.

3.5.1 Sähköisen tunnistamisen kehittämisryhmän 1. väliraportti arjen tietoyhteiskunnan neuvottelukunnalle – Sähköisen tunnistamisen nykytila Suomessa 15.1.2008

3.5.2 Mobiilitunnistusmenetelmät 13.10.2008

3.5.3 Vahvan sähköisen tunnistamisen kansalliset linjaukset 15.10.2008

3.5.4 Toimenpiteet verkkolaskun edistämiseksi 29.1.2009

3.6 ENISA – Ohjeet ja suositukset

3.6.1 Euroopan verkko- ja tietoturvavirasto (European Network and Information Security Agency, ENISA) perustettiin parantamaan unionin, jäsenvaltioiden ja yritysmaailman valmiuksia ehkäistä, käsitellä ja ratkaista verkko- ja tietoturvaongelmia. Tarkoituksen on varmistaa korkeatasoinen ja toimiva verkko- ja tietoturva ja luoda erityinen verkko- ja tietoturvakulttuuri, josta on hyötyä Euroopan unionin kansalaisille, kuluttajille, yrityksille ja julkisen sektorin organisaatioille ja jonka avulla edistetään myös sisämarkkinoiden moitteetonta toimintaa. ENISA antaa jäsenvaltioille suosituksia sekä parhaita käytäntöjä ja julkaisee niitä verkkosivuillaan.ENISA Recommendations to stakeholders

3.6.2 06/2006: Risk Management: Implementation principles and Inventories for Risk Management/Risk assessment methods and tools

3.6.3 02/2007: Information package for SMEs

3.6.4 11/2008: Security Issues in the Context of Authentication Using Mobile Devices

3.6.5 06/2009: Good Practice Guide – Network Security Information Exchanges

3.6.6 12/2009: Good Practice Guide on National Exercises – Enhancing the Resilience of Public Communications Networks

3.6.7 12/2009: Good Practice Guide on Reporting Security Incidents

3.6.8 12/2009: Guidelines for Enhancing the Resilience of Communication Networks

3.6.9 02/2010: Security Issues in Cross-border Electronic Authentication

3.6.10 04/2010: Mobile Identity Management

3.7 Standardit

3.7.1 SFS-ISO/IEC 27000 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. (ISO/IEC 27000:2009)

3.7.2 ISO/IEC 27001:fi Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. (ISO/IEC 27001:2005)

3.7.3 ISO/IEC 27002:fi Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. (ISO/IEC 27002:2005; oli nimeltään ISO/IEC 17799 ennen uudelleennumerointia)

3.7.4 ISO/IEC 27003:2010 Information technology -- Security techniques -- Information security management system implementation guidance.

3.7.5 ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management – Measurement.

3.7.6 SFS-ISO/IEC 27005 Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. (ISO/IEC 27005:2008)

3.7.7 ISO/IEC 15408-1-3:2005 Information technology -- Security techniques -- Evaluation criteria for IT security (tunnetaan yleisesti myös nimellä Common Criteria)

3.7.8 ISO/IEC 21827:2008 (Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)

3.7.9 ISF The Standard of Good Practice for Information Security (ISF (Information Security Forum13) on julkaisut oman standardinsa, jonka kehitys seuraa esimerkiksi COBIT-toimintamallia ja ISO/IEC 27002 -standardia; standardi on käytännönläheinen ja antaa selkeitä ohjeita esimerkiksi tietoturvapolitiikan tekemiseksi tai verkkopalvelun suojaamiseksi)

3.7.10 NIST SP 800 -sarja (tietoturvaan suunnatut SP 800 -sarjan dokumentit ovat menettelyohjeita Yhdysvaltojen lainsäädännön mukaisten, kuten FIPS-vaatimusten, toteuttamiseksi)

3.7.11 BS 7799 (Iso-Britannian standardointi-instituutin julkaisema suositus organisaation tietoturvallisuuden hallintajärjestelmäksi on edelleen yksi tunnetuimmista tietoturvastandardeista; BS 7799 -standardin osan 1 pohjalta luotiin ISO 17799 -

standardi, joka siirrettiin ISO/IEC 27002:2005 -standardiin; nykyään sertifiointi suoritetaan ISO 27000 -sarjan standardeja vastaan)

