Tietosuoja-asetus, yhdistys, hallinto

Teppo Laine

Asianajaja

Legistum

Henkilötieto

- Mikä on henkilötieto?
  - Tieto koskee luonnollista henkilöä.
  - Henkilö on tiedoista yksilöitävissä (ei edellytä nimeä, esim. sukupuoli ja osoite, ikä ja työnantaja, jos yhdistyksessä vain yksittäisiä ko. ikäisiä ihmisiä)
  - Sähköisessä järjestelmässä ”kaikki” paperilla -> että järjestetty ja lajiteltu löydettävään muotoon.
  - Käytetään muuhun kuin yksityiseen käyttöön.
  - Koskee myös tunnistettavaa kuvaa tai videota
- Rajanvetotilanteita
  - Nimellä tai muuten tunnistettavalla tunnisteella varustettu sähköposti
  - Puhelinnumero (oma / puhelinetu on henkilötieto, ”puhdas” työnumero ei ole)
  - Tilastot -> eivät ole henkilötietoja, mikäli yksilöt eivät ole tunnistettavissa
  - Nimettömät henkilöprofiilit (missä menee tunnistettavuuden raja).

Legistum

Käsittelyn lainmukaisuusvaatimus tarkentuu

Käsittelyn lainmukaisuus

1. Käsittely on lainmukaista ainoastaan jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:

a) Suostumus

b)Sopimus tai sen tekemistä varten

c)Lakisääteinen velvollisuus

d)Rekisteröidyn / kolmannen elintärkeä etu

e)Yleistä etua koskeva tehtävä (ja julkisen vallan käyttö)

f)Rekisterinpitäjän / kolmannen oikeutettu etu (jota rekisteröidyn painavammat oikeudet eivät syrjäytä)

Legistum

Rekisterit

- Ensin selvitetään, mitä henkilöstörekistereitä meillä on
  - Henkilörekisteri on rekisteri, josta yksilö on tunnistettavissa
  - Tarkoittaa luonnollisia henkilöitä eli ihmisiä
  - Käsite on siten laaja
- Tarkistetaan, mitä tietoa on kerätty
- Tarkistetaan tiedon keräämisen perusteen olemassaolo
- Tarkistetaan tietojen oikeellisuus ja ajantasaisuus
- Poistetaan perusteettomat, tarpeettomat, virheelliset ja vanhentuneet tiedot
- Tarkistetaan tietojen suojauksen taso
- Selvitetään henkilöstön pääsy tietoon, rajoitetaan vain niille, joilla tarve päästä tietoon

Legistum

Erilaiset rekisterit

- Manuaaliset paperiarkistot
- Sähköiset rekisterit
  - Toiminnanohjausjärjestelmät
  - Asiakashallintajärjestelmät
  - Keskusjärjestelmät
  - Kirjanpito-ohjelma
  - Asiakashallintajärjestelmät ja tiedostot
- ”Piilorekisterit” esim. esimiesten omat tietokannat alaisista
- Eri ilmoituksista muodostuvat rekisterit, esim. vakuutusyhtiöille.
- Sähköpostit, puhelimen yhteystiedot, SoMe jne.
- Valvontakameranauhoitteet
- Muut nauhoitteet (esim. kuvatut henkilöstöesittelyt)
- Valokuva-arkistot

Legistum

Toiminnanohjaus ja kirjanpito / laskutus

- Toiminnanohjausjärjestelmään, laskutukseen ja kirjanpitoon syntyy rekistereitä.
- Rekisterinpito perustuu usein ainakin osin lakiin / sopimukseen.
- Tällöin kuitenkin laki / sopimus tms. peruste määrittää mitä tietoja näillä perustein saa kerätä ja mihin niitä saa käyttää.
- Tämän lisäksi saatetaan haluta muitakin tietoja / laajentaa niiden käyttöalaa, jolloin asiasta pitää saada suostumus.
- Itse tiedon luovuttaminen ei vielä tarkoita oikeutta rekisteröidä (esim. jos pyydetään maksuaikaa terveydentilan perusteella).
- Toiminnanohjausjärjestelmään yms. ”eksyy” helposti perusteetonta / asiatonta tietoa / ”mielipiteitä”.
- Hallinto myös helposti ”jakaa” tai rekisteröi perusteettomasti tai ainakin perusteettomiin paikkoihin tietoa (esim. terveystiedot -> yhteiskalenteri ”Teppo on tänään vatsataudissa”).

