Tietosuojan tehopaketti

Teppo Laine

Asianajaja

Legistum

Päivän teemat

- Top 15 -virheet HR-tietojen käsittelyssä
- Oikein vai väärin toimittu – konkreettisia esimerkkitilanteita
- Asetuksen vaatimat toimenpiteet käytännössä
- Työntekijän tiedot – mikä on henkilötieto ja mikä ei?
- Mikä on arkaluonteinen tieto?
- Mitä tietoja saat työntekijöistäsi kerätä? Mitä et?
- Kuka saa tarkastella tietoja ja kuka ei?
- Missä ja miten tietoja pitää säilyttää? Rajoitukset?
- Mihin tietoja saa käyttää? Mihin ei?
- Mitkä tiedot on poistettava? Milloin?
- Konkreettinen tarkistuslista – tarkista nämä ennen h-hetkeä!

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

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.)

Legistum

Tyypilliset virheet rekistereissä ja niiden käytössä

1. Henkilötietoja käsitellään huolettomasti (sairauslomatodistus, postit, työsopimukset lojuu pöydällä)
2. Tiedot jäävät kolmannen haltuun (esim. kun joukkueenjohtaja vaihtuu ja käytetty henk. Koht. Sähköposteja).
3. ”Piilorekisterit” eli valmentajien / joukkueiden toimihenkilöiden omat tiedostot.
4. Tietojen säilytyspaikka on turvaamatta (lukitsematon kaappi, omat tietokoneet)
5. Tiedon saanti on liian monella.
6. Tietoja tilastoidaan / analysoidaan lain vastaisesti (esim. sairauslomien tilastoiminen nimillä).
7. Tietoja käytetään esim. markkinointiin ilman suostumusta (työntekijöille lähetetään mainoksia ym. Esim. henkilökunta-alennuksista)

Legistum

Tyypilliset virheet rekistereissä ja niiden käytössä

7. Tiedot ovat vanhentuneet / esim. maksukieltomerkintä pitää poistaa, kun ulosotto päättyy).
8. Tietoja ei päivitetä
9. Tiedonsiirtomenetelmät ovat turvaamattomia (salaamaton sähköposti)
10. Rekisteritiedot osin perusteettomia tai asiattomia (lähiesimiesten omat kommentit)
11. Johto käyttää tietoja muihin tarkoituksiin kuin on kerätty eli käyttöala ”laajenee”
12. Kanssatoimijat väärinkäyttävät tietoja
13. Yritysjärjestelyissä tietoja siirretään ilman hyväksyttävää perustetta
14. Asiakirjojen poistamis- ja tuhoamismenettelyissä on puutteita.
15. Kuvien ottaminen ja käyttö villiä.
16. Kuvaaminen ja sosiaalinen media

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.

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
- Paperit salkussa, salkku anastettiin -> tietovuoto.
- Työntekijä lopettaessaan työt kopioi serverin sisällön -> tietovuoto.
- Työsopimuksien kopiot lukitsemattomassa kaapissa -> tietovuotoriski

Legistum

Tyypillisiä rekistereitä

- Sähköiset rekisterit:
  - Toiminnanohjausjärjestelmä
  - Jäsen-, asiakas-, markkinointi-, asiakaspalvelu- ja sopimusrekisterit
  - Kirjanpito- ja laskutusohjelma
  - Henkilöstö- ja palkkakirjanpitorekisteri
  - Opinto- tms. rekisteri
  - Valokuva-arkistot, valvontakameratallenteet jne.
- Manuaaliset rekisterit
  - Paperiarkistot, sairaslomatodistuskansiot, arviointi- ja kehityskeskustelukansiot, viranomaisilmoitukset
- ”Piilorekisterit
  - Sähköpostit, puhelimen yhteystiedot, tekstiviestit, whats upit, opintojen seurantaohjelmat jne.
  - ”Omat rekisteröidyt muistiinpanot

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).

Legistum

Tietoa sisältävään materiaaliin liittyvät inhimilliset riskit

Ihminen on riski!