3.7.12 PCI DSS (PCI DSS (Payment Card Industry Data Security Standard) on korttiyhtiöiden kehittämä kansainvälinen tietoturvastandardi, jonka tarkoituksena on parantaa kortinhaltijoiden tietoja käsittelevien järjestelmien tietoturvaa; standardissa määritellään vaatimukset tietojen turvalliselle tallennukselle ja käsittelylle, testaus- ja tarkastusmenetelmät sekä tarkastusvaatimukset ja tarkastuksia suorittavien tahojen sertifiointi; standardi koskee kaikkia standardin hyväksyneiden maksukorttiyhtiöiden korttitietoja käsitteleviä tahoja)

3.7.13 Finanssivalvonnan Standardi RA4.4b on tiettyihin luottolaitoksiin, sijoituspalveluyrityksiin ja rahastoyhtiöihin sovellettava operatiivisten riskien hallintaa koskeva standardi. Se sisältää tietoturvallisuuden perusvaatimukset sen soveltamisalaan kuuluvien toimijoiden osalta.

3.8 Toimintamallit

3.8.1 COBIT (Control Objectives for Information and related Technology)

Tietojärjestelmien hallinnoinnin viitekehys; ITGI:n (IT Governance Institute) ja ISACA:n (Information Systems Audit and Control Association) luoma viitekehys, jota organisaatio voi hyödyntää määritellessään tietojenkäsittelyn liiketoiminnallisia tavoitteita ja vaatimuksia; laaja organisaation tietohallinnon, tietotekniikan ja -järjestelmien hallintaan kehitetty valvontamalli.

3.8.2 ITIL (Information Technology Infrastructure Library)

Parhaat käytänteet tietojenkäsittelyn palvelutuotantoon; laajalti levinnyt tietotekniikan palveluyritysten suosima viitekehys palvelujen standardoimiseen.

3.8.3 GAISP (Generally Accepted Information Security Principles)

Yleiset tietoturvallisuuden periaatteet; nykyisin GAISPI:ia kehittää ISSA eli Information System Security Association; tavoitteena luoda globaalit yhtenevät tietoturvaperiaatteet julkiselle ja yksityiselle sektorille.[195]

3.9 Itsesääntely

3.9.1 FK: Luottolaitosten henkilötietojen käsittelyä koskevat käytännesäännöt

Käytännesäännöt sisältävät luottolaitoksille tarkoitetut menettelyohjeet HetiL:n soveltamiseen liiketoiminnassa.

3.9.2 FK: TUPAS-tunnistusperiaatteet

TUPAS-tunnistusperiaatteista annettu standardi on pankkien laatima yhteinen menettely, jota kolmannet osapuolet voivat käyttää palveluissaan henkilöasiakkaiden sähköisessä tunnistamisessa. Se sisältää palveluiden toteuttamisen kannalta olennaisia tietoturvavaatimuksia.

3.9.3 FK: TUPAS-varmennepalvelu palveluntarjoajille

---

[195] Laaksonen – Nevasalo – Tomula 2006, s. 100.

Ohje sisältää yksityiskohtaista tunnistuspalvelun toimintaa kuvaavaa teknistä tietoa palveluntarjoajalle.

3.9.4 FK: TUPAS-varmennepalvelun varmenneperiaatteet

Varmenneperiaatteet sisältävät TUPAS-tunnistetietojen myöntämistä ja käsittelyä koskevia periaatteita TUPAS-tunnisteita tarjoaville palveluntarjoajille.

3.9.5 FK: Pankkien asiakasyhteyden tietoturva

PATU - pankkien asiakasyhteyksien tietoturva kattaa yritysten ja yhteisöjen sekä pankin välisten aineistojen suojauksen.

3.9.6 FK: Pankin velvollisuudet, vastuut ja oikeudet

Ohje sisältää selvityksen pankin velvollisuuksista, vastuista ja oikeuksista verkkopankkipalveluiden ja sähköisen tunnistuksen tarjoamisessa.

3.10 Muu sääntely ja ohjeistus

3.10.1 OECD

OECD:n päivitetty ohjeistus vuodelta 2002 esittelee yhdeksän tietoturvaperiaatetta; turvallisuustietoisuuden, vastuullisuuden, vastatoimet, eettisyyden, demokratian, riskien arvioinnin, turvallisuuden suunnittelun ja täytäntöönpanon, turvallisuuden hallinnan ja uudelleenarvioinnin. Ohjeistus on vapaaehtoinen, mutta jäsenvaltioita suositellaan vahvasti ottamaan periaatteet käyttöön. Ohjeistus on otettu huomioon muun muassa edellä käsitellyissä BS7799/ISO17799- standardissa ja valtiovarainministeriön alaisen VAHTI ryhmän tietoturvaohjeistuksessa.