Legistum

Arkaluontoiset tiedot

- Erityinen huomio tulee kiinnittää arkaluontoisten tietojen käsittelyyn:

- Yksilön henkilöön liittyvät tiedot (uskonto, etninen tausta, sukupuolinen suuntautuminen, poliittinen näkemys ym.)
- Terveystiedot
- Taloustiedot (ulosoton asiakkuus)
- Viranomaistiedot (rikosrekisteri tms.)
- Henkilökohtaiset tiedot (harrastukset tms.)

-> Hallinnolle kertyy pääsääntöisesti lähes kaikkea em. Tietoa, mikä on perusteltua rekisteröidä ja minne sekä mihin käyttötarkoitukseen?

Legistum

Rekisterien hallinnointi

- Kuten huomataan tietyn tiedon osalta voi olla useita säilytysperusteita.
- Eri lainsäädäntö ja eriperusteet tuottavat erilaisia säilytysaikoja.
- Samalla tiedolla voi siis olla useita säilytysaikoja, koska sama tieto säilytetään usealla eri perusteella.
- Siten rekisterit olisi hyvä lajitella käyttötarkoituksen perusteella alarekistereiksi, esim:

Henkilöstörekisteri	Jäsenrekisteri
• Työaikakirjanpito	Perustiedot
• Kirjanpito	Toimintatiedot
• Työntekijän perustiedot	Täyttämistiedot
• Työsuhteen täyttämistiedot	Sopimustiedot
• Työntekijän palkkatiedot	Kirjanpito
• Verotus	Suoritetiedot
• Vakuutustapahtumat	Järjestelmätiedot esim. jäsenjärj. tied.
• Suostumukseen perustuvat tiedot	Suostumukseen perustuvat tiedot

- Tämä mahdollistaa myös tietoihin pääsyn rajoittamisen.

Legistum

Ilmoittamisvelvollisuus

Tiedonantovelvollisuus laajenee – rekisteröityä on informoitava.

- Tietosuoja-asetuksen mukaan henkilötietoja käsittelevien on **informoitava rekisteröityjä kattavasti henkilötietojen käsittelystä → tämä velvoite on asiakaspalvelulle tulevaisuudessa tärkeä.**
- Tietosuoja-asetus yhdistää lukuisia EU:n jäsenvaltioissa sovellettuja tiedottamiseen liittyviä velvoitteita, mikä laajentaa merkittävästi nykyisen henkilötietolakiin perustuvan informointivelvoitteen sisältöä.
- Henkilötietoja käsittelevien tulee antaa tietojenkäsittelyä koskevat tiedot **ytimekkäällä, läpinäkyvällä, ymmärrettävällä ja helposti saatavissa olevalla tavalla**.
- EU:n komissio voi myös erikseen päättää informoinnissa käytettävien kuvakkeiden hyödyntämisestä.

Legistum

Tietoa sisältävään materiaaliin liittyvät fyysiset riskit

Tieto on usein fyysisessä muodossa (esim. asiakirjat, paperirekisterit).

Ajatuksena estää ulkopuolisia / tarpeettomia henkilöitä pääsemästä tutustumaan tietoon.

Tiedon säilytys on fyysisesti suojattava niin, että aineisto ei ole ulkopuolisten ulottuvilla:

- Ei helposti löydettävissä (ei näkyvästi ilmoiteta missä on mitäkin aineistoa).
- Ei helposti päästävissä (suljetuissa tiloissa / lukitusten takana / riittävä murtovarmuus).
- Tietovuodon paljastusmekanismit (valvonta).
- Vahingon vähentämismekanismit (tunnistekoodit).

