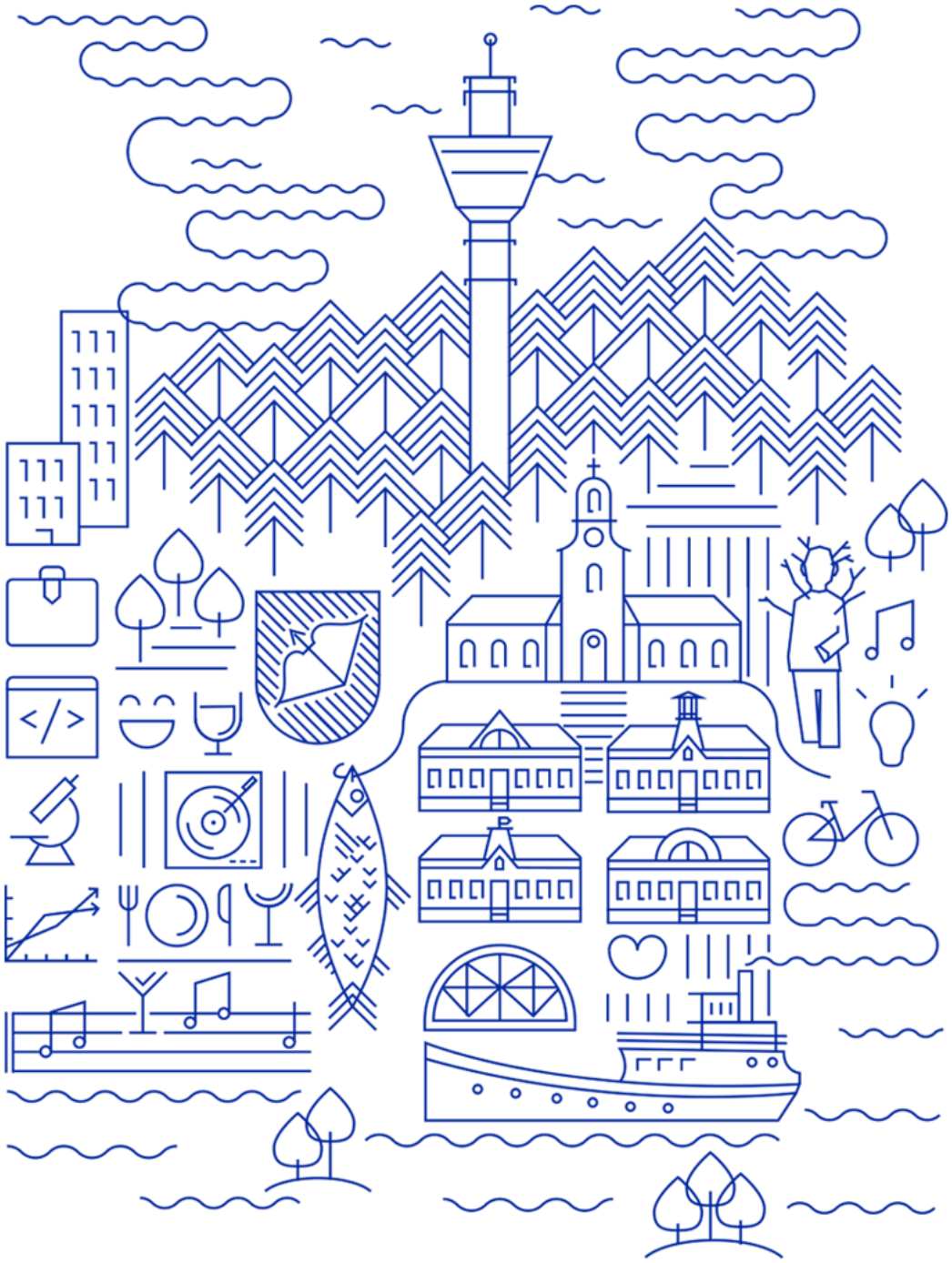
KUOPIO



Ohjeistus henkilötietojen käsittelijälle

Kuopion kaupunki

2.1.2019

Sisällys

2.1.2019

1 Rekisterinpitäjän ohjaus henkilötietojen käsittelyssä

1.1 Ohjeen tarkoitus

Rekisteröityjen oikeusturvan vuoksi on tärkeää, että Kuopion kaupungin sopimuskumppanit käsittelevät toimeksiantojen yhteydessä henkilötietoja huolellisesti. Henkilötietoja tulee käsitellä Kuopion kaupungin yleisen sopimusten tietosuojaliitteen [Henkilötietojen käsittelyn vaatimukset] tai Kuopion kaupungin IT-sopimusten tietosuojaliitteen [JHS166 Liite 1 ja 9] mukaan sekä Liite A [Henkilötietojen käsittelyn kuvaus] ja siitä johdettujen ohjeiden mukaisesti.

