Kuhmon kaupungin tietosuoja- ja tietoturvapolitiikka

Kaupunginhallitus, 21.8.2018 (176 §)

Sisällys

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Kuhmon kaupungin tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee henkilötietojen käsittelyä, jossa Kuhmon kaupunki toimii rekisterinpitäjänä.

Kuhmon kaupungin palveluiden perustana ovat kuntalaisten tarpeet. Palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn Kuhmon kaupungin ja sen konsernin toimintaympäristöissä. Kaupungin palvelutuotanto on riippuvainen ICT-teknologiasta ja -palveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Kustannustehokas digitalisointi edellyttää tietoturvallisuuden kaikkien osa-alueiden huomioimisen lisäksi myös tietosuojan huomioimista jo suunnitteluvaiheessa.

Tietosuojassa ei ole kysymys tiedon ”panttaamisesta” tai ”pimittämisestä” vaan tietosuojaosaamisella voidaan lisätä organisaation tuottavuutta ja tehokkuutta sekä säästää kustannuksia. EU:n yleisen tietosuoja-asetuksen myötä tietosuojasta, tietosuojatyön organisoinnista ja itse tietosuojatyöstä sekä koko henkilöstön tietosuojaosaamisesta tulee organisaatioiden operatiivisen toiminnan menestystekijä.

Kuhmon kaupungin johto tietosuojatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana Kuhmon kaupungin tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee koko kaupunkiorganisaatiota ja sen henkilöstöä mukaan lukien kaupunkikonsernin sekä niitä Kuhmon kaupungin sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Kuhmon kaupungin omistamaa tai hallinnoimaa tietoa. Politiikka kattaa Kuhmon kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä politiikka on saatavissa Kuhinasta. Politiikka liitetään tarvittaessa Kuhmon kaupungin toimeksiantosopimuksiin.

Tietosuojan määritelmä

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla (kts. kappale Tietosuojan toteuttaminen). Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen.

Tietosuojan tavoitteet ja periaatteet

Kuhmon kaupungin lähtökohtana tietosuojassa on riskilähtöisyys. Kuhmon kaupunki rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa Kuhmon kaupungin riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

Kuhmon kaupunki toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

Kuhmon kaupungin toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Kuhmon kaupungin tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

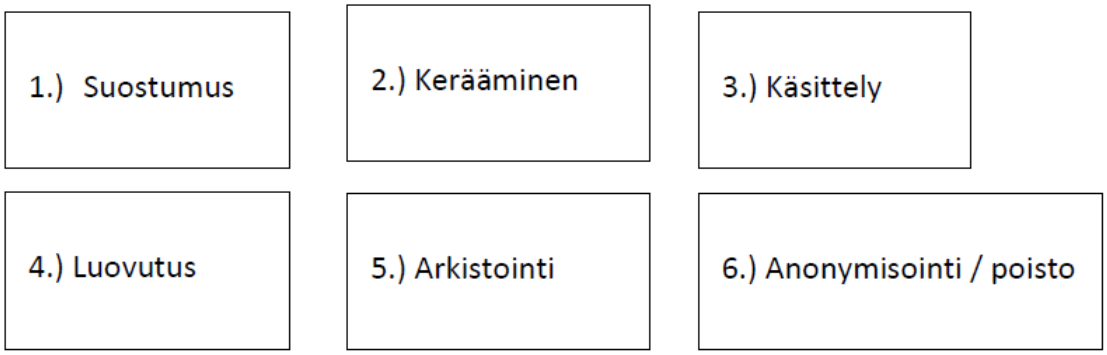
Tietosuojan toteuttaminen

Kuhmon kaupunki haluaa toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Kuhmon kaupunki toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi. Edellä mainittujen toimenpiteiden avulla varmistetaan mm, että:

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen

- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilö määrän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin

Tietosuojan toteuttamisessa Kuhmon kaupunki haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.