Aina, kun ihminen saa tiedon, syntyy riski sen vuodosta.

Vuotoriski voi olla tahallinen (hyötymistarkoitus) tai tahaton (ei tiedä / ei osaa).

Mikään järjestelmä ei auta, jos sitä käyttävä ei ole luotettava!

Inhimillinen riski on aina olemassa.

Tahattomia riskejä voi hallita tiedon ja osaamisen lisäämisellä.

Tahallisia riskejä voi hallita selvittämällä, tiedustelutoimin ja valvomalla sekä estämällä pääsyä tietoon.

Legistum

Fyysisten riskien hallinta

1) Tiedon ”eristäminen” eli sijoittaminen eristettyyn tilaan
2) Tiedon sijoituspaikan valinta
3) Lukitus / avain tai koodihallinnointi
4) Kulun ja tiedon siirron valvonta
5) Ennakkovalvonta (luvat, kirjaukset, perustelut)
6) Jälkivalvonta (valvontakamerat)
7) Tiedon luovutusmenettely (kuka, miksi)
8) Tiedon ja kohteen yhteyden koodaus
9) Sääntöjen valvonta
10) Tietohaun valvonta
11) Tiedon hakijan valvonta
12) Käyttötarkoituksen valvonta
13) Tiedon inventointi

Legistum

Teknisten riskien hallinta

1) Mihin tieto on kerätty (fyysinen sijoituspaikka)
2) Tiedon tallettajan pääsy tietoon estetty / rajoitettu
3) Tiedon salaus
4) Tiedon suojaaminen ulkopuolisilta (palomuurit / virustorjunta).
5) Tiedon ”eristäminen” eli sijoittaminen eristettyyn tilaan
6) Tiedon sijoituspaikan valinta
7) Lukitus / avain tai koodihallinnointi
8) Kulun ja tiedon siirron valvonta
9) Jälkivalvonta (valvontakamerat)
10) Tiedon luovutusmenettely (kuka, miksi)
11) Inventointi
12) Tiedon ja kohteen yhteyden koodaus
13) Sääntöjen valvonta
14) Tietohaun valvonta
15) Tiedon hakijan valvonta
16) Käyttötarkoituksen valvonta

Legistum

Inhimillisten riskien hallinta (1)

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

- Minimoidaan ”access to information”
- Kopioinnin / tiedonsiirron estojärjestelmät
- Käytön seuranta ja valvonta
- Poikkeamailmoitukset

Legistum

Inhimillisten riskien hallinta (2)

1) Pääsy tietoon rajoitetaan (mitä arkaluontoisempi tieto, sitä harvempi pääsee, pääsy perustuu tarpeeseen).
2) Luodaan pääsylle tietoon eri tasot -> työntekijällä pääsy vain sellaiseen tietoon, joka tarpeen työn tekemiseksi.
3) Suojataan tieto identifioivilla salasanoilla -> tieto kuka on käynyt katsomassa tietoja / mahdollisesti tallentanut sitä ulkoiseen paikkaan tai siirtänyt sitä pois.
4) Valvotaan tiedon käyttöä (kuka, milloin, mitä, kuinka paljon, kuinka kauan).
5) Erityisen arkaluontoisen tai vahingollisen tiedon käyttö perusteltava.
6) Tietolähde suojataan ulkoisilta uhilta (fyysinen / tekninen)
7) Ulkoiset laitteet ja yhteydet suojataan salasanoilla. Mitään salasanoja ei tallenneta tai ohiteta.
8) Tiedon säilytys turvataan, tietoa ei siirretä / kopioida tarpeettomasti tai turvaamattomiin sijainteihin.
9) Tiedon käyttö rekisteröidään.

Legistum

Inhimillisten riskien hallinta (3)

9)Tiedon muuttaminen estetään ilman perustetta ja muutokset rekisteröidään ja identifioidaan.

10)Määritellään asiakirjahallintaohje.

