Tietosuoja

- Rekisterin tallentaminen, käyttö ja kerääminen
    - Tallentaminen ja käyttö
    - Sähköinen kerääminen
- Yleisiä ohjeita tietosuoja-asetukseen valmistautumista varten
    - Henkilötietojen käsittelyä koskevat periaatteet
    - Lain noudattamisen käytännössä
        - 1. Henkilötietorekisterien säilytys ja käyttö
        - 2. Rekisteröidyn informointi
        - 3. Periaatteiden noudattamisen osoittaminen
    - Mahdolliset sanktiot
- Usein kysytyt kysymykset:
    - Mikäli mieleenne tulee lisäkysymyksiä, ne voi esittää sähköpostitse AYY:n IT-asiantuntijalle petteri.nummela@ayy.fi .
- Esimerkkidokumentit:
    - Tärkeimmät asiat tietosuojasta yhdistyksille - 09.04.2018.
- Varaa tapaaminen henkilökohtaiseen konsultaatioon

Rekisterin tallentaminen, käyttö ja kerääminen

Henkilötietorekisterin uudet vaatimukset asettavat rajoituksia rekisterin tallennukselle. Rekisterin tulee olla, erikoistilanteita lukuunottamatta, tallennettu EU:n sisälle ja pääsyä rekisteriin tulee rajoittaa entistä tarkemmin. Lisäksi tallennusalustan tulee olla turvallinen tietoturvaltaan. Muista toteutustapaa valitessasi suhteuttaa rekisterien koko valitsemaasi tapaan - Tietosuoja-asetuksen periaatteena on kohtuullisuus, joten pienimuotoiseen rekisteriin ei tarvitse käyttää valtavasti vaivaa.

Alla eri tapoja hyvine ja huonoine puolineen miten tallentamisen, käytön ja keräämisen voi toteuttaa.

Tallentaminen ja käyttö

- Jaettu kryptolevyosiotiedosto - kryptograafisella ohjelmalla, esimerkiksi VeraCrypt, toteutettu tiedosto, jonka sisältö on vahvasti salattu. Tiedosto avataan salasanalla, ja näkyy avaamisen jälkeen omana levyosionaan tietokoneella. Jakamisen voi huoletta hoitaa pilvitallennuspalveluilla kuten Google Drivellä tai OneDrivellä, joilla yhdistyksen vastuuhenkilö voi toteuttaa käyttäjähallintaa.
    - Hyvää: Hyvä tietoturva. Levyn sisälle saa talteen mitä vain, joten rekisteriä voi pitää haluamassaan formaatissa. Nopea toteuttaa.
    - Huonoa: Tietotekniikkaan perehtymättömälle käyttöönotto vaatii oppimista.

- Jaettu exceltaulukko - Myös exceltaulukon voi jakaa pilvitallennuspalveluilla, jos se on suojattu salasanalla. Levyosion tavoin käyttäjähallinta tulee toteuttaa tallennuspalvelun avulla.
    - Hyvää: Todella vaivaton käyttöönotto ja käyttö. Sopii todella hyvin pienimuotoiseen toimintaan.
    - Huonoa: Tallennusformaatti rajoitettu. Tietoturva ei hirveän korkea.

- Oma fyysinen tallennuslevy, esimerkiksi yhdistyksen palvelin - käyttöjärjestelmänä Linuxpohjainen ratkaisu. Hyvä valinta, jos palvelin löytyy jo ennalta ja yhdistyksellä on osaamista palvelimen ylläpitoon. Rekisterien tallennuksessa kannattaa varmistaa tietojen eheys RAID teknologian tai varmuuskopioinnin avulla. Yhteys palvelimeen suoraan verkkosivuilta nykyään ilmaista LetsEncryptin sertifikaateilla.
    - Hyvää: Mahdollistaa todella vahvan tietoturvan ja suoran kommunikaation sovellusten välille. Käyttöoikeushallinta käyttöjärjestelmän puolelta monipuolinen. Mahdollistaa rekistereihin automaatiota.
    - Huonoa: Ylläpito vaihtoehdoista raskainta. Käyttömukavuus linuxmaailmaan perehtymättömälle vaatii paljon oppimista.Vaatii yhdistykselle oman fyysisen tilan ja laitteen.

Sähköinen kerääminen

- G suite - Googlen maksullinen yritysversio. Maksullinen puoli Googlen forms ja drive palveluista kuuluu Privacy Shield -sertifikaatilla tietosuoja-asetuksen piiriin.
    - Hyvää: Toimiva ja helppokäyttöinen tapa luoda ilmolomakkeita
    - Huonoa: Maksullinen, 4€/kk.