Ohjeiden tarkoitus on ohjata käsittelyä käytännössä. Ohjeissa sivutaan keskeisimpiä käsitteitä ja käsittelyn periaatteita, joiden perusteella henkilötietojen käsittelijänä olevan sopimuskumppanin tulee toimia.

Epäselvissä tapauksissa on henkilötietojen käsittelijän vastuulla pyytää lisäinformaatiota Kuopion kaupungin sopimuksen yhteyshenkilöltä sellaisista yksityiskohdista tai asiakokonaisuuksista, joiden toteuttamisesta on mahdollisesti epäselvyyttä tai epävarmuutta.

Henkilötietojen käsittelijällä tarkoitetaan Kuopion kaupungin palveluntuottajana/toimittajana toimivaa sopimuskumppania.

Rekisterinpitäjällä tarkoitetaan Kuopion kaupunkia.

1.2 Mitä tietosuojariskit ovat?

Organisaatiosta riippumatta tietosuojaan liittyvät riskit voidaan jakaa sisäisiin ja ulkoisiin riskeihin.

Sisäisiä riskejä voidaan estää koulutuksen tarjoamisella työntekijöille, ohjeistuksen saatavuudella ja mahdollisuudella kehittää omaa osaamista.

Ulkoisia riskejä ovat usein sopimuskumppanin tekemät virheet henkilötietojen käsittelyssä, luottamuksellisen tiedon vuotaminen organisaation ulkopuolelle tai jokin muu organisaation mainetta vahingoittava tapahtuma.

Myös lainsäädäntöön liittyvät tulkintaepäselvyydet ja väärinkäsitykset voivat muodostua ongelmiksi ja pahimmillaan riskeiksi.

1.3 Keskeisimmät käsitteet

Alla listatut käsitteet ja määritelmät on tarkoitettu helpottamaan tietosuojan aihepiirin ymmärtämistä.

Henkilötiedolla tarkoitetaan henkilöön liittyviä tietoja, joista hänet voidaan tunnistaa suorasti tai epäsuorasti. Henkilö voidaan tunnistaa ns. tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilötiedon määritelmä on näin ollen todella laaja.

Henkilötietojen käsittelijä tarkoittaa luonnollista henkilöä tai organisaatiota, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Henkilötietojen käsittely tarkoittaa toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko tietoteknisesti tai manuaalisesti. Se tarkoittaa esimerkiksi tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä ja käyttöä. Lähes mitkä tahansa henkilöön liittyviin tietoihin kohdistuvat toimet ovat siis henkilötietojen käsittelyä lain näkökulmasta. Myös se, että jonkin henkilötiedon jättää jollakin tavalla saataville tai nähtäville, on henkilötietojen käsittelyä.

Henkilörekisterillä tarkoitetaan mitä tahansa henkilötietojen joukkoa, joka on jäsennelty ja josta tiedot ovat saatavilla tietyin perustein. Sillä ei ole merkitystä, ovatko tiedot eri järjestelmissä. Jos ne ovat yhteenkuuluvia sekä samaa käyttötarkoitusta varten ja samaa logiikkaa noudattaen kerättyjä, ne kuuluvat samaan henkilörekisteriin. Tiedot voivat olla jopa eri maissa ja silti kuulua samaan henkilörekisteriin.

Luonnollinen henkilö tarkoittaa esimerkiksi henkilötietojen käsittelijäorganisaation työntekijää.

Osoitusvelvollisuus koskee sekä rekisterinpitäjä- että henkilötietojen käsittelijäorganisaatiota. Osoitusvelvollisuuden (= tilivelvollisuus / accountability) avulla organisaation on pystyttävä osoittamaan, että se on huolehtinut henkilötietojen käsittelyn periaatteista (ns. tietosuojaperiaatteista):

1. lainmukaisuus, kohtuullisuus ja läpinäkyvyys
2. käyttötarkoitussidonnaisuus
3. tietojen minimointi
4. täsmällisyys
5. säilytyksen rajoittaminen ja
6. eheys ja luottamuksellisuus.

Näiden termien merkitystä on avattu enemmän jäljempänä luvussa 2. ”Henkilötietojen käsittelyn periaatteet”.

