Tietosuojan hallinta metsäurakoinnissa

Metsäteho KONEYRITTÄJÄT

Tämä opas auttaa metsäkone- ja metsäpalveluyrityksiä hyvän tietosuojan hallinnassa. Opas on tehty Koneyrittäjien liiton ja Metsäteho Oy:n yhteistyönä ja löytyy sivulta www.puuhuolto.fi/tietosuoja. Samalta sivulta löytyy myös muuta tietosuojan hallintaan liittyvää materiaalia.

Opasta päivitetään tarpeen mukaan. **Tämä on versio 26.4.2018.**

Sisällys

1. Miksi tietosuoja on tärkeää ja miten se koskee meitä? 2
   1.1. Henkilötiedot 3
   1.2. Rekisterinpitäjä ja henkilötiedon käsittelijä 3
2. Yrityksessä tehtävät toimenpiteet 4
   2.1. Mitä henkilötietoja yrityksessä on? 4
   2.2. Mikä tieto on tarpeellista? 5
   2.3. Kuka henkilötietoja käsittelee? 5
   2.4. Henkilötietojen käsittely ja varastointi 6
   2.5. Henkilötietojen käsittelyn ulkoistaminen 7
   2.6. Henkilötiedon käsittelyn riskiarvio 8
   2.7. Henkilötietojen suojaustoimenpiteet 9
   2.8. Rekisteröidyn oikeudet 9
   2.9. Osoitusvelvollisuus ja dokumentointi 9
   2.10. Tietoturvaloukkauksiin valmistautuminen 10
3. Metsäkonetiedon omistuksen ja käytön suositus 12
4. Lisätietoja 12

1. Miksi tietosuoja on tärkeää ja miten se koskee meitä?

Tietosuoja tarkoittaa henkilötietojen suojausta ja niihin liittyviä toimia. Näistä vastaa lainsäädännön mukaan yrityksen johto. **Jokaisen yrityksen tulee huolehtia siitä, että niissä käsitellään vain tarpeellisia henkilötietoja, tietoja säilytetään vain tarpeellinen aika ja estetään tietojen leviäminen muualle.**

Tietosuojasääntelyn tarkoitus on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä mm. siten,

a) ettei henkilöistä kerätä mitään turhaa/tarpeetonta tietoa *) ja
b) ettei kerättyä tietoa säilytetä tarpeettomasti ja
c) ettei kerättyä tietoa levitetä tarpeettomasti sekä
d) että varmistetaan tietoturva.

**) Henkilötiedon käsittelylle pitää olla oikeusperuste eli miksi henkilötietoa saa säilyttää ja käsitellä.*

EU:n yleinen tietosuoja-asetus (GDPR, General Data Protection Regulation) velvoittaa, että 25.5.2018 alkaen kaikkien EU:n alueella toimivien yritysten täytyy huolehtia, että niiden toiminnassa noudatetaan asetuksen vaatimuksia.

Teknologisen kehityksen ja yli valtiorajojen tapahtuvan kaupankäynnin myötä on tullut tarpeelliseksi tarkentaa ja vahvistaa ihmisten (rekisteröityjen) oikeuksia omista henkilötiedoistaan ja niiden käsittelystä. Samalla yhtenäistetään nykyisin hajallaan oleva lainsäädäntö ja sen tulkinta EU:n alueella.

Tietosuoja-asetuksen rikkomisesta voi seurata muun muassa sakkoja tai henkilötietojen käsittelykielto.

Tämä opas on tehty Koneyrittäjien liiton ja Metsäteho Oy:n yhteistyönä, ja sen tarkoitus on auttaa **metsäkone- ja metsäpalveluyrityksiä sekä muita alan yrityksiä** tietosuoja-asetuksen soveltamisessa ja tietosuojan saamisessa vaaditulle tasolle. Ohjeessa *yrityksellä* tarkoitetaan nimenomaan näitä yrityksiä.

Opasta täydennetään tarpeen mukaan. Tähän oppaaseen on kerätty metsäurakoinnin kannalta oleelliset tietosuojan hallintaan liittyvät asiat. Tarvittaessa lisätietoja saa esimerkiksi tietosuojavaltuutetun verkkosivuilta.

Yksi tärkeimmistä uusista velvoitteista on **osoitusvelvollisuus**: ei riitä enää, että yrityksen tietosuoja on vaaditulla tasolla, vaan se pitää pystyä myös osoittamaan. Liitteenä löytyvää Dokumentoinnin voi halutessaan hoitaa myös muulla valitsemallaan ja vaatimukset huomioiden riittävällä tavalla.

1.1. Henkilötiedot

Olennaista **henkilötiedon** määritelmän kannalta on se, onko tietty henkilö tunnistettavissa tiedon perusteella vai ei. Jos henkilö voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, tai yhden tai useamman hänelle tunnusomaisen tekijän perusteella, kyseessä on henkilötieto.

Henkilötietoa on esimerkiksi nimi, osoite, puhelinnumero, henkilötunnus tai sähköpostiosoite. Henkilön voi suhteellisen helposti tunnistaa tai selvittää myös esimerkiksi vähäisemmistä merkinnöistä, vaikka itse henkilön nimeä ei lukisi tiedossa tai olisi sen yhteydessä. Tällaisia ovat esimerkiksi kiinteistötunnus tai ajoneuvon rekisterinumero.

Käytännössä tieto voi olla esimerkiksi tekstiä paperilla tai tietokoneen tiedostossa, kuva tai äänitallenne.

Henkilötiedot muodostavat **rekisterin** (henkilörekisteri, henkilötietorekisteri).

Metsäalan yrityksissä, kuten kaikissa muissakin yrityksissä, käsitellään henkilötietoja, joten jokaisella yrityksellä on tietosuojaa koskevia velvoitteita. Esimerkiksi henkilöstöön liittyvät tiedot kuten palkanlaskentatiedot ovat henkilötietoa. Lisäksi yrityksissä voi olla esimerkiksi urakanantajien tai metsänomistajien taikka aliurakoitsijan työntekijän henkilötietoja. Tuotantotiedot, kuten mittaustulos, eivät sellaisenaan ole henkilötietoa, mutta jos ne voidaan yhdistää johonkin henkilöön esimerkiksi kiinteistunnuksen perusteella, niistä tulee henkilötietoa.

1.2. Rekisterinpitäjä ja henkilötiedon käsittelijä

Henkilötiedon osalta yritys voi olla rekisterinpitäjä ja/tai tiedon käsittelijä. On tärkeä tunnistaa, milloin yritys on **rekisterinpitäjä** ja milloin **henkilötiedon käsittelijä**, koska näiden velvoitteet ja vastuut ovat erilaiset.

Rekisterinpitäjä on se, joka perustaa rekisterin omaa toimintaansa varten. Se on vastuussa rekisteristä ja määrää rekisterin käytöstä.

Henkilötietojen käsittelijä taas käsittelee rekisterinpitäjän käsittelijän käyttöön antamia henkilötietoja. Kaikki, mitä tehdään henkilötiedoille tai henkilötiedoilla (tietojen lisääminen, hakeminen, muokkaaminen, varastointi, siirtäminen jne.), katsotaan käsittelyksi.

Urakanantajilta saadut työssä tarvittavat tiedot sisältävät usein henkilötietoja, kuten maanomistajan yhteystiedot. Tällöin urakointiyritys toimii yleensä henkilötiedon käsittelijänä.

Rekisterinpitäjänä yritys toimii lähinnä työntekijöidensä henkilötietojen kohdalla. Yrityksen tulee kuitenkin tunnistaa roolinsa kaikissa tapauksissa, jotta voi toimia oikein.

2. Yrityksessä tehtävät toimenpiteet

Tietosuoja-asetuksen myötä yritysten tulee käydä läpi oma toimintansa ja päivittää se vastaamaan velvoitteita. Tämä ohje sekä liitteenä oleva Tarkistuslista auttavat yritystä päivittämään tietosuojaa koskevia toimintatapojaan. Tämän ohjeen lukujen järjestys noudattelee soveltuvin osin Tarkistuslistan mukaista järjestystä.

Jatkossa tietosuoja on huomioitava aina, kun suunnitellaan uusia toimintoja tai kehitetään toimintaa ja koulutusta.

Asetuksen velvoitteet voidaan ottaa metsäkone- ja metsäpalveluyrityksessä haltuun, kun

- Selvitetään nykytila
- Määritetään tarpeelliset henkilötiedot
- Arvioidaan henkilötietojen käsittelyn riskit
- Määritellään tietosuojan toteutus
- Dokumentoidaan, huolehditaan osaamisesta ja kyetään osoittamaan henkilötietojen hallinta

2.1. Mitä henkilötietoja yrityksessä on?

Nykytilan kartoituksessa selvitetään, mitä oman yrityksen tai muilta saatuja henkilötietoja yrityksessä kerätään, säilytetään tai käsitellään.

Tarkistuslistan yleiskuva-välilehdellä (kuva 1) on kuvattu mahdollisia tietolähteitä sekä kenen tietoja niissä todennäköisesti voi olla. Näitä ovat henkilöstöön tai toimeksiantajiin liittyvät listat ja rekisterit. Näistä muodostuu henkilötietoja, jos rekistereissä on edes yksi tunnistamisen mahdollistama kohta, esimerkiksi sähköposti.

Yleiskuva-välilehdellä on esitelty arvio henkilötietojen esiintymisestä metsäkonetiedoissa. Metsäkoneiden tietojärjestelmissä käsiteltäviä henkilötietoja ovat esimerkiksi koneenkuljettajaa sekä metsänomistajaa koskevat tiedot, tyypillisesti henkilöiden tunniste- ja yhteystietoja tai henkilöiden sijaintitietoja. (Tutustu myös Metsäkonetiedon omistuksen ja käytön suositukseen, luku 3).

YLEISKUVAN LUONTI KONEYRITYKSEN HENKILÖTIEDOISTA

Tämän taulukon avulla luodaan yleiskuva siitä, mitä toimintaa varten yrityksessä kerätään taikka käsitellään henkilötietoa, millaisia tietoryhmiä tiedonkäsittely sisältää ja missä henkilötietoa sijaitsee sekä millaisia henkilöryhmiä tieto kattaa.

Päivitetty: pp.kk.vvvv

Ketä koskevaa henkilötietoa toiminto/tietoryhmä sisältää tai voi sisältää:

	Toiminto ja tietoryhmä	Yrityksen ulkopuoliset				Yrityksen sisäiset			
		Metsän-omistaja	Asiakkaan työntekijä	Alihankkijan työntekijä	Muu	Koneyrittäjä / johto	Kuljettaja	Toimi-henkilö	Muu työn-tekijä
		Laita X niiden henkilöryhmien kohdalle, joiden henkilötietoa rivillä oleva toiminto-/tietoryhmä sisältää tai voi sisältää							
A.	**Palvelutuotannon vaatimat taikka tuottamat tiedot (metsäkonetietoa)**								
1.	Työmaa- ja korjuuohjeet	x	x	x				x	
2.	Puutavaralaji- ja puulajiohjeet		x					x	
3.	Tuotantotiedot	x	x	x		x	x	x	
4.	Työaika- ja tuottavuustiedot	x	x			x	x	x	
5.	Mittalaitteen ja kuormainvaa'an kalibrointi- ja tarkastusmittaustiedot	x		x		x	x	x	
6.	Mittaustarkkuuden seurantaraportti			x		x			
7.	Koneella työn yhteydessä muodostettavat paikkatiedot			x		x	x		
8.	Korjuulaadun omavalvontatiedot ja -raportit	x		x		x	x		
9.	Korjuun laskutusperustetiedot			x		x	x		

Kuva 1. Tarkistuslistan etusivu. Täydellinen versio Tarkistuslistassa.

2.2. Mikä tieto on tarpeellista?

Henkilötietoa saa kerätä ja säilyttää vain, jos se on tarpeellista toiminnan kannalta eli käsittelylle on **oikeusperuste**. Peruste muodostuu esimerkiksi henkilön antamalla suostumuksella tai velvollisuuksien hoidon tai asiakkuuden myötä. Esimerkkejä kuvassa 2. Huomioi että perusteita voi olla muitakin kuin tässä esitetyt.

Tietoa ei tule säilyttää, kun sitä ei enää tarvita. Sellaiset henkilötiedot, joiden säilyttämiselle ei ole hyväksyttävää perustetta, on poistettava. Lisäksi säilyttämiselle on hyvä määritellä enimmäissäilytysaika.

Mikä on tiedonkeruun ja/tai käsittelyn tarkoitus?	**Oikeusperuste** (urakointisopimus, vapaaehtoinen suostumus, asiakkuus)	**Mitä henkilötietoa käsitellään**
Puunkorjuupalvelun tuottaminen	Urakointisopimus	Nimi / muu identifiointitunnus, standardin (minkä?) mukaista metsäkonetietoa
Palkanmaksu	Työsopimus	Nimi, syntymäaika, osoite, puhelin, sähköposti, pankkiyhteys, verotiedot, palkkaperusteet ja palkkatiedot sekä työsopimustiedot
Laadun seuranta	Työsopimus/työsuhde	Nimi, ammattinimike, laatutekijätiedot
Tuottavuuden seuranta	Työsopimus/työsuhde/kannustava palkkaus	Nimi, ammattinimike, työsuoritetiedot; määrä, aika, kulutus, tuotto

Kuva 2. Esimerkkejä henkilötietojen keruun ja säilytyksen perusteista. (Tarkistuslistan Dokumentointi-välilehti)

2.3. Kuka henkilötietoja käsittelee?

Pääsy henkilötietoihin on rajattava vain niihin henkilöihin, jotka tarvitsevat tietoja työssään:

Mitä suuremmalla määrällä ihmisiä on pääsy henkilötietoihin, sitä suuremmaksi kasvaa riski, että tietoja joutuu vääriin käsiin, häviää tai muuttuu, tahallisesti kuin tahattomastikin. Henkilötietojen käsittelijöiden minimointi on tämän vuoksi suotavaa.

Yritys voi olla rekisterinpitäjä ja tai henkilötietojen käsittelijä:

Yritys on **rekisterinpitäjä** ainakin oman henkilöstönsä tietojen suhteen. Ulkoistettu palkanlaskenta taas toimii tässä tapauksessa henkilötiedon käsittelijänä. Rekisterinpitäjän täytyy huolehtia, että esimerkiksi aliurakoitsijoilla tai alihankkijoilla (henkilötietojen käsittelijät) on tietoturva rekisterinpitäjän ja asetuksen vaatimalla tasolla. Tietojen käsittelystä ja tietosuojan riittävästä toteuttamisesta sovitaan osapuolten välillä esimerkiksi toimeksiantosopimuksessa (lisää tästä kohdassa 2.5).

Yritys on **henkilötiedon käsittelijä**, kun se saa esimerkiksi urakanantajalta henkilötietoja jossakin muodossa, kuten osana työmaa- ja korjuuohjetietoja tai mittalaitteelle tiedonsiirrossa vietäviä tiedostoja. Ollakseen käsittelijä ei yrityksen tarvitse käsitellä henkilötietoja suoraan. Riittää, että ne ovat esimerkiksi osa hakkuussa tai kuljetuksessa tarvittavaa taikka syntyvää tietoa, vaikka urakoitsija käyttääkin tästä tiedosta vain esimerkiksi tuotantomääriä. Jos henkilötiedot pysyvät tässä tietovarastossa mukana, koko tietovarastoa täytyy käsitellä tietosuoja huomioiden.

Kuka vastaa (nimi, yhteystieto)	Kuka käsittelee
Työnjohto , N.N., etu.sukunimi@yritys.fi, 040-123456 tai vaihtoehtoisesti asema	Yrittäjä N.N , Työnjohto N.N.
Toimistonhoitaja , N.N., etu.sukunimi@yritys.fi, 040-123456	Palkanlaskija Aina Maksettu , Tilitoimisto Oy, etu.sukunimi@yritys.fi, 040-654321

Kuva 3. Esimerkkejä rekisterinpitäjistä ja henkilötiedon käsittelijöistä (Tarkistuslista)

2.4. Henkilötietojen käsittely ja varastointi

Yrityksen on selvitettävä ja dokumentoitava, miten henkilötietoa käsitellään ja varastoidaan. Henkilötietoja kerätään esimerkiksi suoraan henkilöiltä tai tietojärjestelmistä (manuaalisesti hakien tai automaattisesti). Tietoja voi olla erilaisissa tietojärjestelmissä tai omissa laadituissa tiedostoissa (myös paperisissa arkistoissa).

Miten käsitellään	Käsittelyä ulkoistettu (Kyllä/Ei)	Ulkoistuksesta kirjallinen sopimus (Kyllä/Ei)	Säilytys-aika
Kuljettaja rekisteröityy työt aloittaessaan järjestelmään. Kone kerää on line standardin mukaista tietoa, jota lähetetään yrityksen ohjausjärjestelmään (mihin?). Anonymisoituna tietoa lähetetään asiakkaalle.			Työsuhde-aika, minkä jälkeen anonymisointi
Palkanmaksu on yhden pääkäsittelijän ja hänen varahenkilön käsissä. Käytetään xxx-palkanlaskentaohjelmaa, joka toteutettu pilvipalveluna.	kyllä	kyllä	10 vuotta/ työsuhde + x vuotta
Puutavaran laadusta saadaan asiakkaalta raportit. Palaute annetaan työntekijälle. Tiedot tallennetaan tietojärjestelmään.	ei		

Kuva 4. Esimerkki henkilötietojen käsittelyn kuvauksesta. Tarkistuslistan Dokumentointi-välilehdellä on lisää esimerkkejä asiasta.

Kun yritys on henkilötietojen käsittelijä, pitää huolehtia siitä, että

- tietoa käsittelevät vain asiaankuuluvat, tietosuojan vaatimukset työtehtävässään ymmärtävät henkilöt ja alihankkijat
- työmenetelmien ja työkalujen tietoturva on riittävä
- osataan havainnoida tietoturvaloukkauksia ja ilmoittaa niistä rekisterinpitäjälle.

2.5. Henkilötietojen käsittelyn ulkoistaminen

Yritys voi ulkoistaa henkilötietojen käsittelyä, esimerkiksi palkanlaskennan. Siitä huolimatta yritystä (eli rekisterinpitäjää) koskee osoitusvelvollisuus siitä, että tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjä ei voi luovuttaa tätä osoitusvelvollisuuttaan tai vastuutaan kenellekään, ei edes sopimusteitse. Näin ollen yritys on viime kädessä vastuussa, että sen omat alihankkijat (esimerkiksi tilitoimisto tai aliurakoitsija) käsittelevät henkilötietoja oikein. Asiasta sovitaan esimerkiksi toimeksiantosopimuksissa. Henkilötietojen käsittelijän (esimerkkitapauksessa tilitoimiston) taas on annettava riittävät takeet siitä, että sen suorittama henkilötietojen käsittely täyttää asetuksen vaatimukset.

Ulkoistettuja toimintoja, joissa on henkilötietojen käsittelyä ovat mm. kirjanpito, palkanmaksu, työaikojen seuranta, toiminnan tehokkuuden ja laadun seuranta, ajopäiväkirja, hakkuu ja metsäkuljetus aliurakointina. Ulkoistetun palvelun voi tarjota mm. tilitoimisto, konevalmistaja, ohjelmistopalvelun tarjoaja tai toinen koneyritys.

Sopimus henkilötietojen käsittelystä

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee tehdä kirjallinen sopimus, että tietosuoja on huomioitu (Data Processing Agreement, DPA). Sopimus voidaan tehdä erillisenä liitteenä nykyisiin palvelusopimuksiin tai huomioitavat asiat voidaan sisällyttää uusiin sopimuksiin. Tietosuoja-asetus velvoittaa, että tietosuojan laatu on huomioitava jo palveluntarjoajaa valitessa.

Henkilötietojen käsittelyä koskeva sopimus tehdään esimerkiksi rekisterinpitäjän (esim. metsäyhtiö) ja tietojen käsittelijän (esim. koneyritys) välillä. Sopimus voi olla myös kahden henkilötietojen käsittelijän välinen (esim. pääurakoitsija–aliurakoitsija, koneyritys–IT-yhtiö) Henkilötietojen käsittelyä koskevassa sopimuksessa on syytä huomioida seuraavat asiat:

- tietojenkäsittelyn yksilöinti, eli mainitaan tietojen käsittelyn kohde, tarkoitus, luonne ja kesto, henkilötietojen tyyppi
- rekisterinpitäjän oikeudet ja velvollisuudet
- sitoutuminen rekisterinpitäjän ohjeisiin (tietoturva ym.)
- kummankin osapuolen salassapitovelvoitteet on yksilöitävä
- käsittelijän tulee sitoutua noudattamaan asianmukaisia toimenpiteitä henkilötietojen käsittelyn riskiä vastaavan turvallisuustason varmistamiseksi
- alihankinta on mahdollista vain rekisterinpitäjän luvalla, ja käsittelijällä on vastuu alihankkijastaan
- käsittelijän on sitouduttava avustamaan rekisterinpitäjää tämän vastatessa rekisteröityjen pyyntöihin esimerkiksi tilanteissa, joissa rekisteröidyt haluavat pääsyn omiin tietoihinsa

- käsittelijällä on vastuu auttaa rekisterinpitäjää varmistamaan tiettyjen rekisterinpitäjän velvoitteiden noudattaminen, esimerkiksi tietojen poistopyynnön noudattaminen
- rekisteriin liitettävälle: suostumus, jolla hyväksyy henkilötietojen käsittelyn
- henkilötietojen poistosta tai palautuksesta käsittelyyn liittyvien palveluiden päättyessä on syytä sopia (jollei muu lainsäädäntö edellytä tietojen säilyttämistä).

Asiasta on valmisteilla sopimusmalli, joka liitetään verkkoon www.puuhuolto.fi/tietosuoja.

2.6. Henkilötiedon käsittelyn riskiarvio

Tietosuoja-asetus määrää, että kaikki tiedot on suojattava ja tietojen suojaus on toteutettava suhteessa rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Tällä halutaan välttää ylisääntelyn vaara, mutta turvata asianmukainen suojaus. Mikäli riskit ovat pienet, tarvitaan vähäisempiä tietoturvatoimenpiteitä kuin vakaviin seurauksiin johtavien tietovuotojen estämisessä. Rekisterinpitäjän ja henkilötietojen käsittelijän on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja toimittava näiden riskien lieventämiseksi.

Henkilötiedon käsittelyyn liittyvät riskit kartoitetaan ja kuvataan. Henkilötietoihin liittyviä riskejä ovat esimerkiksi tietojen häviäminen, joutuminen vääriin käsiin ja tietojen muuntuminen. Ei ole merkityksellistä, tapahtuisiko esimerkiksi tietojen häviäminen tahallisesti tai tahattomasti. Jos riski toteutuu, tapahtuu **tietoturvaloukkaus** (asiasta lisää kohdassa 2.10).

Tunnistetuille riskeille arvioidaan niiden toteutumisen todennäköisyys ja vaikutus. Riskin todennäköisyys tarkoittaa sitä, miten todennäköisesti tiedot voivat levitä, hävitä tai muuntua. Riskin vaikutus tarkoittaa sitä, miten vakavia vahinkoja, menetyksiä tms. rekisteröidylle aiheutuu tietojen häviämisestä tai tietojen väärinkäytöstä. Puhutaan ”riskistä henkilön oikeuksille ja vapauksille”.

Esimerkki palkanlaskennassa olevan henkilötiedon riskinarvioinnista:

Riski: henkilön nimi, henkilötunnus ja pankkitieto joutuvat vääriin käsiin
Riskin toteutumisen seuraus: identiteettivarkaus -> suuri haitta
Riskin todennäköisyys: pieni (jos tietosuoja hoidettu hyvin)
Oleelliset toimenpiteet riskin pienentämiseksi: suppea käsittelijäjoukko, koulutus, tietojärjestelmien suojaus, dokumenttien suojaus

Riskin kuvaus	Todennä-köisyys (1…5)	* Vaikutus (1..5)	Kokonais-riski
Ulkopuolinen näkee yrityksen henkilöstön yhteystiedot	2	1	2
Identiteettivarkaus; nimi, hetu, pankkitieto joutuvat vääriin käsiin	2	5	10
Asiakkaan laatutiedot vääriin käsiin	1	0	0

Kuva 5. Riskin todennäköisyyttä ja vaikutusta voi arvioida esimerkiksi viisiportaisella asteikolla ja niiden kokonaisriskinä (todennäköisyys kertaa vaikutus). (Tarkistuslistan dokumentointi-välilehti)

2.7. Henkilötietojen suojaustoimenpiteet

Henkilötietojen suojaamiseksi on tärkeää miettiä henkilötietojen käsittelyn menettelyt sellaisiksi, että tietoturvaloukkausten todennäköisyys on minimoitu. Tällöin huomioitavia tietosuojaa ylläpitäviä toimintoja ovat esimerkiksi käsittelijäjoukon pitäminen mahdollisimman pienenä, henkilöstön koulutus ja heille annetut ohjeet ja määräykset, salassapitosopimukset, valvonta, omavalvonta, tietojärjestelmien tietoturva ja tietojen salaus, auditoinnit, tekniset rajoitukset, tarkastus- ja valvontajärjestelmät jne.

Tietosuojatoimenpiteet
Tietojenkäsittely perustuu pilvipalvelun käyttöön, jonne rajatut pääsyoikeudet
-Paperit lukitussa kaapissa -Palkanlaskentaohjelma palveluntarjoajan suojaamana, salasanan takana, käyttöoikeudet rajoitettu
Tietojen varastointi ja raportointi on ulkoistettu Esimerkki Oy:lle. Palvelun tuottaja vastaa asianmukaisesta tietosuojasta. Raportoinnin käyttöoikeudeton rajattu yrityksen johdolle.

Kuva 6. Esimerkkejä tietosuojatoimenpiteistä. Lisää käytännön esimerkkejä on Tarkistuslistassa.

2.8. Rekisteröidyn oikeudet

Rekisteröidyllä on tietosuoja-asetuksen mukaan oikeus tarkistaa rekisterissä olevat tiedot ja pyytää niiden oikaisua tai poistoa. Lisäksi jos rekisteröity niin haluaa, hänelle pitää pystyä toimittamaan jäljennös häntä koskevista henkilötiedoista kuukauden sisällä pyynnöstä. Tiedot on toimitettava sähköisesti, mikäli myös pyyntö on esitetty sähköisesti.

Kun tietoja kerätään, rekisteröidyllä tulee olla saatavilla tieto, miksi ja millä perusteella henkilötietoja käsitellään ja tiedon käsittelijät. Tiedon voi toimittaa paperilla, suullisesti tai sähköisesti.

Koneyrityksissä rekisterinpito koskee pääasiassa kuljettaja- ja henkilöstötietoa, joten oikeuksia ei todennäköisesti tulla käyttämään paljoa. Yritysten tulee kuitenkin olla tietoisia tästä oikeudesta.

2.9. Osoitusvelvollisuus ja dokumentointi

Asetus vaatii, että organisaatiolla on oltava kyky osoittaa noudattavansa tietosuoja-asetusta myös käytännössä. Tätä kutsutaan **osoitusvelvollisuudeksi.** Tämä tarkoittaa sitä, että yrityksen on käytävä läpi niitä koskevat velvollisuudet ja velvollisuuksien soveltaminen omaan toimintaan ja kaikki tarvittava on myös dokumentoitava.

Tämän oppaan liitteenä on Tarkistuslista (Excel-dokumentti), joka on tarkoitettu työkaluksi, jonka avulla yritys voi tehdä dokumentoinnin. Dokumentti toimii myös välineenä täytettäessä edellä mainittua osoitusvelvollisuutta.

Tarkistuslista on hyvä käydä säännöllisesti esim. vuosittain läpi, jotta huomataan mahdolliset puutteet ja pidetään asia muistissa. Tarkistuslista on syytä käydä läpi myös silloin, kun yrityksen toiminnassa muuttuu jotain olennaista.

2.10. Tietoturvaloukkauksiin valmistautuminen

Tietoturvaloukkaus on tilanne, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Rekisterinpitäjä on velvollinen ilmoittamaan tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle tietyin ehdoin.

- Rekisterinpitäjän on ilmoitettava 72 tunnin kuluessa loukkauksen ilmitulosta valvontaviranomaiselle. Ilmoituksen voi jättää tekemättä, jos loukkauksesta ei todennäköisesti aiheudu riskiä henkilön oikeuksille tai vapauksille.
- Rekisterinpitäjän on ilmoitettava asiasta ilman viivytystä rekisteröidylle, mikäli tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin henkilön oikeuksille tai vapauksille. Ilmoitusta ei tarvitse antaa, jos tiedot ovat sellaisessa muodossa, ettei ulkopuolinen pysty niitä ymmärtämään (esimerkiksi salattu).
- Jos epäilyttää, tarkista kuitenkin mieluummin asia (ja ilmoita eteenpäin) kuin jätät mitään tekemättä.
- Tarkista esimerkiksi tietosuojavaltuutetun verkkosivulta, mitä ilmoituksessa tulee olla.

Henkilötietojen käsittelijä on velvollinen ilmoittamaan tietoturvaloukkauksista aina ja ilman viivytystä rekisterinpitäjälle.

Rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset ja niihin liittyvät seikat ja korjatut toimet. Viranomainen voi tarkistaa näiden avulla, että rekisterinpitäjä on noudattanut velvollisuuksiaan.

Tärkeintä on tunnistaa, että tietoturvaloukkaus on tapahtunut ja toimia välittömästi.

Asetus velvoittaa valmistautumaan tietoturvaloukkauksiin, joten tee vähintään pienimuotoinen toimintasuunnitelma tietoturvaloukkausten varalle, jotta osaat toimia nopeasti ja suunnitelman mukaisesti. Kouluta myös henkilökunta tunnistamaan tietoturvaloukkaukset, ja miten niiden kohdalla toimitaan. Seuraavassa on mallidokumentissa asioita, jota voit hyödyntää. Suunnitelma on syytä olla nähtävillä ja käydä läpi henkilöstön kanssa.

Tärkeä asia huomiotavaksi	***Oma vastaus***
Miten tunnistetaan tietoturvaloukkaus?	Yrityksessä rekisteröitävät ja käsiteltävät henkilötiedot informoidaan henkilöstölle. Henkilöstölle opastetaan, mikä on tietoturvaloukkaus – tiedon häviäminen, muuttuminen, tuhoutuminen, luvaton antaminen toisen käyttöön. Seurataan, että henkilötietoja sisältävät dokumentit säilytetään tarkastuslistan mukaisesti. Jos tästä poiketaan, niin se on tietoturvaloukkaus
Kenelle ilmoitetaan tietoturvaloukkauksesta?	Työntekijä tietää kenelle ilmoittaa havaitsemastaan mahdollisesta tietoturvaloukkauksesta. Pääsääntönä on, että työntekijä ilmoittaa asiasta yrittäjälle (rekisterinpitäjälle) ja/tai yrittäjä (tietojen käsittelijänä) urakanantajalle (rekisterinpitäjä)
Miten selvitetään?	Kirjataan heti havainto ja haastatellaan tiedoista vastuussa olevia. Estetään tietoturvaloukkauksen jatkuminen ja uusien vastaavien syntyminen täsmentämällä ohjeistusta ja kouluttamalla henkilöstöä. Yritys hankkii itselleen asiantuntevan tahon, jonka kanssa tietoturvaloukkauksen aiheuttamista toimenpiteistä se saa konsulttiapua ja tarvittavia ohjeita. Jos asia koskee urakanantajaa, on informoitava taho ja yhteistyötaho.
Miten tietoturvaloukkaukset dokumentoidaan?	Loukkaukset dokumentoidaan kirjallisesti, jotta niiden perusteella voidaan tehdä korjaavat toimenpiteet.
Miten on huolehdittu, että henkilöstö osaa toimia tietoturvaloukkaustilanteissa?	Yritys on tehnyt ohjeet näiden tilanteiden varalle ja ne on koulutettu henkilöstölle.

Taulukko 1. Tietoturvaloukkauksiin valmistautumisen toimintasuunnitelma (esimerkkejä omassa suunnitelmassa hyödynnettäväksi). Oma suunnitelma on syytä tehdä yksityiskohtaisemmaksi oman yrityksen asiat huomioiden.

3. Metsäkonetiedon omistuksen ja käytön suositus

Metsäkonetiedon omistukselle ja käytölle on julkaistu yhteinen suositus syksyllä 2017. Suosituksen tarkoituksena on selkeyttää tiedon omistuksen, käytön ja käyttöoikeuksien luovutuksen pelisääntöjä sekä edistää metsäkonetietoon perustuvien sovellusten rakentamista ja palvelujen tuottamista alan toimijoita varten. Suositus on nähty tarpeelliseksi, kun tietoja välitetään puunkorjuun tai metsänhoitotöiden sopimusosapuolien välillä tai kun niitä luovutetaan ulkopuolisille toimijoille tai kun tietoa prosessoidaan, jatkojalostetaan taikka sitä yhdistetään toisiin tietoaineistoihin ja muodostetaan uusia tietotuotteita käytettäväksi muissa sovelluksissa ja palveluissa kuin alkuperäisessä tarkoituksessaan.

Metsäkoneiden ja niiden laitteiden tuottama data ja siitä muodostettavat tiedot ovat yleensä osa puunkorjuun ja metsänhoitotöiden palvelua, josta sopimusosapuolet keskinäisesti sopivat. Osa palvelun yhteydessä tuotettavasta tiedosta on luonteeltaan sensitiivistä joko urakanantajan tai koneyrittäjän liiketoimintaan liittyvää tietoa, joka on lähtökohtaisesti vain osapuolen itsensä käytössä olevaa, mutta johon toisella osapuolella voi kuitenkin olla rajattu käyttöoikeus niin erikseen sovittaessa.

Suositukseen voi tutustua verkossa: www.metsateho.fi/yhteinen-suositus-metsakonetiedon-omistukselle-ja-kaytolle.

4. Lisätietoja

Opasta ja siihen liittyviä dokumentteja täydennetään, mikäli uutta tarkentavaa tietoa tietosuojan hallintaan ja asetuksen soveltamiseen ilmenee. Uusin versio löytyy osoitteesta www.puuhuolto.fi/tietosuoja.

Ajankohtaista tietoa ja lisämateriaalia löytyy muun muassa tietosuojavaltuutetun verkkosivustolla www.tietosuoja.fi.

Liite: Esimerkki täytetystä Tarkistuslistan sivusta, jonka jokainen yritys voi täyttää ja täydentää omalla tavallaan.

TARKISTUSLISTA, ESIMERKKI

Rekisterinpitäjä	Koneyritys Oy	Konetie 2	12345 Konela	reino.rekisterinpitaja@koneyritys.fi

X **Periaate: Rekisteröityjen tietoja ei luovuteta kolmansiin maihin tai kansainvälisiin järjestöihin. (Kirjaa huomioihin jos poikkeuksia.)**

Henkilötietojen käsittelyn dokumentointi (vastaa sarakkeen otsakkeen kysymykseen sen alla oleviin soluihin/riveihin)

Riski henkilön oikeuksien ja vapauksien loukkaamiselle eli tietojen joutumisesta vääriin käsiin

Henkilöryhmä, jonka henkilötiedoista on kyse?	**Mikä on tiedonkeruun ja/tai käsittelyn tarkoitus?**	**Oikeusperuste** (urakointisopimus, vapaaehtoinen suostumus, asiakkuus)	**Mitä henkilötietoa käsitellään**	**Kuka vastaa (nimi, yhteystieto)**	**Kuka käsittelee**	**Miten käsitellään**	**Käsittelyä ulkoistettu (Kyllä/Ei)**	**Ulkoistuksesta kirjallinen sopimus (Kyllä / Ei)**	**Säilytysaika**	**Riskin kuvaus**	**Todennäköisyys (1…5)**	*** Vaikutus (1..5)**	**Kokonaisriski**	**Tietosuojatoimenpiteet**
Koneenkuljettajat	Puunkorjuupalvelun tuottaminen	Urakointisopimus	Nimi / muu identifiointitunnus, ?-standardin mukaista metsäkonetietoa	Työnjohto , N.N., etu.nimi@yritys.fi, 040-123456 tai vaihtoehtoisesti asema	Yrittäjä N.N , Työnjohto N.N.	Kuljettaja rekisteröityy työt aloittaessaan järjestelmään. Kone kerää on line -standardin mukaista tietoa, jota lähetetään yrityksen ohjausjärjestelmään (esim. mikä). Anonymisoituna tietoa lähetetään asiakkaalle.			Työsuhdeaika, jonka jälkeen anonymisointi		2	1	2	Tietojenkäsittely perustuu pilvipalvelun käyttöön, jonne rajatut pääsyoikeudet
Koneenkuljettajat	Palkanmaksu	Työsopimus	Nimi, syntymäaika, osoite, puhelin, sähköposti, pankkiyhteys, verotiedot, palkkaperusteet ja palkkatiedot sekä työsopimustiedot	Toimistonhoitaja , N.N., etu.nimi@yritys.fi, 040-123456	Palkanlaskija Aina Maksettu , Tilitoimisto Oy, etu.sukunimi@yritys.fi, 040-654321	Palkanmaksu on yhden pääkäsittelijän ja hänen varahenkilön käsissä. Käytetään xxx-palkanlaskentaohjelmaa, joka toteutettu pilvipalveluna.	kyllä	kyllä	10 vuotta/ työsuhde+ x vuotta	Identiteettivarkaus; nimi, hetu, pankkitieto joutuvat vääriin käsiin	2	5	10	-Paperit lukitussa kaapissa -Palkanlaskentaohjelma palveluntarjoajan suojaamana, salasanan takana, käyttöoikeudet rajoitettu
Koneenkuljettajat	Laadun seuranta	Työsopimus/työsuhde	Nimi, ammattinimike, laatutekijätiedot	Työnjoht. N.N. etu.nimi@yritys.fi, 040-112233	sama kuin edellä	Puutavaran laadusta saadaan asiakkaalta raportit. Palaute annetaan työntekijälle. Tiedot tallennetaan tietojärjestelmään.	ei			Asiakkaan laatutiedot vääriin käsiin	1	3	3	Laatupalaute tietojärjestelmissä. Kuljattajalle vain hänen työtään kosketa palaute.
Koneenkuljettajat	Tuottavuuden seuranta	Työsopimus/työsuhde/ kannustava palkkaus	Nimi, ammattinimike, työsuoritetiedot ; määrä, aika, kulutus, tuotto	Yrittäjä N.N. etu.nimi@yritys.fi, 040-111222	sama kuin edellä	Koneista kerätty tuottavuus ja aikatieto varastoidaan Koneyrittäjän Datapankkiin, josta tieto on raportoitavissa mm. kuljettajittain. Raporttien käsittely on rajattu käyttöoikeuksin.	kyllä	kyllä	Työsuhdeaika		1	2	2	Tietojen varastointi ja raportointi on ulkoistettu Esimerkki Oy:lle. Palvelun tuottaja vastaa asianmukaisesta tietosuojasta. Raportoinnin käyttöoikeudeton rajattu yrityksen johdolle.
Koneenkuljettajat	Osaamisen varmistaminen	Työsopimus / Asiakkaan vaatimusten täyttäminen	Nimi, ammatillinen koulutus, työkokemus, ammattiin liittyvät kurssit	Yrittäjä N.N. etu.sukunimi@yritys.fi, 040-111223	Työnjoht. N.N. etu.sukunimi@yritys.fi, 040-112233	Tiedot tallennetaan koulutus- ja osaamisrekisteriin. Tiedot päivittyvät suoritettujen kurssien mukaan.	ei		Työsuhdeaika		1	1	1	
Aliurakoitsija/ aliurakoitsijan työntekijä	Laadun seuranta		Nimi, ammattinimike, laatutekijätiedot											
Metsänomistaja kiinteistönomistajana	Puunkorjuupalvelun tuottaminen	Urakointisopimus asiakkaan kanssa, joka ostanut puuta metsänomistajalta	Metsänomistajan nimi / identifiointitunnus, kiinteistötunnus, työmaan paikkatieto											
Asiakkaan edustaja	Yhteydenpito asiakkaaseen sopimusasioissa	Urakointisopimus, palvelun tuottaminen sopimukseen perustuen	Yritysyhteyshenkilön nimi , työosoite, puhelin, sähköposti	Yrityksen johto N.N	Yrittäjä N.N. , Työnjohto N.N. , Koneen kuljettajat	Urakointiasiakkaiden yhteyshenkilöistä sopimusasioissa sovitaan sopimuksessa. Yhteystietoja käytetään yhteydenpitoon asiakkaaseen.	ei	ei	sopimus-aika		1	1	1	Sopimusasiakirjat säilytetään mapissa lukitussa kaapissa. Yhteystieto on yrittäjän puhelinnumeromuistiossa ja sähköpostiosoitemuistiossa puhelimessa.
	Yhteydenpito asiakkaaseen käytännön urakointiasioissa	Urakointisopimus, palvelun tuottaminen sopimukseen perustuen	Operatiivisen tason yhteyshenkilön nimi, työosoite, puhelin, sähköposti	Yrityksen johto N.N / työnjohto N.N.	Työnjohto N.N. , Koneen kuljettajat	Urakointiasiakkaiden yhteyshenkilöistä urakointi-asioissa sovitaan sopimuksessa. Sopimusasiakirjat säilytetään mapissa lukitussa kaapissa. Yhteystieto on yrittäjän, työnjohdon ja kuljettajien puhelinnumero-muistiossa puhelimessa.	ei	ei	sopimus-aika		1	1	1	Sopimusasiakirjat säilytetään mapissa lukitussa kaapissa. Yhteystieto on yrittäjän puhelinnumeromuistiossa ja sähköpostiosoitemuistiossa puhelimessa.

(Tietosuojan hallinta metsäurakoinnissa -opas. www.puuhuolto.fi/tietosuoja)