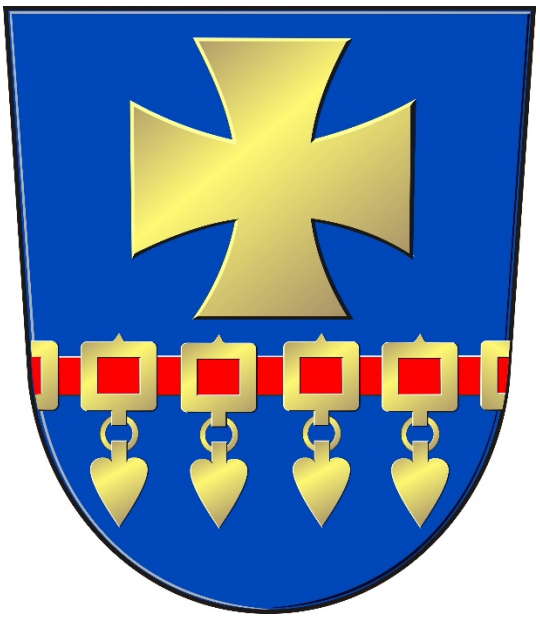

Kauhavan kaupunki

Tietoturvapolitiikka ja tietosuojaohjeistukset

Sisällys

I Tietoturvapolitiikka

1. Johdanto

Kauhavan kaupunki korostaa kaikessa toiminnassaan tietoturvaa. Tietoturvan tärkeyttä lisäävät sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäyttö, pilvipalvelut sekä eri organisaatioiden mm. kuntien yhteistyö palvelujen järjestämisessä.

Järvinet Oy vastaa Kauhavan kaupungin ICT- ja tietosuojavastaavan palveluista. Järvinet Oy:n hallituksessa on hyväksytty tietoturvapolitikka, joka koskee kaikkia yhtiön työntekijöitä, palveluiden tuottamiseen osallistuvia kumppaneita sekä luottamushenkilöitä, jotka työnsä tai toimeksiantonsa puitteissa käsittelevät yhtiön omistamaa tai hallinnoimaa tietoa. Kauhavan kaupunki hyväksyy Järvinet Oy:n tietoturvapolitiikkaa koskevat periaatteet ja sitoutuu noudattamaan niitä myös omassa toiminnassaan.

Tätä tietoturvapolitiikkaa sovelletaan kaikkeen tietoon ja muuhun dataan (myöh. tieto) riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

2. Tietoturvapolitiikan sisältö

Tietoturvapolitiikassa otetaan huomioon seuraavat asiakokonaisuudet:

- Keskeisten käsitteiden määrittely
- Tietoturvaperiaatteet
- Tietoturvavastuut
- Tietoturvallisuuden hallintajärjestelmä
- Tietoturvallisuuden toteutumista tukevat käytännöt
- Turvatoimien priorisointi
- Tietoturva- ja tietosuojakoulutus ja –ohjeet
- Tietoturvallisuuden toteutumisen valvonta
- Toiminta häiriötilanteissa ja poikkeusoloissa
- Tiedottaminen
- Tietoturvapolitiikan ajan tasalla pitäminen ja oikeudet tehdä siihen tarvittavia muutoksia (esim. organisaatiorakenteen muuttuessa).

3. Tietoturvapolitiikan tavoite

Tietoturvallisuuden ensisijaisena päämääränä on Kauhavan kaupungin vastuulla olevien palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa. Tietoturvapolitiikalla sekä tietoturva- ja tietosuoja-asioiden hoitamista koskevilla määräyksillä varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely varmistaen samalla kansalaisten yksityisyyden suoja.

Kaupunginjohtaja vastaa viime kädessä organisaation tietoturvallisuusvastuista sekä sen toteuttamistavoista.

3.1 Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan kaupungin omistamaa tai hallinnoimaa tietoa normaalitilanteissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tietoturvallisuus tulee huomioida mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Toteutuakseen tietoturvallisuus vaatii seuraavien ehtojen toteutumista:

- Luottamuksellisuus; kukaan asiaton/sivullinen ei näe tai saa haltuunsa salassa pidettävää tietoa.
- Eheys; tiedon yhtäpitävyys alkuperäisen tiedon kanssa
- Saatavuus ja käytettävyys: Tieto, tietojärjestelmä tai palvelu on siihen oikeutettujen henkilöiden ja järjestelmien saatavilla ja käytettävissä silloin kun sitä tarvitaan.
- Kiistämättömyys: Tiedonkäsittelytoimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana ja sen jälkeen.
- Tietojen käsittelyn valvonta: Tietojen käsittelyä valvotaan niin, etteivät asiattomat pääse tietoja käsittelemään tai sitä näkemään. Valvonnalla voidaan myös puuttua luvattomaan henkilötietojen käsittelyyn.

Tietoturvallisuuteen liittyvät uhat

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle. Henkilöiden mahdollinen osaamattomuus, huolimattomuus tai välinpitämättömyys saattavat aiheuttaa uhkan organisaation tietoturvallisuudelle. Lisäksi uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset, haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat.

Uhkia voi liittyä myös ulkopuolisten palvelujen tuottamiseen, mikäli palveluntuottajien kanssa tehdyissä sopimuksissa ei ole huomioitu tietoturvaan, tietosuojaan ja varautumiseen liittyviä asioita riittävästi tai jos niistä puuttuu rikkomuksiin liittyvät sanktiot. Jokaisessa organisaatiossa, prosessissa, projektissa ja tietojärjestelmässä tulee huolehtia tietoturvaan ja tietosuojaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta. Mahdollisesti toteutuvien riskien negatiivisia vaikutuksia pitää minimoida teknisillä ja hallinnollisilla keinoilla. Tavoitteena on, että toimenpiteet skaalataan riskilähtöisesti.

Tietoturva

Hyvä tietoturvataso saavutetaan tietoturvapolitiikan ja ohjeiden mukaisilla tietoturvallisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva tulee luonnollisena osana mukaan toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa kunnan yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Turvallisuusjohtaminen

Turvallisuusjohtaminen on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla turvallisuuden osa-alueilla, mukaan lukien riskienhallinta ja varautuminen.