Legistum

Tietoa sisältävään materiaaliin liittyvät tekniset riskit

Tieto on yhä useammin sähköisessä muodossa.

Sähköinen tieto on aina altis tietovuodoille, mikään järjestelmä ei ole ”murtovarma”.

Tämän tiedon tietoturvassa on monta näkökulmaa, esim:

1) Missä tieto säilytetään? Pilvipalvelu (missä) / kiinteä serveri, miten fyysisesti on säilytetty?
2) Tiedon siirtyminen säilytyspaikasta käyttäjälle (yhteyden turvallisuus)?
3) Siirtotavan turvallisuus (kryptattu vai selkokielinen)?
4) Tiedon käsittelyn turvallisuus (kuka oikeasti käyttää, salasanaturvallisuus, yhteys auki, kuka näkee näytön yms).
5) Tiedon siirron turvallisuus (salattu sp / vastapuolen varmistus).

Legistium

Inhimillisten riski

Ihminen on riski! Aina, kun ihminen saa tiedon, syntyy riski sen vuodosta.

Tietämättömyys / osaamattomuus

- Hallitaan kouluttamalla ja ohjeilla sekä tietosuojatuella

Huolimattomuus

- Luodaan varmennejärjestelmiä, joilla vähennetään riskiä
  - yhteyden automaattinen katkaisu
  - automaattinen varmistuskuittaus
  - Pääsynestojärjestelmä
- Hälytysjärjestelmä poikkeamatapauksissa
- Automaattinen varmistuskysely

Tahallisuus (henkilökohtainen rikosvastuu)

- Yhdistys valvoo
- Tästä tulee seuraamaan rajoitteita, joiden peruste on riskin vähentäminen

Legistum

Inhimillisten riskien hallinta

1) Tiedon käyttö -> saanko minä käyttää (työperuste)?
    1) Mitä tietoa otetaan käyttöön, miten sitä käytetään ja millaisessa fyysisessä / teknisessä ympäristössä. Tästä tietosuojaohjeessa.
    2) Tiedon tallentamisen hallinta eri menetelmillä (tulostus, kuvaus, tallennus jne). Pyritään minimoimaan.
2) Tiedon luovutus / siirto -> saanko minä luovuttaa?
    1) Luovutuksen / siirron perusteiden tarkistus (saako luovuttaa / siirtää)
    2) Luovutusmenetelmät / tiedonsiirron salaus
    3) Vastaanottajan luotettava varmistus
3) Tiedon muokkaus -> saanko minä muokata?
    1) Tiedon muuttamisen rekisteröiminen sekä muutosten identifiointi
    2) Valvontatietoihin pääsy erityisesti suojattava / rajattava ja muuttaminen / poistaminen estettävä
4) Tiedon poistaminen -> saanko minä ja jos saan mitä?
    1) Turhan, tarpeettoman, väärän ja vanhentuneen tiedon poistaminen
    2) Tilanteissa, kun rekisteröintivelvollisuus -> aktiiviset (käyttörekisterit) ja passiiviset (säilytysrekisterit)
    3) Suostumuksen perusteella luovutetut -> oikeus tulla unohdetuksi.
    4) Muilla perusteille -> säilytysajat
5) Käyttöalusta
    1) Henkilöstön koulutus -> RISKIEN YMMÄRTÄMINEN!
    2) Henkilöstön perehdytys -> järjestelmien ja menetelmien osaaminen
    3) Alustojen minimointi ja standardisointi
    4) Tekniset salaukset / suojaukset, niiden poistamisen estäminen, tiedon siirron rajoitukset ja käytettävät menetelmät

Legistum

Tietosuojan ”ketju”

- Tiedon keräämistapa (miten tieto saatu ja mihin tallentunut)
  - Mihin tieto tallennetaan (serveri, pilvipalvelu)
    - Tietoon pääsy (kirjautumisjärjestelmä)
      - Yhteyden turvallisuus
        - Tiedon siirtotapa (salasanasuojattu, kryptattu)
          - Päätelaitteen turvallisuus
            - Salasana- ja käyttöolosuhdeturvallisuus
              - Henkilön toiminta