3.10.2 IT2010 YSE – Yleiset sopimusehdot

IT2010-ehdot on laadittu käytettäväksi yritysten välisissä kotimaisissa IT-toimituksissa. Ehtoja ei ole tarkoitettu käytettäväksi kuluttajien kanssa tehtävissä sopimuksissa. Vanhoissa IT2000-sopimusehdoissa ei ollut tietosuojaa käsitteleviä sopimusehtoja, vaikka IT-palvelujen ja -toimitusten yhteydessä käsitellään usein henkilötietoja. Uusiin ehtoihin on otettu henkilötietojen käsittelyyn liittyen kolme yleistä ehtoa, joilla pyritään turvaamaan se, että sopijapuolet huomioisivat tilanteen erityispiirteet, selvittäisivät oikeudelliset reunaehdot sekä sopisivat asiasta tarkemmin ja kirjallisesti. IT2010-ehtojen jaksossa 8 esitetyt tietoturvaa, henkilötietojen käsittelyä ja varmuuskopiointia koskevat ehdot ovat seuraavat:

- 8.1 Sopijapuolen ja sen alihankkijoiden on huolehdittava tietoturvallisuudesta, yksityisyyden suojasta henkilötietoja käsiteltäessä ja varmuuskopioinnista noudattamalla sopijapuolten kirjallisesti sopimia järjestelyjä ja kyseistä sopijapuolta velvoittavaa lainsäädäntöä. Siltä osin kuin sopijapuolet eivät ole tietoturvallisuudesta, yksityisyyden suojasta henkilötietoja käsiteltäessä ja varmuuskopioinnista kirjallisesti toisin sopineet, sovelletaan kohtien 8.2 – 8.4 mukaisia ehtoja.

- 8.2 Sopijapuolen on huolehdittava, että sen vastuulla sopimuksen mukaan oleva osa toimituksen kohteesta ja sopijapuolen omasta ympäristöstä, kuten sopijapuolen vastuulla olevat laitteet, palvelutuotannon tilat ja toimitilat, on sopijapuolen noudattamien ja asianmukaisten tietoturvakäytäntöjen

mukaisesti suojattu tietoturvariskejä vastaan ja että suojaukseen ja tiedonvarmistukseen liittyviä menettelyjä noudatetaan.

- 8.3 Sopijapuolet sopivat kirjallisesti, jos asiakas luovuttaa henkilötietoja toimittajalle. Asiakas vastaa siitä, että sillä on oikeus luovuttaa kyseiset henkilötiedot toimittajalle sopimuksen mukaiseen tarkoitukseen. Toimittaja ei siirrä asiakkaan toimittajalle luovuttamia henkilötietoja Euroopan talousalueelta sen ulkopuolelle tai mahdollista pääsyä kyseisiin Euroopan talousalueella oleviin henkilötietoihin Euroopan talousalueen ulkopuolelta.
- 8.4 Sopijapuoli vastaa omia tietojaan ja tiedostojaan koskevien varmuuskopioiden ottamisesta sekä niiden toimivuuden tarkastamisesta.

3.10.3 Puolustusministeriö: KATAKRI – Kansallinen turvallisuusauditointikriteeristö

3.10.4 Huoltovarmuuskeskus: SOPIVA - Toiminnan jatkuvuuden hallintaa koskevat suositukset

3.10.5 Tieke ry: Sähköisen kaupankäynnin aapinen

3.10.6 Tietoturvaopas.fi: Tietoturvasuunnitelman avainkohdat

LÄHDEKIRJALLISUUS

Hakala, Mika – Vainio, Mika – Vuorinen, Olli, Tietoturvallisuuden käsikirja. Docendo Finland Oy, Jyväskylä 2006. (Hakala – Vainio – Vuorinen 2006)

Helopuro, Sanna – Perttula, Juha – Ristola, Juhapekka, Sähköisen viestinnän tietosuoja. Talentum Media Oy, Karisto 2009. (Helopuro – Perttula – Ristola 2009)

Laaksonen, Mika – Nevasalo, Terho – Tomula, Karri, Yrityksen tietoturvakäsikirja – Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy, Helsinki 2006. (Laaksonen – Nevasalo – Tomula 2006)

Salminen, Markku, Tietosuoja sähköisessä liiketoiminnassa. Talentum Media Oy, Karisto 2009. (Salminen 2009)

Viemerö, Mikko, Tietosuoja sähköisessä kaupassa ja sähköisessä viestinnässä. Helsingin kauppakorkeakoulun julkaisuja B-110. Helsingin kauppakorkeakoulu – HSE Print 2009. (Viemerö 2009)

VIE PALVELUSI TIETOTURVALLISESTI VERKKOON
-
JOHDON TARKASTUSLISTA

TARKASTUSLISTA			Teemme itse, kuka?	Ulkoistamme, kenelle?
Palvelun sisältö (ks. jakso 1)	Sisältö ja sen ylläpito	Kuka toteuttaa[1]?		
		Kuka ylläpitää[2]?		
		Kuka valvoo[3]?		
	Palvelun suunnittelu ja muuttaminen	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
Toteutusvastuu ja yhteistyökumppanit (ks. jakso 2)	Osa-alueiden vastuuttaminen	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Tietoturvan huomioiminen sopimuksissa	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
Palvelimen sijoittaminen (ks. jakso 3)	Palvelimen sijoituspaikan valinta	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Palvelimen suojaaminen	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
Palvelun näkyminen verkossa (ks. jakso 4)	Tietoliikenneyhteys	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Verkkotunnus	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Nimipalvelut	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
Ohjelmisto ja palvelin (ks. jakso 5)	Käyttöönotto ja ylläpito	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Päivitykset ja niiden asentaminen	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Sovelluskehitys	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Varmuuskopiointi ja muu vikasietoisuus	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
Palvelun ylläpitoprosessi (ks. jakso 6)	Käyttäjätunnusten ja salasanojen hallinta	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Palvelun valvonta	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		
	Tietoturvaongelmiin varautuminen	Kuka toteuttaa?		
		Kuka ylläpitää?		
		Kuka valvoo?		

[1] Toteuttaminen tarkoittaa tässä palvelun toteutusprojektin aikaista tekemistä tai esim. toimintatapojen määrittelyä.
[2] Ylläpitäminen tarkoittaa tässä palvelun tietoturvallisuudesta huolehtimista jatkuvana prosessina.
[3] Johdon vastuulla on valvoa itse tai osoittaa joku valvomaan, että toteutus ja ylläpito suoritetaan sovitun mukaisesti ja että palvelu on lain ja muiden vaatimusten mukainen.

Ohjeita tarkastuslistan käyttäjälle

Tämä tarkastuslista on suunnattu pienten ja keskisuurten yritysten johdolle. Tarkastuslistassa tuodaan esiin tietoturvallisuuteen liittyviä seikkoja, jotka johdon on hyvä huomioida, kun se suunnittelee verkkosivujen tai jonkin muun verkkopalvelun toteuttamista tai siirtämistä verkkoon. Tarkastuslista on pyritty laatimaan siten, että sitä voidaan hyödyntää palvelun luonteesta riippumatta.

Verkkopalvelut voidaan toteuttaa lukemattomilla erilaisilla tavoilla: palvelu voidaan rakentaa itse, ostaa kokonaan ulkoa tai kaikkea tältä väliltä. Tästä johtuen myöskään palvelun tietoturvalliseksi toteuttamiseksi ei voida antaa yhtä mallia, joka soveltuisi kaikkiin mahdollisiin tilanteisiin.

Tarkastuslistaa voidaan hyödyntää varmistettaessa, että verkkopalvelun tietoturvan kannalta keskeiset osatekijät on vastuutettu. Palvelujen erilaisuudesta johtuen tapauskohtaisesti voi olla tarpeen lisätä tarkastuslistaan uusia kohtia tai poistaa siinä olevia osa-alueita. Verkkopalvelua toteutettaessa voi olla tarpeen huomioida tarkastuslistassa esitettyjen asioiden lisäksi esimerkiksi seuraavia asioita:

- **Tietoturvasta viestiminen palvelun käyttäjille**. Palvelussa on hyvä kertoa asiakkaalle, mihin sen tietoturvallisuus perustuu ja miten asiakas voi ottaa yhteyttä palveluntarjoajaan mahdollisissa ongelmatapauksissa. Palvelun käyttäjille on myös hyvä kertoa, miten he voivat huolehtia palvelun käyttämiseksi tarpeellisten laitteidensa ja ohjelmistojensa tietoturvasta.