Henkilöstöturvallisuus on henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvavastuut ja - tehtävät on selkeästi perehdytetty. Henkilöstöturvallisuuteen pyritään vaikuttamaan palvelussuhteen kaikissa vaiheissa – rekrytointivaiheessa, työsuhteen aikana ja työsuhteen päätyttyä tehtävillä toimenpiteillä.

Fyysinen turvallisuus käsittää toimenpiteet, järjestelmät ja rakenteet, joiden avulla yrityksen tiloja ja siellä olevia ihmisiä, tietoa ja muuta omaisuutta, suojataan fyysisiltä vahingoilta, vahingoittamisyrityksiltä, oikeudettomilta henkilöiltä ja erilaisilta kiinteistövahingoilta. Fyysistä turvallisuutta toteutetaan mm. kameravalvonnalla, kulunvalvonnalla ja turvallisilla rakenteilla.

Tietosuoja tarkoittaa henkilön yksityisyyden ja henkilötietojen suojaamista niin, että henkilön yksilöiviä tietoja ei paljastu asiattomille käsittelyprosessin missään vaiheessa. Kuntalaisia ja asiakkaita koskevat yksilöivät henkilötiedot ovat kunnan keskeisimpiä suojattavia tietoja ja vaativat siten käsittelijöiltä erityistä huomiota. Henkilötietojen käsittelijöiden perehdytys tulee olla riittävällä tasolla ja osaamista tulee päivittää siten, että toimintatavat ovat lain vaatimalla tasolla. Yksityisyyden suoja on kaikkien oikeus, eikä henkilötietojen käsittelyn tule vaarantaa sitä.

Työturvallisuus ja -suojelu kattavat sekä henkilöstöön kohdistuvien, että henkilöstön aiheuttamien, tahallisten ja tahattomien, vahingontekojen estämiseen tähtäävät toimenpiteet.

3.2 Tietoturvatyö

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön päämäärä on turvata kunnan toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin, poikkeusolojen viestintään ja näistä uhkatilanteista toipumiseen.

Kauhavan kaupunki on nimennyt jokaiselle tietojärjestelmälle oman vastuuhenkilön. Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esimies.

Jokainen kaupungin työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä ovat omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä

tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan ja tietosuojaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen, tietohallintokoordinaattorille ja tietosuojavastaavalle.

3.3 Tietoturvallisuustavoitteet

Kauhavan kaupungin tietoturvallisuustavoitteet ovat seuraavat:

- Henkilökunnalla on vähintään perustason tietoturva- ja tietosuojaosaaminen tehtäviensä suorittamiseksi.
- Tekniset ja hallinnolliset tietoturvajärjestelyt täyttävät keskeisiltä osin perustason vaatimukset.
- Kaupungin käsittelemää tai käyttämää tietoa ei paljastu oikeudettomille tahoille.

4. Tietoturvatoimintaa ohjaavat tekijät

Tietoturvatoimintaa ohjataan säädöksin, määräyksin, ohjein ja suosituksin. Esimerkkejä toimintaa tietoturvallisuuden ja tietosuojan näkökulmasta ohjaavista säädöksistä ovat mm:

- Suomen perustuslaki
- EU:n tietosuoja-asetus ja kotimainen tietosuojaan liittyvä lainsäädäntö
- laki viranomaisten toiminnan julkisuudesta
- laki yksityisyyden suojasta työelämässä
- tietoyhteiskuntakaari
- laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista
- laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä
- rikoslaki
- muut eri toimialueiden toimintaa ohjaavat erityislait.

Lainsäädännön lisäksi noudatetaan omalle organisaatiolle hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä.

Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan. Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietoverkon toiminnan turvaaminen sekä palvelujen tuottaminen normaali- ja poikkeusoloissa.

5. Organisointi

5.1 Johtaminen ja valtuudet

Tietoturvallisuuden johtaminen, sen ylläpitäminen ja toteutumisen seuranta ovat osa kunnan johtamista. Jokainen toteuttaa tietoturvallisuutta omien johtamis- ja toimintavaltuuksiensa puitteissa.

Ohjelmien pääkäyttäjillä on oikeus suorittaa lain sallimat toimet palvelun toimintaa ja tietoturvallisuutta vaarantavien poikkeamien paikallistamiseksi ja korjaamiseksi. Tietosuojavastaavalla, tietohallintokoordinaattorilla ja kaupunginjohtajalla on oikeus keskeyttää toiminta, josta aiheutuu olennaista vaaraa kunnan tietoturvallisuudelle. Tietoturvariskeistä ja – rikkomuksista tulee raportoida heti, kun ne huomataan.

5.2 Vastuut

Pääsääntö on, että valta ja vastuu ovat samoissa käsissä. Tietoturvatyöryhmän ja tietosuojavastaavan tehtävä on auttaa kaikkia tämän vastuun kantamisessa.

- Jokainen vastaa hallittavissaan olevan tiedon tietoturvallisuudesta omalta osaltaan.
- Jokainen on velvollinen noudattamaan sääntöjä ja käyttöohjeita.
- Jokainen on velvollinen joko korjaamaan tai edelleen ilmoittamaan havaitsemansa tietoturvaongelman.

5.3 Roolit ja vastuut

5.3.1 Hallitus

Kaupunginhallitus hyväksyy tietoturvapolitiikan.

5.3.2 Kaupunginjohtaja

Kaupunginjohtaja vastaa:

- tietoturvapolitiikan noudattamisesta
- tietoturvan ja tietosuojan järjestämisestä ja toimintaedellytysten luomisesta
- poikkeusolojen viestinnän johtamisesta
- varautumisesta ja jatkuvuudenhallinnasta yhdessä kunnan johtoryhmän kanssa.

5.3.3 Tietohallinto

Tietohallinnon päätösten suunnittelusta ja toimeenpanosta vastaa tietohallinto yhdessä Järvinet Oy:n kanssa.

5.3.4 Tietoturvatyöryhmä

Huolehtii kaupungin tiedon ja tietojärjestelmien tietosuojasta ja tietoturvallisuudesta.

5.3.5 Tietosuojavastaava

Kauhavan kaupunki ostaa Tietosuojavastaavan palvelun Järvinet Oy:ltä. Tietosuojavastaava vastaa:

- Auttaa kaupunkia saavuttamaan tietosuoja-asetuksen ja kotimaisen lainsäädännön edellyttämän tietosuojan tason.
- Tukee ja avustaa henkilöstöä sekä johtoa projekteissa, hankinnoissa ja ongelmatilanteissa.
- Huolehtii henkilöstön riittävästä tietosuojakoulutuksesta ja –osaamisesta.
- Huolehtii rekisteröidyn oikeuksista riippumattomana asiantuntijana.
- Raportoi ylimmälle johdolle havaituista ongelmista ja väärinkäytöksistä.
- Toimii yhteiskanavana valvontaviranomaisen ja organisaation välillä.

5.3.6 Pääkäyttäjä

Pääkäyttäjät määräytyvät ohjelmistokohtaisesti. Pääkäyttäjät pystyvät mm. antamaan ohjelmiin käyttöoikeuksia ja valvomaan ohjelmiston oikeanlaista käyttöä

- Tietoturvan toteutumisen valvonta omalla vastuualueellaan.
- Sovelluksen ylläpitotoiminnoista huolehtiminen ja varmistaminen, että järjestelmää käytetään lakien, säädösten ja ohjeiden mukaisesti.
- Tietosuojavastaavan avustaminen, henkilöstön neuvonta ja kouluttaminen.
- Käyttäjien ja käyttöoikeuksien toteuttaminen.
- Vastuu ylläpitosäännön noudattamisesta.

5.3.7 Tiedon ja tietojärjestelmien käyttäjä

Kaikki Kauhavan kaupungin tietojärjestelmien käyttäjät hyväksyvät ja allekirjoittavat tietosuoja-, tietoturva- ja salassapitositoumuksen joka käsitellään yt-menettelyssä ja jonka hyväksyy konserni- ja henkilöstöjaosto.

Jokaisen kaupungin työntekijän ja luottamushenkilön vastuulla on:

- Määräysten ja ohjeiden noudattaminen
- Tietoturvaan liittyvien poikkeuksien, uhkien ja riskien välitön ilmoittaminen joko esimiehelle, tietohallintokoordinaattorille tai tietosuojavastaavalle.

5.4 Tietojärjestelmien käyttö

Kaupungin käytössä olevat ICT-palvelut, -järjestelmät, -laitteet ja -ohjelmistot on tarkoitettu työtehtävien hoitamista varten. Tietojärjestelmiä ei saa käyttää toimintaan, joka voi välittömästi tai välillisesti, vaarantaa kaupungin vastuulla olevan tiedon ja/tai järjestelmien turvallisuuden ja aiheuttaa haittaa kaupungin toiminnalle, rekisteröidylle tai käyttäjälle itselleen.

Tietojärjestelmiä, laitteita ja ohjelmistoja, Kauhavan kaupungin käyttöön, saa asentaa vain Järvinet Oy:n ICT-asiantuntijat, tietohallintohenkilöstö tai poikkeustapauksissa ohjelmiston toimittaja.

Käyttöoikeudet kunnan tietojärjestelmiin ja tietoon myönnetään vain tehtävien hoitoon liittyen. Jokainen käyttäjä vastaa omista käyttäjätunnuksistaan ja niillä tehdyistä toimista.

Kauhavan kaupungin järjestelmät keräävät lokitietoja, joita seurataan säännöllisesti ja aina tarvittaessa. Kauhavan kaupunki omistaa keräämänsä lokitiedot ja on niiden tietosuojalain mukainen rekisterinpitäjä

Syyt lokitietojen keräämiseen:

- Järjestelmän oikeanlaisen toiminnan varmistaminen
- Väärinkäytösten selvittäminen ja ehkäiseminen
- Seurannan toteuttaminen
- Käyttöoikeuksien oikeellisuuden varmistaminen

Tietojärjestelmien turvallinen käyttäminen etätyötä tehdessä vaati VPN-yhteyden käyttämistä ja etätyöntekijältä huolellisuutta ja sitoutumista tietoturvaohjeiden noudattamiseen. Laite on pidettävä aina lukittuna, kun sillä ei työskennellä.

Kauhavan kaupunki käyttää toiminnassaan Järvinet Oy:n tietoverkkoja, joita valvotaan erityisillä valvontamenetelmillä ja -ohjelmistoilla. Toiminnan ja turvallisuuden takaamiseksi tietoliikenteestä suodatetaan palomuurilla ja muilla tekniikoilla haittaohjelmat ja muu asiaton sisältö sekä estetään pääsy haitalliseksi luokitelluille sivustoille.

6. Tietoturvallisuuden toteuttaminen

6.1 Turvamekanismit

Tietoturvallisuudesta huolehtiminen edellyttää tiedon elinkaaren kaikkiin vaiheisiin sekä näiden aikana tiedon käsittelyyn käytettyihin välineisiin, järjestelmiin ja menetelmiin kohdistettuja oikein valittuja ja toteutettuja toimenpiteitä sekä tietoa käsittelevien henkilöiden toiminnan ohjaamiseen tarkoitettuja sääntöjä ja ohjeita sekä koulutusta. Yhteisellä nimellä näitä kaikkia kutsutaan turvamekanismeiksi.

Turvamekanismeilla varmistetaan kullekin tiedolle hyväksyttävä saatavuusviive eli aika, jonka kuluessa tiedon on oltava saatavissa ja käsiteltävissä ilman, että viiveestä aiheutuu haittaa työlle. Joissakin tiedoissa hyväksyttävä saatavuusviive voi olla sekunteja, joissakin päiviä. Jos tiedon eheyttä on syytä epäillä, saatavuusviiveen laskentaan on laskettava mukaan tiedon palauttaminen eheäksi.

Turvamekanismien valinnassa haetaan tasapaino tietoturvallisuuden ja turvamekanismien käytöstä aiheutuvien kustannusten välillä. Kustannukset voivat olla luonteeltaan välittömiä taloudellisia investointeja, mutta ne voivat aiheutua myös välillisesti työn hidastumisesta.

Tietoturvallisuuden tavoitteet asetetaan ja sen toteuttamistavat valitaan niin, että lain takaama tietosuoja ja yksityisyyden suoja toteutuvat kunnan toiminnassa parhaalla mahdollisella tavalla.

6.2 Ennakkosuunnittelu

Palveluja tai tietojärjestelmiä suunniteltaessa on ennen käyttöönottoa suunniteltava seuraavat asiat:

- Palvelusta on oltava riittävä dokumentaatio. Dokumentaatiosta tulee käydä ilmi palvelun rakenne, käyttötarkoitus, käyttöohjeet, pääkäyttäjän ohjeet, riippuvuudet toisista palveluista, turvamekanismit, sopimusasiat, palvelun suunniteltu elinkaari sekä palveluun liittyvät mahdolliset erityisvelvoitteet. Dokumentaation suojaus on suunniteltava (salassa pidettävä osa, esim. turvamekanismit ja julkinen osa; selosteet, palvelukuvaukset, toimintakäsikirjat ja käyttöohjeet). Henkilötietojen suoja ja suojaus tulee ottaa myös huomioon jo suunnitteluvaiheessa.
- Kauhavan kaupungin palvelutoiminnan tulee jatkua mahdollisimman häiriöttömästi kaikissa olosuhteissa.
- Tietosuojaselosteet on laadittava ja pidettävä ajan tasalla. Tällaisia ovat esim. henkilötietoja käsittelevien järjestelmien tietosuojaselosteet tai vastaavat. Palveluun voi kohdistua myös muita velvoitteita (sertifioinnit, kumppanuussopimuksen auditointipykälät tai muita arkaluonteisia tietoja koskevat erityismääräykset jne.), jotka tulee huomioida suunnitteluvaiheessa.

6.3 Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Tietoturvallisuustavoitteiden toteutumista ja järjestelyjen riittävyyttä seurataan säännöllisesti yhdessä Järvinet Oy:n kanssa. Tietoturvallisuuden ylläpito ja kehittäminen sovitetaan yhteen palveluiden, toimintatapojen ja teknisten ratkaisujen kehittämisen kanssa. Lisäksi säännöllinen tiedottaminen, osaamisen ylläpito ja koulutus ovat olennaisessa roolissa tietoturvallisuuden kehittämisessä.

Henkilökunnan, järjestelmien käyttäjien ja niitä ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta tietohallintokoordinaattorille tai tietosuojavastaavalle.

Tietohallintokoordinaattorin ja tietosuojavastaavan tehtävänä on seurata ja valvoa tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

7. Riskienhallinta

Tietoturvallisuus on kiinteä osa Kauhavan kaupungin riskienhallintakäytäntöjä ja kuuluu jokaisen työntekijän vastuulle. Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä kartoitetaan, analysoidaan ja hallitaan järjestelmällisesti yhteistyössä Järvinet Oy:n kanssa.

Riskienhallintakäytäntöjen tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että käytetyt keinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen.

8. Tämän dokumenttikokonaisuuden päivittäminen

Tätä dokumenttikokonaisuutta pidetään ajan tasalla tietoturvatyöryhmän toimesta.

Muutoksia tehdään

- lainsäädännön muuttuessa,
- lainsäädännön tulkintatapojen muuttuessa,
- ohjeistuksia tai vaikutustenarviointeja tarvitsee päivittää tai muokata
- kaupungin organisaatiorakenteen muuttuessa

II Tietosuojavastaavan ohjeistusta jokapäiväiseen työhön

1 Taustaa

Uutta tietosuoja-asetusta on sovellettu 25.5.2018 lähtien ja se on tuonut organisaatioille rekisterinpitäjänä sekä osaltaan henkilötietojen käsittelijänä uusia velvollisuuksia ja lisävastuita. Asetuksen astuttua voimaan rekisteröidyn oikeuksiin kiinnitetään entistä enemmän huomioita ja henkilötietojen käsittelytoiminnan läpinäkyvyyteen on annettu ohjeistuksia, joihin organisaatioiden tulee vastata. Tietosuojan tasoa pitää nostaa ja tietosuojaan kiinnittää entistä enemmän huomiota johtamisessa, resursoinnissa ja organisaatiotason ratkaisuissa.

Kyselyt liittyen asiakkaan tai työntekijän henkilötietojen käsittelyyn ja sen lainmukaisuuteen ovat lisääntyneet merkittävästi. Se jo itsessään luo paineita käsitellä tietoja asianmukaisesti ja lain sanelemalla tavalla. Mikäli henkilötietoja ei käsitellä asetuksen vaatimalla tavalla, voidaan rekisterinpitäjää rangaista varoituksella, henkilötietojen käsittelykiellolla ja sakoilla. Käsittelyn lainmukaisuus on osaltaan myös imagokysymys, joka takaa uskottavuuden asiakkaiden ja rekisteröityjen silmissä. Yksityisyydensuoja ja henkilötietojen suoja ovat jokaisen perusoikeus.

2 Henkilötieto ja –rekisteri

Mikä on henkilötietoa? Henkilötietoa on paljon muutakin kuin pelkästään nimi ja henkilötunnus. Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Näitä ovat esimerkiksi; nimi, Hetu, osoite, kuva, IP-osoite, video, tilinumero, ruokavalio jne.. Jos erinäisiä tietoja yhdistämällä saadaan tunnistettua henkilö, niin nämä yhdistetyt tiedot lasketaan myös henkilötiedoiksi.

Arkaluonteiseksi henkilötiedoksi lasketaan mm. rotu, uskonto, ammattiyhdistysliikejäsenyys, seksuaalinen suuntautuminen, poliittinen mielipide, terveydentila, sosiaalihuollon tarve, rikoksiin ja rangaistuksiin liittyvät tiedot. Näiden henkilötietojen kerääminen ja käsittely ovat lähtökohtaisesti kiellettyä, ilman erittäin hyvin perusteltua oikeusperiaatetta sekä käyttötarkoitusta.

Henkilörekisteri on puolestaan mikä tahansa lista, tiedosto, paperi, luettelo jne., missä näitä edellä mainittuja henkilötietoja on. Sillä ei ole merkitystä onko lista sähköinen vai paperinen tai onko se esim. Excel-tiedostossa, toiminnanohjausjärjestelmässä, sähköpostissa, avolehtiössä tai arkistossa.

Organisaation henkilöstön tulisi tarkkaan miettiä, mitä henkilörekistereitä he työssään käyttävät, sillä asetus määrää, että organisaation henkilötietovarannot on kartoitettava ja kuvattava. Tätä on jo varmasti tehty, mutta kaikkia henkilötietorekistereitä ei ole vielä, hyvin todennäköisesti, löydetty. Rekisterit pitää myös kuvata ja hyvä keino tähän on laatia tietosuojaselosteita. Tietosuojaselosteissa kerrotaan mm., mitä henkilötietoja kukin rekisteri sisältää, mitkä ovat käsittelyn tarkoitukset, mistä tiedot rekisteriin on saatu ja minne niitä luovutetaan. Nämä dokumentit, jotka kertovat rekisterin ominaisuuksista, tulisi kirjoittaa mahdollisimman ymmärrettävästi ja maanläheisesti, koska rekisteröidyillä on oikeus halutessaan nähdä nämä dokumentit, samalla tavalla kuin heillä on oikeus tehdä kysely omien henkilötietojensa käsittelystä ja sen lainmukaisuudesta. Kaupungilla on käytössä Digiturvamalli- (ent Tietosuojamalli) -ohjelma, jonka avulla tulee jokainen rekisteri kirjata ylös. Sen avulla pystytään todistamaan valvovalle viranomaiselle, että kaupungin rekisterit ovat kartoitettu ja

niiden suojaamiseen on kiinnitetty huomiota. Ohjelma toimii myös merkittävänä apuna henkilötietokyselyihin vastaamisessa ja muissa tietosuojaan liittyvissä raportoinneissa.

3 Henkilötietojen käsittely

Kaikki aktiiviset ja passiiviset toimenpiteet liittyen henkilötietoihin katsotaan niiden käsittelyksi, aina niiden keräämisestä poistamiseen saakka. Tähän luetaan myös tallennus, siirto, säilytys ja hävitys. Hyväksyttäväksi perusteeksi ei lueta, että henkilötietoja saatetaan vielä joskus tarvita. Hyväksyttäviä perusteita ovat laki, yleinen etu, suostumus ja sopimus. Henkilötietojen käsittelylle on aina oltava peruste. Kunnilla hoitaessaan viranomaistehtäviä, käsittelyperuste on yleensä laki.

Jos käsittelyperustetta ei ole, ei henkilötietoja saa olla, ja se katsotaan tietosuoja-asetuksen vastaiseksi toiminnaksi rekisterinpitäjältä. Henkilötietoja saa ainoastaan käsitellä siihen tarkoitukseen, mihin ne on kerätty. Jos uusia käsittelytarpeita ilmenee, pitää niihin olla lakisääteinen tarkoitus tai rekisteröidyn suostumus. Tietosuoja-asetus ei lähtökohtaisesti mene minkään muun lain yläpuolelle (arkistolaki, kuntalaki, viranomaisen toiminnan julkisuus, koululaki, jne.).

Esimerkki: Jos henkilötiedot on kerätty hiihtokisojen osallistujien ilmoittautumista varten, ei niitä saa käyttää muihin tarkoituksiin, kuten muiden kilpailuiden ilmoittautumistiedusteluihin. Näin saa ainoastaan toimia, jos nimiä kerätessä on suostumus rekisteröidyltä, että tietoja käytetään tähän lisätarkoitukseen.

4 Miten noudattaa uutta lakia jokapäiväisessä työelämässä?

1. Pidä huoneesi, autosi ja tietokoneesi aina lukossa, äläkä jätä mitään henkilötietoja paikkaan, mistä ne voi ulkopuolinen nähdä (myös kollega voi olla ulkopuolinen, jos hänellä ei ole oikeutta kyseisiin tietoihin). Henkilötietoja sisältäviä dokumentteja ei saa jättää pöydille tai postilokeroihin ilman kirjekuorta (ei mielellään edes siinä).
2. Henkilötietoja sisältävät dokumentit tulee säilyttää lukollisissa kaapeissa tai tiloissa, ja mitä arkaluonteisempaa tietoa, sitä varmempi paikka (kassakaappi, arkisto jne.)
3. Käytä aina salasanasuojattuja tietokoneita ja ohjelmia. Näytön aikakatkaisun tulee olla hyvin lyhyt (esim. 2 min) ja sen jälkeen on tultava aina salasanakysely.
4. Salasanakyselyä ei saa ohittaa, eikä salasanoja tallentaa. Salasanan tulee olla tarpeeksi vaikea ja sitä on vaihdettava säännöllisesti. Älä kerro salasanaasi kenellekään, äläkä kirjoita sitä ylös, mistä se on helppo löytää.
5. Käyttöoikeudet ja avaimet vain niitä oikeasti tarvitseville. Turhat käyttöoikeudet ja avaimet pois, kun niitä ei enää tarvita. Mikäli sinulla on käyttöoikeus ohjelmaan, jossa on henkilötietoja, älä käytä rekisteriä muuten kuin työhön liittyvissä asioissa.
6. Käytä vain työnantajan omistamia tai hyväksymiä laitteita, kun käsittelet henkilötietoja.
7. Poista kaikki sellaiset henkilötiedot ajallaan, joille käyttötarkoitusta ei enää ole ja jota lait eivät määrää säilyttämään (mm. Arkistolaki, julkisuuslaki).
8. Älä puhu työasioista, etenkään henkilötiedoista ulkopuolisille, jos et ole varma rikkooko asia tietosuojakäytänteitä ja ovatko kyseiset tiedot julkista.
9. Älä jaa rekisteröityjen henkilötietoja sosiaalisessa mediassa tai internetissä, jos ei suostumusta ole. Tämä koskee myös valokuvia.
10. Hävitä arkaluonteiset paperit ja muut dokumentit aina oikealla tavalla. Käytä silppuria tai tietoturva-astiaa.

11. Edellytä toimittajilta (ohjelmistot, kuljetuspalvelut, ravintopalvelut, siivouspalvelut, muuttopalvelut, kiinteistöhuolto jne.), että he noudattavat tietosuojalakeja. Sopimuksen päivittäminen tai toimittajan antama tietosuojaliite ovat mm. hyviä vaihtoehtoja.
12. Muista mahdollisuus, että työpaikallenne tulee viranomainen tarkastamaan, että asetusta noudatetaan.
13. Suurin osa tietosuojarikkeistä johtuu inhimillisestä virheestä, huolimattomuudesta tai tietämättömyydestä. Ei siis hakkeroinneista tai muista suunnitelmallisista rikoksista. Ole siis huolellinen.
14. Ota yhteyttä tietosuojavastaavaan tai tietohallintokoordinaattoriin, mikäli mitään kysyttävää ilmaantuu.
15. Noudata aina varovaisuutta ja harkintaa, kun käsittelet henkilötietoja työssäsi. Pieneltä tuntuva asia saattaa johtaa toimenpiteisiin, joilla on vakavat seuraamukset.

III Tietokyselyt

1 Tietokyselyihin vastaaminen

Uutta tietosuoja-asetusta on sovellettu 25.5.2018 alkaen ja se on tuonut mukanaan tarpeen vastata rekisteröityjen kyselyihin kaupungin hallussa olevista henkilötiedoista. Tässä seuraavasta ohjeistusta miten toimia, kun asiakas haluaa tehdä kyselyn.

Toimi näin kaupunkilaisen tai muun rekisteröidyn halutessa tehdä tietokyselyitä tai tulla unohdetuksi.

1. Pyydä pyyntö kirjallisena ja tarkista henkilöllisyys. Mikäli pyyntö tehdään puhelimitse, niin pyytäkää laittamaan sama pyyntö sähköpostilla tai ohjeistakaa kysyjää tulemaan kaupungintalolle / palvelutoimistoon täyttämään lomake. Henkilöpaperit on silti nähtävä, että voimme olla varma henkilöstä. Pyydä yhteystiedot kysyjältä. Henkilötietopyyntöä voi pyytä myös Suomi.fi Viestit-palvelun kautta, jolloin kysyjän ei tarvitse tulla kaupungintalolle / palvelutoimistoon.
2. Pyydä kysyjältä tarkennusta siitä, mitä hänen tietopyyntönsä koskee. Siis mahdollisesti palveluja, joihin häneltä on henkilötietoja kerätty. Kysyjällä on velvollisuus kertoa asiasta, mikäli mahdollista ja samalla helpottaa tiedon etsimistä ja tietopyyntöön vastaamista.
3. Ota ylös myös miten rekisteröity haluaa, että toimitamme vastauksen hänen pyyntöönsä.
4. Ota yhteys tietosuojavastaavaan: Teemu Karhunen Järvinet Oy, 040 757 5515, teemu.karhunen@jarvinet.fi . Näin voimme yhdessä miettiä, miten toimimme ja miten lähdemme viemään asiaa eteenpäin

2 Perusteet ohjeistukselle ja menetelmistä

On tärkeää, että tietoja ei anneta kysyjälle ilman tätä ”virallista tapaa”, koska silloin on mahdollista, että annetaan tietoa, mitä ei saa antaa tai kysyjä näkee muiden rekisteröityjen tietoja.

Pyyntöön, joka on suhteellisen helposti toteutettavissa, reagointiaikaa on 2-4 viikkoa ja jos pyyntö on laaja, voidaan ilmoittaa, että tarvitsemme lisäaikaa. Kun olemme yhdessä miettineet, miten pyyntöön vastataan, mitä tietoa tarvitsee etsiä ja lopuksi kun olemme löytäneet tarvittavat dokumentit, voidaan vastaus suorittaa kysyjälle.

Suomi.fi Viestit-palvelu on hyvä väline henkilötietokyselyiden vastaanottamiseen ja niihin vastaamiseen.

Kaupunkilainen pystyy verkon kautta ottamaan yhteyttä ja viesti välittyy kaupungin kirjaamo -sähköpostiin tai asianhallintajärjestelmään. Tätä kautta tehty henkilötietokysely on varma ja turvallinen vaihtoehto.

Ennen kuin kaupunkilainen pystyy lähettämään viestiä palvelusta, on hänen kirjauduttava sinne pankkitunnuksia tai mobiilivarmennetta käyttäen. Näin voidaan olla varmoja siitä, että kysyjä on sama henkilö kuin kenen henkilötietoja kysytään. Vastaaminen tapahtuu niin, että kaupungista lähetään viesti kysyjälle sähköpostitse tai asianhallintajärjestelmästä. Käytettäessä sähköpostia, osoitteeksi tulee henkilötunnus (xxxx-xxxx) @asiointitili.fi. Kun viesti lähetetään edellä mainitulla tavalla, voimme olla varmoja, että viesti menee juuri halutulle henkilölle.

Kaupunkilainen käy lukemassa vastauksen Suomi.fi Viestit-palvelusta, kirjautumalla sinne omilla pankkitunnuksillaan, eikä kukaan muu pysty lukemaan viestiä kuin henkilö, jolle se on tarkoitettu.

3 Henkilötietokysely- ja korjauslomake

Rekisteröity täyttää

Nimi (Etu- ja sukunimi): _____

Puhelinnumero: _____

Sähköpostiosoite: _____

Osoite: _____

Rekisterinpitäjä täyttää

Päivämäärä jolloin kysely otettu vastaan: _____

Kyselyn vastaanottaja: _____

Tapa jolla rekisteröidyn henkilöllisyys on todettu: _____

IV Kauhavan kaupungin alueella suoritettavan kameravalvonnan vaikutusten arviointi

Kaupunki suorittaa kameravalvontaa omistamissaan kiinteistöissä, palveluja tuottavissa yksiköissä, yleisillä paikoilla ja harrastuskohteissa.

Näitä kohteita ovat:

- Koulut
- Päiväkodit
- Kirjastot ja omatoimikirjastot
- Kaupungintalo
- Palvelutoimistot

Kamerat tallentavat videokuvaa sekä sisä- että ulkotiloissa. Valvottavien kohteiden kameroiden katseluoikeudet ovat teknisen toimen palveluksessa olevilla kiinteistönhoitajilla ja tapauskohtaisesti yksiköiden esimiehillä (esim. rehtoreilla). Jos oikeudet ovat yksiköiden esimiehillä, tulee olla ennalta määritelty, että asia on näin. Tekninen johtaja myöntää tarvittaessa oikeudet tunnuksiin erillisten yksiköiden esimiehille tai muille asiantuntijoille. Kameravalvonnan ja valvontajärjestelmän vastuuhenkilöinä toimivat tekninen johtaja ja tilapalvelupäällikkö. Valvontakamerat tallentavat tietoa digitaalisesti palvelimille ja paikallisille laitteille. Tallenteisiin pääsy on suojattu käyttäjätunnuksilla ja salasanalla. Mahdollisesti myös tietyillä palvelujen ylläpitäjien työntekijöillä on pääsy palvelimille ja tallenteisiin. Mikäli palvelun ylläpitäjillä on oikeus tallenteisiin, tulee siitä olla sovittu etukäteen ja nauhoja tulee katsella vain kaupungin edustajan toimeksiannosta ja tarpeen mukaan.

Kameravalvonnalla saatu tieto tallennetaan ja sitä käytetään vain tarvittaessa, mikäli kohteissa ilmenee ongelmia tai vahingontekoja. Videoita seurataan myös reaaliaikaisesti, mikäli kohde vaatii jatkuvaa valvontaa. Kohteet joissa reaaliaikaista valvontaa suoritetaan, tulee sen tarpeellisuus olla perusteltua. Tallenteiden säilytysaika on ennalta määrätty ja sen jälkeen vanhimpien päälle nauhoitettaan uutta materiaalia. Nauhojen säilytysaika vaihtelee kohteittain, ja on 3 – 8 viikkoa, riippuen tallennuskohteesta ja palvelun ylläpitäjästä. Palvelimella tai paikallisilla laitteilla olevien vanhojen tallenteiden korvaaminen uusilla tallenteilla tapahtuu automaattisesti ja ennalta määrätysti.

Kameroiden tarkoitus on turvata kaupungin tarjoamien palvelujen häiriötöntä jatkumista, suojata henkilöitä, ehkäistä vahingontekoja sekä väärinkäytöksiä jotka kohdistuvat kaupungin omaisuuteen sekä jos vahingontekoja ilmenee, saattaa rikoksentekijät vastuuseen teoistaan. Jo itsessään kameroiden asentamisella valvottaviin kohteisiin toivotaan olevan rikoksia ja väärinkäytöksiä ehkäisevä vaikutus. Kamerat ovat sijoitettu siten, että ne valvovat rekisterinpitäjän yhteiskunnallisesti tärkeitä kohteita ja rahallisesti arvokasta omaisuutta sekä harrastuspaikkoja ja kouluja missä jatkuvampaa valvontaa tarvitaan. Rekisterinpitäjällä tässä kohtaan voidaan katsoa olevan oikeus omaisuutensa valvontaan sekä rekisteröityjen suojelemiseen vahingoilta. Valvonnalla kuvataan ja turvataan omaisuutta jonka tuhoutumisesta tai häviämisestä voisi koitua rekisterinpitäjälle suuret kustannukset sekä kohteita joiden valvonta ilman ympärivuorokautista kuvaamista olisi vaikeaa ja hyvin kallista. Reaaliaikaisella valvonnalla pyritään mm. estämään onnettomuuksia sekä kiusaamista.

Palveluiden jatkuvuuden turvaamisen, kohteiden yhteiskunnallisen merkityksellisyyden ja kohteissa olevan omaisuuden rahallisen arvon perusteella valvonta nähdään tarpeelliseksi. Henkilöiden suojelun ja mm. oppilaiden valvonnan katsotaan olevan myös hyvä peruste kameravalvonnalle. Kameroiden määrä kohteittain on mitoitettu sen mukaan, että suojaus saadaan hyväksytylle tasolle,

ja niin, että kuvauksen kohteena olisi mahdollisimman vähän alueita joissa rekisteriin tallentuu henkilöitä, joita ei alueen tai henkilöiden suojaamisen kannalta tarvitse kuvata.

Työnantajan velvollisuudet

Työnantaja saa käyttää kameravalvontaa käytössään olevissa tiloissa työntekijöidensä ja muiden tiloissa oleskelevien henkilökohtaisen turvallisuuden varmistamiseksi, omaisuuden suojelemiseksi ja prosessien asianmukaisen toiminnan valvomiseksi. Kameravalvonta on sallittua myös turvallisuutta, omaisuutta tai organisaation toimintaa vaarantavien tilanteiden ennaltaehkäisemiseksi tai selvittämiseksi.

Kameravalvontaa ei saa käyttää tietyn työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla. Se ei ole sallittua myöskään käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa tai muissa henkilöstötiloissa.

Kameravalvontaa ei saa käyttää työntekijän henkilökohtaiseen käyttöön osoitetussa työtilassa. Kameravalvonta voidaan edellä esitetystä poiketen kohdistaa tiettyyn työpisteeseen vain laissa säädetyin perustein. Kameravalvonnasta on ilmoitettava työntekijöille.

Rekisteröidyn oikeudet

Rekisteröidyn oikeuksien kannalta kameravalvonta on haasteellinen. Omien tietojen katselu ei aina tule kysymykseen, koska muiden rekisteröityjen oikeudet voivat vaarantua. Nauhaa ei aina voi rekisteröidylle näyttää, jos siinä näkyy muita rekisteröityjä. Rekisteröidyn on kuitenkin mahdollista tapauskohtaisesti katsoa nauhoja, mikäli muille rekisteröidyille ei siitä koidu haittaa. Rekisteröidyn tulee kuitenkin tehdä selvitys siitä, mitä kohtaa ja tapahtumaa hän haluaa nauhalta katsoa. Pitää myös varmistaa jo etukäteen, että rekisteröity itse esiintyy tallenteilla, että tämä ei pääse luvatta katsomaan toisia henkilöitä tallenteista. Nämä tietopyynnöt käsitellään aina tapauskohtaisesti tietosuojavastaavan kanssa. Jos tallenteen osia pystytään kopioimaan siten, että siitä voidaan ottaa osia, joissa vain kyseinen rekisteröity näkyy, on tiedon antaminen rekisteröidylle mahdollista. Tietojen poistaminen ei käytännössä ole mahdollista koska nauhan tulee olla eheä, jos sitä käytetään esimerkiksi todisteena, eikä sitä silloin saa muokata.

Kameravalvonnasta informointi

Rekisteröityjä informoidaan kohteissa kylteillä, joissa ilmoitetaan kameravalvonnasta, mutta käytännössä ei ole mahdollista informoida niin, että kaikki rekisteröidyt tietäisivät, kun heitä kuvataan. Tämä pätee varsinkin kohteissa jotka ovat ulkotiloissa ja yleisillä alueilla missä liikkuminen ei ole rajoitettua.

Kameravalvonnasta pyritään tiedottamaan kohteissa mahdollisimman hyvin ja kamerat pyritään sijoittamaan siten, että kohteen suojaamisen kannalta epäolennaisia henkilöitä kuvataan mahdollisimman vähän ja, että jos henkilö päätyy nauhalle, informointi kuvauksesta olisi todennäköistä kyltin sijoituksen perusteella.

Tallenteiden katseluoikeudet

Sen lisäksi, että tallenteet tallentuvat palvelimille jotka ovat käyttäjätunnuksen ja salasanan takana, on myös reaaliaikaisen kuvan katsomiseen kirjautuminen pakollinen. Oikeudet tallenteisiin ja reaaliaikaiseen videon katsomiseen on rajoitettu siten, että vain valvontaan työnsä puolesta valtuutetut ihmiset pääsevät videoita katsomaan. Henkilöt, jotka tallenteita katsovat eivät saa luovuttaa tallenteita tai tallenteilla olevaa tietoa muille kuin työnsä puolesta katseluun valtuutetuille henkilöille, viranomaiselle ja mahdollisesti rekisteröidylle.

Tietokoneet, joilta tallenteita tai reaaliaikaista kuvaa voidaan katsoa, ovat sijoitettu yksityisiin ja lukollisiin tiloihin siten, että ulkopuolisilla ei ole mahdollisuutta tallenteita nähdä. Kyseiset tietokoneet ovat myös suojattu salasanoin. Ohjelmat, millä kuvaa katsotaan ja tietokoneet, joilla niitä käytetään, on suojattu tietoturvallisesti siten, että ulkopuolinen ei pääse murtautumaan tietoihin. Katseluoikeuksia voidaan jakaa kamerakohtaisesti tai vain reaalikuvaan tai vain tallenteisiin.

Kameran tallenteet voidaan antaa poliisille, jos on kyse rikoksesta, joka vaatii viranomaisen osallisuutta asiaan. Tiedon poliisille voi antaa rekisterinpitäjä tai myös tapauskohtaisesti kameroiden ja tallenteiden ylläpitäjä. (poistettu Järvinet Oy) Ylläpitäjän tulee kuitenkin saada toimeksianto tallenteiden luovutuksesta poliisille rekisterinpitäjältä. Tietosuojavastaavan on oltava mukana tai tietoinen nauhojen luovutuksesta tai katselusta.

Kameravalvonnan tallenteiden katselu

Mikäli valvontakameroiden tallenteita katsellaan jälkikäteen, tulee tapahtumasta tehdä riittävä dokumentaatio. Dokumentaatiosta tulee ilmetä: Miksi tallenteita on katsottu (mahdollisimman tarkka kuvaus, että jälkikäteen voidaan tietää varmasti kyseinen tapaus), miltä aikaväliltä tallenteita on katsottu (vuosi, pvm ja kellonaika esim. 14.00-15.00), kohde missä tallenne on nauhoitettu ja ketkä ovat olleet katsomassa tallennetta. Tämän lisäksi dokumentaatioon tulee merkitä tieto, onko tallenteita luovutettu tapauksen johdosta viranomaiselle.

Tallenteiden katselutapahtumien dokumentaatio on säilytettävä. Arkistosäilytyksestä vastaa Kauhavan kaupungin tietohallintokoordinaattori.

Kameravalvonnan tietosuojaseloste

Kameravalvonta, jota Kauhavan kaupunki alueellaan suorittaa on kuvattu tietosuoja-asetuksen mukaisesti tietosuojaselosteella. Valvontaan on tehty vaikutustenarviointi, jonka asetus edellyttää. Vaikutustenarvioinnilla pyritään kartoittamaan riskejä, joita kameravalvonta voi rekisteröidylle tai hänen oikeuksilleen tuottaa. Siinä myös kartoitetaan valvonnan tarvetta ja sen oikeasuhteisuutta sekä valvontaa suorittavan organisaation henkilöstön velvollisuuksia ja valmiuksia suorittaa tehtäväänsä niin, että rekisteröityjen oikeudet eivät vaarannu, eikä lakia rikota.