Legistum

Tietosuojan ”tasot”

- Tekninen tietoturva
  - Käytettävät järjestelmät ja ohjelmistot
  - Käytettävät yhteydet
  - Käytettävät laitteet
- Menettelyllinen tietosuoja
  - Osaaminen / asiantuntemus
  - Tietoisuus omista valtuuksista
  - Käytettävät menettelyt
  - Dokumentointi
- Inhimillinen tietosuoja
  - Osaaminen
  - Ohjeiden ja sääntöjen noudattaminen
  - Tuki

Legistum

Tietosuojaohje

1) Työntekijän salassapitovelvollisuuden korostaminen.
2) Salassa pidettävän / suojattavan tiedon yksilöinti.
3) Rekisterin käyttö – tarpeellisuusvaatimus.
4) Sallittu rekisteröinti – luvanvarainen rekisteröinti – kielletty rekisteröinti.
5) Sallittu käyttö – luvanvarainen käyttö – kielletty käyttö.
6) Sallittu luovutus – rajoitettu luovutus – kielletty luovutus.
7) Mihin mitäkin tietoa saa – ei saa rekisteröidä.
8) Rekisteröinnin perusteet, mitä ja millä perusteella saa / ei saa rekisteröidä.
9) Menettely rekisterin käyttäjän tunnistamiseksi.
10) Korostettava loukkauksen voivan johtaa rikosoikeudelliseen seuraamukseen.
11) Ohjeet salasanojen ym. Säilytyksestä.
12) Ohjeet salasanojen vaihtamisesta.
13) Ohjeet käytettävistä laitteista.

Legistum

Tietosuojaohje (2)

14) Kielto tallettaa salasanoja.
15) Kielto ohittaa salasanoja / salauksia.
16) Kielto käyttää ”omia” laitteita.
17) Velvollisuus valvoa hallussa olevien laitteiden tietoturvajärjestelmien / virustorjunnan toimivuutta / voimassaoloa (toimiiko / herjaako kone?)
18) Tiedon siirtoa / tallentamista / kopioimista koskevat kiellot, rajoitukset ja ohjeet.
19) Ohjeet fyysiseen turvallisuuteen (asiakirjojen ym. Säilytys).
20) Menettely epätietoisuustilanteessa.
21) Tuki / neuvot (tietosuojavastaava). ”Kysy ensin tee vasta sitten periaate”.
22) Valvonnan menetelmät ja periaatteet.
23) Raportointivelvollisuudet.
24) Poikkeamailmoitusvelvollisuus.
25) Ohjeen rikkomisen seuraukset.

Legistum

Tietojen säilytys- ja poistosuunnitelma

Tiedon poistaminen:

- Virheelliset poistetaan.
- Vanhentuneet poistetaan (vanhentuneet tiedot).
- Kun suostumusaika päättyy tai se peruutetaan, tieto poistetaan.
- Oikeutta tulla unohdetuksi kunnioitetaan poistamalla tiedot oikeutta käytettäessä.
- Tiedon poistaminen tapahduttava ”kokonaan”, myös back upp –järjestelmät, mapit yms.
- Poistaminen oltava tietoturvallista.
    - Tiedostot poistettava kokonaan (palauttaminen ei onnistu ns. normaalikeinoin.
    - Vanhat laitteet, niiden muistit tuhottava tietoturvallisesti.
    - Paperit hävitettävä asianmukaisesti (silputtava, tietoturva-astia tms.)

Suunnitelma

- Säilyttämisestä ja poistamisesta olisi hyvä tehdä kirjallinen suunnitelma.
- TSA lähtee rekisterinpitäjän näyttötaakasta.
- Määriteltävä säilytyspaikat ja –ajat.
- Määriteltävä käytettävät tiedon poistamismenetelmät.