- **Käyttäjien tunnistaminen ja rekisteröityminen**. Jos palvelun käyttö edellyttää käyttäjien tunnistamista tai rekisteröitymistä, tähän liittyvä prosessi on suunniteltava huolellisesti etukäteen. Esimerkiksi palvelun käyttäjien tunnustenhallinta on suunniteltava. Myös turhien tunnusten poistamiseen on syytä miettiä käytännöt. Salasanoja ei saa säilyttää tietokannassa, vaan sen sijaan on talletettava esimerkiksi salasanasta muodostettu tiiviste (Hash), jonka avulla salasanan oikeellisuus voidaan myöhemmin tarkistaa.

- **Väärinkäytöksiin varautuminen**. Palvelun väärinkäytöksiin kannattaa varautua. Joissain tapauksissa palvelun käytön systemaattinen valvonta voi olla välttämätöntä palvelua tarjoavaan yritykseen ja sen käyttäjiin kohdistuvien riskien hallitsemiseksi.

1 Palvelun sisältö

1.1 Sisältö ja sen ylläpito

Valta päättää palvelun sisällöstä on palvelun omistajalla. Siten omistajalla on viime kädessä myös vastuu sisällön lainmukaisuudesta.

Palvelussa käsiteltävien tietojen luonne määrittelee niihin sovellettavat käsittelysäännöt ja lainsäädännön sekä toimii palvelulle asetettavien tietoturvavaatimusten perustana. Palvelun toteuttamisen kannalta keskeisiä säännöksiä löytyy muun muassa seuraavista laeista:

- Henkilötietolaki
- Kuluttajansuojalaki
- Kauppalaki
- Tekijänoikeuslaki
- Laki tietoyhteiskunnan palvelujen tarjoamisesta
- Sähköisen viestinnän tietosuojalaki
- Laki sopimattomasta menettelystä elinkeinotoiminnassa
- Laki vahvasta sähköisestä tunnistamisesta
- Rikoslaki

Palvelun sisällön virheettömyys ja ajantasaisuus kannattaa varmistaa säännöllisesti. Myös sisällön päivittämisprosessista on syytä huolehtia. Lakikysymyksiä on avattu yksityiskohtaisemmin esimerkiksi kansallisen tietoturvastrategian toimenpideohjelman hankkeen 2 loppuraportin liitteenä 1 olevassa selvityksessä.

1.2 Palvelun suunnittelu ja muuttaminen

Suorituskyvyltään liian pieni toteutustapa estää asiakkaiden pääsyn palveluun. Toisaalta liian suuri toteutustapa aiheuttaa tarpeettomia kuluja.

Harva palvelu pysyy koko elinkaarensa ajan sisällöllisesti ja tekniseltä toteutukseltaan muuttumattomana. Siten jo palvelua suunniteltaessa on hyvä miettiä prosessia palvelun muuttamiseen ja kehittämiseen.

Palvelun suorituskyky on suhteutettava palvelun suunniteltuun asiakaskuntaan. Jo etukäteen on syytä miettiä malli palvelun laajentamiseen, jos palvelun käyttäjäjoukko kasvaa tulevaisuudessa merkittävästi. Myös palvelun erilaiset käyttötilanteet ja käytettävät päätelaitteet on syytä ottaa huomioon.

2 Toteutusvastuu ja yhteistyökumppanit

2.1 Osa-alueiden vastuuttaminen

Vaikka olet sopinut palvelun osa-alueen toteuttamisesta sopimuskumppanisi kanssa, olet vastuussa palvelun käyttäjille.

Verkkopalvelun toteuttamisesta on suositeltavaa sopia kaikkien palvelun toteuttamiseen osallistuvien tahojen kesken mahdollisimman selvästi. Parhaiten kunkin vastuulle osoitettujen seikkojen määritteleminen ja sovittuun vetoaminen onnistuu kirjallisten dokumenttien avulla. Pelkkä toteutusvastuista sopiminen ei kuitenkaan riitä. Lisäksi on valvottava, että kaikki sopijapuolet täyttävät velvoitteensa.

Kaikki tarjolla olevat sopimuskumppanit eivät ole välttämättä halukkaita muuttamaan omia vakiosopimusehtojaan asiakkaidensa tarpeita paremmin vastaaviksi, vaan tarjoavat asiakaskohtaisten palvelujen sijaan vakiomuotoisia palveluja. Tällaisissa tilanteissa on syytä tutustua yksityiskohtaisesti tarjottavan palvelun sisältöön ja tarvittaessa pyrkiä löytämään paremmin yrityksen tarpeisiin soveltuva yhteistyökumppani.

2.2 Tietoturvan huomioiminen sopimuksissa

Muiden toteuttajien tekemien toimenpiteiden merkitys vähenee ratkaisevasti, jos yksikin toteuttajista ei huolehdi oman vastuualueensa tietoturvasta.

Verkkopalvelun toteuttamista koskevissa tarjouspyynnössä, tarjouksessa ja niitä mahdollisesti seuraavassa sopimuksessa on suositeltavaa määritellä palvelun tietoturvavaatimukset ja kunkin sopijapuolen vastuu palvelun tietoturvallisessa toteuttamisessa ottaen huomioon palvelun koko elinkaari. Tarvittaessa voidaan sopia myös siitä, että palvelu auditoidaan tietyin väliajoin tietoturvan ajantasaisuuden varmistamiseksi.

Tärkeimpiä sovittavia asioita ovat tietoturvan kannalta ainakin:

- Käytettävien järjestelmien turvallinen asennus
- Tietoturvaongelmien seuranta, käsittely ja tiedottaminen
- Tietoturvakorjausten asennus järjestelmiin
- Haittaohjelmien torjunta
- Tietojen omistajuus ja luottamuksellisuus
- Sovelluksen tietoturvallinen toteutus ja vastuu korjauksista
- Varmistukset
- Toimittajan sitoutuminen jatkuvuuden varmistamiseen
- Tietojen luovutus ja poistaminen sopimuksen päättyessä
- Osapuolten yhteyshenkilöt ja yhteystiedot

Palveluntarjoajien kanssa on hyvä sopia asiakastuen ehdoista ja yhteyspisteistä etukäteen, jotta kiiretilanteissa saadaan apua mahdollisimman nopeasti. Myös neuvotteluasema on parempi palvelua ostettaessa kuin häiriötilanteessa.

3 Palvelimen sijoittaminen

3.1 Palvelimen sijoituspaikan valinta

Palvelimen ylläpitäminen vaatii osaamista ja työaikaa.

Tietoturva on usein helpointa järjestää hankittaessa palvelin ja sen ylläpito palveluna. Tällöin asiakkaalla voi kuitenkin olla vähemmän vaikutusmahdollisuuksia palvelun toteuttavan yrityksen noudattamiin ylläpitoprosesseihin.

Jos palvelin asennetaan yrityksen omaan ympäristöön, ylläpitoprosessien määritteleminen on täysin yrityksen omassa harkinnassa. Tällöin on kuitenkin tärkeää varmistaa, että yrityksestä löytyy riittävästi käytännön osaamista palvelimen ylläpitämiseen.

3.2 Palvelimen suojaaminen

Suojaamattoman palvelun tietoturvallisuus voidaan menettää sekunneissa.

Rikolliset etsivät verkosta jatkuvasti suojaamattomia palvelimia ja palveluja muun muassa skannausohjelmien avulla. Palvelin voidaan suojata esimerkiksi

palomuurin tai tietoliikenneyhteyden tarjoavan teleyrityksen tarjoamien suodatuspalveluiden avulla.

4 Palvelun näkyminen verkossa

4.1 Tietoliikenneyhteys

Paraskin suojaus palvelussa menettää merkityksensä, jos tiedot voidaan kerätä suoraan verkkoliikenteestä.

Jos hankittavaan palveluun ei sisälly tietoliikenneyhteyttä, se on hankittava itse. Palvelun toteuttamiseen käytettävä yhteys voidaan tarvittaessa salata. Yhteyden salaaminen on tarpeen esimerkiksi aina silloin, kun palvelussa käsitellään asiakkaan luottamuksellisia tietoja.

Web-palveluiden salaus toteutetaan tyypillisesti hankkimalla palvelulle maksullinen SSL-varmenne[4] luotettavalta taholta. Varmenne toimii myös asiakkaalle osoituksena palvelun verkkotunnuksen aitoudesta. SSL-varmenne on myös muistettava uusia määräajoin.

4.2 Verkkotunnus (domain-nimi)

Verkkotunnusta hankittaessa on syytä varmistua siitä, että tunnuksella ei loukata muiden suojattuja nimiä tai merkkejä.

Verkkotunnus voidaan usein hankkia oman tietoliikenneyhteyden tarjoajan kautta. Verkkotunnuksen voi hankkia myös suoraan esimerkiksi Viestintäviraston ylläpitämästä fi-verkkotunnuspalvelusta.

Käytettävän verkkotunnuksen omistajaksi merkittävään tahoon kannattaa kiinnittää erityistä huomiota. Palveluntarjoajalle on yleensä tärkeää, että sen palvelujen verkkotunnukset ovat sen omissa nimissä. Verkkotunnukset on myös muistettava uusia määräajoin.

4.3 Nimipalvelut (DNS-palvelut)

Verkkopalvelu ei toimi ilman nimipalvelinta.

Ilman verkkotunnukselle määriteltyjä nimipalvelimia verkkotunnuksen www-sivuja ei löydy internetistä eikä sähköposti mene perille. Nimipalvelut voidaan hankkia usein oman tietoliikenneyhteyden tarjoajan kautta.

5 Ohjelmisto ja palvelin

5.1 Käyttöönotto ja ylläpito

Kaikki ylimääräiset toiminnot lisäävät yhden uuden tavan menettää palvelun tietoturva ja toisaalta yhden uuden kokonaisuuden, jonka tietoturvallisuudesta on huolehdittava.

Käyttöönottovaiheessa on syytä huolehtia, että tuotteista ja palveluista otetaan käyttöön ainoastaan palvelun toimivuuden kannalta välttämättömät ominaisuudet. Lisäksi on syytä huomioida palvelun ylläpitämiseen käytettävien etäyhteyksien tietoturvallisuus.

---

[4] SSL-salausta käytettäessä tarvitaan varmenne (sertifikaatti). Varmenteen avulla käyttäjä voi paremmin selvittää, minkä palvelimen kanssa verkossa todellisuudessa asioi.

Palvelin vaatii jatkuvia ylläpitotoimia, kuten esimerkiksi levyjen täyttymisen seurannan ja vikojen havainnoinnin.

5.2 Päivitykset ja niiden asentaminen

Jokaisessa ohjelmistossa on tietoturvaongelmia. Koska merkittävä osa ongelmista löytyy vasta ohjelmistojen hankkimisen ja asentamisen jälkeen, ohjelmistoja on jatkuvasti päivitettävä.

Teknisen tietoturvallisuuden näkökulmasta on keskeistä huolehtia kaikkien palvelun toteuttamiseen käytettävien tuotteiden päivittämisestä. Päivittämistä vaativat ainakin seuraavat tuotteet:

- Palvelinalusta
- Julkaisujärjestelmä
- Käytetyt varusohjelmistot (esim. tietokanta-, palomuuri- tai virusohjelmistot).

Lähtökohtana voidaan pitää sitä, että mitä suositumpi ja siten hyökkääjien näkökulmasta houkuttelevampi sisällönhallintajärjestelmä tai palvelinalusta on, sitä todennäköisemmin tuotteesta löytyy tietoturvapuutteita.

Kaikki tuotteet eivät ilmoita päivitystarpeesta automaattisesti, vaan asiaa on seurattava itse esimerkiksi tuotteen verkkosivujen tai sähköpostilistan avulla. Päivitykset on myös asennettava.

5.3 Sovelluskehitys

Omassa ohjelmistokehityksessä on suurempi riski ajatteluvirheisiin, mikä voi avata uusia väärinkäyttömahdollisuuksia.

Jos palveluun liittyy itse tehtyjä tai ostettuja räätälöityjä sovelluksia, sovellusten riittävästä tietoturvatasosta on varmistauduttava kattavalla tietoturvatestauksella. Ostettaessa sovelluskehitystyötä, toimittajalle on tehtävä selväksi palvelun tietoturvavaatimukset sekä edellytettävä toimittajalta riittävää tietoturvaosaamista ja näyttöä lopputuloksen tietoturvallisuudesta.

5.4 Varmuuskopiointi ja muu vikasietoisuus

Laitteet rikkoutuvat ja ohjelmistoasennukset korruptoituvat ennemmin tai myöhemmin. Tietojen menetys voi pahimmassa tapauksessa johtaa yrityksen liiketoiminnan loppumiseen.

Palvelusta ja käsiteltävistä tiedoista on otettava säännöllisesti varmuuskopiot. Tällöin laitteiden hajoamisesta, tietoturvaloukkauksesta tai muusta syystä johtuva tietojen tai niiden luotettavuuden menetys häiritsee varsinaista toimintaa mahdollisimman vähän. Varmuuskopioiden toimivuus on hyvä testata säännöllisesti.

Verkkopalvelun saavutettavuudessa on huomioitava mahdolliset katkokset sähkön tai tietoliikenneyhteyksien saatavuudessa.

Tietoliikenneyhteyksien ja palvelimien kahdentaminen voi osoittautua yrityksen tarpeet huomioiden työlääksi ja kalliiksi. Tällaisissa tilanteissa hyllyssä pidettävä valmiiksi konfiguroitu varalaite voi olla hyvä vaihtoehto. Vikasietoinen RAID-levyjärjestelmä on kuitenkin välttämätön.

6 Palvelun ylläpitoprosessi

6.1 Käyttäjätunnusten ja salasanojen hallinta

Palvelun ylläpitämisestä vastaavien henkilöiden vaihtuessa tai unohtaessa tunnuksensa tai salasanansa, kirjautumismahdollisuus on pystyttävä palauttamaan.

Palvelun ylläpitäjien tunnustenhallintaprosessi on suunniteltava etukäteen. Prosessissa on varauduttava siihen, että kirjautumistunnukset ovat saatavilla esimerkiksi tunnusten unohtuessa tai henkilöstön vaihtuessa. Myös varahenkilöjärjestelyt on syytä miettiä esimerkiksi lomien ajaksi. Lisäksi on huolehdittava tarpeettomiksi käyneiden tunnusten poistamisesta.

6.2 Palvelun valvonta

Palveluun kohdistuvien väärinkäytösten havaitseminen edellyttää usein sellaista tietoa palvelun toiminnasta, jota palvelun teknisestä toteutuksesta vastaavalla yhteistyökumppanilla ei ole.

Verkkosivujen yleistä toimivuutta voidaan seurata suoraan palvelimelta. Hyödyllisempää on kuitenkin toimivuuden seuraaminen verkosta, jolloin voidaan todeta miten verkkosivut näkyvät asiakkaille. Palvelun yleisen toimivuuden lisäksi on syytä valvoa myös palvelun kannalta keskeisten toimintojen toimivuutta.

Verkkosivujen kävijöiden ja näiden käyttäytymisen seuranta toteutetaan tyypillisesti verkkosivuille lisättävällä selainkoodilla (JavaScript) ja ulkopuolisella seurantapalvelulla.

Palveluun kohdistuvien tahallisten tietoturvaloukkausyritysten selvittäminen vaatii usein manuaalista palvelun tallentamien tietojen läpikäyntiä. Esteinä tietoturvaongelmien tehokkaalle selvittämiselle ovat tyypillisesti lokien puuttuminen, tietojärjestelmien kellojen epätarkkuudesta tai sekavista aikavyöhykemerkinnöistä johtuva lokien epäyhteensopivuus tai harjaantumattomuus lokien analysointiin.

6.3 Tietoturvaongelmiin varautuminen

Tietoturvaongelmia voi esiintyä kaikissa palveluissa. Niihin on syytä varautua etukäteen.

Ongelmatilanteisiin on syytä varautua jo etukäteen. Toimintaprosesseissa on syytä huomioida ainakin toipumisen edellyttämien toimenpiteiden ja yhteistyökumppaneiden tunnistaminen.

Tietoturvaloukkauksesta voidaan tarvittaessa tiedottaa niille asiakkaille, joita loukkaus koskee. Muualta tullut tieto tapahtuneesta kolhaisee palvelun mainetta yleensä omaa ilmoitusta enemmän. Tietoturvaloukkauksista kannattaa ilmoittaa tarvittaessa myös kansalliselle tietoturvaviranomaiselle CERT-FI:lle, joka voi tarjota apuaan loukkauksesta toipumiseen. CERT-FI:llä on lakisääteinen salassapitovelvollisuus saamistaan tiedoista. Rikoksen tunnusmerkistön täyttävistä teoista kannattaa ilmoittaa myös poliisille.