Kuva: Henkilötietojen elinkaaren vaiheet

Kuhmon kaupungin järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tietosuojavaatimuksia ovat toimialakohtaiset lait esimerkiksi käsiteltäessä työntekijöiden henkilötietoja työnantajan roolissa. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Kuhmon kaupunki voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Kuhmon kaupunki valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Kuhmon kaupungin ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti. Kuhmon kaupunki rekisterinpitäjänä sisällyttää tietosuojan myös hankehallintamallinsa osaksi.

Rekisteröityjen tietopyyntöprosessi

Kuhmon kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Tämän prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.
Käytännössä rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa toimitaan siten, että kysely ohjataan sähköpostiosoitteeseen tietosuoja@kuhmo.fi
Jatkossa kyselyissä tullaan huomioimaan kyselyjen tekeminen suomi.fi –sivuston kautta.

Henkilöstön tietosuojakoulutus

Kuhmon kaupunki huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Myös organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä rooleissa, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Kuhmon kaupungissa on määritetty toimintaprosessi liittyen toimintaan tietoturvaloukkausten tapahtuessa. Tämän prosessin mukaista toimintatapaa noudatetaan tietosuojapoikkeamien sattuessa. Ohjeistus annetaan tietosuojavastaavan toimesta. Henkilöstölle koulutetaan, miten toimitaan tietoturva- ja tietosuojapoikkeamatilanteissa.

Kaupungin toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Varautumistyötä johtaa kaupunginjohtaja yhdessä kaupunginhallituksen kanssa.

Suunnittelussa tulee varautua pieneen, keskisuureen ja suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin. Poikkeusoloissa toimintaa johtaa viranomainen (johtovastuu voi muuttua tilanteen edetessä) ja kaupungin valmiussuunnitelma / häiriötilanteiden suunnittelu ja organisaatio tukee sen toimintaa. Poikkeusolojen ja vakavien häiriötilanteiden varalta on päätökset käskyvaltasuhteiden muutoksista valmisteltava huolellisesti ennakolta, jotta tilanteen niin vaatiessa siirtyminen toimimaan linjaorganisaationa on nopeasti toteutettavissa. Huolellista ennakkovalmistelua edellyttävät erityisesti sopimusohjaustilanteet.

Kuhmon kaupunginvaltuusto hyväksyy kaupunkikonsernia koskevat sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa. Sisäisen valvonnan ja riskienhallinnan organisointi on kuvattu Kuhmon kaupungin hallintosäännössä §:ssä 78.

Henkilötietojen tietoturvaloukkauksen sattuessa Kuhmon kaupungilla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

Rikkomukset ja seuraamukset

Tietosuojarikkomukset käsitellään tapauskohtaisesti ja mahdollisiin seuraamuksiin sovelletaan liitteissä olevaa tietosuojarikkomusten seuraamustaulukkoa (Liite 4).

Liitteet

Liite 1 Lakiluettelo

Liite 2 Tietosuojavastuut

Liite 3 Keskeiset käsitteet

Liite 4 Tietosuojarikkomusten seuraamustaulukko

LIITE 1 Tietosuojaan liittyvää lainsäädäntöä

Perustuslaki (731/1999)

Kuntalaki (410/2015)

Hallintolaki (434/2003)

Arkistolaki (831/1994)

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

Laki viranomaisen toiminnan julkisuudesta (621/1999)

Henkilötietolaki (523/1999)

Euroopan unionin yleinen tietosuoja-asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU 679/2016)

Euroopan parlamentin ja neuvoston direktiivi, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (EU 680/2016)

Laki yksityisyyden suojasta työelämässä (759/2004)

Laki kunnallisesta viranhaltijasta (304/2003)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)

Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)

Rikoslaki (39/1889)

Työsopimuslaki (55/2001)

Valmiuslaki (1552/2011)

Tietoyhteiskuntakaari (917/2014)

Tekijänoikeuslaki (404/1961)

Lukiolaki (629/1998)

Perusopetuslaki (628/1998)

Oppilas- ja opiskelijahuoltolaki (1287/2013)

LIITE 2

Tietosuojavastuut Kuhmon kaupungissa

Tämä dokumentti kuvaa tietosuojan vastuut ja velvollisuudet Kuhmon kaupungissa.