- Microsoft Forms aallon tarjoaman o365 kautta. **Huom: Aallolta ei vielä virallista vastausta onko käyttöehtojen mukaista käyttöä.** Toimie ssaan Google formsia vastaava palvelu. Otetaan käyttöön **https://it.aalto.fi/fi/ohjeet/onedrive-business-kayttoonotto** ohjeiden mukaisesti.
    - Hyvää: Ilmainen ja kätevä.
    - Huonoa: Kyselyn tekijän oltava aktiivinen opiskelija Aallolla. Ei virallista varmistusta käyttöehdoista.

- Omat nettisivuformit - kätevä toteutttaa esimerkiksi wordpressin päälle.
    - Hyvää: Ilmainen, hyvin kustomoitavissa alustan kautta.
    - Huonoa: Vaihtoehtoihin nähden työläs toteuttaa.

Yleisiä ohjeita tietosuoja-asetukseen valmistautumista varten

EU:n uuden tietosuoja-asetuksen ydinasia on parantaa EU:n kansalaisten oikeutta omiin henkilötietoihinsa. Laissa on 99 artiklaa, ja se on EU lainsäädännön tapaan monin kohdin ympäripyöreästi kuvattua ja vaikeaselkoista. Lain vaatimukset kuitenkin skaalaavat kerättyjen henkilötietojen määrän, keräystarkoituksen sekä tietojen arkaluontoisuuden mukaan. Tämän ansiosta normaalille yhdistykselle lain noudattaminen ei ole ylitsepääsemätön este.

Henkilötietojen oikeaoppista käsittelyä määrittävät lain 5 artiklassa määritetyt periaatteet. Rekisterinpitäjän, tässä tapauksessa yhdistyksen, on pystyttävä viranomaisen pyynnöstä osoittamaan, että periaatteita on noudatettu yhdistyksen rekisterien kohdalla.

Tämän lisäksi laki määrittää rekisteröidylle oikeuden pyytää rekisterinpitäjältä hänestä kerätyt tiedot itselleen nähtäväksi ja korjattavaksi. Rekisteröity voi myös pyytää tietojen poistoa.

Henkilötietojen käsittelyä koskevat periaatteet

Henkilötietoja tulee käsitellä seuraavien periaatteiden mukaisesti:

- Käsittelyn tulee olla lainmukaista, kohtuullista ja läpinäkyvää.
- Käsittelyn tulee olla nimenomaista ja laillista tarkoitusta varten.
    - Esimerkiksi jäsenrekisteriin kerättyä tietoa ei saa käyttää myöhemmin esimerkiksi suoramarkkinointia varten.
- Käsiteltyä tietoa tulee pyrkiä minimoimaan.
    - On hyvin perusteltavissa kerätä sähköpostiosoitteita jäsenrekisteriin, mutta henkilön IP-tietoa on paljon vaikeampi perustella kohtuulliseksi tai tarkoituksenmukaiseksi.
- Tietojen tulee olla ajan tasalla.
    - AYY:n piirissä toimivien yhdistysten tulee ilmoittaa tukihakemuksessaan AYY:n jäsenten osuus ja määrä yhdistyksen jäsenistöstä, joka usein aiheuttaa ajantasaisuuden kannalta ongelman. Viime kädessä tietojen päivitys on rekisteröitävän henkilön itsensä vastuulla, jos yhdistys ei muilla tavoin kuten poistuneen sähköpostiosoitteen perusteella pysty tätä toteamaan.
- Tietoja ei tule säilyttää sen jälkeen, kun ne eivät enää täytä tarkoitustaan.
    - Jäsenrekisterissä on oltava kaikkien jäsenten tiedot, joten tiedot tulee poistaa yhdistyksestä erottamisen tai eroamisen yhteydessä.
    - Tapahtumien järjestämiseen kerätyt tiedot tulee poistaa kohtuullisessa ajassa tapahtuman jälkeen. 2 - 4 viikkoa on kohtuullista, ja yksittäisiä tietoja voidaan säilyttää pidempään mikäli niiden osalta on jotain tapahtumaan liittyvää kesken, kuten maksamaton osallistumismaksu.
- Tietoja tulee säilyttää turvallisesti.
    - Tiedot tulee säilyttää niin, että niihin pääsee käsiksi vain yhdistyksen asianomaiset, nimetyt henkilöt. Tiedot tulisi aina salata niin, että esimerkiksi kolmannen osapuolen tallennussijainnin järjestelmävalvojat eivät niitä pääse lukemaan. Salaaminen voidaan toteuttaa yhdistyksen yhteisellä salasanalla, mikäli tietoihin pääsy on myös rajattu henkilökohtaisilla käyttäjätunnuksilla.
    - Myös tietojen eheys tulee varmistaa.
- Rekisterinpitäjä on vastuussa näiden periaatteiden toteutuksesta, ja siitä, että pystyy pyydettäessä osoittamaan viranomaiselle noudattaneensa periaatteita.

Lain noudattamisen käytännössä

Tietosuoja-asetuksen noudattaminen pienehköllä yhdistyksellä jakaa kolmeen kokonaisuuteen:

1. Henkilötietorekisterien säilytys ja käyttö

Rekisterien säilytys elektronisessa muodossa tulee toteuttaa niin, että

a) Vain nimetyt henkilöt pääsevät rekisteriin käsiksi. Tämä voidaan toteuttaa käyttäjätunnushallinnalla niin, että kaikille tietoja käsitteleville henkilöille myönnetään oma, henkilökohtainen käyttäjätunnus. Yhteisen tunnuksen käyttö voi olla mahdollista esimerkiksi Otaxin säilytyksessä, mikäli tunnuksen itsensä käyttö edellyttää jotain henkilökohtaista (Otaxin kohdalla henkilökohtaisilla privaattiavaimilla).

b) Mikäli tieto tallennetaan sijaintiin missä yhdistyksen lisäksi toimii korkeamman käyttöoikeuden omaavia tahoja, kuten pilvipalveluissa tai Otaxissa, tulee tiedot salata näiltä henkilöiltä. Tässä tapauksessa toimikausittain vaihdettava, yhdistyksen oma yhteinen salasana riittää. Tiedot voidaan salata esimerkiksi exceltaulukoiden tukemalla salasanalla, tai paketoimalla tiedot salasanasuojatun zip/7z paketin sisään.

c) Tietojen eheys varmistetaan. Ulkopuolisen tahon ylläpitämässä palvelussa tämä todennäköisesti täyttyy heidän toimestaan, mutta asia olisi hyvä varmistaa palvelun tiedoista.

Käytettäessä omaa tallennusmediaa, kuten yhdistyksen omaa palvelinta, tulisi tiedoista tehdä säännölliset, automaattiset varmuuskopiot. Varmuuskopioiden tulee sijaita erillisellä fyysisellä tallennusmedialla. Esimerkiksi RAID 1 teknologian käyttö ja sähköpostihälytyksen asettaminen hajoamisista yleisosoitteeseen (esimerkiksi hallitus@yhdistys.fi , tärkeintä on, että sähköposti ei ole henkilöriippuvainen) on hyvin riittävä toteutus.

d) Käyttäjätunnusten ja salasanojen palautus varmistetaan. On äärimmäisen tärkeää, että jäsenrekisteri ei tuhoudu salasanojen kadotessa. Jos yhdistyksellä on kassakaappi, root-oikeuksien salasanaa voidaan säilyttää siellä. Muutoin rekisterivastaavan koti riittää, jos tieto ei ole ylenpalttisen esillä. Salasanan säilytys palvelimen vieressä tai näyttöön teipattuna on ehdottoman laitonta.

2. Rekisteröidyn informointi

Rekisteröidylle tulee ilmoittaa rekisteröitymishetkellä rekisteriin kerättävistä tiedoista, niiden käyttötarkoituksesta, säilytyksen periaatteista, valitusoikeudesta ja monesta muusta asiasta. Tältä sivulta löytyvät esimerkkidokumentit tietosuojaselosteista sisältävät kaiken tarvittavan. Huomaa, että käyttäessäsi esimerkkidokumentteja sinun tulee varmistaa, että yhdistyksesi oikeasti toteuttaa kaikki siinä mainitut toimenpiteet. Mikäli osa asioista on teille mahdottomia toteuttaa, niitä ei tule luvata. Tietosuojaselosteeseen viittaava linkki rekisteröintivaiheessa täyttää tehokkaasti tämän vaatimuksen.

Rekisteröity voi vaatia rekisterinpitäjää luovuttamaan hallussaan olevat tiedot hänestä. Vaatimukseen vastaaminen tulee toteuttaa kohtuullisessa ajassa, korkeintaan kuukaudessa, ja ilmaiseksi. Rekisteröityä voidaan vaatia tunnistamaan itsensä paremmin, mikäli luovutettavat ovat mittavia tai arkaluontoisia.

Mikäli pyyntö on kohtuuton, esimerkiksi suljetusta kuvagalleriasta pyydettäessä kaikkia henkilöstä itsestään olevia kuvia, voidaan tarkastuksesta pyytää kohtuullinen veloitus tai pyytää rekisteröityä tarkentamaan pyyntöään. Tämänkaltaiset tilanteet kannattaa kuitenkin ratkoa tapauskohtaisesti, ja tarvittaessa pyytää tietosuojavaltuutetulta apua tilanteen ratkaisemiseen, mikäli rekisteröity on yhteistyökyvytön.

Huomaa, että tietosuojaseloste on pakollinen vasta rekisterinpitäjän ylittäessä 250 työntekijän rajan. Lain vaatimukset rekisteröidyn informoinnista voidaan toteuttaa myös muilla tavoin, mikäli välttämättä haluaa näin tehdä.

3. Periaatteiden noudattamisen osoittaminen

Rekisterinpitäjän osoitusvelvollisuus voidaan toteuttaa niin ikään dokumentaatiolla. Tältä sivulta löytyvä tietosuojapolitiikkamalli antaa hyvän pohjan sille, miten periaatteita voidaan noudattaa. Politiikan laatimisessa tulee noudattaa samaa kuin tietosuojaselosteessakin, eli vain asiat joita rekisterinpitäjä aikoo toteuttaa, tulee sinne kirjata.

Mahdolliset sanktiot

Tietosuoja-asetuksen sanktiot voivat vaikuttaa astronomisen kookkailta; 20 miljoonaa euroa tai 4% organisaation globaalista liikevaihdosta *per rikkomus*. Sanktioiden suuruudesta johtuen julkiskeskustelussa on päässyt valloilleen myyjän markkinat, missä lakiasiaintoimistot ja ohjelmistotalot tuottavat kallista konsultaatiota avuksi organisaation turvaksi. Todellisuudessa kuitenkaan sanktiot kohtuullistetaan rikkomusten aiheuttamaan haittaan. Yhdistystasolla sanktiot tulevat todennäköisesti olemaan huomautus Suomen tietosuojavaltuutetulta.

Usein kysytyt kysymykset:

- K: Edellisen hallituksen jäljiltä oli jäänyt vanha sitsi-ilmorekisteri, onko uusi hallitus siitä vastuussa?
- V: On vastuussa. Kannattaa käydä yhdistyksen tiedostot läpi jo ennen GDPR:n voimaantuloa ja poistaa turhat rekisterit.

- K: Laki määrää säilyttämään dokumentteja 10 vuotta. Pitääkö niistä nyt poistaa henkilötiedot?
- V: Ei. GDPR on yleislaki, erityislait kuten yhdistyslaki ovat ristiriitatilanteissa etuasemassa.

- K: Voinko täyttää omalla koneellani rekisterin tietoja?
- V: Voit. Tiedonsiirto oman koneesi ja rekisterin säilytyspaikan välillä kannattaa salata, esimerkiksi https tai ssh liikenteen avulla.

- K: Voinko antaa henkilöiden tietoja eteenpäin, esimerkiksi laivayhtiölle tai majapaikan järjestäjälle?
- V: Voit, jos mainitset tietojen keräysvaiheessa tietojen eteenpäin luovutuksesta. Kannattaa myös kertoa syy tietojen luovutukselle.

- K: Voinko käyttää Google Driveä tallennuspaikkana?
- V: Ilmaisversio Google Drivestä ei täytä GDPR:n vaatimuksia. Aallon opiskelijoille tarjoaman office 365 mukana tuleva OneDrive täyttää, mikäli data on suojattu palvelun admineilta. Suojauksen voi toteuttaa esimerkiksi salaamalla tiedostot salasanalla (excel tukee tätä suoraan tallennusvaihtoehdoissa)

- K: Henkilö pyysi meiltä tietonsa yhdistyksemme hallussa olevista kuvista. Kuvissa esiintyy muitakin henkilöitä, saammeko luovuttaa kuvat?
- V: Jos kuvat eivät ole jo yleisessä jaossa (kuten esimerkiksi killan omassa kuvapankissa), muitakin henkilöitä sisältäviä kuvia ei saa luovuttaa eteenpäin.

- K: Miten voin tunnistaa oikein tietojaan pyytävän henkilön?
- V: Mitä arkaluontoisempaa ja laajempaa tietoa pyydetään, sitä varmemmin henkilö tulee tunnistaa. Pienemmissä tietopyynnöissä riittää esimerkiksi se, jos pyytö tulee samasta sähköpostiosoitteesta kuin mikä tietoihin on tallennettuna. Suuressa tietopyynnössä voi olla kohtuullista pyytää henkilöä tulemaan esittämään henkilöllisyytensä henkilöllisyyspapereista.

Mikäli mieleenne tulee lisäkysymyksiä, ne voi esittää sähköpostitse AYY:n IT-asiantuntijalle petteri.nummela@ayy.fi .

Esimerkkidokumentit:

tietosuojaselos...ahtumare

tietosuojaselost...arkkikerh

Tietosuojapolitii...karkkiker

Tärkeimmät asiat tietosuojasta yhdistyksille - 09.04.2018.

Varaa tapaaminen henkilökohtaiseen konsultaatioon

Mikäli yhdistyksellänne on vielä avoimia kysymyksiä mihin vastausten löytäminen on vaikeaa, voitte varata ajan AYY:n IT-asiantuntijan kanssa keskusteluun. Aikaa pääset varaamaan täältä: https://doodle.com/poll/4zp45pc5m7n54dhe