Legistum

Toimet käytännössä

- Opettele tietosuojaohje ja kysy, jos et ymmärrä.
- Salasanat talteen, ei ohiteta, laiteta muistiin. Salasanat vieraiden hallinnassa yksi keskeinen riski!
- Huolellisuus, kadonneet kannettavat ja työpuhelimet yksi aivan keskeinen riski!
- Rekisteröinnistä ilmoittaminen (yhdistykselle tulee rekisteri-ilmoitukset).
- Tutustu yhdistyksen ilmoituksiin, koska niistä ilmenee, mitä tietoa kerätään ja millä perusteella. Ne rajoittavat myös sinun toimintaasi.
- Rekisteröinnille tulee pyytää suostumus, jos muuta perustetta ei ole.
- Perehdy laitteiden ja järjestelmien ominaisuuksiin huolellisesti, kysy jos epäselvää.
- Raportoi yhdistykselle puutteista, virheellisyyksistä ja poikkeuksista.
- Ilmoita yhdistykselle, jos havaitse tietosuojan laiminlyöntejä.

Legistum

Tietosuojan noudattamisen ongelmakohtia top 10

1. Kerätään / kerääntyy tarpeetonta / perusteetonta tietoa
2. Syntyy rekistereitä, joita ei edes tunnisteta
3. Tiedot eivät ole ajan tasalla, vanhentuneita tietoja ei poisteta
4. Tietoon pääsy on henkilöillä, joilla ei ole siihen tarvetta tai ei edes tiedetä, kenellä on pääsy mihinkäkin tietoon
5. Tietoja käytetään muuhun kuin siihen tarkoitukseen, mihin ne on kerätty
6. Tietoja luovutetaan kolmansille ilman asiallista perustetta
7. Rekisterit hajallaan -> vaikea edes määritellä mitä tietoa ja minne on kerätty, etätyössä tiedot ”levällään” ja ”Piilorekisterit”
8. Tietojen käyttötarkoitukset eivät ole määritelty
9. Tietoturva päivittämättä, uudet uhkakuvat, sääntöjen noudattaminen
10. Inhimillinen uhkatekijä

Legistum

Tapauksia

- Rekisteröity työntekijöiden ammattiliittoon kuulumiset. seksuaalinen suuntautuminen -> perusteeton rekisteröinti.
- TT:t pääsivät toisten TT:iden lääkärinlausuntoihin käsiksi -> liian laaja pääsy.
- Yksityisiä tietoja oli mennyt yleiseen roska-astiaan -> käsittelyvirhe.
- Käytiin katsomassa tapauksen salaisia tietoja (poliisit) -> liian laaja pääsy.
- Kuvat julkaistaan internetiin kaikkien nähtäväksi.
- Vanhat tietokoneet kellarissa, muistit koneissa, varastettiin -> tietovuoto.
- Paperit muuttolaatikossa näkyvillä (muuttomiehet ja sivullisetkin siirtovaiheessa) -> tietovuoto.
- Tietomurto terapiatietoihin (puutteellinen suojaus, ilmoituksen laiminlyönti, seuraamusmaksu, vahingonkorvausvelvollisuus, rikosvastuu)

Legistum

Tapauksia

- Kävi katsomassa tietoja, joiden katsomiseen ei suostumusta (potilastiedot, luovutuskielto) -> tutkitaan rikoksena.
- Työsuhde päättyi, työtietokone jäi työntekijälle, sisälsi tietoja -> tietovuoto.
- Tehtiin työtä avoimessa langattomassa verkossa, tapahtui tietomurto -> tietovuoto.
- Kuva julkaistiin lehdessä, henkilön anonymiteetti murtui – henkilökohtainen uhka
- Kerättiin arkaluontoisia tietoja sähköpostilla -> tietovuoto
- Google –tapaukset, oikeudeton tieto, vanhentunut tieto, väärä tieto
- Työntekijä lopettaessaan työt kopioi serverin sisällön -> tietovuoto.
- Työsopimuksien kopiot lukitsemattomassa kaapissa -> tietovuotoriski

Legistum

KIITOS!

Teppo Laine

Asianajotoimisto Legistum Oy
Vilhonkatu 9 C
FI-00100 Helsinki

Puh 040 047 4074
teppo.laine@legistum.fi