Tietosuojan vastuujärjestelyn tulee seurata kaupungin toiminnan mahdollisia muutoksia. Monet alla mainituista vastuista voivat kuulua samankin henkilön tehtäviin ja vastuisiin. Olennaista on, että näiden tehtävien hoito on järjestetty, myös varahenkilöiden osalta.

Yleinen vastuu tietosuojan valvonnasta ja ylläpitämisestä

Tietosuojan toteutumisen valvontaan ja ylläpitämiseen osallistuu jokainen kaupungin henkilöstöön ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan.

Tietosuoja on osa työtehtäviä

Suurin osa tietosuojan toteuttamiseksi tehdystä työstä sisältyy Kuhmon kaupungissa työskentelevien normaaleihin tehtäviin. Tietosuojan ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä vastuuhenkilöitä.

Tietosuojan vastuutaulukko

Rooli	Vastuu	Valvontavastuu
Kaupunginhallitus	Tietosuojapolitiikan hyväksyminen	
Kaupungin johtoryhmä	Tietosuojapolitiikan käsittely Tietojen turvaluokittelujärjestelmä Tietojen omistajien määrittäminen - yksikkökohtaisten erityisvaatimusten määrittäminen Tiedon ja tietojärjestelmien omistajien nimeäminen	Hallintojohtaja vie johtoryhmäkäsittelyä varten ja varmistaa, että asia valmistellaan ja viedään päätöksentekoon.
Hallintojohtaja	Tietosuojapolitiikan valmistelu Tietosuojapolitiikan ylläpitäminen Tietosuojaryhmän johtaminen Tietosuojan hallinnointi, ohjeistus ja koordinointi Organisaation järjestelmien tietosuojan toteutumisen valvonta Organisaation tietosuojaan liittyvä tiedottaminen Tietosuojakoulutuksen suunnittelu yhdessä HR:n kanssa Tietosuojatietämyksen hankkiminen ja ajan tasalla pitäminen sekä tietämyksen jakaminen Poikkeustilanteiden koordinointi	Kaupunginjohtaja
Tietoturvaorganisaatio (riskienhallinnan johtoryhmä)	Organisaation tietosuojaratkaisujen määrittäminen, kehittäminen ja muutoksien hyväksyminen Viestiä tietosuoja-asioista ja tietosuojapuutteiden ja poikkeamien käsittelyn käynnistämisestä Osallistua tietosuojaperiaatteiden määrittelyyn Avustaa johtoa ja yksiköitä tietosuoja-asioiden toimeenpanossa Tietosuojasuunnitelman valmistelu osana kaupungin riskienhallintaa Tietosuojan mittariston valmistelu ja tietosuojaa koskevan seurannan järjestäminen Raportointi ylimmälle johdolle tietosuojan tilanteesta Yrityksen tietosuojaohjeiden- ja käytäntöjen kehittäminen, valmistelu ja muutosten hallinta Vastuu poikkeustilanteiden käsittelystä	Hallintojohtaja
Tietosuojaryhmä	Organisaation tietosuojaratkaisujen ja niihin liittyvien ohjeiden määrittämisen ja kehittämisen valmistelu	Hallintojohtaja
Tietosuojavastaava	Tietosuoja-asioiden neuvonta ja opastus Tietosuoja-asetuksen noudattamisen seuranta Yhteistyö valvontaviranomaisen kanssa	Hallintojohtaja
HR	Tietosuojakoulutuksen suunnittelu, organisointi ja seuranta	Talousjohtaja