11)Menettelyt asiakirjahallinnalle ja niiden mahdolliselle poistamiselle / tuhoamiselle (tietoturvallinen tuhoaminen).

12)Erityistilanteiden hallintaohje

1) Esim. tarve ottaa tietoa mukaan työtehtävään esim. kannettavalle, huolehdittava poistamisesta, kun tarve loppuu. Samoin ohjeistettava säilytys ja käyttö päätelaitteella.0

13)Päätelaitteiden ja yhteyksien käyttöohjeistus

14)Ennakkovalvonta (perusteluvelvollisuus)

15)Jälkivalvonta

1) Pistotarkastukset (rekisterien käyttö)
2) Fyysisten tilojen valvonta (kameravalvonta)
3) Poikkeamailmoitukset (isot latausmäärät / paljon käyntejä)
4) Erityistiedot (esim. ”houkuttelevat tiedot) eriyisvalvontaan

Legistum

Inhimillisten riskien hallinta (4)

Toimenpiteet:

Lähde (rekisteri)

- Tietoon ja siihen pääsyn rajaus
- Esto-, varmistus- ja rajoitusjärjestelmät
- Rekisterin luomisen ja käytön dokumentointi
- Tiedon keräämisen ja käytön valvonta ennakollinen ja jälkikäteinen

Käyttöalusta

- Henkilöstön koulutus -> RISKIEN YMMÄRTÄMINEN!
- Henkilöstön perehdytys
- Ohjeet käyttämiseen (tietosuojaohje)

Legistum

Inhimillisten riskien hallinta (5)

Toimenpiteet:

Käyttötavat
- Standardoidut käyttötavat
- Käyttöpaikkojen fyysinen suojaaminen / käyttöpaikkojen ohjeistus

Poikkeamatilanteiden hallinta
- Tietokantojen ”siivoaminen”
- Arkistojen tuhoaminen
- Tiedonsiirrot / muutot

Ulkoistamisten hallinnointi
- Sopimus huomio tietosuojan ja salassapidon
- Toimeksisaajan salassapito ja vastuu
- Toimeksisaajan valvonta (sopimusvalvonta)

Legistum

Suunnitelma tietosuojan varmistamiseksi

- Määritellään mihin toimiin on ryhdyttävä
- tiedon määrä ja luonne
- Määritellään arkaluontoiset tiedot, niiden määrä ja luonne
- Arvioidaan tietojen vahingollisuus rekisteröidylle
- Mitä enemmän tietoa, mitä arkaluontoisempaa, mitä useampi pääsee näkemään, mitä vahingollisempaa, sitä korkeampi riskitaso
- Riskitason perusteella arvioidaan tarvittava, riittävä tietosuojan taso

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

Rekistereistä tietosuojaseloste

- Rekistereistä pitää olla laadittuna tietosuojaseloste
- Tietosuojaselostevaatimus koskee kaikkia rekistereitä
- Myös henkilöstörekisteristä pitää olla seloste
- Nykyään henkilörekisterilain mukaan rekisteriselosteessa pitää olla:
    - Rekisterinpitäjä (tämä tarkoittaa rekisterinpitäjää, ei sen ylläpitäjää)
    - Yhteyshenkilö
    - Rekisterin nimi
    - Tietojen käsittelyn tarkoitus
    - Rekisterin tietosisältö
    - Säännönmukaiset tietolähteet
    - Tietojen säännönmukaiset luovutukset
    - Tietojen siirto EU / ETA –alueen ulkopuolelle
    - Rekisterin suojauksen periaatteet

Legistum

Rekistereistä tietosuojaseloste

Rekisteriselosteessakin ilmoitettavien tietojen lisäksi pitää ilmoittaa vielä:

- Tarkastusoikeus
- Oikeus vaatia tietojen korjausta
- Muut henkilötietojen käsittelyyn liittyvät oikeudet

Ilmoitusvelvollisuus, laadulliset vaatimukset, miten pitää ilmoittaa:

”Kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä varsinkin silloin, kun tiedot on tarkoitettu erityisesti lapselle. Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa. Jos rekisteröity sitä pyytää, tiedot voidaan antaa suullisesti edellyttäen, että rekisteröidyn henkilöllisyys on vahvistettu muulla tavoin.”

Tietosuoja-asetus asettaa siis ilmoitukselle (ent. seloste) laadullisia vaatimuksia. Helppo saatavuus, ymmärrettävyys. Tällä hetkellä rekisteri- / tietosuojaselosteet eivät näitä täyty.

Legistum

Ilmoitusvelvollisuudesta

Ilmoitusvelvollisuus, sisältö:

- Erotellaan sen mukaan, saadaanko tiedot rekisteröidyltä itseltään vai muualta.
- Jälkimmäisessä tapauksessa lisävaatimuksia.
- Ilmoitusvelvollisuus sisältää kaiken sen, mitä tietosuojaseloste on nykylain mukaan edellyttänyt, mutta sen lisäksi tulee lisää ilmoitettavia asioita.

Ilmoitusvelvollisuus (kun tiedot saatu rekisteröidyltä), lisäykset:

- Mahdollinen tietosuojavastaava ja hänen yhteystiedot
- Henkilötietojen käsittelyn oikeudellinen peruste (laki, suostumus jne.)
- Rekisterinpitäjän / kolmannen oikeutetut edut 6 artikla 1 f:n perusteella
- Säilytysaika / sen määrittämiskriteerit
- Oikeudesta rajata käsittelyä tai vastustaa sitä
- Oikeudesta peruuttaa annettu suostumus ja oikeudesta valittaa
- Mihin henkilötietojen vaatiminen perustuu (laki, sopimus, sopimuksen tekemiseen perustuva)
- Onko tietojen luovuttaminen pakollista ja mitä seuraa, mikäli ei luovuta.
- Mahdollisesta automaattisesta päätöksenteosta (profilointi), sen merkittävyys ja mahdolliset seuraukset rekisteröidyille
- Jos aiotaan käyttää muuhun, tarkoitukseen kuin mihin kerätty -> ilmoitettava ennen jatkokäsittelyä tästä muusta tarkoituksesta antaen em. Tiedot.

Legistum

Ilmoitusvelvollisuudesta

Ilmoitusvelvollisuus (mikäli tiedot saatu muualta kuin rekisteröidyltä), lisäykset:

- Tietojen vastaanottajat ja vastaanottajaryhmät
- Mistä tiedot on saatu ja tieto siitä, onko tiedot yleisesti saatavilla
- Määräykset siitä, koska ilmoitusvelvollisuuden mukaiset tiedot pitää ilmoittaa rekisteröidylle (kohtuullinen aika / oltaessa ensimmäistä kertaa yhteydessä rekisteröityyn, jos aiotaan luovuttaa, viimeistää luovutettaessa.
- Poikkeukset em. Määräyksistä.

Legistum

Rekisteröityjen oikeuksista

- Rekisteröidyn oikeudet:
  - Onko rekisteröity vai ei
  - Jos on, oikeus saada pääsy
  - Oikeus siirtää
  - Oikeus tarkistaa
  - Oikeus korjauttaa
  - Mahdollinen oikeus poistattaa
  - Oikeus rajoittaa / vastustaa
  - Oikeus valittaa
  - Oikeus saada tieto tietojen alkuperästä
  - Profilointi, merkittävyys ja vaikutukset
  - Tieto mahdollisen siirron suojaustoimista

Kun edellä mainitut oikeudet täsmentyvät ja voimistuvat nämä pitää huomioida ilmoituksessa. Henkilötietolain mukaiset selosteet eivät siten miltään osin ole riittäviä!

Legistum

KIITOS!

Teppo Laine

Asianajotoimisto Legistum Oy
Vilhonkatu 9 C
FI-00100 Helsinki

Puh 040 047 4074
teppo.laine@legistum.fi

Legistum