opsec

Lomakkeet -liite

Tietosuojaopas pienille yrityksille

Helmikuu 2019

Suomen Yrittäjäopisto

Euroopan maaseudun kehittämisen maatalousrahasto: Eurooppa investoi maaseutualueisiin

MAASEUTU 2020

Elinkeino-, liikenne- ja ympäristökeskus

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 1, Henkilötietojen kartoittaminen

Ketä tieto koskee?	Missä tietoa on?	Mitä tieto on (yleiskuvaus)?

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 2, Henkilötietojoukot

Henkilötietojoukko ja yrityksen rooli (rekisterinpitäjä vai käsittelijä)	
Mitä henkilötietoa tietojoukko sisältää?	
Käsittelijät	
Henkilötietojen siirrot Eta-alueen ulkopuolelle	
Käsittelyn tarkoitus	
Käsittelyn lakiperuste	
Erityistietoryhmät ja erityiset rekisteröityjen ryhmät	

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 3, Henkilötietovirrat

	Henkilötietojen kerääminen	**Henkilötietojen säilytys ja käsittely**	**Henkilötietojen poisto ja ulos siirrot**
Asiakas			
Yritys			
(Henkilötietojen käsittelijä 1)			
(Henkilötietojen käsittelijä 2)			

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 4, Henkilötietoriskit

Tapahtuma	Riskin syyt	Riskin seuraukset	Vaikutuskeinot
Henkilötietoa joutuu vääriin käsiin			
Henkilötieto ei ole saatavilla			
Henkilötieto vääristyy			

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 5, Tietoriskien arviointi

	Prosessit ja toimintamalli		Henkilöstö		Kumppanit ja sidosryhmät
	Tämä lomake on tarkoitettu tietoriskien arvioinnin tueksi. Sen on tarkoitus antaa yleisnäkymä siihen, miten organisaatiossasi on varauduttu liiketoimintakriittisen tiedon suojaamiseen. Muistathan huomioida henkilötiedon osalta samat havainnot.		Henkilöstöllä on käytössä ohjeistus tiedon käsittelyyn		Kriittiset yhteistyökumppanit on tunnistettu
			Henkilöstö perehdytetään ja koulutetaan säännöllisesti		Kumppaneiden välillä siirrettävä tieto on tunnistettu ja riskiarviot tietovirtojen osalta on tehty
			Taustatarkastukset ja luottotiedot tarkastetaan rekrytointivaiheessa tarvittaessa		Riskienhallinnasta saadaan sopimuksille kumppaneihin liittyvät riskit sopimuksentekovaiheessa (prosessi)
	Merkitse organisaatiosi tilanne jokaiseen kohtaan, esim.: ***K = Kunnossa, A = Aloitettu työ*** ***E = Ei tehtyjä toimenpiteitä*** ***Voit yliviivata kohdan, joka ei koske organisaatiotasi. Lisää muistiinpanot erilliselle lomakkeelle ja huomioi havainnot riskiarvioita tehdessä.***		Henkilöstölle tehdään salassapitosopimus tiedon käsittelyyn liittyen		Auditoinneista ja katselmoinneista on sovittu sopimuksilla
			Esimiehillä on ohjeistus työsuhteen päättämiseen liittyviin toimiin (laitteiden ja tunnusten poisto, jne.)		Tunnuksia ja pääsyoikeuksia luovutettaessa on olemassa myös ohjeistuskäytäntö
			Henkilöstö on koulutettu käyttämään teknisiä suojausratkaisuja, jos niitä on käytössä (postien salaus, salatut etäyhteydet, ym.)		Sopimuksilla on määritelty tiedon merkityksen perusteella kumppaneilta vaadittavat tietoturvakontrollit
					Kumppanien pääsyoikeushallinta on suunniteltu
	Johtaminen ja organisoituminen		**Toimitilat ja fyysinen ympäristö**		**Tietojärjestelmä- ja IT-ympäristö**
	Johdon allekirjoittama tietoturvapolitiikka / vast.		Tilojen jakaminen turvallisuustasoihin ja erottaminen		Järjestelmien omistajat ja/tai pääkäyttäjät nimetty
	Tietovirtojen kartoitukset ja dokumentointi		Kulunvalvonta		Paperiaineistojen käsittelyohjeet
	Kriittisen informaation tunnistaminen tehty		Rikosilmoitinjärjestelmät ja muu tilaturvallisuus		Käyttövaltuushallinta ja sen valvonta
	Johdettu jatkuva riskienhallintaprosessi		Palontorjunta		Etätyölaitteiden ja yhteyksien turvallisuus
	Tietoturvallisuustyön tavoitteet kirjattu		Kulkuoikeuksien hallinta		IT-ympäristön valvonta ja raportointi (käyttöasteet, vikatiheydet, ym.)
	Tietoturvallisuustyön seuranta ja mittaaminen		Arkistointi		Sähköisen tietoaineiston arkistointimenettelyt
	Tietoturvatyö organisoitu ja vastuut jaettu		Onnettomuustekijöiden tunnistaminen (vesivahingot, ym.)		Muutostenhallintaprosessi ja testausmenettelyt
	Poikkeamien seuranta ja mittaaminen		Tulostimet, näytöt, ym. laitesijoittelu salakatselun osalta on huomioitu		Tietojen poisto järjestelmistä
	Pääsyoikeuksien hallinta ja hyväksymismenettelyt		Asiakastilojen riittävä erottaminen		Ohjelmistohankintaprosessi
	Jatkuvuudenhallinta ja toipumissuunnitelmat		Vierailijaohjeistus tiloissa vierailijoiden osalta		Tietojen varmuuskopiointi ja palautustestaus
	Avainhenkilöiden tunnistaminen		Luottamuksellisen paperiaineiston poisto		Henkilökohtaiset käyttäjätunnukset ja salasanaohjeet
	Varahenkilöjärjestelmät tärkeisiin toimintoihin		Varmuuskopioiden ja arkistojen säilytys		Tietoliikenneyhteyksien ja siirtojen turvallisuus
	Tietojen luokitteluohje olemassa		Kumppanien pääsy tiloihin (esim. siivouspalvelut, ym.)		Valvottu virustorjuntaohjelmisto
					UPS- ja jäähdytystarpeiden mitoitus ja varmistus

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 6, Rekisteröityjen oikeuksien toteutuminen

	Selvitettä ja ohjeistettava	Tila (kesken / valmis / lisätiedot)
1.	Mihin rekisteröidyillä on oikeus?	
2.	Mistä löytyvät rekisteröidyille informoitavat tiedot?	
3.	Miten käyttöpyynnön voi jättää?	
4.	Mitä tietoja käyttöpyyntöä jättäessä pyydetään henkilöltä?	
5.	Kuka käsittelee käyttöpyynnöt organisaatiossa ja kenelle ne missäkin tapauksessa toimitetaan?	
6.	Mitä tietoa voidaan luovuttaa puhelimitse ja mitä tietoa vastaan?	
7.	Milloin rekisteröity on tunnistettava vahvemmin (esimerkiksi ajokortti)?	
8.	Mitkä ovat tunnistamistavat?	
9.	Millä lisätiedoilla yksiselitteinen tunnistaminen voidaan tehdä esim. puhelimessa?	
10.	Millaisissa tapauksissa luovutettava tieto voi aiheuttaa riskin jollekulle muulle? (Riskiarviot!)	
11.	Kuka tekee päätöksen tai toimittaa tiedot, miten?	
12.	Kuka / miten tiedot kerätään?	
13.	Riippuen oikeuden käyttöpyynnön sisällön laajuudesta...	
13. a	- Mistä tiedot kerätään?	
13. b	- Kenelle siitä on ilmoitettava?	
14.	Miten varmistutaan, että toimitettavat tiedot eivät sisällä ylimääräistä tietoa?	
15.	Missä tapauksessa tiedot on varmistettava ennen toimittamista?	
16.	Kuka saa tehdä päätöksen tietojen toimittamisesta ja missä tapauksissa?	

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 7, Tietosuojapoikkeamien arviointi

POIKKEAMAN OTSIKKO:	
	Selvitettävät asiat
Tietosuojavastaava / lisätietoja toimittavan taho	*Yhteystiedot*
Poikkeaman havaitsemisaika	*Päivämäärä ja kellonaika*
Poikkeaman alkamisaika (ja päättymisaika, jos ohi)	*Päivämäärä ja kellonaika*
Poikkeaman kuvaus	*Yleiskuvaus tapahtumasta. Samassa yhteydessä on hyvä kuvata, onko kyseessä tiedon luottamuksellisuuteen, eheyteen vai saatavuuteen liittyvä poikkeama.*
Henkilötiedon kuvaus	*Millaista henkilötietoa poikkeama koskee? Arvio* - *henkilötietojen luonteesta ja kuvaus henkilötietoryhmistä* - *arkaluonteisuudesta* - *miten montaa henkilöä/henkilötietoyksikköä poikkeama koskee* - *henkilöiden tunnistettavuus poikkeamaan liittyvästä henkilötiedosta* - *rekisteröityjen erityispiirteet (onko kohteena lapsia tai muita erityisryhmiä)*
Seuraukset poikkeamasta	*Tähän arvioidaan sekä* - *todelliset ja välittömät seuraukset rekisteröidyille* - *todennäköiset, potentiaaliset tai välilliset seuraukset tai vaikutukset rekisteröidyille*
Suoritetut korjaustoimenpiteet	*Mitä toimenpiteitä on suoritettu poikkeaman vaikutusten rajaamiseksi sekä normaalitilanteeseen palaamiseksi ja missä järjestyksessä. Tehtiinkö ilmoitus ja perustelut sen tekemiselle tai tekemättä jättämiselle*

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 8, Kysymyslista (otsikosta näet, mihin oppaan osaan kysymykset viittaavat)

<table>
<tr>
<td>3. Kartoita, mitä henkilötietoa käsittelet
• Missä henkilötietosi sijaitsee?
• Miten se tulee sinulle?
• Missä sitä säilytetään (tietokoneet, ohjelmat ja paperiarkistot?
• Miten henkilötieto poistuu?
• Onko erityistietoryhmät ja arkaluonteiset tiedot tunnistettu?</td>
<td>4. Henkilötietojen käsittelyn tarkoitusten ja lainmukaisuuden selvittäminen
• Onko kaiken henkilötiedon käsittelyn tarkoitukset selvitetty?
• Löytyykö kaikelle käsittelylle lainmukaisuusperuste?
• Löytyykö suostumukset tallennettuna?</td>
<td>5. Riskienhallinta
• Onko henkilötietoihin ja rekisteröityihin kohdistuvat riskit kartoitettu?
• Onko riskien osalta suunniteltu ja toteutettu riittävät tietoturvatoimet?
• Onko kaikki suunnitelmat ja käytössä olevat keinot dokumentoitu</td>
<td>6. Tietojen siirrot ja sopimukset käsittelijöiden kanssa
• Onko kaikki henkikötietojesi käsittelijät tai muut rekisterinpitäjät tunnistettu?
• Onko kaikkien kanssa tehty asianmukaiset sopimukset?
• Siirrätkö tietoja EU-alueen ulkopuolelle?
• Jos siirrät, onko tietojen lainmukaisuusperusteet selvitetty?</td>
<td>7. Rekisteröidyn oikeudet
• Onko yrityksessä suunnitelma, miten rekisteröityjen pyyntöihin vastataan?
• Onko ohjeistus oikeuksien käyttämisestä olemassa? Työntekijöille? Muille rekisteröidyille?</td>
</tr>
<tr>
<td>8. Rekisteröidyille informointi
• Kerrotaanko rekisteröidyille selkeästi ja tarkoituksenmukaisesti heidän tietojensa käsittelystä?
• Kerrotaanko tarvittavat ydinasiat jo tietoja kerätessä?
• Onko seloste käsittelytoimista tehty tarvittavilta osin?
• Onko rekisteröidyille informoitu, mistä saa halutessaan lisätietoa käsittelystä?</td>
<td>9. Poikkeamien hallinta ja ilmoitusvelvollisuus
• Onko henkilötietoihin kohdistuvien tietoturvapoikkeamien osalta selvillä niistä ilmoittaminen, tallentaminen, niihin reagointi ja riskien tunnistamisesta poikkeamiin liittyen?
• Kuka yrityksessäsi vastaa yhteistyöstä viranomaisen suuntaan?</td>
<td>10. Nettisivut ja evästeet
• Kerrotaanko nettisivuillasi selvästi, mitä tietoja kerää vierailijoista?
• Tekeekö yrityksesi henkilöiden profilointia ja miten siitä voi halutessaan kieltäytyä?

11. Sähköpostimarkkinointi
• Onko suoramarkkinoinnin osalta selvitetty lainmukaisuusperusteet ja tehty tarvittaessa tasapainotesti?</td>
<td>12. Tietosuojavastaava
• Onko yrityksellläsi lakisääteinen velvoite nimittää tietosuojavastaava?
• Onko yrityksessäsi nimetty tietosuojan seurannasta ja kehittämisestä vastaava henkilö tai oletko suunnitellut esimerkiksi ulkoistavasi tehtävän?</td>
<td>13. Jatkuvaa toimintaa ja laadun kehittämistä
• Onko yrityksellläsi suunnitelma henkilötietojen käsittelyn vuosittaisesta seurannasta ja kehittämisestä?
• Arvioidaanko käsittelyssä tapahtuvat muutokset ja riskit määrävälein?</td>
</tr>
</table>

Kannattaa myös selvittää, että henkilötietojen käsittelyn yhteydessä toteutuvat aina artiklan 5 perusperiaatteet (lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus). Periaatteita varmistavat toimet kannattaa kirjata ylös, jotta voi myöhemmin osoittaa noudattavansa niitä. Lisäksi kannattaa laatia tarvittavat ohjeet henkilöstölle, varsinkin työhönottotilanteisiin. Ohjeet kannattaa pitää ajan tasalla ja kerrata henkilöstön kanssa aina tarvittaessa.

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

Lomake 9, Tarkistuslista

Ketä koskee	Vaatimus	Omat muistiinpanot
Rekisterinpitäjiä koskevat velvoitteet	Tietosuojaperiaatteet (artikla 5): • lainmukaisuus, kohtuullisuus ja läpinäkyvyys • käyttötarkoitussidonnaisuus • tietojen minimointi • täsmällisyys • säilytyksen rajoittaminen • eheys ja luottamuksellisuus Miten edelläolevien periaatteiden toteutuminen näkyy henkilötietojeni käsittelyssä? Miten osoitusvelvollisuus periaatteiden noudattamisen osalta näkyy? Miten todistan, että noudatan periaatteita?	
	Käsittelyn lainmukaisuusperuste (artikla 6) Onko kaikkien henkilötietojen käsittelylle löydettävissä jokin lainmukaisuusperuste? • suostumus • sopimuksen täytäntöönpano / sopimusosapuolena oleminen • lakisääteinen velvollisuus • rekisteröidyn elintärkeät edut • yrityksen oikeutettu etu • (yleinen etu, ei tavallinen)	
	Erityistietoryhmien käsittelyn lainmukaisuusperuste (artikla 9) Onko kaikkien henkilötietojen käsittelylle löydettävissä jokin lainmukaisuusperuste, esim: • nimenomainen suostumus • käsittely on tarpeen velvoitteiden ja erityisten oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla • käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän yhteisön laillisen toiminnan yhteydessä	

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

	• käsittely on tarpeen ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi	
	Rekisteröityjen informointi (artiklat 12 – 14) Kerrotaanko tarpeeksi avoimesti ja selkeästi siitä, mihin tarkoituksiin yritys käsittelee henkilötietoja? Onko viestintätapa ja kanavat tarkoituksenmukaiset kohderyhmään nähden?	
	Rekisteröityjen oikeudet (artiklat 15 – 22) • oikeus saada pääsy henkilötietoihin • oikeus tietojen oikaisemiseen • oikeus tietojen poistamiseen • oikeus käsittelyn rajoittamiseen • oikeus tietojen siirrettävyyteen • vastustamisoikeus • automatisoidut yksittäispäätökset ja profilointi Onko rekisteröidyille ohje, miten oikeuksia käytetään? Onko varmistuttu, että oikeuksien käyttäminen on mahdollista ja ohjeistettu myös yrityksen sisällä?	
	Rekisterinpitäjän velvoitteet (artikla 24) Onko henkilötietojen käsittelyyn kohdistuvat riskit kartoitettu ja niihin suojakeinot suunniteltu? Sisäänrakennettu ja oletusarvoinen tietosuoja (artikla 25) Onko yrityksessä käytössä sellaiset työmenetelmät ja tietojärjestelmien ja ohjelmistojen ominaisuudet, joilla voidaan taata tietosuojaperiaatteiden (artikla 5) toteutuminen kaikessa toiminnassa?	
	Tietosuojan vaikutustenarviointi ja ennakkokuuleminen (artiklat 35 – 36) Jos henkilötietojen käsittely tai siihen kohdistuvat muutokset (kuten uudet tietojärjestelmät tai käsittelytavat) voivat aiheuttaa riskejä rekisteröityjen oikeuksille ja vapauksille, käsittelytoiminnasta tehdään aina ensin tietosuojan vaikutustenarviointi.	

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

	Jos käsittely edellisestä huolimatta voi aiheuttaa rekisteröidyille korkean riskin, on yrityksen ensin kuultava asiassa tietosuojaviranomaista.	
Rekisterinpitäjiä ja käsittelijöitä koskevat velvoitteet	Käsittelijän vastuut ja sopimusvelvoite (artikla 28) Rekisterinpitäjä on velvollinen valitsemaan ja ohjeistamaan käsittelijänsä huolellisesti. Henkilötietojen käsittelystä sopimussuhteessa on laadittava sopimus yhtiöiden välille.	
	Seloste käsittelytoimista (artikla 30) Selosteen ylläpito niiden henkilötietojen käsittelyn osalta, joka ei ole satunnaista tai jos käsittely aiheuttaa rekisteröidyille riskin tai jos käsitellään erityistietoryhmiä (artikla 9).	
	Yhteistyö valvontaviranomaisen kanssa (artikla 31)	
	Tietoturvan varmistaminen (artikla 32) Henkilötietojen eheyden, saatavuuden ja luottamuksellisuuden varmistavat tietoturvatoimet on suunniteltu ja otettu käyttöön.	
	Poikkeamienhallinta ja ilmoitusvelvollisuus (artiklat 33 -34) Henkilötietojen käsittelyyn liittyvät tietosuojan vaarantavat poikkeamat tallennetaan ja niitä seurataan säännöllisesti. Jos poikkeama aiheuttaa rekisteröidyille riskin, on yrityksellä valmis malli siitä, miten ilmoitusvelvollisuutta käytetään missäkin tapauksessa.	
	Tietosuojavastaavan nimittäminen (artiklat 37 – 39) Yrityksessä on selvitetty, onko tietosuojavastaavan nimittäminen pakollista. Vaikka nimittämisvelvoitetta ei olisi, tietosuojaan liittyvät tehtävät on vastuutettu ja organisoitu tarkoituksenmukaisella tavalla.	
	Henkilötietojen siirrot EU-alueen ulkopuolelle (artiklat 44 – 49) Yritys on selvittänyt mitä henkilötietoja siirretään EU tai ETA-alueen ulkopuolelle.	

Tietosuojaopas pienille yrityksille Yritys: _____ Pvm: _____

	Tietojen siirtojen osalta on käytössä soveltuva siirtoperuste, esim: • EU-komission tietosuojan riittävyyslausunto, Privacy Shield tai vastaava • EU-komission vakiosopimuslausekkeet • erityistilanteita koskevat poikkeukset	
	Paikallinen lainsäädäntö Yrityksessä on selvitetty myös se, miten maan oma lainsäädäntö poikkeaa tietosuojan osalta siitä, mitä tietosuoja-asetus määrittelee tai antaa liikkumavapauksia jäsenvaltioille. Suomessa esimerkiksi Tietosuojalaki. Lisäksi on hyvä huomata erityislainsäädännön – esimerkiksi työlainsäädännön (artikla 88) – mahdolliset poikkeamat ja tarkennukset oman maan lainsäädännössä.	
Vain käsittelijöitä koskevat velvoitteet	Rekisterinpitäjän ohjeiden noudattaminen Yrityksessä on kerätty rekisterinpitäjiltä henkilötietojen käsittelyn ohjeistukset. Ohjeet on viety työntekijöiden perehdytys- ja koulutusmateriaaleihin ja ohjeisiin ja tarvittaessa sisällytetty myös koulutussuunnitelmaan.	