Tiedon omistaja	Tietojen luottamuksellisuuden ja käytettävyyden varmistaminen lakien, asetusten, tietosuojapolitiikan ja ohjeiden mukaisesti. Pääkäyttäjien nimeäminen vastuulla olevien järjestelmien osalta	Ao. esimies
Henkilötietojen käsittelijä (ulkoistettu)	Henkilötietojen huolellinen käsitteleminen Kuhmon kaupungin lukuun kirjallisen sopimuksen ja rekisterinpitäjän ohjeiden mukaisesti	Sopimuksen vastuuhenkilö(t)
Tietojärjestelmien omistajat	Käyttövaltuushallinnan määrittely, kuvaaminen ja ohjeistus	Ao. esimies
Palvelualuejohtajat, vastuuyksiköiden esimiehet ja palveluyksiköiden esimiehet	Tietosuojan toteutuminen alaisessaan toiminnassa	Johtoryhmä
Esimies	Tietosuojan toteutumisen valvonta Tiedon omistajien määrittäminen johtamisjärjestelmän vastuiden mukaisesti Oman yksikkönsä tietosuojakoulutukseen osallistumisesta huolehtiminen Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietosuojatavoitteet ja periaatteet Nimeää tietosuojayhteyshenkilön, joka raportoi tietosuojaryhmälle yksikön aikaansaannoksista ja tekemistä	Ao. esimies

Liite 3 Keskeiset käsitteet

Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.

Tietosuojapolitiikka

Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot

Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.

Henkilötietojen käsittelijä

Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Henkilötietojen käsittely

Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.

Osoitusvelvollisuus

Osoitusvelvollisuuden (accountability) avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen ja
- eheys ja luottamuksellisuus.

Rekisterinpitäjä

Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden
kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity

Henkilö, jonka henkilötietoja käsitellään.

Tietosuojavastaava

Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä määritellyissä tilanteissa:

- jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin),
- ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa laajassa mitassa, tai
- ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin.

Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan. Yritysryhmä voi nimittää yhden tietosuojavastaavan samoin kuin yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.

Hallinnollinen sakko

Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella. Sakon enimmäismäärä on 20 milj. € tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.

Hallinnolliset seuraamukset

Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.

Anonymisointi

Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista.

Pseudonymisointi

Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Rekisteriseloste, tietosuojaseloste

Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitetyssä, avoimessa ja helposti ymmärrettävässä muodossa.

Tietotilinpäätös

Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä.

Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden (accountability) toteuttamisessa.

Vaikutustenarviointi

Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.

Lapsen henkilötietojen käsittely

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuojaperiaatteiden sisällyttäminen aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Periaatteiden huomioiminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä, siten että varmistetaan käsittelyn vastaavuus tietosuoja-asetuksen vaatimusten kanssa. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta mm.

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilyttää suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen

- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilö määrän saataville
- taataan rekisteröityjen oikeuksien toteutuminen

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta aina koko käsiteltävien henkilötietojen elinkaaren loppuun.

LIITE 4

TEON TAHALLISUUDEN ASTE

RIKKOMUKSEN VAKAVUUS

	Tietämättömyys **Osaamattomuus** **Huolimattomuus** **Vahinko** **Tahattomuus**	**Piittaamattomuus** **Törkeä huolimattomuus** **Välinpitämättömyys** **Tahallisuus** **Toistuvuus**	**Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, aseman/väärinkäyttö)** **Hyötymistarkoitus**
Vakava rikkomus/rikos Potilastiedon tai liikesalaisuuden luvaton käsittely ja luovuttaminen Hakkerointi, tunkeutuminen Rikoslain alaisen materiaalin oikeudeton käsittely Tekijänoikeuslain alaisen materiaalin laiton levittäminen Virusten tahallinen levittäminen	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen) Ohjelmien ja pelien luvaton kopiointi Luvattomien ohjelmien asentaminen Ylläpitäjän työkalujen luvaton hallussapito Palvelun luvaton pystytys Tunnuksen luovuttaminen Tiedon luottamuksellisuuden vaarantaminen	Kirjallinen varoitus Huomautus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Käyttöoikeuden peruminen Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämismenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus
Lievä rikkomus (väärinkäytös) Henkilökohtaisen tietoturvan laiminlyönti Epäasiallinen käytös Haitan aiheuttaminen Resurssien tuhlaus Virustorjunnan laiminlyönti Luvaton kaupallinen tai poliittinen toiminta Kulunvalvontasääntöjen rikkominen	Huomautus Opastus Puheeksi ottaminen	Kirjallinen varoitus Opastus Huomautus Puheeksi ottaminen	Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus