MAATALOUSYRITTÄJÄN LYHYT DATAOPAS

Luke
LUONNONVARAKESKUS

SeAMK

Euroopan maaseudun kehittämisen maatalousrahasto: Eurooppa investoi maaseutualueisiin

MAASEUTU 2020

Elinkeino-, liikenne- ja ympäristökeskus

Tämä opas on Lisäarvoa maatilayrityksille datasta ja sen hallinnasta -hankkeen (Dataosuuskunta-hankkeen) tuotos. Luonnonvarakeskuksen ja Seinäjoen ammattikorkeakoulun Dataosuuskunta-hanke toteutettiin vuosina 2022–2024. Hankkeen rahoitus koostui Manner-Suomen maaseudun valtakunnallisesta kehittämisohjelmasta 2014–2020. Euroopan unionin osuus rahoituksesta oli 120 120 €. Hankkeeseen osallistui kolme valtakunnallista tuottajaverkostoa, sekä joukko yksittäisiä tuottajia, joilla oli kiinnostusta kehittää dataosaamistaan ja verkostoitua muiden tuottajien kanssa. Hankkeessa valmisteltiin verkostoja tulevaan digivihreään siirtymään ja pyrittiin demonstroimaan sitä, että verkostoitumalla ja omaa dataa jakamalla yrittäjät saavat valmiudet toimia datataloudessa. Verkostoja aktivoitiin dataan perustuvan liiketoiminnan kehittämiseen, sekä yhteistyön ja tiedonvaihdon lisäämiseen. Verkostojen sisäisten yhteiskehittämistilaisuuksien lisäksi hankkeessa järjestettiin avoimia webinaareja.

Tekijät: Jussi Ylinen, Jori Lahti ja Matti Saari

ISBN: 978-952-7515-65-5

Kansikuva: Shutterstock

Seinäjoki 2024

SISÄLLYS

Johdanto 4

Mitä data on? 5

- Maatalousyrityksen datalähteet 6
- Kuka omistaa datan? 8

Datan käsittely 9

Datan hallinta 11

- Datan validointi eli varmistus 12
- Datan laatu varmistetaan metadatalla 12

Datakaupankäynti 14

- Datan arvo 15

Mitä on kyberturvallisuus? 16

- Miksi kyberturvallisuus on tärkeää maatilayrittäjälle? 16
- Käyttäjätunnukset ja salasanat 17
- Päivitykset 18
- Varmuuskopiointi 21
- Tietojen kalasteluyritykset 23
- Sähkön saanti ja kaapelirikot 24

EU:n data- ja digilainsäädäntö lyhyesti 25

Sanasto 26

JOHDANTO

Digitalisaatio on lisännyt maataloudessa syntyvän datan määrää 2010-luvulta alkaen. Maatalousyrittäjillä on käsissään suuri määrä dataa, mutta sitä ei juurikaan hyödynnetä. Datan avulla pystytään tekemään parempia päätöksiä liiketoiminnan johtamiseen, mutta sitä pystytään hyödyntämään myös jakamalla dataa muille toimijoille, esimerkiksi hiilijalanjäljen laskentaa varten. Euroopan unionin datalainsäädäntö tuo nyt myös datakaupankäynnin kaikkien ulottuville sisämarkkinoilla, mikä avaa aivan uudenlaisia mahdollisuuksia oman ja myös muualta saadun datan hyödyntämiselle. Datakaupankäynnin myötä myös maatalouden alalle tulee mahdollisuus ottaa data mukaan liiketoimintaan.

Tämä lyhyehkö opas pyrkii antamaan nykyisille ja tuleville maatalousyrittäjille peruskäsityksen siitä, miten dataa pystytään hyödyntämään omassa toiminnassa. Toivomme sen kannustavan pohtimaan omaa toimintaa myös dataliiketoiminnan näkökulmasta ja miten oman maatalousyrityksen toimintaa voidaan lähteä viemään datalähtöisempään suuntaan. Dataan perustuvaan toimintaan liittyy tiivisti myös kyberturvallisuus, johon oppaan toinen puolisko antaa perusvalmiudet. Oppaan lopussa on myös sanasto, josta toivottavasti löydätte apua lukuisiin dataan liittyviin termeihin.

MITÄ DATA ON?

Data on tekstiä, merkkejä ja symboleita, jotka ovat koneellisesti käsiteltävässä muodossa. Yleisesti tämä tarkoittaa, että data on digitaalisessa muodossa. Maatilayrityksissä syntyy dataa monista eri lähteistä. Dataa on myös sellainen materiaali, jota ei välttämättä mielletä dataksi. Tällaisia ovat esimerkiksi kännykkäkameran kuvat kasvustoista tai sähköiset tiliotteet. Myös paperille kirjatut muistiinpanot ja yrittäjän päässä tekemät laskelmat muuttuvat dataksi, kun ne kirjataan kunnolla talteen tietokoneelle. Kaikki, mistä kerätään jotain informaatiota, on muutettavissa dataksi ja siitä edelleen jalostettavissa tiedoksi.

Yleensä maatilayrityksissä syntyvä data on sidottuna johonkin paikkatietoon. Esimerkiksi maanäytteet ja satotiedot ovat peltolohkokohtaisia, ja kuivikkeen kulutus tuotantotilakohtainen. Satokartoituskartat voivat olla jopa neliömetritarkkuudella pellolle kohdistettavissa. Mitä tarkempaan paikkatietoon data pystytään sitomaan, sen parempi. Tarkempi paikkatieto mahdollistaa täsmäviljelyn lisäksi erilaisten laskenta- ja tekoälymallien rakentamisen ja hyötykäytön, esimerkiksi satoennusteiden ja tautilevintämallien muodostamiseen. Mitä pidemmältä ajalta dataa saadaan mallien käyttöön, sitä tarkempia niistä tulee. Aikasarjoista syntynyttä dataa ja niistä johdettua tietoa voidaan myös luotettavammin käyttää yrityksen päätöksenteossa.

Maatalousyrityksen datalähteet

Oman datapääoman tunteminen on ensiaskel dataan painottavaan toimintaan ja johtamiseen. Alla oleva listaus auttaa alkuun, mutta kaikkia mahdollisia datalähteitä ei tässä voida luetella. Jokainen yritys on erilaisensa, ja siten myös niissä syntyvä data on erilaista.

1. Työkoneet	▪ CAN-väylä ▪ ISOBUS	▪ RTK/GPS ▪ Täsmälevityskoneet ja -laitteistot	▪ Satokartoittimet ▪ Huolto- ja korjaustiedot
2. Pellolta	▪ Kasvustohavainnot ja -kuvaus ▪ Satelliittikuvaus ▪ Sääasema ▪ Sadon laatumittaukset ▪ Kasvustoanturit ▪ Viljelymuistiinpanot ▪ Viljavuusanalyysit ▪ Kasvustoanalyysit ▪ Maaperäskannaus ▪ Tautiennusteet	▪ Satoennusteet ▪ Salaojakartat ▪ Säätösalaojat ▪ Maan rakenne ▪ Peltomaan laatutesti ▪ Rikkakasvien torjunta ▪ Tautitorjunta ▪ Tuholaistorjunta	▪ Kasvinsuojeluaineiden käyttö ▪ Kasvuaste ▪ Kalkitus ▪ Lannan ja apulannan levitysmäärät ▪ Kylvösiemenen määrä ja -itävyys ▪ Viljelytoimenpidehistoria ▪ Aiemmat viljelykasvit
3. Tuotanto-eläimet	▪ Lypsyrobotti ▪ Syönti ja juonti ▪ Eläinten sijainti ▪ Terveystiedot	▪ Poikimisen seuranta ▪ Aktiivisuusmittaus ▪ Laidunseuranta ▪ Ruokinta-suunnitelmat	▪ Maidon ja lihan laatu ▪ Lanta-analyysit ▪ Tuotantotiladata (lämpö, kosteus, ilmanlaatu) ▪ Valvontakamerat
4. Muu data	▪ Kirjanpito ▪ Tukihaku ▪ Ostot ▪ Myynnit	▪ Ajoneuvovaaka ▪ Varastotiedot ▪ Energiankulutus ▪ Mobiiliverkon kuuluvuus ja laatu	▪ Valokuvat ▪ Videot ▪ Dokumentit ▪ Pilvipalvelut ▪ Eläinpalkkiojärjestelmät

TEHTÄVÄ 1: Mitä dataa omalla tilallasi syntyy?
Data tarkoittaa digitaalisessa muodossa olevaa tietoa

TEHTÄVÄ 2: Mitä ei-digitaalisessa muodossa olevaa informaatiota sinulla on, joka on muutettavissa dataksi? (esim. paperiset viljelymuistiinpanot ja ruokintasuunnitelmat)

Kuka omistaa datan?

Datan omistajuus tarkoittaa oikeutta hallita ja päättää kerätystä tiedosta. Se myös määrittelee vastuun, kuka on velvollinen suojaamaan tiedot ja huolehtimaan lainmukaisuudesta. Datan omistajuus on kiinni sopimuksista. On tärkeää selvittää, mitä ehtoja sopimuksissa on esimerkiksi viljelysuunnitteluohjelmiston käyttöön liittyen. Tämä voi määritellä, kuka tietoja saa käyttää, jakaa tai myydä, ja mihin tarkoitukseen. Datan omistajan vastuulla on myös datan ylläpito sekä laadun korjaaminen ja kehittäminen.

Maatalousyritykselle datan omistajuus on avainasemassa tietojen hallinnan ja arvon suhteen. Jos yrittäjä omistaa datan, hänellä on vapaat kädet hyödyntää, myydä ja jakaa sitä. Jos omistajuutta ei ole määritelty selkeästi, yrittäjä voi menettää oikeutensa datan käyttöön tai jopa pääsyn dataan. Yrittäjä voi jopa joutua maksamaan pääsystä dataan, minkä on ostamallaan laitteella itse kerännyt. Vaikka dataan ei olisikaan pääsyä, niin monesti laitteistot ja ohjelmistot antavat kuitenkin datan analysoinnista syntyneen lopputuloksen, esimerkiksi kasvustokuvauksesta syntyneen kartan, yrittäjän käyttöön.

Pääsääntönä voidaan ajatella, että maatilan tuotantoon liittyvän datan tulisi olla maatalousyrittäjän itsensä omistamaa. Muun, tuotantoon liittymättömän datan, omistajuus ja käyttöluvat sovitaan sopimuksissa. Jos esimerkiksi urakoitsija tulee lannoittamaan täsmälevittimellä lohkollesi, levityksen seurauksena syntyvän lannoituskartan datan omistajuus voi siirtyä urakointisopimuksen myötä viljelijälle. Traktorin polttoainekulutus ja kuljetut kilometrit taas ovat urakoitsijalle itselleen kuuluvaa dataa. Urakoitsijan käyttämien laitteiden ja koneiden tekniseen toimintaan liittyvä data taas kuuluu laite- ja konevalmistajille. Tähän esimerkkiin ei kannata takertua liiaksi. Datan omistajuus on aina sopimuksissa määriteltynä. Ne kannattaakin lukea tarkkaan, jotta tiedät, miten saat dataa käyttää ja kuka muu sitä voi hyödyntää. Eri toimijoiden sopimuksissa saattaa olla myös mainintoja datan tai sen pohjalta laskettavien analyysien luovuttamisesta kolmansille osapuolille.

Datakaupankäynnissä datan omistajuus on välttämätöntä selvittää. Näin ei synny tilanteita, joissa ostetaan tai myydään dataa, johon ei todellisuudessa olekaan oikeuksia. Selkeä omistajuussuhteen määrittely suojaa yrittäjän oikeuksia ja mahdollistaa neuvotteluaseman parantamisen.

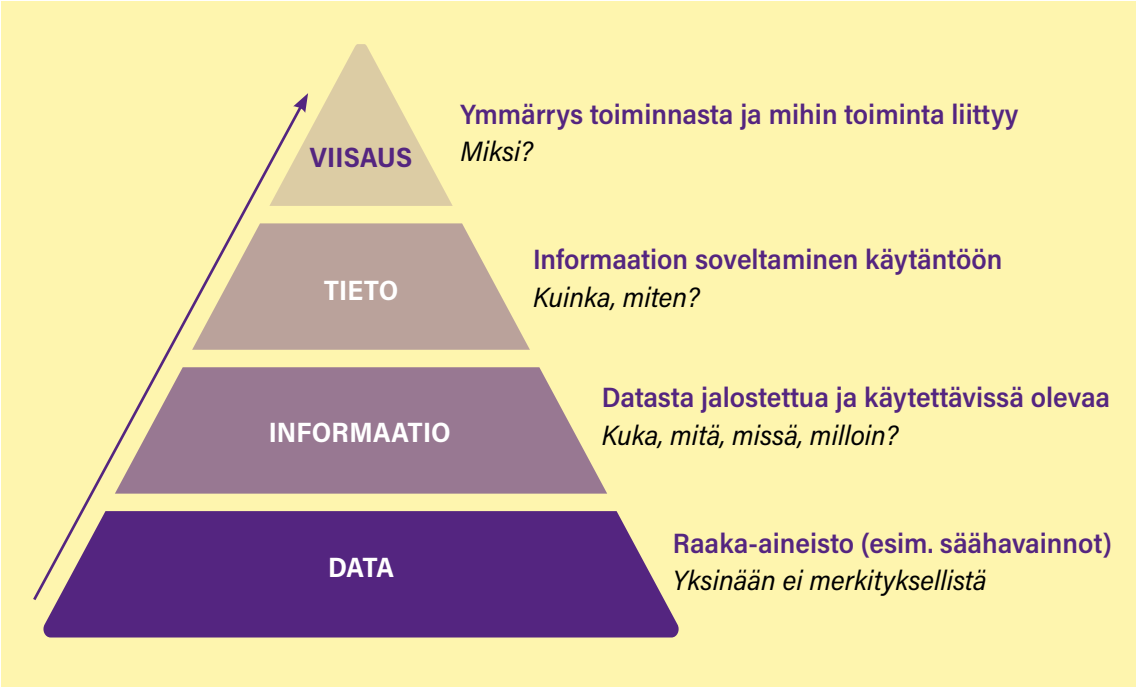
Datasäädöksen myötä yhdistettyjen laitteiden, kuten IoT-laitteiden, ja niihin liittyvien digitaalisten palveluiden tuottaman datan omistajuus siirtyy laitteiden ja palveluiden tuottajilta laitteiden ja palveluiden käyttäjille. Datasäädöstä aletaan soveltamaan 12.9.2025.*

TEHTÄVÄ 3: Tarkastele, onko omissa laite-, kone-, ohjelmistosopimuksissa yms. mainintoja datasta ja sen omistajuudesta tai käyttöluvista.

**https://fondia.com/fi/fi/ajankohtaista/artikkelit/datasaadoksen-data-act-paakohdat-kasittelyyn*

DATAN KÄSITTELY

Data ei yksinään ole välttämättä kovinkaan käyttökelpoista. Esimerkiksi sääaseman tallentama sademäärädata on yleensä melko arvotonta, jos sitä ei yhdistetä mittausaikaan. Syntyy tarve käsitellä dataa. Yksinkertaisimmillaan käsittely saattaa olla sääaseman taulukkotiedoston avaaminen ja tietyn ajankohdan selaaminen auki sekä datan tarkastelu sieltä. Tämä yksinkertainen käsittely koskettaa myös maatalouden työkoneita. Aina dataa ei tarvitse siirtää työkoneiden näytöiltä pois, vaan se saattaa jalostua tiedoksi jo työkoneen näytöllä ja on siitä suoraan luettavissa. Tällöin tiedon saanti nopeutuu huomattavasti, jos tarpeellinen tieto saadaan yhdellä katsauksella ulos. Monimutkaisimmillaan dataa käsitellessä sitä saattaa joutua siivoamaan, korjaamaan tai muuntamaan sopivaan muotoon. Tällainen monimutkainen datan käsittely vaatii yleensä käyttäjältään jonkin verran enemmän tietoteknisiä taitoja kuin pelkkä tarkastelu.



Kuva 1. Datan jalostaminen.
Mukailtu lähteestä: Nurmi ja Pyykönen. 2022. Viisauden hierarkia.

Data voi olla käytettävissä yleisimmillä tietokoneohjelmistoilla, tai siihen voi olla oma ohjelmistonsa. Jos dataa ei voi lukea muuta kuin siihen tarkoitetulla ohjelmistolla, se rajoittaa myös datan käsittelyä. Lukuun tarkoitetulla ohjelmistolla voi olla rajoitteita käsittelymahdollisuuksissa ja siitä voidaan veloittaa lisenssimaksuja. Avoimesti käsiteltävä tiedostomuoto mahdollistaa käsittelyn monipuolisemmin, mutta voi vaatia edellä mainittuja tietoteknisiä taitoja enemmän.

TEHTÄVÄ 4: **Tehtävässä 1 ja 2 selvitit eri datalähteitä. Kuinka paljon niitä täytyy käsitellä, että niistä saa käyttökelpoista tietoa? Tarvitseeko kaikkea dataa käsitellä itse?**

CSV-tiedoston avaaminen Excelillä

Csv-tiedosto (comma-separated values, eli pilkuilla erotetut arvot) on edelleen yksi käytetyimmistä dataformaateista. Nimestä huolimatta arvojen erotin voi olla myös esimerkiksi puolipiste. Sen avaaminen tekstitiedostona saattaa saada datan näyttämään pelkältä hölynpölyltä, mutta se on helposti muunnettavissa ymmärrettävämpään taulukkomuotoon.

Microsoft Excel:

1. Avaa uusi työkirja
2. Mene Tiedot-välilehdelle ja klikkaa Tekstistä/CSV:stä
3. Valitse csv-tiedosto
4. Aukeavassa esikatseluikkunassa varmista, että Erotin-kohdassa on oikea merkkityyppi valittuna
5. Paina Lataa. Tiedosto on nyt muunnettu taulukkomuotoon.

LibreOffice Calc

1. Valitse Tiedosto → Avaa
2. Valitse csv-tiedosto → Valitse Avaa
3. Aukeavassa Tekstin tuonti -ikkunassa varmista, että Erottimen asetukset -kohdassa on vain oikea merkkityyppi valittuna
4. Paina OK.

Google Sheets

1. Luo uusi laskentataulukko
2. Valitse Tiedosto → Tuo
3. Valitse Lähetä-välilehti → Selaa → Valitse csv-tiedosto
4. Aukeavassa ikkunassa varmista, että Erotintyyppi on oikein. Vaihtoehtoisesti voit jättää tähän kohtaan Tunnista automaattisesti
5. Paina Tuo data.

DATAN HALLINTA

Datan hallinta vaatii hieman suunnittelua ja huolellisuutta. Se kuitenkin helpottaa merkittävästi datan käyttöä, hallintaa ja tulevaa kaupankäyntiä. Ehdoton vähimmäisvaatimus on, että data kuvaillaan siten, että sen pystyy tunnistamaan myöhemmin. Tämä voi tarkoittaa esimerkiksi datan keräyspaikan, -ajan ja käytettyjen mittausvälineiden kirjaamista. Monet ohjelmistot, tietojärjestelmät ja laitteet kirjaavat automaattisesti nämä tiedot ylös, mutta se kannattaa aina tarkistaa.

Ajan myötä dataa kertyy säilytykseen yhä enemmän ja niistä pystytään muodostamaan pitkiäkin aikasarjoja, esimerkiksi kasvukausien mukaan. Teknologian ja ohjelmistojen kehityksen myötä tiedostomuodot ja ohjelmistot saattavat kuitenkin asettaa esteitä datan myöhemmälle käsittelylle. Kannattaa pohtia, saatko esimerkiksi nykyisellä viljelysuunnitelmaohjelmistollasi auki 5 tai 10 vuotta vanhoja viljelysuunnitelmiasi, tai vastaavasti 10 vuoden päästä auki nykyisiä suunnitelmia. Jos haluat vaihtaa ohjelmistoa, saatko uudella enää vanhan ohjelmiston tiedostoja auki? Dataa täytyy pystyä käsittelemään vuosienkin päästä, joten pitää varmistua siitä, että sitä säilytetään sellaisessa muodossa, johon pääsee käsiksi myös tulevilla ohjelmistoilla ja laitteilla.

Datan käsittely ja hallinta voi olla työlästä, jos sen toteuttaa täysin yksin. Kannattaa pohtia, voisitko maatalousyrittäjänä saada hyötyä tekemällä yhteistyötä muiden yrittäjien ja yhteistyökumppaneiden kanssa. Datan jakaminen muiden kanssa antaa myös vertailupohjaa tuotannon päätöksenteon tueksi. Yhdessä datasta voidaan myös saada liiketoimintaa. Tällainen yhteenliittymä voisi olla esimerkiksi dataosuuskunta, joka kerää, hallinnoi ja käy neuvotteluita ja kauppaa datalla jäsenten sille antamien oikeuksien puitteissa. Yhteisöllisestä datan hallinnasta ja dataosuuskunnasta löydät tietoa Dataosuuskunta-hankkeen oppaasta Kasvatamme datavoimaa yhdessä!

DATAN VALIDOINTI ELI VARMISTUS

Datan validoinnilla tarkoitetaan sitä, että data tarkistetaan ennen kuin sitä käytetään. Yksinkertaisimmillaan ruutuvihkomerkinnöissäkin voi olla jokin hullu lukema vaikkapa viljan kuivausajassa, mutta voi käydä ilmi että kyseessä on kirjoitusvirhe. Näitä tarkistuksia voidaan tehdä parista eri näkökulmasta, jotka liittyvät paljon datan käyttäjään. Maatalousyrityksessä kiinnostaa erityisesti datan laadun varmistus esimerkiksi edellä mainitun virheen kannalta. Teknisemmissä ratkaisuissa toki kyse voi olla esimerkiksi anturihäiriöstä. Toisena maatalousyritystäkin voi kiinnostaa se, että data on käyttökelpoisessa muodossa. Tästä on kirjoitettu enemmän kohdassa "Datan käsittely". Datakaupankäynnissä validointia tehdään datan oikeellisuuden ja käyttökelpoisuuden varmistamiseksi, mutta myös huijausten pois sulkemiseksi. Tätä saatetaan tehdä esimerkiksi seuraavassa kappaleessa kuvatun metadatan tarkastelun perusteella.

Datan laatu varmistetaan metadatalla

Metadata tarkoittaa dataa, joka kuvailee jotain muuta dataa. Se on siis eräänlaista taustatietoa varsinaiselle datalle. Esimerkiksi satokartoittimen tai sääaseman tuottaman satotaso- ja säädatan kyljessä oleva metadata voisi sisältää tietoa siitä, milloin ja missä data on kerätty, kuka ne on kerännyt, mitä ovat käytetyt mittayksiköt, millä laitteistolla, menetelmillä ja tarkkuudella data on hankittu. Metadata on hyvin tärkeää tietoa, kun dataa aletaan tulkitsemaan ja hyödyntämään, ja ilman sitä datan luotettavuutta ja alkuperää ei voida varmistaa. Jos joskus olet ladannut esimerkiksi Maanmittauslaitoksen Karttapaikka-palvelusta jotain karttadatapaketteja, niiden sisältö on kuvailtu aika hyvin ilman metadataakin. Sitten, jos sukellat syvemmälle netin syövereihin ja löydät jonkun "harrastelijan" tekemän datapaketin, siitä ei välttämättä ole mitään taustatietoa tekstinä olemassa. Tällaisissa tapauksissa yleensä metadatatiedoista löytyy, mitä dataa on kyseessä ja voitko sitä itse omassa toiminnassasi hyödyntää. Metadata voi olla liitettynä samaan tiedostoon varsinaisen datan kanssa tai se voi olla omana tiedostonaan, esimerkiksi teksti- tai taulukkolaskentatiedostona.

Ilman metadataa varsinainen data voi olla hyvin vaikeasti tulkittavaa. Jos esimerkiksi dataa kerätään useammasta eri anturista ja eri ajankohtina, metadatan avulla voidaan pitää kaikki kerätty data järjestyksessä ja ymmärrettävänä. Tämä on tärkeää, jos dataa aletaan jakamaan esimerkiksi muiden tilojen tai yhteistyökumppaneiden kanssa. Hyvälaatuinen metadata mahdollistaa tietojen vertailun keskenään, minkä myötä saadaan tarkempia tulkintoja toiminnan kehittämiseen ja tehostamiseen. Pitkällä aikavälillä, esimerkiksi kymmenen kasvukauden tietojen vertailussa ja yhdistelyssä, metadatan tärkeys korostuu, koska mittauskoneet, -laitteet ja mittaavat ihmisetkin, voivat vaihtua ja sitä myötä mittausten laatu myös muuttuu.

Kaupankäyntitilanteessa ostajat haluavat tietää, onko myymäsi tavara laadukasta. Näin on myös datan kohdalla, mutta sen myynnissä myös datan luotettavuus korostuu. Metadatasta ostaja näkee, mistä data on peräisin, milloin se on kerätty ja millä menetelmillä. Metadata

voidaan antaa ostajalle jo ennen kaupankäyntitilannetta arvioitavaksi, jolloin ostaja voi tarkistaa, onko data sopivaa omaan tarpeeseen ja asettaa mahdollisesti sille myös hinnan. Ilman metadataa data voi olla täysin arvotonta. Hyvin kirjattu data taas voi olla markkinoilla paljon arvokkaampaa, koska ostaja voi olla varma tiedon käyttökelpoisuudesta ja tarkkuudesta. Selkeästi kirjattu tieto auttaa myös välttämään väärinkäsityksiä osapuolten välillä.

Maatilayrityksen omaan sisäiseen käyttöön riittää, että metadatan kirjaamisessa on selkeä rutiini. Metadatan kerääminen ja tallennus tulee tehdä aina samalla lailla, vaikka Excel- tai tekstitiedostoon, jos laitteistot jne. eivät metadataa automaattisesti tallenna. Suurin osa ohjelmistoista, tietojärjestelmistä ja laitteista kirjaa metadatan onneksi valmiiksi standardoidussa muodossa. Standardisoidun muodon käyttäminen mahdollistaa nopean tietojen yhteensopivuuden varmistamisen ja datan tarkistamisen. Hyvin järjestetty tieto on myös digitaalisesti helpompi ottaa käyttöön päätöksenteossa, kuten paperimappienkin tapauksessa.

Mitä metadatassa pitää vähintään olla?

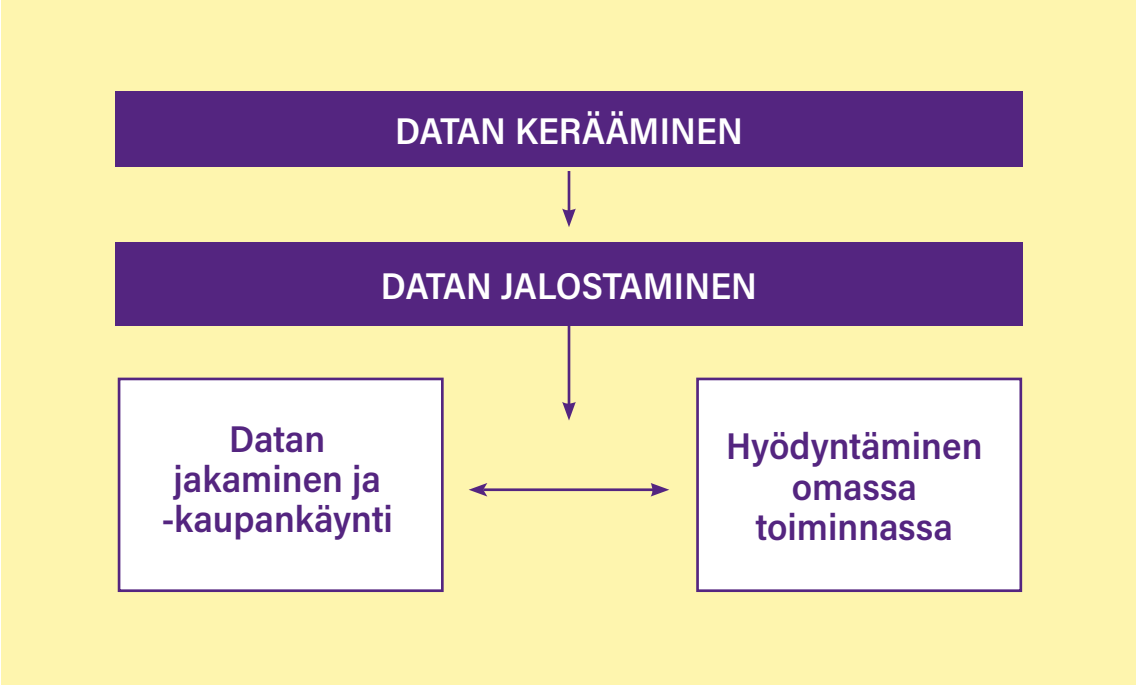
Eri metadatastandardeissa määritetään erilaisia kuvailutietoja. Esimerkiksi Dublin Core -standardissa määritetään metadatan kuvaamiseen ainakin seuraavat tiedot:

- Otsikko
- Tekijä
- Aihe
- Kuvaus datasta
- Päiväys
- Tyyppi (esim. teksti, kuva)
- Dataformaatti
- Lähde (esim. sääaseman sadehavaintodatassa laitettaisiin sääaseman sadetunnistimen merkki ja malli)
- Kieli
- Kattavuus (esim. ajallinen)
- Käyttöoikeudet

DATAKAUPANKÄYNTI

Datalla on fyysiseen tavaraan nähden etuna, että se ei kulu. Samaa dataa voidaan myydä yhä uudestaan ja uudestaan, ja erilaisina paketteina. Datakaupankäynnin kannalta olennaisia ovat data-avaruudet. Data-avaruus mahdollistaa lyhyesti sen, että dataa ei enää jaeta pilvipalvelualustojen kautta, vaan data liikkuu vapaasti toimijalta toiselle. Tämän mahdollistavat uudet teknologiat, kuten datanvälityspalvelut. Datakaupankäynnin voi ajatella tapahtuvan data-avaruudessa samalla lailla kuin fyysisenkin tavaran myynti, datalla on myyjä, ostaja ja välittäjä. Välittäjänä toimivat datanvälityspalvelut, jotka luvittavat datan ja hoitavat kaupankäyntiin liittyvät sopimusasiat. Kirjoitushetkellä Suomessa on yksi EU-tasolla hyväksytty datanvälityspalvelu, DataSpace Europe Oy:n Tritom.

Datakaupankäynnissä sopimukset ovat elintärkeässä osassa. Sopimuksissa tulee määritellä muun muassa, mitä dataa myydään/ostetaan ja miten datan omistajuus määräytyy kaupan jälkeen. Lisäksi määritellään datan jatkokäyttö, saako ostaja myydä/analysoida dataa eteenpäin tai käyttää useammassa eri käyttötarkoituksessa. Sopimuksessa määritellään myös myyntihinta. Data voidaan rahan lisäksi myydä myös esimerkiksi palvelutarjontaa vastaan.



Kuva 2. Datan hyödyntäminen.

Datan arvo

Käsittelemätön data ei sellaisenaan ole arvokasta. Jalostamalla ja tulkitsemalla siitä syntyy informaatiota ja edelleen tietoa, joka on hyödyllistä sekä maatilan toiminnan kehittämisen että datan myynnin kannalta. Tietysti käsittelemättömällekin datalle voi löytyä ostajia, esimerkiksi tutkimuslaitoksia, mutta ollaanko siitä valmiita maksamaan rahana tai palveluina?

Datakaupankäynti on vielä alkutekijöissään suuremmassa mittakaavassa. Ei voida olla varmoja siitä, minkälainen data saa minkälaisen arvon kaupankäynnissä. Datan arvon voidaan ajatella riippuvan ainakin laadusta ja määrästä. Mitä enemmän dataa on ja mitä pidemmälle se on jalostettu, analysoitu ja yhdistelty muuhun dataan, sitä arvokkaampaa se on. Laatua ei saa tehtyä jälkikäteen, se lähtee jo datan keräämisestä. Huonolaatuisesta käsittelemättömästä datasta ei saa analyysillä tehtyä hyvälaatuista tietoa, vaikka kuinka haluaisi. Myös metadatan, eli varsinaisen datan kuvaustietojen, laatu vaikuttaa arvoon. Jos data on kerätty anturilla, jonka päivitysväli on 5 sekuntia, niin sen arvo todennäköisesti on pienempi kuin datalla, joka on kerätty puolen sekunnin välein.

TEHTÄVÄ 5: Pohdi, onko itselläsi dataa, joka voisi olla hyödyllistä tai arvokasta joillekin muille toimijoille. Pitääkö dataa analysoida ja jalostaa tiedoksi, esimerkiksi luomalla dataan perustuva lohkokartta, jotta sillä olisi hyötyyn perustuva arvo?

MITÄ ON KYBERTURVALLISUUS?

Dataan ja kaikenlaiseen tiedonsiirtoon liittyy olennaisesti kyberturvallisuus. Vaikka edelleenkin maatalouden toimintaympäristössä työntekijöiden oma tekeminen, koneiden ja laitteiden kuluminen ym. fyysiseen toimintaan liittyvät tekijät ovat yleisempiä murheenaiheita, niin kyberturvallisuudesta on hyvä tietää perusteet. Näin pystytään suojaamaan omaa toimintaa ja myös varmistamaan, ettei omia laitteita käytetä muihin kohdistuvien hyökkäysten tekoon.

Kyberturvallisuus on laaja käsite, joka kattaa toimenpiteet, menetelmät ja teknologiat, joilla suojataan tietojärjestelmiä, dataa ja laitteita verkossa tapahtuvilta uhkilta ja hyökkäyksiltä. Se pyrkii estämään haitallisten toimijoiden pääsyn kriittisiin järjestelmiin ja tietoihin sekä varmistamaan, että tieto pysyy luottamuksellisena, ehyenä ja oikeiden käyttäjien saatavilla. Kyberturvallisuus ei rajoitu pelkästään tietoverkkoihin, vaan sillä pyritään turvaamaan myös yksittäisiä laitteita, kuten älypuhelimia, kannettavia tietokoneita ja muita laitteita, jotka ovat yhteydessä verkkoon.

Kyberturvallisuustoimet voivat olla teknisiä, kuten palomuurit ja virustorjuntaohjelmistot, mutta ne voivat sisältää myös hallinnollisia toimenpiteitä, kuten käyttäjäoikeuksien ja salasanojen hallinta sekä henkilöstön koulutus. Kaiken kaikkiaan kyberturvallisuus pyrkii takaamaan turvallisen toiminnan nykyaikaisessa digitaalisessa yhteiskunnassa.

Kyberturvallisuutta käsiteltäessä on tärkeää ymmärtää ero kyberturvallisuuden ja tietoturvallisuuden välillä. Tietoturvallisuus on laajempi käsite, joka sisältää paitsi digitaalisessa muodossa olevan tiedon suojauksen, myös fyysisessä muodossa olevan tiedon, kuten paperiasiakirjojen turvaamisen.

Miksi kyberturvallisuus on tärkeää maatilayrittäjälle?

Aiemmin yrityksen omaisuuden ja tiedon suojaaminen oli pitkälti fyysisten turvatoimien varassa. Riitti, että ovet lukittiin, arvotavarat säilytettiin kassakaapissa ja arkaluonteiset asiakirjat pidettiin paperiarkistoissa, joihin pääsivät vain valitut henkilöt. Yrityksen toiminnan turvaaminen oli helpompaa, koska tiedot sijaitsivat pääasiassa fyysisesti yrityksen tiloissa. Tämä antoi yrityksille luonnollista tietoturvaa, sillä ilman pääsyä tiloihin ei ollut mahdollista päästä käsiksi tietoihin.

Teknologian nopea kehitys on muuttanut merkittävästi yritysten toimintaympäristöä ja tuonut mukanaan uusia tietoturvahaasteita, jotka edellyttävät moderneja suojautumisratkaisuja. Nykyisin yritysten tietokoneet, ohjelmistot, koneet ja laitteet ovat jatkuvasti verkossa, ja yrityksen data kulkee usein pilvipalveluiden ja internetin välityksellä. Jatkuva verkkoyhteys tarjoaa monia etuja, mutta samalla se avaa ovia uusille uhille, joihin perinteiset suojakeinot eivät enää riitä vastaamaan.

Kyberhyökkäyksiä voivat toteuttaa rikolliset, kilpailijat tai jopa valtiolliset tahot, ja niiden taustalla voi olla monenlaisia motiiveja – taloudellisesta hyödyn tavoittelusta yrityksen maineen vahingoittamiseen, mutta myös pelkkään häirintään tai huomion herättämiseen. Viime vuosina

yksi vakavimmista uhista on ollut kiristyshaittaohjelmat, joiden avulla hyökkääjät pyrkivät lukitsemaan yrityksen tiedostot, estäen niiden käytön, ellei yritys maksa lunnaiksi vaadittua summaa. Tällainen hyökkäys voi pahimmillaan lamaannuttaa yrityksen toiminnan, mikäli kaikki tärkeät tiedot, kuten asiakastiedot ja tilausjärjestelmät, katoavat tai jäävät hyökkääjän hallintaan. Kiristyshaittaohjelmien lisäksi yrityksen varoja voidaan anastaa digitaalisesti esimerkiksi huijausviesteillä tai tietojenkalastelulla.

Yrityksen toiminnan ja tiedon suojaaminen vaatiikin tänä päivänä kattavaa kyberturvastrategiaa, joka huomioi tietojen tallennuksen, siirron ja käsittelyn turvallisuuden. Yritykselle sopivat kyberturvaratkaisut vaihtelevat sen mukaan, minkälaista tietoa yritys käsittelee, millaisia järjestelmiä käytetään ja minkälaisiin uhkiin erityisesti tulisi varautua. Kustannustehokkuuden kannalta kaikkein kallein tai turvallisin mahdollinen ratkaisu ei aina ole paras, sillä yrityksen täytyy myös pystyä toimimaan joustavasti ja tehokkaasti.

Kyberturvallisuuden kehitys on jatkuvaa, sillä uusia uhkia ja haavoittuvuuksia löytyy säännöllisesti. Tämä vaatii yrityksiltä jatkuvaa hereillä oloa ja ajan tasalla pysymistä. Henkilöstöä on koulutettava säännöllisesti, ja yrityksen suojausjärjestelmiä on päivitettävä uusimpien uhkien mukaisiksi.

Seuraavissa kappaleissa käydään läpi kyberturvallisuuteen liittyviä tärkeimpiä asioita, joihin maatilayrittäjän tulee kiinnittää huomiota.

Käyttäjätunnukset ja salasanat

Perinteisen käyttäjätunnuksen (esim. admin, hallinta tai etunimi.sukunimi) muuttamisesta on vain vähäistä hyötyä. Tärkeämpää on tilien suojaaminen vahvoilla salasanoilla ja monivaiheisella tunnistautumisella. Helposti arvattavat tai yleisesti käytetyt salasanat ovat suuri tietoturvariski, ja vakiosalasanat tulisi vaihtaa heti jokaisessa laitteessa.

Jos yrityksellä on useampi työntekijä, käyttäjätunnusten jako ja hallinta tulisi tehdä niin, että kaikille käyttäjille ei anneta automaattisesti kaikkia käyttöoikeuksia kaikkiin palveluihin, jos siihen ei ole selkeää tarvetta. Parhaimmillaan jaettuja tunnuksia (esimerkiksi ”admin” tai ”ylläpito”) ei käytetä ollenkaan, vaan jokaisella työntekijällä on oma, henkilökohtainen tunnus samaan järjestelmään.

Monivaiheinen tai kaksivaiheinen tunnistautuminen (eli MFA ja 2FA) tarjoaa lisäturvaa pyytämällä salasanan lisäksi toista tunnistautumiskeinoa, kuten tekstiviestitse lähetettyä koodia tai mobiilisovelluksen vahvistusta. Näin varmistetaan, että järjestelmään kirjautuva käyttäjä omistaa myös oikean puhelimen tai muun tunnistautumistyökalun, eikä pelkällä salasanalla pääse sisään.

Älä koskaan käytä samaa salasanaa useissa eri palveluissa. Salasana on turvallinen vain heikoimman käytetyn kohteen tasolla, joten jos jokin palveluista joutuu tietomurron kohteeksi, sama salasana voi vaarantaa myös muiden palvelujen tietoturvan. Tämä tekee salasanan kierrättämisestä erityisen riskialtista.

Monet laitteet, kuten reitittimet ja IoT-laitteet, tulevat tehtaalta valmiiksi asetetuilla vakiokäyttäjätunnuksilla ja -salasanoilla, jotka ovat yleisesti tiedossa ja helposti saatavilla internetissä. Tästä syystä on erityisen tärkeää vaihtaa näiden laitteiden vakiosalasanat heti

turvallisempiin salasanoihin, jotka eivät ole helposti arvattavissa. Jokaisen työntekijän on myös tärkeää käyttää omia henkilökohtaisia salasanojaan eri palveluissa sen sijaan, että jaettaisiin yksi yhteinen salasana. Henkilökohtaiset käyttäjätunnukset ja salasanat lisäävät turvallisuutta, koska ne rajoittavat pääsyä vain siihen, mihin kyseisellä käyttäjällä on oikeus.

Turvallisen salasanan tulisi olla mahdollisimman pitkä, sillä salasanan pituus parantaa sen suojaa. Hyvä salasana voi olla esimerkiksi salalause, jonka muistaa helposti, kuten "KeltainenPuimuriPellolla_2065". Tämäntyyppiset salasanat ovat yksilöllisiä ja helposti muistettavissa, mutta niiden arvaaminen on vaikeaa.

Koska eri käyttäjätunnusten ja salasanojen muistaminen jokaiselle palvelulle voi olla haastavaa, suositellaan käyttämään salasanojen hallintatyökalua. Tällaiset työkalut, kuten Bitwarden, NordPass ja KeePassXC, auttavat säilyttämään kaikki tunnukset ja salasanat turvallisesti yhdessä paikassa, jolloin käyttäjän tarvitsee muistaa vain yksi pääsalasana. Hallintatyökalu luo ja tallentaa tunnukset eri palveluihin, mikä varmistaa, että jokainen käyttäjätunnus ja salasana on yksilöllinen ja turvallinen.

- Vältä avaamasta kaikille täyttä pääsyä kaikkiin palveluihin, mikäli se ei ole tarpeen
- Jaettuja tunnuksia (kuten "admin" tai "ylläpito") ei tule käyttää, vaan jokaisella työntekijällä on oma tunnus samaan palveluun
- Tilien turvaaminen tulee tehdä turvallisilla salasanoilla ja monivaiheisella tunnistautumisella MFA tai 2FA
- Vaihda perusmuotoiset salasanat ja vakiosalasanat parempiin. Mitä pidempi, sen turvallisempi.
- Hyvä salasana voi olla pitkä erikoismerkkejä sisältävä salalause, joka on helppo itse muistaa, esimerkiksi: KeltainenPuimuriPellolla_2065
- Älä käytä samaa salasanaa monessa eri palvelussa
- Käytä salasanojen hallintatyökalua, esimerkiksi Bitwarden tai NordPass

Päivitykset

Suurin osa nykyajan tietokoneista ja älypuhelimista osaa päivittää ohjelmistonsa automaattisesti, kunhan niissä on asetuksista laitettu automaattiset päivitykset päälle. Tämä varmistaa sen, että laitteet saavat uusimmat turvallisuus- ja ohjelmistopäivitykset automaattisesti, eikä käyttäjän tarvitse huolehtia niistä. Myös monet pilvipalvelut päivittyvät taustalla palveluntarjoajan toimesta, ellei käyttöehdoissa ole toisin määritelty. Tällaiset automaattiset päivitykset ovat yksi kyberturvallisuuden peruspilareista, sillä ne suojaavat laitteita ja tietoja uusilta uhkilta.

Erityistä huomiota tulee kiinnittää laitteisiin ja sovelluksiin, joiden päivitykset eivät välttämättä ole automaattisesti päällä tai vaativat manuaalista ylläpitoa. Tällaisten järjestelmien ajantasainen päivitys on erittäin tärkeää, sillä niiden haavoittuvuudet voivat altistaa koko yrityksen tietoturvariskeille. Esimerkiksi reitittimen päivitykset eivät välttämättä asennu automaattisesti,

jolloin ulkopuolinen hyökkääjä voi käyttää reititintä päästäkseen sotkemaan reitittimeen kytkettyjen laitteiden toimintaa tai tekemään muita tuhoja.

Jos käytössä on suuri määrä laitteita, ohjelmistoja tai käyttäjiä, on järkevää ottaa käyttöön ohjelmistorekisteri. Rekisteri auttaa seuraamaan, mitkä laitteet ja ohjelmistot ovat käytössä, kuka niitä käyttää ja milloin viimeisimmät päivitykset on tehty. Yksinkertaisimmillaan ohjelmistorekisteri voi olla esimerkiksi Excel-taulukko tai Word-dokumentti.

Lisäksi on tärkeää huomioida, että laitteet, joille valmistaja ei enää tarjoa päivityksiä tai tukea, muuttuvat ajan myötä turvallisuusriskeiksi. Ilman säännöllisiä tietoturvapäivityksiä vanhentuneista laitteista tulee helppo kohde hyökkäyksille. Tällaiset laitteet tulee joko vaihtaa uusiin tai ainakin eristää muusta verkosta, jotta ne eivät pääse altistamaan muita laitteita tietoturvauhkille. Turvallisuusriskien lisäksi laitteiden ja koneiden toiminta voi myös rajoittua tai estyä kokonaan, kun ylläpitoa ei enää ole. Uusia hankintoja, esimerkiksi traktoreita ja automaatiojärjestelmiä, suunniteltaessa kannattaa selvittää, millaista ylläpitoa ja päivityksiä laitteiden ja koneiden valmistajat lupaavat. Toimivatko uusien traktoreiden tietojärjestelmät enää 10 vuoden päästä, vaikka itse traktorilla pystyykin vielä ajamaan? Muun muassa automaatiojärjestelmien ohjaustietokoneet todennäköisesti vaativat uusimista järjestelmien elinkaaren aikana.

On myös suositeltavaa poistaa tietokoneilta kaikki tarpeettomat ohjelmistot, erityisesti silloin, jos kyseisiä laitteita käytetään arkaluontoisen tai kriittisen tiedon käsittelyyn. Vähemmän ohjelmistoja tarkoittaa vähemmän mahdollisia haavoittuvuuksia, mikä lisää tietoturvaa.

- Varmista, että automaattipäivitykset ovat käytössä
- Aikatauluta laitteistojen ja ohjelmistojen päivitysten seuranta ja asennus
- Älä käytä ohjelmia tai laitteita, joita ei tueta ja joille ei enää tehdä päivityksiä
- Poista työkoneilta tarpeettomat ohjelmistot – mitä enemmän ohjelmia on koneella, sitä enemmän on myös tietomurtomahdollisuuksia

Windows 10 -käyttöjärjestelmän ylläpito loppuu 14.10.2025. Tämän jälkeen kyseiselle käyttöjärjestelmälle ei enää saa päivityksiä ja siitä tulee haavoittuva. Monet sovellukset, joilla ohjataan esim. tuotantotilojen automatiikkaa, eivät välttämättä toimi kunnolla tai ollenkaan Windows 11- tai Linux-pohjaisessa käyttöjärjestelmässä. Ennen tietokoneen päivittämistä tai uuden koneen hankkimista, kannattaa selvittää toimivatko sovellukset uudessa järjestelmässä tai saako niitä ylipäätään asennettua. Sovelluksilla voi olla myös rinnakkaisia asennusversioita, jotka toimivat muilla käyttöjärjestelmillä. Jos käyttämäsi sovelluksien päivityksistä on jo useampi vuosi, voi niistä olla julkaistuna uudempi versio, joka saattaa toimia uudella käyttöjärjestelmällä. Se voi kuitenkin poiketa ulkoasultaan tai käyttöominaisuuksiltaan vanhasta versiosta, joten sen opetteluun kannattaa varata aikaa.

TEHTÄVÄ 6: **Tee itsellesi yksinkertainen ohjelmistorekisteri esimerkiksi Word- tai Excel-tiedostoon. Mitä kriittisiä laitteita ja ohjelmistoja omistat, jotka vaativat säännöllistä ylläpitoa ja päivityksiä.**

Varmuuskopiointi

Varmuuskopioiden palautusprosessi opitaan usein vasta kantapään kautta, kun tärkeää tietoa on jo mennyt peruuttamattomasti hukkaan. Pelkkä varmuuskopion tekeminen ei kuitenkaan riitä, vaan sen toimivuus on testattava, jotta voidaan olla varmoja, että tiedot saadaan palautettua tarvittaessa. Tietojen palauttamista on syytä testata säännöllisesti. Esimerkiksi uuden tietokoneen käyttöönoton yhteydessä voi harjoitella palautusprosessia tuomalla vanhan koneen varmuuskopio uuteen koneeseen. Näin saadaan selville, kuinka hyvin varmuuskopiot toimivat ja kuinka nopeasti tiedot saadaan käyttöön uudella laitteella. Toinen hyvä tapa on yrittää palauttaa satunnainen tiedosto, esimerkiksi viime viikolta, varmuuskopioista ja tarkistaa että se on käyttökelpoinen ja ajantasainen.

Varmuuskopioiden toimivuuden tarkistaminen on tärkeää erityisesti silloin, kun tietoja on mahdollista ylikirjoittaa vahingossa. Jos esimerkiksi vahingossa korvataan tärkeä dokumentti samannimisellä muulla tiedostolla tai se poistetaan kokonaan, palautuvatko alkuperäiset tiedot varmuuskopioista? On myös hyödyllistä arvioida, kuinka nopeasti ja sujuvasti uusi tietokone saataisiin käyttökuntoon tietojen hävitessä, jos varmuuskopiot ovat ainoa tietolähde. Tällaisessa tilanteessa on olennaista, että kaikki tarvittava tieto saadaan nopeasti palautettua ja kone on käyttökunnossa.

Tietojen tallentaminen pilvipalveluihin, kuten esimerkiksi Onedriveen, helpottaa huomattavasti tiedostojen palauttamista mahdollisen laitteen rikkoutuessa tai kadotessa. Pilvipohjaiset synkronointipalvelut toimivat niin, että ne tallentavat tiedostot yhtä aikaa sekä käyttäjän laitteelle että pilveen. Näin ollen tietokoneen vaihdon yhteydessä tai esimerkiksi kovalevyn hajoamisen jälkeen käyttäjä voi asentaa pilvipalvelun ohjelmiston uuteen laitteeseen, kirjautua sisään ja saada kaikki tiedostonsa takaisin ilman suurempia järjestelyitä.

Vaikka pilvipalvelu tarjoaa pääsääntöisesti helpon tavan säilyttää tiedostoja, sitä ei kuitenkaan kannata ajatella pelkästään varmuuskopiona. Jos tiedot säilytetään vain pilvipalvelussa ilman paikallisia laitteiden muistissa olevia kopioita, ne ovat edelleen alttiita häiriöille ja datan menetyksille. Esimerkiksi, jos pilvipalvelu synkronoi automaattisesti paikallisia ja pilvessä olevia tiedostoja keskenään, niin toisessa paikassa korruptoitunut tiedosto korruptoituu myös toisessa. Jos pilvipalvelussa ei pääse tällaisessa tilanteessa käsiksi tiedostojen vanhempiin versioihin, niin tiedostot saattavat olla kokonaan menetetty. Tiedot tulisikin säilyttää vähintään kahdessa paikassa, jotta varmuuskopiointikäytäntö on riittävän luotettava.

Liiketoiminnan kannalta tärkeiden tietojen tallennuksessa kannattaa soveltaa 3–2–1-Varmuuskopion ottaminen: varmuuskopiointisääntöä. Säännön mukaan samasta tiedosta tulee olla kolme kopiota, kaksi erillistä tallennusmuotoa, kuten kovalevy ja pilvipalvelu, ja yksi kopio fyysisesti eri paikassa kuin muut. Yksi kopio voidaan säilyttää esimerkiksi pilvipalvelussa, toinen tietokoneen kovalevyllä ja kolmas ulkoisella kovalevyllä, joka on fyysisesti eri tilassa kuin muut varmuuskopiot. Tämä varmistaa sen, että vaikka yksi tallennusväline hajoaisi tai tuhoutuisi, tarvittavat tiedot ovat silti tallessa muualla.

Windows 10
Tiedostojen varmuuskopiointi ja palauttaminen tallennusasemalta

Varmuuskopion ottaminen:

- Varmista, että sinulla on verkkosijainti tai ulkoinen asema yhdistettynä tietokoneeseen
- Avaa Käynnistä-valikko (Windows-kuvake vasemmassa alanurkassa)
- Avaa Asetukset (Rattaan kuvake)
- Avaa "Päivittäminen ja suojaus" → "Tiedostojen varmuuskopiointi"
- Varmuuskopioi tiedostohistorian avulla -kohdan alta "Lisää asema"
- Valitse asema, jota haluat käyttää varmuuskopioinnissa ja paina OK
- Tiedostohistoria varmuuskopioi automaattisesti Tiedostot, Kuvat, Videot ja Työpöytä-kirjastot. Voit lisätä näihin kuulumattoman kansion tai tiedoston varmuuskopiointiin kopioimalla sen johonkin näistä, tai klikkaamalla hiiren oikealla painikkeella → Sisällytä kirjastoon → Valitse sopiva kirjasto.

Tiedostojen palauttaminen varmuuskopiosta:

1. Varmista, että sinulla on verkkosijainti tai ulkoinen asema yhdistettynä tietokoneeseen, joka sisältää tiedostojen varmuuskopiot
2. Avaa Resurssienhallinta (keltainen kansion kuvake alapalkissa tai kirjoita Haku-kenttään Resurssienhallinta)
3. Siirry kansioon, jossa tiedosto(t) olivat tai jonka haluat palauttaa aiempaan tilaan
4. Klikkaa hiiren oikealla painikkeella kansion nimeä ja valitse "Palauta aiemmat versiot".
5. Edelliset versiot -välilehdellä on lueteltuna käytettävissä olevat aiemmat versiot. Voit tässä näkymässä esikatsella sisältöä valitsemalla "Avaa" → "Avaa tiedostohistoriassa"
6. Kun löydät sopivan palautettavan version, valitse "Palauta". Voit myös palauttaa tiedoston toiseen sijaintiin, jolloin nykyinen versio säilyy omassa sijainnissaan. Huom. Jos korvaat nykyisen version vanhemmalla versiolla, ei korvaamista voi kumota!

Säilytä tieto vähintään kahdessa paikassa, esim. pilvipalvelu ja kovalevy

- Liiketoimintakriittisen tiedon tallennus: 3–2–1-sääntö
- Joissakin tapauksissa (esim. suuri datamäärä) kannattaa varmuuskopioida vain ne tiedostot tai tiedostojen muutokset, jotka ovat tapahtuneet edellisen varmuuskopion jälkeen
- Yleisesti suositellaan säilyttämään vähintään 3–7 eri aikaan otettuja varmuuskopioversiota à antaa riittävän puskurin mahdollisia virheitä, korruptoituneita tiedostoja yms. vastaan
- Testaa tietojen palautus varmuuskopioista
- Testaa myös tietojen ylikirjoittamisesta palautuminen (saako varmuuskopiosta oikeat tiedot palautettua, jos tärkeän tiedoston päälle kopioi samalla nimellä väärän tiedoston)

Tietojen kalasteluyritykset

Tietojen kalasteluyritykset ovat edelleen yleisin kyberrikollisuuden muoto ja niiden määrä kasvaa koko ajan. Kalastelun yleisin muoto on sähköpostiviestit. Sähköpostilinkkien kanssa tulisi toimia varoen. Linkit saattavat ohjata käyttäjän esimerkiksi väärennetylle sivustolle, jossa pyydetään käyttäjätunnuksia. Väärennettyjä sisäänkirjautumissivuja ei välttämättä pysty ulkonäön perusteella erottamaan oikeasta. Osoitekentän vasemmalla puolella on yleensä lukon kuva, joka tarkoittaa sitä, että yhteys avatulle sivulle on salattu. Se ei kuitenkaan tarkoita, että sivun sisältö olisi mitenkään luotettava. Lisäksi hakukoneiden ensimmäiset hakutulokset saattavat sisältää maksettuja mainoksia, joihin ei voi luottaa.

Etenkin verkkopankki kannattaa aina avata kirjoittamalla osoite itse selaimen osoiteriville. Itse käytetyt palvelut voidaan kerätä esimerkiksi selaimen kirjanmerkkeihin, jolloin niihin kirjautuminen on nopeaa ja turvallista. Pankkitunnusten lisäksi erilaiset sosiaalisen median tunnukset ja sähköpostitilit kannattaa suojata hyvin. Identiteettivarkaus voi johtaa maineen menetykseen, ja kaapattua sähköpostia voidaan käyttää asiakkaiden tai yhteistyökumppanien huijaamiseen.

Tietojen kalastelua tapahtuu myös puhelimen välityksellä. Tekstiviestihuijaukset ovat tekstiviestejä, joiden lähettäjätieto on yleensä väärennetty esimerkiksi samaksi kuin pankki tai posti. Viesti sisältää linkin, jota klikkaamalla henkilö päätyy huijaussivustolle ja jossa hän voi antaa väärennetylle sivustolle käyttäjätietonsa. Puheluissa huijarit voivat esiintyvät esimerkiksi viranomaisina tai jonkin yrityksen edustajina, ja näin yrittävät saada tietoonsa salasanoja tai verkkopankkitunnuksia. Koska puhelimessa kalastelu voi tapahtua nopeasti ja salakavalasti, on tärkeää tiedostaa riskit ja oppia tunnistamaan huijausyritykset. Yksinkertainen varotoimi, kuten soittajan henkilöllisyyden tarkistaminen ennen tietojen antamista, voi olla ratkaiseva askel turvallisuuden varmistamisessa. Henkilökohtaisia tietoja tai salasanoja ei pidä antaa koskaan toiselle osapuolelle, ellei ole täysin varmaa siitä, kenen kanssa puhuu. Viranomaiset eivät kysy käyttäjätunnuksia ja salasanoja puhelimitse.

- Avaa verkkopankki kirjoittamalla osoite itse selaimen osoiteriville / tallenna sivu kirjanmerkkeihin
- Suojaa sähköpostitilit ja sosiaalisen median tilit hyvin
- Älä avaa epäilyttäviä sähköposti- tai tekstiviestilinkkejä/tiedostoja
- Älä anna puhelimisessa/sähköpostilla käyttäjätunnuksia tai salasanoja

Sähkön saanti ja kaapelirikot

Sähkön saannin turvaaminen on keskeistä kyberturvallisuudessa, sillä tietoverkkojen, tietojärjestelmien ja erilaisten laitteiden toiminta perustuu sähkön jatkuvaan saatavuuteen. Sähkökatkosten vaikutukset voivat ulottua laajalti yrityksen kriittisten toimintojen lamaantumiseen, mikä heikentää kykyä suojautua kyberuhilta, estää hyökkäyksiä ja reagoida niihin tehokkaasti. Sähkökatkot ja ukkonen voivat myös rikkoa laitteita.

Sähkökatkon sattuessa perinteinen aggregaatti on edelleen hyvä vaihtoehto maatiloilla. Sen tuottama sähkön laatu voi olla kuitenkin epätasaista, ja voi rikkoa herkimpiä laitteita. Varsinkin automaatiolaitteissa syötetyn varavoiman tulisi olla laadultaan samaa kuin verkkovirta. Nykyaikaisempi ja isompaan kokoluokkaan sopiva menetelmä on käyttää automatisoituja varavoimajärjestelmiä. Ne huolehtivat siitä, että varavoima kytkeytyy päälle automaattisesti myös silloin, kun kukaan ei ole paikalla. Ne varmistavat sähkönsaannin laitteille, joiden toiminta on turvatta pidemmänkin sähkökatkon aikana, kuten navetan ilmanvaihto, lypsyrobotti ja varastoautomatiikka.

Yhden tai muutaman laitteen ratkaisu lyhyeen sähkökatkoon tai syöttöjännitteen tasaamiseen on keskeytymätön virransyöttö (UPS, Uninterruptible Power Supply). Yleensä se on noin pöytätietokoneen keskusyksikön kokoinen järjestelmä tai laite, jonka tehtävä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa. UPS liitetään virtalähteen ja virtaa käyttävän laitteen (esimerkiksi tietokoneen) väliin.

Sähkön, ja tietoliikenteenkin, osalta tässä kyberturvallisuusosiossa mainittuja asioita tyypillisempiä uhkia ovat kaapelirikot. Kaivuutyöt maatilan ympäristössä, eläimet ja sääkin aiheuttavat sähkö- ja tietoliikennekatkoksia paljon enemmän kuin ulkoiset uhat. Sähkö- ja tietoliikennekaapelit kannattaa suojata jo asennusvaiheessa, tai jälkikäteen jos mahdollista, suojaputkilla, jotta hiirien, lehmien ja muiden tekijöiden aiheuttaman tuhon riskejä saadaan pienennettyä. Maan alle kaapeleita kaivaessa tulee laittaa varoitusnauha kaivantoon reilusti kaapelien yläpuolelle. Ohjearvona on 30 cm maan pinnan alapuolella. Näin myöhemmin kaivettaessa varoitusnauha tulee vastaan ennen kuin kaapeli ehditään kaivaa poikki.

- Käytä automaattista varavoimajärjestelmää / UPS-laitetta ja testaa, että se toimii
- Suojaa kaapelit asennuksen yhteydessä tai jälkikäteen, jos mahdollista

EU:N DATA- JA DIGILAINSÄÄDÄNTÖ LYHYESTI*

Datanhallinta-asetus (DGA)

Säätelee julkisen ja yksityisen sektorin välistä datan jakamista ja hyödyntämistä, tarkoituksena helpottaa datan liikkuvuutta ja hyötykäyttöä.

Digipalveluasetus (DSA)

Edistää verkkopalveluiden luotettavuutta ja turvallisuutta luomalla velvoitteet ja vastuut sähköiselle kaupankäynnille ja välityspalveluille.

Digimarkkinasäädös (DMA)

Luo yhtenäisen sääntelyn verkkoalustojen kaupan käytänteisiin asettamalla suurille toimijoille uusia velvoitteita kilpailun edistämiseksi.

Datasäädös (DA)

Tavoittelee helpompaa datan saatavuutta ja hyödyntämistä. Helpottaa datan käyttöoikeuksien haltijan pääsyä dataansa ja datan jakamista. Säädöksellä tavoitellaan myös datankäsittelypalvelujen helpompaa vaihtamista.
Säädös on jo voimassa, mutta sitä aletaan soveltamaan 12.9.2025.

Tekoälyasetus (AIA)

Luo riskiperusteisen lainsäädäntökehikon tekoälylle ja sen hyödyntämiselle
Säädös on jo voimassa, mutta sitä aletaan soveltamaan portaittain 2.8.2025.

**https://www.traficom.fi/fi/viestinta/datatalous-ja-digipalvelut/eun-digi-ja-datasaantely-pahkinankuoressa*

SANASTO

2FA (Two-Factor Authentication)	Kaksivaiheinen tunnistautuminen on tietoturvamenetelmä, jossa käyttäjän henkilöllisyys varmennetaan kahden eri tekijän avulla.
Anonymisointi	Tunnistetietojen poistaminen tai muuntaminen siten, että henkilöiden tunnistaminen ei enää onnistu eikä henkilöitä voi identifioida. Tunnistetietoja ovat esimerkiksi nimet, osoitteet, puhelinnumerot tai henkilötunnukset.
Avoin data	Data, jota kuka tahansa voi vapaasti käyttää ja jaella.
Data	Koneellisesti käsiteltävässä muodossa olevaa tietoa. Yleiskielessä sanojen data, informaatio (engl. information) ja tieto (engl. knowledge) käytössä ei ole useinkaan selvää eroa. Tieto-sanalla voidaan viitata myös dataan ja informaatioon.
Data-avaruus	Yhteisesti sovittujen periaatteiden ja pelisääntöjen muodostama kokonaisuus, joka on tarkoitettu datan jakamiseen ja vaihtoon tietyllä toimialalla tai toimialojen välillä.
Dataekosysteemi	Useista dataverkostoista koostuva verkosto, jossa toimijat tekevät yhteistyötä tavoitteenaan jakaa ja käyttää dataa verkoston sisällä sekä edistää innovointia ja uutta liiketoimintaa.
Dataformaatti	Tiedostomuoto, johon dataa tallennetaan. Ilmaisee tietokoneelle tallennetun tiedoston tallennusmuodon eli rakenteen. Esimerkkejä: CSV, XML.
Datalähtöinen liiketoimintamalli	Liiketoimintamalli, joka on erityisesti suunniteltu tuottamaan liiketoiminnalle lisäarvoa datan keräämisen, jalostamisen ja hyödyntämisen avulla.
Datan jakaminen	Datan siirtämistä kahden tai useamman tahon kesken suoraan tai datanvälityspalvelun kautta
Datan jakaminen	Kahden tai useamman osapuolen välinen tiedonsiirto.
Datan siirrettävyys	Mahdollisuus käyttää samaa dataa eri tietokonejärjestelmissä.
Datan uudelleenkäyttö	Datan käyttö muuhun tarkoitukseen kuin mihin se on alun perin kerätty tai tuotettu.

Datan välityspalvelu	Datanhallinta-asetuksen mukainen datan välityspalvelu. Datan välityspalvelua tarjoavan yrityksen roolia palveluntarjoajana voi verrata puhelinoperaattoriin. Datan välityspalvelu reitittää dataviestit lähettäjältä vastaanottajille.
Datanhallinta-asetus	Datanhallinta-asetus on Euroopan parlamentin ja neuvoston asetus eurooppalaisen datan hallinnoinnista (Data Governance Act, DGA). Asetuksella luodaan datan hallinnalle eurooppalaiseen arvopohjaan pohjautuva kehys, joka lisää datan saatavuutta ja yhtenäistää sen jakamista EU:n alueella.
Dataosuuskunta	Yhteenliittymä, jonka toiminnan tavoitteena on helpottaa yksilöiden datan hallintaa.
Datastrategia	Strategia tarkoittaa suunnitelmaa, eli sen avulla pyritään saavuttamaan tavoiteltu päämäärä. Hyvin laadittu strategia vastaa kysymykseen "miten". Siinä kuvataan riittävällä tasolla, mitä tehdään, jotta saavutetaan yhteistesti sovitut tavoitteet ja visiot. Euroopan datastrategian tavoitteena on viedä EU datavetoisen yhteiskunnan eturiviin.
Datasäädös	Datasäädös on Euroopan parlamentin ja neuvoston asetus datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä. Datasäädöksen tavoitteena on edistää dataan pääsyä ja käyttöä sisämarkkinoilla. Se säätää käyttäjän ja kuluttajan oikeudesta koneiden ja laitteiden tuottamaan ja niiden välillä liikkuvaan (ns. teolliseen) dataan. Lisäksi julkisen sektorin viranomaisille tulisi poikkeuksellisissa tarpeissa käyttöoikeus yrityksen dataan. Säädöksellä kiellettäisiin datan hyödyntämistä ja jakamista koskevat kohtuuttomat sopimusehdot ja velvoitetaan pilvipalveluita yhteentoimivuuteen.
Datatalouden ekosysteemi	Datatalouden ekosysteemit muodostavat verkoston, joka koostuu dataa liiketoiminnan lähteenä käyttävistä ekosysteemin jäsenistä. Eri sidosryhmät ovat verkoston ja sen arvoketjujen kautta toisiinsa suorassa tai epäsuorassa yhteydessä. Datatalouden ekosysteemiin kuuluvat myös (viralliset tai epäviralliset) säännöt, jotka määrittävät verkostossa sallitun toiminnan.
Datatalous	Talouden osa-alue, jossa datan kerääminen ja hyödyntäminen on keskeinen osa toimintaa.
Datayhteisö	Yhteenliittymä, jonka toiminnan tavoitteena on helpottaa yksilöiden datan hallintaa.
Digitalisaatio	Digitaalisen tietotekniikan yleistymistä arjen toiminnoissa.

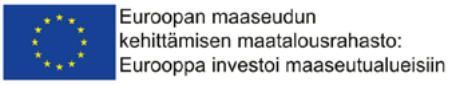
Euroopan datastrategia	Visio ja toimenpiteet (strategia), joilla edistetään kokonaisvaltaista lähestymistapaa Euroopan datavetoiseen talouteen ja joilla pyritään lisäämään datan ja datapohjaisten tuotteiden ja palvelujen käyttöä ja kysyntää kaikkialla EU:n sisämarkkinoilla.
Eurooppalainen datan sisämarkkina	Aito datan sisämarkkina, joka ovat avoin kaikkialta maailmasta tulevalle datalle, ja jossa henkilöön liittyvä data ja muu data, myös arkaluonteinen yritysdata, ovat turvassa. Yrityksillä on myös helppo pääsy korkealaatuiseen teollisuusdataan, mikä edistää kasvua ja luo arvoa.
GDPR (General Data Protection Regulation)	Euroopan unionin tietosuoja-asetus, joka säätelee henkilötietojen keräämistä, käsittelyä ja säilyttämistä, ja jonka tavoitteena on suojata yksilöiden yksityisyyttä ja oikeuksia digitaalisessa ympäristössä.
Henkilökohtainen data	Mikä tahansa data, joka viittaa tunnistettavaan tai jo tunnistettuun henkilöön
IoT-laite (Internet of Things)	Fyysinen laite, joka on liitetty internetiin ja voi kerätä, lähettää tai vastaanottaa dataa ilman suoraa ihmisen väliintuloa.
Kyberhyökkäys	Tarkoituksellinen digitaalinen hyökkäys, jossa pyritään vahingoittamaan, varastamaan tietoa tai häiritsemään tietojärjestelmiä ja verkkopalveluja.
Kyberuhka	Mahdollinen vaaratilanne, jossa digitaalisiin järjestelmiin, tietoihin tai verkkoihin kohdistuu riski vahingoittamisesta, luvattomasta käytöstä, tiedon varastamisesta tai häirinnästä.
Käyttölupa	Käyttöluvassa määritellään käyttöehdot, joilla avattua dataa saa käyttää. Käyttöluvasta käytetään myös sanaa lisenssi.
Liiketoimintaekosysteemi	Verkosto, jossa erityyppiset yksityiset ja julkiset toimijat tekevät yhteistyötä ja luovat toisiaan täydentäviä tuotteita ja palveluja tai kehittävät uudenlaista osaamista ja tuotantoresursseja. Tällaisia löytyy esimerkiksi biokaasun ympäriltä.
Lisenssi	Ks. käyttölupa
Luvitus	Suostumuksen antaminen esimerkiksi datan jakamiseen tai hyödyntämiseen.

Metadata eli metatieto	Tietoa tiedosta, datan kuvailutiedot. Metadatassa kerrotaan datan sisältöä ja rakennetta kuvaavat olennaiset tiedot, joiden pohjalta dataa pystyy hyödyntämään oikein. Metadata mahdollistaa myös aineiston löytämisen datakatalogista erilaisin hakukriteerein.
MFA (Multi-Factor Authentication)	Monivaiheinen tunnistautuminen on tietoturvamenetelmä, joka vaatii käyttäjää vahvistamaan henkilöllisyytensä useamman kuin yhden todentamistekijän avulla.
Omadata	Omadata on henkilötietojen hallinnan ja käsittelyn periaate, jonka mukaan ihmisillä on oltava mahdollisuus hallita, hyödyntää ja luovuttaa eteenpäin heistä kerättäviä henkilötietoja (esim. terveystiedot, energiatiedot tai ostotiedot). Omadata ei ole koskaan avointa dataa.
Pakotettu luottamus	Pakotettu luottamus kuvaa tilannetta, jossa henkilön on pakko käyttää ekosysteemiä, tietojärjestelmää tai ICT-tuotetta/-palvelua ja luottaa siihen. Luottamus on pakotettua, kun käyttäjällä – asiakkaalla, organisaatiolla tai jopa julkishallinnon viranomaisella – ei ole valinnanvapautta, vaan hänen on käytettävä tiettyä tietojärjestelmää.
Palomuuri	Tietoturvalaite tai ohjelmisto, joka valvoo ja hallitsee tietoliikennettä suojaten verkkoa luvattomilta pääsy- ja hyökkäysyrityksiltä.
Pilvipalvelu	Internetin kautta tarjottava palvelu, joka mahdollistaa tiedon tallentamisen, käsittelyn ja jakamisen etäpalvelimilla ilman, että käyttäjän tarvitsee hallita omaa laitteistoa. Esimerkiksi Google Drive ja Microsoft OneDrive.
Reilu datatalous	Se talouden osa-alue, joka keskittyy luomaan palveluja ja dataan perustuvia tuotteita eettisesti. Reiluus tarkoittaa sitä, että yksilöiden oikeuksia suojellaan ja kaikkien sidosryhmien tarpeet otetaan huomioon datataloudessa.
Reititin	Laite, joka ohjaa verkkoliikennettä eri verkkojen välillä ja yhdistää laitteet toisiinsa sekä internetiin, mahdollistamalla tiedonsiirron eri verkkojen välillä.
Salasanojen hallintaohjelma	Sovellus, joka tallentaa, hallitsee ja suojaa käyttäjien salasanat ja kirjautumistiedot, helpottaen niiden hallintaa ja parantaen turvallisuutta.
Suostumukseen perustuva tiedon jakaminen	Tietoja jaetaan vain silloin, kun henkilöt, joita tiedot koskevat, ovat antaneet siihen suostumuksensa.
Tiedostomuoto	Ks. dataformaatti

Tietojenkalastelu (Phishing)	Huijausmenetelmä, jossa hyökkääjä yrittää huijata ihmisiä luovuttamaan arkaluonteisia tietoja, kuten käyttäjätunnuksia, salasanoja tai maksukorttitietoja.
UPS-laite (Uninterruptible Power Supply)	Laite, joka tarjoaa varavirtalähteen ja suojaa laitteita sähkökatkoksilta, jännitehäiriöiltä tai virtapiikeiltä, mahdollistaen laitteen turvallisen sammutuksen tai jatkamisen.
Virustorjuntaohjelma	Tietoturvasovellus, joka tunnistaa, estää ja poistaa haittaohjelmia, kuten tietokoneviruksia, suojaten järjestelmää uhilta.
Yhteiset eurooppalaiset data-avaruudet	Euroopan sisämarkkinoilla perustetut aluekohtaiset/alakohtaiset data-avaruudet, joiden soveltamisala on EU:n laajuinen. Näissä noudatetaan eurooppalaisia sääntöjä ja arvoja.
Älymaatalous	Älymaatalous hyödyntää digitaalisia järjestelmiä ja työkaluja maatilan johtamiseksi ja sen toiminnan perustamiseksi dataan ja tietoon.


Luke
LUONNONVARAKESKUS


SeAMK


Euroopan maaseudun
kehittämisen maatalousrahasto:
Eurooppa investoi maaseutualueisiin