Tietoturva kattaa kaikkeen tietoon, sen eri muodoissa, liittyvät tekniset ja hallinnolliset toimenpiteet, joilla mahdollistetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyminen. Henkilötieto on eräs tärkeä suojattavan tiedon muoto, jonka suojaaminen katetaan termillä tietosuoja.

Tietoturvaloukkaus on tapahtuma, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai luvaton pääsy tietoihin. Tämän asian käytännön hallitseminen on erittäin tärkeää rekisteröityjen oikeusturvan kannalta. Henkilötietojen käsittelijätaholla tulee olla selkeä toimintamalli sen varalle, miten se toimii esimerkiksi tiedottamisen osalta tietoturvaloukkaustilanteessa. Toimintamalli tulee pystyä näyttämään toteen myös rekisterinpitäjälle eli Kuopion kaupungille.

Profilointi tarkoittaa mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietojen avulla arvioidaan tiettyjä henkilön ominaisuuksia tai analysoidaan tai ennakoidaan näkökohtia, jotka liittyvät kyseiseen henkilöön. Profiloinnissa analysoidaan tai ennakoidaan esimerkiksi työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin tai kiinnostuksen kohteisiin, luotettavuuteen tai käyttäytymiseen sekä sijaintiin tai liikkeisiin liittyviä asioita. Profilointia käytetään esimerkiksi lukuisissa sosiaalisen

median palveluissa. Käsittelijätaholla ei ole oikeutta käsittelemiensä tietojen pohjalta suorittaa profilointia omiin tarkoituksiinsa. Profilointi on sallittua ainoastaan silloin kun Kuopion kaupunki on valtuuttanut käsittelijän suorittamaan profilointia.

Rekisteröity on luonnollinen henkilö (ei yritys tai organisaatio), jonka henkilötietoja käsitellään.

Rekisterinpitäjällä tarkoitetaan ihmistä tai oikeushenkilöä eli viranomaista, virastoa tai muuta elintä, joka yksin (tai yhdessä toisten kanssa) määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä on siis se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

Yhteisrekisterinpitäjiä ovat ne, jotka yhdessä toisten kanssa määrittelevät henkilötietojen käsittelyn tarkoitukset ja keinot.

2 Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyn periaatteet ovat henkilötietojen oikeanlaisen käsittelyn perusta ja kaikkien Kuopion kaupungin sopimuskumppaneiden tulee henkilötietoja käsitellessään toimia niiden mukaisesti. Käsittelyn periaatteiden noudattamisella voidaan varmistaa rekisteröityjen oikeuksien toteutuminen käytännössä. Henkilötietojen käsittelyssä tulee aina huomioida yhtäaikaisesti kaikki alla mainitut periaatteet. Tietosuojaperiaatteet tulee huomioida koko henkilötietojen käsittelyn elinkaaren ajan, eli niiden keräämisestä niiden arkistointiin tai tuhoamiseen.

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys tarkoittavat, että rekisteröityjen tulee tietää, miten heitä koskevia tietoja kerätään ja käsitellään. Käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä rekisteröityjen näkökulmasta. Rekisteröityjen tulee tietää rekisterinpitäjän henkilöllisyys ja käsittelyn tarkoitukset. Kuopion kaupungin pitää pystyä antamaan rekisteröidyille tieto heitä koskevien henkilötietojen käsittelystä sekä siitä, miten Kuopion kaupunki varmistaa henkilötietojen käsittelyn asianmukaisuuden ja läpinäkyvyyden. Tämän vuoksi myös henkilötietojen käsittelijän toiminta on erityisen tärkeässä asemassa rekisteröityjen oikeuksien toteuttamisessa.

Käyttötarkoitussidonnaisuuden mukaan henkilötietojen keräämisen tulee olla sidonnainen käyttötarkoitukseen, eli tietojen keräämisen tulee tapahtua aina jotakin tiettyä (tarkoin määritelty kohde), nimenomaista (vain jotakin tiettyä ennalta suunniteltua) ja laillista tarkoitusta (käsittelyn oikeusperuste) varten. Kerättyä tietoa ei saa käyttää myöhemmin muuhun tarkoitukseen. On olemassa joitakin harvinaisia poikkeuksia käyttötarkoitussidonnaisuudesta poikkeamiseen.

Tietojen minimoinnin periaatteen mukaan henkilötietojen on oltava asianmukaisia, olennaisia, riittäviä ja rajoituttava siihen, mikä on tarpeellista niiden käsittelyn tarkoitusten kannalta. Henkilötietojen säilytysajan on oltava mahdollisimman lyhyt. Henkilötietoja ei voi säilyttää vain varmuuden vuoksi, vaan niiden säilyttämiselle tulee aina olla jokin lainmukainen peruste. Kuopion kaupunki asettaa määräajat henkilötietojen poistolle, joita käsittelijä noudattaa. Jos tarkkoja määräaikoja ei voida asettaa, Kuopion kaupunki antaa kriteerit henkilötietojen poiston määräajoille.

Tietojen täsmällisyyden periaatteen mukaan henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Kuopion kaupungin on kohtuullisin toimenpitein varmistettava, että

käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä, esimerkiksi muutoksenhakuajan päätyttyä. Tällöin henkilötietojen käsittelijän velvollisuutena on toimia Kuopion kaupungin ohjeistuksen mukaan. Rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitystä kuten muuttunut osoite tmv. tieto, jolloin henkilötietojen käsittelijän tulee avustaa Kuopion kaupunkia rekisterinpitäjänä ylläpitämään henkilötiedot tarkkoina ja täsmällisinä.

Tietojen säilytyksen rajoittaminen tarkoittaa, että henkilötiedot on säilytettävä sellaisessa muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin se on tarpeellista tietojen käsittelyä varten. Tietoja voi kuitenkin säilyttää kauemmin, mikäli tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten. Tällaisista poikkeuksista Kuopion kaupunki kuitenkin tiedottaa henkilötietojen käsittelijää erikseen, joten henkilötietojen käsittelijän vastuulla on noudattaa sitä toimintamallia, jonka mukaan Kuopion kaupunki on velvollinen toimimaan näissä tapauksissa.

Tietojen eheyden ja luottamuksellisuuden periaatteiden mukaisesti henkilötietoja käsiteltäessä on varmistettava asianmukainen tietoturvallisuus eli tietojen eheys, luottamuksellisuus ja saatavuus. Tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tekniset toimet kuten tietojen salaus ja erilaisten tunnistautumiskeinojen käyttö on toteutettava myös henkilötietojen käsittelijän toiminnassa, jotta henkilötiedot säilyisivät ulkopuolisten ulottumattomissa ja sellaisessa muodossa, josta ei voida tunnistaa tiettyä henkilöä tai hänen yksityiselämäänsä kuuluvia muita henkilöitä. Hallinnollisia keinoja, kuten ohjeistuksen saatavilla pito ja toimittaminen organisaatiolle ovat myös olennaisia eheyttä ja luottamuksellisuutta ylläpitäviä toimia.

3 Henkilötietojen käsittelyyn oltava aina peruste

Henkilötietojen käsittelyyn on aina oltava peruste, joka on määritelty laissa. Kuopion kaupungin ja sen valitseman sopimuskumppanin välinen yhteistyö perustuu niiden keskinäiseen sopimukseen. Näin ollen henkilötietojen käsittelijän oikeusperuste käsitellä kyseisiä henkilötietoja on sopimus.

Henkilötietojen käsittelyn tulee aina rajoittua sovittuun laajuuteen ja liittyä käsittelytarpeeseen ja -perusteeseen. Jos käsittelijä on epävarma oikeudestaan käsitellä henkilötietoa, hänen tulee olla yhteydessä oman organisaationsa tietosuojayhteyshenkilöön tai Kuopion kaupungin sopimuksen yhteyshenkilöön.

4 Henkilötietojen luovuttaminen Kuopion kaupungin henkilörekisteristä

Se, onko henkilörekisterissä oleva tieto julkista, määräytyy julkisuuslain säännösten nojalla. Suuri osa henkilötiedosta on luottamuksellista. Käsittelijä ei siis itse voi tehdä päätöstä siitä, milloin hän antaa rekisteröityjen henkilötietoja julkisuuteen. Pääsääntöisesti voidaan todeta, että mikäli Kuopion kaupunki ei rekisterinpitäjänä ole ohjeistanut henkilötietojen käsittelijää tietojen antamisesta rekisteristä eikä aihetta ole otettu huomioon sopimuksessa, käsittelijä ei ole oikeutettu antamaan henkilötietoja julkaistavaksi kenenkään toimesta.

Vaikka henkilörekisterissä olisi jo sinänsä julkisia henkilötietoja, niitä ei saa ilman rekisterinpitäjän erillistä varmistusta luovuttaa sivulliselle. Sivullisilla tarkoitetaan muita kuin rekisterinpitäjää, henkilötietojen käsittelijää tai rekisteröityä. Ainoastaan Kuopion kaupunki voi kirjallisesti ohjeistaa toimimaan tällä tavalla, ja vain silloin henkilötietojen käsittelijä voi luovuttaa henkilötietoja sivulliselle. Käsittelijän tulisi aina varmistua siitä, onko tiedon pyytäjällä, ”luovutuksensaajalla”, oikeus saada haltuunsa kyseinen henkilötieto. Näissä tapauksissa tulee siis aina kääntyä Kuopion kaupungin sopimuksen yhteyshenkilön puoleen.

5 Henkilötietojen käsittelijän velvollisuuksia

Henkilötietojen käsittelijänä toimivan sopimuskumppanin tietojärjestelmän tai palvelun ylläpitämiseen tarkoitettuja tunnuksia ja oikeuksia saa käyttää vain järjestelmän tai palvelun ylläpitämisen vaatimissa työtehtävissä. Käsittelijätahon tietosuojayhteyshenkilö sitoutuu huolehtimaan, että tämä toteutuu käytännössä.

Tietojärjestelmän sisältämät henkilötiedot ylläpidetään, tallennetaan ja suojataan tietosuojaa ja tietoturvaa koskevien sopimusliitteiden mukaisesti. Silloin kun henkilötietojen käsittelijän ei ole tarpeen käsitellä henkilötietoja Kuopion kaupungin järjestelmässä, sillä ei ole pääsyoikeutta kyseiseen Kuopion kaupungin järjestelmään. Mikäli tähän pääsääntöön tulee poikkeuksia, niistä sovitaan erikseen Kuopion kaupungin edustajan kanssa ja niistä tehdään erilliset sitoumukset.

Henkilötietojen käsittelijän ylläpitoyhteyksien tulee olla salattuja ja kerätä lokitietoja. Henkilötietojen käsittelytoimien lokitiedot tulee säilyttää henkilötietojen käsittelijän järjestelmässä siten, että henkilötietojen käsittelijän puolelta ei ole mahdollisuutta muuttaa, poistaa tai siirtää lokitietoja. Lokitiedot säilytetään, kuten lainsäädännössä edellytetään tai kuten Kuopion kaupungin erillisessä lokitietojen ohjeistuksessa kerrotaan.

Käsitellessään arkaluonteisia henkilötietoja henkilötietojen käsittelijän on noudatettava erityistä huolellisuutta ja varovaisuutta, kuten varmistettava, että tietoihin pääsy on rajattu tavanomaista pienemmälle käsittelijäjoukolle sekä toteutettava muita erityisiä organisatorisia ja teknisiä sekä muita erityisten henkilötietoryhmien käsittelyn vaatimia varmistuksia. Tämän mukaisesti henkilötietojen käsittelijän tulee muun muassa varmistaa, että kyseiset palvelut ja tietojärjestelmät keräävät lokitietoja, joiden avulla voidaan varmistaa kyseisten henkilötietojen käsittelyn asianmukaisuus ja tietoturvallisuus.

Kuopion kaupungilla on oikeus ja velvollisuus tarpeen vaatiessa päivittää näitä ohjeita ja henkilötietojen käsittelijä on osapuolten välillä sovitun mukaisesti sitoutunut noudattamaan päivitettäviä ehtoja. Henkilötietojen käsittelijän tulee myös viipymättä ilmoittaa Kuopion kaupungille, jos se pitää saamaansa ohjetta henkilötietojen käsittelyä koskevan lainsäädännön vastaisena.

Henkilötietojen käsittelijän tulee ilmoittaa Kuopion kaupungille henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa siitä, kun loukkaus on tullut käsittelijän tietoon. Lisäksi käsittelijän tulee ilmoittaa ilman aiheetonta viivytystä muista toimittamansa järjestelmän tai palvelun olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.

Tietoturvaloukkauksesta ilmoitettaessa käsittelijän tulee kuvata:

(i) tietoturvaloukkaus sekä asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät sillä tarkkuudella kuin nämä ovat tiedossa;
(ii) tietosuojavastaavan tai muun yhteyshenkilön nimi ja yhteystiedot, jolta voi saada asiassa lisätietoja;
(iii) kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja
(iv) kuvaus toimenpiteistä, joita toimittaja ehdottaa tai joita se on jo toteuttanut tietoturvaloukkauksen johdosta, ja tarvittaessa toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Tietoturvaloukkauksen havaittuaan käsittelijän tulee ryhtyä viipymättä toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi.