



Vaasan yliopisto
UNIVERSITY OF VAASA

Jemina Yliluoma

Henkilötietojen käsittely ja tietosuoja yrityskaupoissa

Oikeudelliset velvoitteet henkilötietojen siirrossa ja luovutuksessa

Laskentatoimen ja rahoituksen akateeminen yksikkö
Talousoikeuden pro gradu -tutkielma
Talousoikeuden maisteriohjelma

Vaasa 2026

Sisällys

Kuviot	4
1 Johdanto	6
1.1 Tutkimuksen kohde	8
1.2 Tutkimusongelma ja tutkimuksen rajaus	11
1.3 Tutkimusmenetelmä- ja aineisto	12
1.4 Tutkimuksen rakenne	14
2 Sääntelykehikko	15
2.1 Yleistä henkilötiedoista ja yrityskaupasta	21
2.2 Osapuolet	25
2.2.1 Rekisteröity	25
2.2.2 Rekisterinpitäjä ja henkilötietojen käsittelijä	27
2.3 Oletusarvoinen ja sisäänrakennettu tietosuoja	30
3 Suunnittelu- ja valmisteluvaihe	35
3.1 Käsittelyn suunnittelu ja tietojen määrittely	39
3.2 Perusteet henkilötietojen käsittelylle	43
3.3 Tietojen anonymisointi ja salassapitosopimus	50
4 Kaupan toteutusvaihe	54
4.1 Tietojen siirto ja luovutus	57
4.2 Kansainväliset tiedonsiirrot	60
5 Integraatiovaihe ja jälkitoimet	65
5.1 Tietosuoja kaupan jälkeen	68
5.2 Vastuiden jakautuminen	70
6 Johtopäätökset	76
Lähteet	82

Kuviot

Kuvio 1. Tietoturvan ulottuvuudet.	19
Kuvio 2. Yrityskaupan kolmiportainen vaiheistus.	23
Kuvio 3. Rekisteröidyn oikeuksien ja vapauksien riskialueet.	32
Kuvio 4. Henkilötietojen käsittelyn oikeusperusteet.	40
Kuvio 5. Henkilötietojen käsittelyperusteet.	45

Lyhenteet

BCR	Sitovat säännöt
GDPR	Yleinen tietosuoja-asetus (General Data Protection Regulation)
DPIA	Vaikutustenarviointi
ETA	Euroopan talousalue
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
HE	Hallituksen esitys
NDA	Salassapitosopimus
PeVL	Perustuslakivaliokunta
SEUT	Sopimus Euroopan unionin toiminnasta

Säädösluettelo

Euroopan unionin perusoikeuskirja (2000/C 364/01)

Suomen perustuslaki (731/1999)

Tietosuojalaki (1050/2018)

Työelämän tietosuojalaki

Laki yksityisyyden suojasta työelämässä (759/2004)

Yleinen tietosuoja-asetus

Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus, GDPR)

1 Johdanto

Mikään yritys, yhteiskunta, yhteisö tai ihminen ei koskaan ole staattisessa tilassa tai valmis, vaan aina edistymässä tai edistämässä, uudistumassa tai uudistamassa sekä myös sopeutumassa tai sopeuttamassa toimintaansa. Tietoon, kuten henkilötietoihin ja niiden käsittelyyn, on aina liittynyt ja tulee aina liittymään valtaa, joten vastuuta ei saa unohtaa. Erilaisten tietojen varassa tehdään päätöksiä, joiden niissä vastuussa sekä niiden kohteena olevista haluavat perustuvan totuudenmukaiseen tietoon, luulon sijasta. Henkilötiedoilla on elinkaari, joka alkaa niiden keräämisestä ja päättyy, kun tietoja ei enää ole. Tämän elinkaaren aikana lainsäätäjän vaatimuksilla sekä henkilötietojen käsittelyn suunnittelijoiden ideoilla, toteutustavoilla sekä ajatuksilla on merkitystä pohdittaessa, mitä tiedoille tapahtuu¹.

Tiedon määrän ollessa valtaisa, on organisaatioiden pystyttävä jatkuvasti huolehtimaan tietosuojavaatimusten noudattamisesta, sillä yrityksen tehdessä mitä tahansa, liittyy toimintaan yleensä aina henkilötietojen käsittelyä. Vuonna 2016 voimaan tullut Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus, GDPR) on tuonut organisaatioille uusia velvoitteita samalla mahdollistaen virtaviivaisemman toiminnan koko Euroopan unionin alueella. Yrityksen on pystyttävä osoittamaan, että se noudattaa tietosuoja-asetuksen mukaisia vaatimuksia. Yrityksellä on siten tietosuoja-asetuksen myötä oltava kattava käsitys siitä, mitä henkilötietoja, mitä tarkoitusta varten sekä missä niitä käsitellään. Huomioiden nykyaikana käsiteltävien tietojen valtaisa määrä, voidaan todeta, että ei ihan helppo tehtävä².

¹ Raatikainen, 2002, s. 9, 11.

² Keller, 2023, s. 216.

Asetuksen myötä henkilötietojen suoja nykyaikaisessa yhteiskunnassa on ollut ylenpalttisen huomion kohteena sekä korostunut yhä tärkeämmässä roolissa osana oikeusjärjestelmää. Viime vuosien tietomurrot sekä niistä aiheutuneet vahingot organisaatioille ja yrityksille ovat olleet merkittäviä. Erilaiset skandaalit, kuten Psykoterapiakeskus Vastaamo, ja suurten yritysten tekemät virheet henkilötietojen käsittelyssä, ovatkin saaneet ihmiset erityisen kiinnostuneiksi tietoihinsa liittyvistä oikeuksista sekä yritykset ottamaan henkilötietojen käsittelyyn liittyvät riskit vakavammin³.

Henkilötietojen liittyessä vahvasti henkilöiden identiteettiin, muodostavat ne osan perusoikeutena suojattua yksityisyyden suojaa. Osallistuminen digitalisoituvaan yhteiskuntaan edellyttää usein henkilötietojen käsittelyn sallimista, ilman mahdollisuutta vaikuttaa digitaalisissa palveluissa tapahtuvaan henkilötietojen käsittelyyn ja niiden keräämiseen. Henkilötietojen suoja rakentuu oikeusjärjestelmän osasta, jonka tehtävänä on varmistaa informationaalisen yksityisyyden ja henkilöön liitettävissä olevan tiedon suojan⁴.

Tulevaisuudessa työpaikoilla ja eri organisaatioissa tapahtuva henkilötietojen käsittely laajenee ja tehostuu. Globalisaatio sekä teknologian nopea kehitys tuottavat enemmän henkilötietoja kuin aikaisemmin, tarjoten uusia mahdollisuuksia henkilötietojen käsittelyyn. Yleisen tietosuoja-asetuksen mukaan teknologian myötä yritykset voivat toiminnassaan hyödyntää erilaisia henkilötietoja ennennäkemättömän laajasti. Globalisaatio ja teknologian kehittyminen ovat muuttaneet henkilötietojen käyttämiseen ja niiden keräämiseen liittyviä menettelytapoja⁵. Digitalisaation myötä yrityksillä on mahdollisuus yhä kattavampaan datan keräämiseen, minkä ohella uudet teknologiat mahdollistavat laaja-alaisen tietojen käsittelemisen, hyödyntämisen sekä muokkaamisen⁶.

³ Aalto-Setälä & Viitaila, 2018, s. 4; Korpisaari ja muut, 2022, s. 19–20; Voutilainen, 2012, s. 27, 30.

⁴ Lehtioksa ja muut, 2019, s. 865.

⁵ Korpisaari ja muut, 2022, s. 1.

⁶ Koskinen ja muut, 2012, s. 402–403; Lehtioksa ja muut, 2019, s. 865.

1.1 Tutkimuksen kohde

Viimeisten vuosikymmenten aikana yrityskaupan due diligence-prosessista on tullut enemmän tai vähemmän välttämätön edellytys yrityksen hankkimisessa⁷. Tutkimus pyrkii osoittamaan, miten henkilötietojen suoja toteutuu ja miten se turvataan yrityskauppaprosessissa, erityisesti yrityskaupan due diligence- vaiheessa, sekä millaisia erilaisia oikeudellisia ja liiketoiminnallisia haasteita tähän liittyy. Tutkimuksen tavoitteena on tuoda esiin myös vahvasti osana yrityskauppoja olevia salassapitokysymyksiä, eli toisin sanoen liikesalaisuuksiksi määriteltyjen tietojen luovuttamisen rajoja.

Tavoitteena on tutkia, miten Euroopan unionin yleinen tietosuojalaki (GDPR), tietosuojalaki sekä yksityisyyden suojasta työelämässä annetut lait, Euroopan perusoikeuskirja, kansalliset sopimukset sekä tietosuojavaikuttetun ja tietosuojatyöryhmän ohjeet vaikuttavat henkilötietojen käsittelyyn ja millaisia rajoja ne asettavat yrityskauppojen osalta. Tutkimuksessa tutkitaan lainsäädännön asettamia oikeusperusteita sekä velvollisuuksia henkilötietojen käsittelylle, yrityskauppaprosessille ominaisten vaiheiden kautta. Tutkimuksessa tarkastellaan henkilötietojen käsittelyn ytimen eli luottamuksellisuuden, eheyden sekä lainmukaisuuden säilymistä yrityskauppaprosessin eri vaiheissa.

Yrityskaupat ovat osapuolten välillä yleensä luonteeltaan hyvin luottamuksellisia, sillä kaupan mukana siirtyy myös yksityisiä tietoja. Osapuolet solmivat tästä syystä usein tiukkoja salassapitosopimuksia ja salassapitoehtoja⁸. Henkilötietojen käsittelyn merkityksen on katsottu kasvaneen yhteiskunnan ja talouden siirtyessä yhä suuremmilta osin digitaaliseen ympäristöön. Pyrkimykset ilmiön sääntelyyn ovat tuoneet muutoksia, joista merkittävimpänä voidaan pitää keväällä 2018 sovellettavaksi tullutta Euroopan unionin yleistä tietosuojalakiä. Tietojen käsittelyyn liittyvät taloudelliset vastuut ja kasvavat

⁷ Gustafsson, 2001, s. 125.

⁸ Vapaavuori, 2019, s. 635–637.

riskit ovat nostaneet vastuiden kohdentumisen relevantiksi kysymykseksi. Tällaiset vastuun kohdentamista koskevat kysymykset ovat nousseet esiin erityisesti yritysjärjestelyissä⁹.

Aiemmat tutkimukset

Andersson on tutkinut (2024) väitöskirjassaan *organisaation hyvä tietoturvan sääntelyjärjestelmä* organisaatioiden työkaluja sekä keinoja tietoturvatason vahvistamiseen sekä omien riskienhallintakeinojensa tehostamiseen tietoturvallisuuden sääntelyjärjestelmän kautta. Andersson on väitöskirjassaan todennut tietosuojalainsäädännön omaavan kaikkia organisaatioita koskevia ja henkilötietojen suojaa parantavia tietoturva vaatimuksia sekä tunnistettavissa olevia tietoturvaan linkittyviä perusoikeuksia¹⁰.

Tietosuoja on oleellinen osa hyvää tietoturvatapaa. Henkilötietojen suojaan liittyy olennaisesti Anderssonin väitöskirjassaan esiin tuodut tietosuoja-asetuksen 5 artiklan yleiset periaatteet eli tietosuojaperiaatteet, jotka organisaatioiden on huomioitava toiminnassaan sekä osoittaa niiden toteutuminen käytännössä (osoitusvelvollisuus). Andersson on todennut tutkimuksessaan, että tietosuojaperiaatteet kertovat hyvän tietojenkäsittelytavan vaatimuksista ja sisällöstä. Hyvällä henkilötietojenkäsittelytavalla tarkoitetaan Anderssonin mukaan lainmukaista henkilötietojen käsittelyä¹¹. Tietosuoja-asetuksen mukaisia tietosuojaperiaatteita käsitellään tämän tutkimuksen luvuissa 3–5.

Tall on (2014) väitöskirjassaan *yrityskauppa ja strateginen uudistuminen* korostanut yrityskaupprosessin monitasoisuutta sekä monivaiheisuutta. Tapauskohtaisesti yrityskaupat ovat yksilöllisiä, jokaisen yrityskaupan ollessa oma dynaaminen prosessinsa. Prosessi voidaan kuitenkin lähtökohtaisesti jakaa kolmeen erilaiseen vaiheeseen: 1) ennen

⁹ Lång ja muut, 2022, s. 171–172.

¹⁰ Andersson, 2024, s. 6-7.

¹¹ Andersson, 2024, s. 36.

yrittäjäkauppaa, 2) yrityskauppa ja 3) yrityskaupan jälkeen. Yrityskaupan ollessa monimutkainen sekä aikaa ja rahaa vievä prosessi, on yrityskaupan eri vaiheissa huolehdittava päivittäisestä johtamisesta¹².

Korja on (2016) väitöskirjassaan *biometrinen tunnistaminen ja henkilötietojen suoja* tutkinut mitä tarkoitetaan henkilötiedoilla ja henkilötietojen käsittelyllä sekä miten niitä säännellään Suomessa ja EU:n lainsäädännössä. Henkilötietojen suojan käsite on Korjan mukaan vakiintunut viime vuosikymmenten aikana osaksi eurooppalaista oikeuskäsitystä ja nykyään sitä pidetään oikeudellisena peruskäsitteenä, synonyyminä tietosuojalle. Henkilötietojen suoja on tietosuojalainsäädännön avulla toteutettavaa perusoikeuksien suojaa. Se on siis ennen kaikkea yksilön suojaa, ei tietojen suojaa. Henkilötietojen suojaa koskeva lainsäädäntö pyrkii toteuttamaan mahdollisimman avoimen tietojen käsittelyn, varmistaen kuitenkin vain tarpeellisten tietojen keräämisen. Henkilötietojen suojan pääasiallinen tarkoitus Korjan mukaan on suojata yksilöä perusteettomalta henkilötietojen käytöltä, keräämiseltä, luovuttamiselta sekä tallentamiselta. Kuten Korja on väitöskirjassaan todennut, on jokaisella lähtökohtaisesti oikeus itse määrätä omien henkilötietojen käytöstä ja luovutuksesta¹³.

Työelämässä kohdattavat tilanteet ovat moninaisia ja tulevaisuudessa esiin nousevia kysymyksiä on vaikea ennustaa. Henkilötietojen käsittelyyn liittyvissä käytännön ongelma- ja soveltamistilanteissa on tietosuojan yleisillä periaatteilla ja erityisesti tarpeellisuusvaatimuksella erittäin tärkeä merkitys¹⁴. Työnantajan ja työntekijän välisessä suhteessa tietyt tiedot ja asiat ovat yksityisasiota eivätkä kuulu työnantajalle ilman erityistä perustetta. Tätä korostaa työnantajan oikeutta henkilötietojen käsittelyyn rajoittava tarpeellisuusvaatimus. Korja korostaa väitöskirjassaan, että työnantaja saa käsitellä

¹² Tall, 2014, s. 19.

¹³ Korja, 2016, s. 115, 220.

¹⁴ Koskinen ja muut, 2012, s. 403.

ainoastaan välittömästi työn kannalta tarpeellisia henkilötietoja ja ylläpitää rekisterinpitäjänä vain tarpeellisia rekistereitä ja niissä tarpeellisia tietoja¹⁵. Henkilötietoja käsitellään tämän tutkimuksen luvussa 2 ja henkilötietojen käsittelyä luvuissa 3–5.

1.2 Tutkimusongelma ja tutkimuksen rajaus

Tämän työn tavoitteena on selvittää henkilötietojen suojan merkitystä osana yrityskauppaprosessia, erityisesti Euroopan unionin yleisen tietosuoja-asetuksen näkökulmasta. Tutkimuksessa pyritään tunnistaa toimet, joilla henkilötietoja voidaan suojata ja tarkastelemaan erityisesti sitä, missä kulkee henkilötietojen suojan, yksityisyyden ja liiketoimintatiedon raja. Tavoitteena on tuoda esiin myös se, millaisia tietoja sekä missä vaiheessa niitä saa tai pitää luovuttaa ja kenelle.

Oikeuden ollessa tietoa ja tietojenkäsittelyä, perustuvat oikeudelliset toiminnot tietojen käsittelyyn ja hallintaan. Tieto nähdään hyödykkeenä, jota on pystyttävä käsittelemään ja hallinnoimaan siten, että se on ajantasaista, luotettavaa ja laadukasta¹⁶. Tutkimus pyrkii oikeustapausten sekä yleisen tietosuoja-asetuksen säännösten avulla selvittämään, miten henkilötietojen suoja ja sen myötä henkilötietojen käsittely toteutetaan yrityskaupassa ja erityisesti sen due diligence-prosessissa. Tutkimuksessa systematisoidaan ja selvitetään toimet, joilla henkilötietoja voidaan suojata. Tutkimuksessa selvitetään lainsäädännön ja oikeuskirjallisuuden avulla, miten henkilötietojen suoja toteutuu ja turvataan yrityskauppaprosessissa sekä millaisia haasteita siihen liittyy. Tutkimuskysymyksinä on käytetty seuraavia:

- *Miten henkilötietojen suoja ja yleisen tietosuoja-asetuksen mukainen käsittely voidaan turvata yrityskaupoissa, erityisesti due diligence-prosessissa?*
- *Miten tietosuoja vaikuttaa tietojen siirtoihin ja luovutuksiin eri osapuolten välillä?*

¹⁵ Korja, 2016, s. 299–300.

¹⁶ Raatikainen, 2002, s. 9–11.

- *Millaisia ongelmia tai riskejä henkilötietojen käsittelyyn yrityskauppaprosessissa liittyy?*

Yritykseen liittyviä tietoja ei luokitella henkilötiedoiksi, eikä tietosuoja-asetusta sovelleta niihin ollenkaan. Tutkimus kattaa luonnollisiin henkilöihin liittyvän henkilötietojen käsittelyn, joten tutkimuksesta on rajattu pois tietosuoja-asetuksen mukaisesti oikeushenkilöiden ja erityisesti oikeushenkilön muodossa perustettujen yritysten henkilötietojen käsittely. Tutkimuksesta on rajattu pois myös sellainen luonnollisen henkilön suorittama henkilötietojen käsittely, joka on kotitaloutta tai yksinomaan henkilökohtaista toimintaa eikä näin ollen ole sidoksissa ammatilliseen tai kaupalliseen toimintaan.

1.3 Tutkimusmenetelmä- ja aineisto

Tässä tutkimuksessa henkilötietojen suojaa yrityskaupoissa tarkastellaan oikeusdogmaattisesta eli lainopillisesta näkökulmasta. Oikeus nähdään velvoittavana ja voimassa olevana oikeutena. Oikeustieteen selvittäessä voimassa olevien oikeussääntöjen sisältöä, vastaa oikeusdogmatiikka kysymykseen voimassa olevan oikeuden sisällöstä ja oikeusjärjestykseen kuuluvien sääntöjä eli voimassa olevien, sitovia oikeussääntöjen tutkimisesta. Lainoppi tulkitsee ja systematisoi oikeusnormilauseen taustalla olevaa totuutta eli oikeusnormeja sekä oikeusjärjestystä ja siihen kuuluvia sääntöjä¹⁷. Oikeusnormilause toisin sanoen antaa informaatiota oikeusnormin ajatussisällöstä, jota lainoppi pyrkii ilmaisemaan, selvittämään ja täsmentämään. Lainopin keskeisimpänä menetelmänä voidaan siten pitää tulkintaa, sillä lainoppi tuottaa erilaisilla tulkinnan menetelmillä merkityssisällön oikeusnormille¹⁸.

Oikeusnormien systematisointi ja tulkinta lukeutuu osaksi lainoppia. Lainoppi pitää sisällään metodisia sääntöjä ja periaatteita, joiden pyrkimyksenä on osoittaa millä tavalla oikeuslähteitä voidaan ja miten niitä tulee päättelyssä käyttää. Lainoppi toisin sanoen

¹⁷ Aarnio, 1989, s. 48–50; Hirvonen, 2011, s. 22.

¹⁸ Hirvonen, 2011, s. 36–37.

selvittää voimassa olevien oikeusnormien sisältöä kahdenlaisten oikeusnormeista esitettyjen väitteiden kautta: tulkintakannanotot ja normikannanotot. Normikannanotot ovat väitteitä voimassa olevaan oikeuteen kuuluvista normeista, kun taas tulkintakannanotot väitteitä oikeusnormin sisällöstä. Lainopille on ominaista arvosidonnaisuus, määrättyihin metodisiin sääntöihin ja periaatteisiin nojautuminen, tietyn oikeuslähdeluettelon hyväksyminen sekä jonkinasteinen lakipositivistinen taustaoletus¹⁹.

Tutkimuksen tarkoituksena on löytää käsitteiden perustelut ja niiden tulkinnat. Oikeusdogmatiikan tutkiessa oikeussääntöjä, nousevat tulkinnalliset menetelmät, erityisesti systemaattinen tulkinta, sanamuodon mukainen tulkinta sekä juridinen tulkinahermaneutiikka tämän tutkimuksen keskeisimmiksi tutkimusmenetelmiksi²⁰. Tutkimukseni metodeihin lukeutuu myös empiirisistä tutkimusmenetelmistä kvalitatiivinen eli laadullinen tutkimus. Tyypillistä laadulliselle tutkimukselle on hypoteesien esittäminen, aiemmat teoriat sekä erilaisten käsitteiden määrittely. Joukko lakeja muodostaa teorian, joiden tarkoitus on systematisoida ilmiöaluetta koskevia empiirisiä sääntökokonaisuuksia²¹.

Tieto-oppi käsittelee tieteellisen tiedon olemusta pohtimalla mitä tieto on, miten tietoa voidaan saada, mitkä ovat tiedon rajat sekä millaista luotettava tieto on. Tieteen tunnusmerkit löytyvät tutkimusprosessista, niistä menetelmistä ja tavoista, joilla tavoitellaan, muodostetaan, hankitaan tai perustellaan tieteellistä tietoa²². Tutkimuksen tutkimusaineisto koostuu erilaisista yrityskauppoihin ja henkilötietoihin liittyvistä ajantasaisesta lainsäädännöstä, lain esitöistä, oikeustapauksista sekä oikeuskirjallisuudesta. Keskeisimmät lait tutkimuksen kannalta ovat tietosuojalaki (1050/2018) ja yksityisyyden suojasta työelämässä annettu laki (759/2004). EU-sääntelystä keskeinen oikeuslähde on Euroopan unionin yleinen tietosuoja-asetus (2016/679) sekä EU:n tietosuojaneuvoston (EDPB) ohjeet. Tutkimuksessa käytetyssä oikeuskirjallisuudessa on huomioitava luotettavuus, ajantasaisuus, pätevyys, eettisyys sekä merkityksellisyys.

¹⁹ Aarnio, 1989, s. 48–51; Hirvonen, 2011, s. 22; Husa ja muut, 2008, s. 20.

²⁰ Husa ja muut, 2008, s. 20.

²¹ Hirsjärvi ja muut, 2018, s. 141.

²² Hirvonen, 2011, s. 12, 15.

1.4 Tutkimuksen rakenne

Tutkimus koostuu kuudesta pääluvusta. Johdantoluvussa havainnollistetaan tutkielman tausta sekä sen merkitys, määritellään tutkimuskysymykset sekä rajaukset ja tuodaan esiin käytetyt menetelmät sekä aineistot. Lisäksi luvussa jäsenellään tutkimuksen kokonaisrakennetta, käsitellään tutkielmalle asetettuja tavoitteita ja tuodaan esiin esimerkkejä aiemmista tutkimuksista. Johdantolukua seuraavassa toisessa pääluvussa tarkastellaan laaja-alaisesti henkilötietojen käsittelylle yrityskaupassa asetettua oikeudellista perustaa. Luvussa esitetään henkilötietojen käsittelyyn liittyvän sääntelyn keskeistä viitekehystä, tietosuojavaltuutetun ohjeita ja määräyksiä, tietoturvan asettamia edellytyksiä, tietosuojaperiaatteita sekä sisäänrakennettua ja oletusarvoista tietosuojaa.

Tutkimuksen kolmannessa pääluvussa käsitellään yrityskauppaprosessin suunnittelu- ja valmisteluvaihetta osana henkilötietojen käsittelyä. Luvussa tarkastellaan henkilötietojen käsittelyä ja tietosuojaperiaatteita erityisesti due diligence-tarkastuksen näkökulmasta. Neljännessä pääluvussa keskitytään henkilötietojen käsittelyyn ja siirtoon yrityskauppaprosessin toteutusvaiheessa sekä tarkastellaan rajat ylittävälle siirroille asetettuja vaatimuksia. Viidennessä pääluvussa käsitellään yrityskauppaprosessin integraatiovaiheen ja jälkitoimien merkitystä henkilötietojen käsittelyssä. Luku havainnollistaa tietojen säilytyksen rajoittamista ja siihen liittyvää valvontaa sekä vastuiden jakautumista yrityskauppaprosessin jälkeen.

Kuudennessa ja viimeisessä pääluvussa pyritään johdonmukaiseen tutkimustulosten koamiseen sekä tarkasteluun. Luvussa tuodaan esiin myös tulevaisuudessa mahdollisesti esiin nousevia haasteita ja ongelmia osana yrityskauppoja tapahtuvan henkilötietojen käsittelyn näkökulmasta. Luku pyrkii tarkastelemaan myös henkilötietojen käsittelylle asetetun ytimen eli eheyden, luottamuksellisuuden ja lainmukaisuuden säilymistä läpi yrityskauppaprosessin eri vaiheiden.

2 Sääntelykehikko

Oikeus henkilötietojen suojaan rakentuu, ihmis- ja perusoikeutena yksityisyyden suojan kautta, henkilötietojen suojalle ja tietoturvalle. Tietosuoja-asetuksen mukaan luonnollisten henkilöiden suojelua henkilötietojen käsittelyä koskevissa säännöissä ja periaatteissa on otettava huomioon henkilöiden perusoikeudet- ja vapaudet, mutta erityisesti oikeus henkilötietojen suojaan. Oikeus henkilötietojen suojaan ei tietosuoja-asetuksen myötä kuitenkaan ole absoluuttinen, sillä sen on oltava oikeassa suhteessa muihin perusoikeuksiin ja sitä on tarkasteltava suhteessa sen tehtävään yhteiskunnassa. Yksityisyyden suojan ollessa riippuvainen henkilötietojen käyttöyhteydestä, on huomioitava myös se, että siihen vaikuttavat kaikki työelämän eri vaiheet, jotka vaativat henkilötietojen käsittelyä²³.

Puhuttaessa *tietosuojasta*, tarkoitetaan sillä henkilön yksityisyyden suojaamista, henkilöön yhdistettävissä olevien tietojen käsittelyssä. Tietosuoja on asianmukaista henkilötietojen käsittelyä, jonka myötä tiedot tulee suojata oikeudettomalta ja vahingoittavalta käytöltä²⁴. Henkilöllä tulisi olla mahdollisimman suuri tiedollinen itsemääräämisoikeus eli mahdollisuus vaikuttaa siihen, miten, missä ja kuka henkilötietoja käsittelee. Euroopan unionin perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojen suojaan. Henkilötietoja on artiklan mukaisesti käsiteltävä asianmukaisesti, tiettyä tarkoitusta varten²⁵. Suunniteltaessa, kehitettäessä, valittaessa sekä käytettäessä erilaisia järjestelmiä tai palveluita, joissa käsitellään henkilötietoja, on aina otettava huomioon ihmisen oikeus tietosuojaan. Tietosuoja toisin sanoen tarkoittaa kaikkea sitä, millä tämä oikeus pyritään takaamaan²⁶.

²³ Koskinen ja muut, 2012, s. 36; Neuvonen, 2014, s. 61–63.

²⁴ HE 125/2003 vp, s. 9; Keller, 2023, s. 89.

²⁵ Neuvonen, 2014, s. 60.

²⁶ Andersson, 2018, s. 2; Korpisaari ja muut, 2022, s. 313

Tietosuojan tarkoituksena ei ole suojata ainoastaan tietoja, vaan nimenomaisesti turvata tiedon kohteen eli luonnollisen henkilön etuja ja yksityisyyttä²⁷. Tietosuojalainsäädännön tarkoituksena on toteuttaa henkilötietojen suojaa. Tietosuojassa ei ole kyse tiedon kätkemisestä, panttaamisesta tai salaamisesta, vaan tietosuojan oikein mitoittamisesta sekä toteuttamisesta henkilötietojen käsittelykäytännöissä. Henkilötietojen käsittelyssä kaikkien edun mukaista ja olennaista on se, ettei henkilön tietosuojaa ole liian heikko eikä tarpeettoman tiukka. Tietojen korkea laatu sekä lainmukaiset, toimivat, menettelytavat tietojen käsittelyssä vaikuttavat kaikkiin organisaation toiminnan osa-alueisiin, sillä tieto on arvokas ja voimakkaasti kasvava tuotannontekijä²⁸.

Henkilötietojen käsittelyn määritelmä on hyvin laaja. Käytännössä se tarkoittaa sitä, että aina kun henkilötietoja käytetään miten tai mihin tarkoitukseen vain, on kyse käsittelystä. Henkilötietojen käsittely tarkoittaa siten kaikenlaisia henkilötietoihin kohdistuvia toimenpiteitä, henkilötietojen keräämisestä niiden tuhoamiseen saakka. Henkilötietojen käsittelyllä on toimintoja tai toimintoja, jotka kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin, automaattista tai manuaalista tietojenkäsittelyä käyttäen. Käsittely voi olla tietojen tallentamista, keräämistä, jäsentämistä, järjestämistä, säilyttämistä, muuttamista tai muokkaamista, hakua, käyttöä, kyselyä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhdistämistä tai yhteensovittamista, poistamista tai tuhoamista sekä rajoittamista²⁹. Määritelmässä olennaista on se, että se tarkoittaa ”merkintää”. Merkitystä ei ole sillä, miten tai mille alustalle tieto on talletettu, vaan se, että tiedon on oltava jollakin alustalla, jotta laki tulee sovellettavaksi. On siten merkittävää huomioda, että yksinomaan suullisesti annetut tiedot eivät ole henkilötietoja, jotka katsotaan kuuluvaksi lain soveltamisen piiriin³⁰.

²⁷ Koskinen ja muut, 2012, s. 40.

²⁸ Andersson ja muut, 2017, s. 12–13; Andersson & Ylipartanen, 2022, s. 14.

²⁹ Hanninen ja muut, 2017, s. 20.

³⁰ Hietala ja muut, 2021, 11.29.1.; Koskinen ja muut, 2012, s. 45.

Tietosuojaan liittyvän oikeuden suojan taso on Euroopan unionissa korkea ja sitä voidaan rajoittaa ainoastaan lailla sekä kunnioittaen oikeuden keskeistä sisältöä. Euroopan unionin primaarioikeudessa oikeus tietosuojaan onkin katsottu perusoikeudeksi. Oikeus henkilötietojen suojaan ei ole absoluuttinen oikeus, vaan sitä tulee tarkastella suhteessa sen merkitykseen ja tehtävään yhteiskunnassa. Suhteellisuusperiaatteen mukaisesti, oikeus henkilötietojen suojaan on oltava oikeassa suhteessa muihin perusoikeuksiin³¹.

Tietosuojalainsäädännön perustan muodostavat kansallinen tietosuojalaki sekä EU:n yleinen tietosuoja-asetus. Tietosuojalainsäädäntö määrittelee reunaehdot henkilötietojen käsittelylle, rekisteröidyn oikeuksille sekä asettaa velvoitteita henkilötietojen käsitteijöille³². Tietosuojalainsäädäntö määrittelee edellytykset myös sille, miten kerättyjä henkilötietoja voidaan käyttää, voidaanko niitä käsitellä uusia tarkoituksia varten tai onko henkilötietojen yhdistäminen sallittua. Se asettaa velvoitteita henkilötietojen käsittelyn hallinnollisiin ja operatiivisiin toteutustapoihin edellyttäen esimerkiksi henkilötietojen käsittelyn läpinäkyvyyttä suhteessa rekisteröityihin sekä henkilötietojen käsittelyä kuvaavan dokumentaation laatimista³³.

Yleisen tietosuoja-asetuksen soveltamisalaan kuuluvat kaikki henkilötietoja käsittelevät organisaatiot ja sitä sovelletaan niin julkisella kuin yksityiselläkin sektorilla, riippumatta henkilötietojen luonteesta, laajuudesta tai käytetyistä teknisistä ratkaisuista³⁴. Tietosuoja-asetusta sovelletaan henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista sekä muussa kuin automaattisessa muodossa muodostaen tai tarkoituksena muodostaa rekisterin osan.

Henkilötietojen suojaaminen tehokkaasti kaikkialla Euroopan unionissa edellyttää tietosuoja-asetuksen mukaisesti rekisteröityjen oikeuksien sekä henkilötietoja käsittelevien ja käsittelystä päättävien velvollisuuksien vahvistamista ja täsmentämistä. Perustuslain

³¹ European Data Protection Board, Suositukset 1/2020, s. 9.

³² Krakau & Haapalehto, 2020, s. 194; Lehtioksa ja muut, 2019, s. 866.

³³ Lehtioksa ja muut, 2019, s. 867.

³⁴ Hietala ja muut, 2021, 11.29.1.

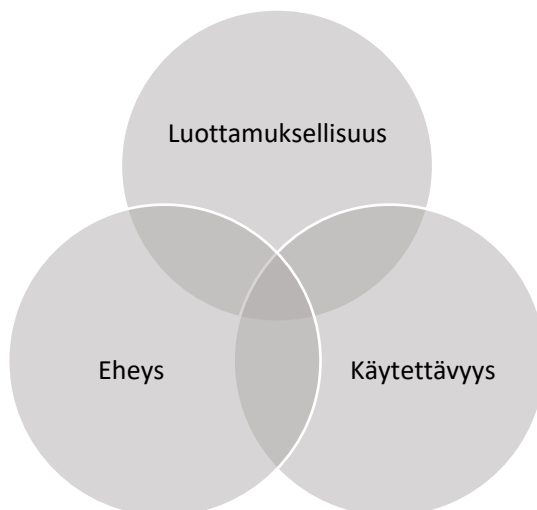
(731/1999) 2 luku sisältää säädökset perusoikeuksista. Lain 10 §:n mukaan henkilötietojen suojasta ja niiden käsittelystä tulee säätää lain tasoisesti³⁵. Oikeus henkilötietojen suojaan on perusoikeus, joka on vahvistettu primäärioikeudessa, erityisesti Euroopan unionin perusoikeuskirjan 8 artiklan 1 kohdassa ja Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdassa³⁶. Henkilötietojen suojan piiriin kuuluvien tietojen käsittelyn on Euroopan unionin perusoikeuskirjan mukaisesti oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten, asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Artiklan 2 kohdassa todetaan, että jokaisella on myös oikeus tutustua sellaisiin tietoihin, joita on kerätty sekä saada ne oikeuksi.

Henkilötietojen käsittely on aina perusteltava ja käsittely perustuttava siihen tarkoitukseen, johon tiedot on kerätty. Peruslähtökohtana sääntelyssä ovat yksilön henkilökohtaisen itsemääräämisoikeuden sekä vapauden turvaaminen. Tietosuojan ollessa perusoikeus, tulee tietojenkäsittelyssä yksilölle taata mahdollisuus vaikuttaa omien tietojensa käyttöön. *Henkilötietojen suoja* määrittelee henkilötiedot ja niiden käsittelyn edellytykset, kun taas *tietoturva* asettaa konkreettisen viitekehyksen tietojen käsittelylle. Tietoturva tarkoittaa ennen kaikkea sellaisia organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon eheys ja luottamuksellisuus, rekisteröidyn oikeuksien turvaaminen ja järjestelmien käytettävyys³⁷.

³⁵ Andersson ja muut, 2016, s. 31–34; Korpisaari ja muut, 2018, s. 104.

³⁶ Euroopan unionin tuomioistuimen muistio, 2024, s. 3.

³⁷ Koskinen ja muut, 2012, s. 36; Krakau & Haapalehto, 2020, s. 197; Neuvonen, 2014, s. 61–63.



Kuvio 1. Tietoturvan ulottuvuudet.

Euroopan unionin perusoikeuskirjan taatessa jokaiselle oikeuden henkilötietojen suojaan, takaa tietosuoja yksilölle oikeudet omiin henkilötietoihin sekä suojaa yksityisyyteen henkilötietoja käsiteltäessä³⁸. Henkilötietojen käsittely on perustuttava luottamuksellisuuteen, eheyteen ja käytettävyyteen. Käsittelyllä on varmistettava henkilötietojen asianmukainen luottamuksellisuus ja turvallisuus. Tietoturvan varmistessa henkilötietojen käsittelyn eheyden eli oikeellisuuden, on kerätyn, käsitellyn tai siirretyn tiedon yritys-kauppaprosessin aikana säilyttävä muuttumattomana. Eheydellä tarkoitetaan tässä yhteydessä sitä, ettei tietoja ole rekisterinpitäjän suostumuksetta muutettu. Henkilötiedot tulee suojata lainvastaiselta ja luvattomalta käytöltä sekä vahingossa tapahtuvalta vahingoittumiselta, tuhoutumiselta tai häviämiseltä. Suojaamisesta tulee huolehtia käsittelyn kaikissa vaiheissa eli tietojen keräämisestä niiden poistamiseen saakka. Rekisterinpitäjän on toiminnallaan ehkäistävä luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettäviin laitteistoihin³⁹. Käytettävyysvaatimus sisältää toimenpiteet, joilla varmistetaan ainoastaan henkilötietojen käsittelyyn oikeutettujen henkilöiden pääsy tietoihin⁴⁰.

³⁸ Aalto-Setälä & Viitaila, 2018, s. 4.

³⁹ Aalto-Setälä & Viitaila, 2018, s. 13–15; Hanninen ja muut, 2017, s. 51; Korpisaari ja muut, 2018, s. 24.

⁴⁰ Hanninen ja muut, 2017, s. 107.

Kun tulkitaan henkilötietojen suojan ulottuvuuksia, on tukea haettava aineellisesta lainsäädännöstä, jonka avulla pyritään turvaamaan oikeus henkilötietojen suojaan sekä erinäiset tietoruvavaatimukset. Näistä keskeisimpinä voidaan mainita 1) tarkoitussidonnaisuus, 2) huolellisuusvelvoite, 3) virheettömyysvaatimus, 4) tarpeellisuusvaatimus sekä 5) yhteysvaatimus. Jotta henkilöllä on mahdollisuus tietää, mihin hänen luovuttamiaan henkilötietoja tullaan käyttämään, on henkilötietojen käsittely tarkoitussidonnaisuuden perusteella oltava perusteltua ja niiden käsittely perustuttava ainoastaan siihen tarkoitukseen, johon ne on kerätty⁴¹. Tarpeellisuusvaatimus nähdään työelämässä tapahtuvan henkilötietojen käsittelyn kulmakivenä, sillä mikäli tieto ei ole välittömästi lain edellyttämällä tavalla tarpeellinen, ei sitä saa kerätä tai muutoin käsitellä⁴².

Henkilötietojen käsittelyssä huolellisuusvelvoitteen tarkoituksena on turvata tietosuojan taso. Velvoite toteutetaan muotoilemalla hyvä tietojenkäsittelytapa, joka täydentää kunnioittamista yksityisyyden suojasta perusoikeutena sekä sitä toteuttavasta lainsäädännöstä. Yleisluonteisen periaatteensa vuoksi, sille tyypillistä on yksityisyyden suojan perusoikeuskokonaisuuden läpileikkaaminen. Yksityisyyden suojalla on merkitystä yksittäisen kansalaisen jokapäiväiseen elämään, sen ollessa konkreettinen perusoikeus. Henkilötietojen suojaan ja yksityisyyteen liittyvien tietojen, asioiden ja toimien käsittelyssä on noudatettava erityistä huolellisuutta. Huolellisuutta korostaa virheettömyysvaatimus, jonka mukaan vanhentuneita, virheellisiä tai epätäydellisiä henkilötietoja ei saa käsitellä⁴³.

Työntekijöiden henkilötietoja käsiteltäessä on noudatettava yksityisyyden suojasta työelämässä (759/2004) annettua lakia. Lain mukaan työnantajalla on oikeus käsitellä vain välittömästi työntekijän työsuhteen kannalta, työsuhteen osapuolten oikeuksien ja vel-

⁴¹ Neuvonen, 2014, s. 62.

⁴² Koskinen ja muut, 2012, s. 403.

⁴³ Neuvonen, 2014, s. 62.

vollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka työtehtävien erityisluonteeseen liittyviä tarpeellisia henkilötietoja. Työnantajalla ei lain perusteella ole siten oikeutta käsitellä mitä tahansa työntekijää koskevia henkilötietoja⁴⁴.

Tietosuojalain (1050/2018) tarkoituksena on täsmentää ja täydentää luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä vapaasta liikkuvuudesta annettua tietosuoja-asetusta. Lakia sovelletaan tietosuoja-asetuksen 2 artiklan ja 6 artiklan 1 kohdan e alakohdan soveltamisalan mukaisesti ja se sisältää poikkeuksia asetuksen säännöksiin. Tietosuojalain 1 luvun 2 §:n mukaisesti henkilötietoja saa käsitellä tietosuoja-asetuksen 6 artiklan 1 kohdan mukaan ainoastaan, jos käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista tavoiteluun oikeutettuun päämäärään nähden.

Henkilötietojen käsittelyyn, joka tapahtuu EU:n alueella sijaitsevaan rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikkaan liittyvän toiminnan yhteydessä, sovelletaan tietosuojalain 2 §:n mukaan Suomen lakia, mikäli toimipaikka sijaitsee Suomessa. Tietosuojalain 2 §:n 2 momentin mukaan henkilötietojen käsittelyyn sovellettaessa vieraan valtion lakia ja sen nojalla poikettaessa tietosuoja-asetuksen 89 artiklan 2 kohdan mukaisesti rekisteröidyn suojaksi säädetyistä oikeuksista, on rekisteröidyn suojaksi tietosuojalain 31 §:ssä rekisteröidyn suojaksi säädetyjä suojatoimia noudatettava lainvalinnasta riippumatta.

2.1 Yleistä henkilötiedoista ja yrityskaupasta

On monia erilaisia tarkoituksia, joita varten yrityksissä käsitellään henkilötietoja. Toiminnan kannalta keskeisimmiksi henkilötiedoiksi nousevat henkilöstöä ja asiakkaita koskevat tiedot. Yrityksen toiminnan uudelleenjärjestelyssä, kuten yrityskaupoissa, ilmenee tilanteita, joissa henkilötietoja luovutetaan yritykseltä toiselle. Henkilötietojen käsittely kat-

⁴⁴ Krakau & Haapalehto, 2020, s. 200.

taa käytännössä kaikki henkilötietoihin kohdistuvat toimenpiteet, kuten niiden luovuttamisen, tallentamisen sekä keräämisen. Henkilötietojen käsittelyn ja luovutuksen on oltava lainmukaisuutta korostavaa ja huomioitava henkilötietoja sääntelevän lainsäädännön näkökulmat⁴⁵.

Yksityisyyden suoja henkilötietojen käsittelyssä muodostuu henkilötietojen ja yksityisyyden suojan lisäksi muista perusoikeuksista, kuten turvallisuus, yhdenvertaisuus sekä oikeus vaikuttaa itseään koskeviin asioihin. Euroopan perusoikeuskirjan 7 ja 8 artikloissa on tunnistettu oikeus yksityiselämän kunnioittamiseen. Oikeus koskee käsittelyssä tunnistettuja tai tunnistettavissa olevia luonnollista henkilöä koskevia tietoja. On kuitenkin syytä todeta, että henkilötieto voi olla yksityiselämää koskeva tieto, mutta kaikki henkilötiedot eivät kuulu yksityiselämän suojan alaan. Yksityiselämää koskevat tiedot ovat puolestaan myös henkilötietoja, mikäli ne voidaan yhdistää tiettyyn henkilöön. Huomioitavaa on, ettei henkilötietojen tarvitse olla tietyssä rekisterissä, jotta ne katsotaan kuuluvaksi asetuksen soveltamisalaan, vaan kaikki digitaalisessa muodossa olevat henkilötiedot kuuluvat asetuksen piiriin⁴⁶.

Tietosuojadirektiivin (95/46/EY) nojalla luodun työryhmän (WP29) kannanoton mukaan henkilötietojen käsitteelle on pyritty takaamaan mahdollisimman laaja, muttei rajoittamaton soveltaminen⁴⁷. Yleisen tietosuojasetuksen mukaan *henkilötietoja* ovat muun muassa: nimi, osoite, tulot, IP-osoite sekä kulttuurinen profiili. Kyse on henkilötiedoista, mikäli niiden perusteella voidaan saada selville tai tietää, kenestä on kyse⁴⁸. Tiedot, jotka koskevat henkilön poliittista mielipidettä, rotua, sukupuolista suuntautumista, uskonnollista vakaumusta, ammattiliittoon kuulumista, terveydellisiä tietoja tai rikostuomioita, eivät tietosuojasetuksen mukaisesti lukeudu yrityksen käsiteltävissä oleviin henkilötietoihin.

⁴⁵ Kaisko & Warma, 2007, s. 20.

⁴⁶ Korpisaari ja muut, 2022, s. 16–17.

⁴⁷ Kaisko & Warma, 2007, s. 20.

⁴⁸ Hanninen ja muut, 2017, s. 19.

Yrityskauppa on yleisin keino yrityksen toiminnan tai omistuksen uudelleenjärjestämiseen⁴⁹. Se kattaa kaikki sellaiset sopimusjärjestelyt, jotka kohdistuvat yrityksen omistukseen ja jonka tuloksena määräysvalta siirtyy toiselle yritykselle tai yksityishenkilölle. Se on jakautumisen, fuusion sekä liiketoimintasiirron alkuvaihe, jonka jälkeen kohdeyhtiö otetaan haltuun ja sen omaisuutta tai toimintaa järjestetään uudelleen. Onnistunut yrityskauppa edellyttää ostettavan yrityksen sekä sen liiketoiminnan kokonaisvaltaista ja syvällistä tuntemusta⁵⁰. Jokaisen yrityskaupaprosessin olessa ainutlaatuinen, voidaan sitä tarkastella ja vaiheistaa monella erilaisella tavalla. Prosessin painotus voi riippua tarkasteltavasta tilanteesta tai tarkastelijan mieltymyksistä. Tästä syystä jakoa voidaan pitää valinnaisena. Usein käytetty kolmiportainen vaiheistus on yrityskaupaprosessille tyypillinen: 1) suunnittelu, 2) toteuttaminen ja 3) integrointi eli sopeuttaminen⁵¹.



Kuvio 2. Yrityskaupan kolmiportainen vaiheistus.

Prosessin suunnitteluvaiheen tarkoitus on määritellä yritysoston suuntaviivat sekä laatia ostostrategia. Huomio suunnitteluvaiheessa on oltava myös yrityksen ympäriltä ja sisältä muodostuviin mahdollisuuksiin ja uhkiin. Vaiheeseen sisältyy ostokohteiden kartoitusta, kohteiden seulontaa sekä taloudellisen turvallisuuden määrittämistä. Jotta kaupan kohteesta voidaan varmistua, suoritetaan suunnitteluvaiheessa kaupan kohteen tarkastaminen eli due diligence-ennakkotarkastus. Yrityskaupaprosessin edetessä

⁴⁹ Immonen, 2018, s. 35.

⁵⁰ Hietala ja muut, 2021, 5.8.5; Immonen, 2022, s. 37.

⁵¹ Immonen, 2018, s. 46.

toteuttamisvaiheeseen, neuvotellaan yrityskaupan ehdoista sekä toteutetaan kauppasopimus. Toteutusvaiheelle on olennaista myös tietojen luovutus ja siirto. Sopimuksista ja ehdoista neuvottelun jälkeen etenee yrityskauppaprosessi sopeuttamisvaiheeseen, jolloin ostettu yritys integroidaan osaksi ostajayritystä⁵².

Henkilötietojen suoja on viime vuosina saanut merkittävän roolin yhteiskunnassa. Digitalisaation kehittyessä henkilötiedoista on tullut yhä suuremmissa osin myös kauppavaraa⁵³. Yrityskaupat ovat usein monimutkaisia prosesseja, joissa yhdistyvät strategiset, oikeudelliset sekä taloudelliset näkökulmat. Tällaisten prosessien aikana käsitellään luottamuksellisia tietoja, kuten talous- ja henkilöstötietoja. Henkilötietojen tärkeyttä organisaatioiden toiminnassa on tunnustettu kasvavissa määrin ja niiden käsittelyyn liittyvät vaatimustenmukaisuudet sekä toiminnot ovatkin olleet viime aikoina keskiössä⁵⁴. Voimaantullut tietosuojasetus ja sen sääntely vaikuttaa lähes jokaisen yrityksen toimintaan, niiden koosta riippumatta. Tietosuojasetuksen määräyksiltä ei voi yksikään yritys välttyä, nimittäin jokaisessa yrityksessä käsitellään henkilötietoja⁵⁵.

Useimpien kauppojen edellyttäessä kaupan kohteen huolellista tarkastusta, edellyttää myös yrityskauppa ostajanehdokkaan toimesta suoritettavaa perusteellista due diligence- tarkastusta. Potentiaalinen ostajaehdokas pyrkii tarkastuksessa saamaan selkeän kuvan yrityksestä sekä sen arvosta ennen sitovaa kauppaa. Myyjän on tässä vaiheessa luovutettava ostajaehdokkaalle yhtiötä koskevia arkaluonteisia ja luottamuksellisia tietoja. Yrityskauppa on usein yksi merkittävimmistä keinoista liikesalaisuuksien hankkimisessa. On siten todettava, että mitä salaisempia luovutettavat tiedot ovat, sitä harvemmalle ostajaehdokkaalle ja myöhemmässä vaiheessa ne on syytä luovuttaa⁵⁶.

⁵² Immonen, 2018, s. 46–47.

⁵³ Krakau & Haapalehto, 2020, s. 11–12.

⁵⁴ Korpisaari ja muut, 2022, s. 755.

⁵⁵ Hanninen ja muut, 2017, s. 13–16.

⁵⁶ Kurkela & Ståhlberg, 1997, s. 914, 920; Vapaavuori, 2019, s. 635–637.

2.2 Osapuolet

Yrityskauppojen sisältö ja laajuus riippuvat osapuolten tavoitteista sekä huolellisuuden noudattamisesta, mutta ennen kaikkea myös henkilöihin liittyvistä seikoista. Henkilötietojen käsittely tapahtuu yhteistyönä monen eri toimijan välillä. Lainsäädännön asettamien vaatimusten merkitys korostuu yritysten liiketoimintamallin perustuessa datan hyödyntämiseen tai keräämiseen⁵⁷. Yrityskaupan osapuolet voidaan karkeasti rajata myyjään ja ostajaan, mutta tosiasiallisesti henkilötietojen käsittelyn vaikutus vaatii tarkkarajaisemman määrittelyn osapuolten rooleista ja niiden merkityksestä suhteessa lainsäädännön asettamiin vaatimuksiin.

2.2.1 Rekisteröity

Arvioitaessa osana yrityskauppaa tapahtuvan henkilötietojen käsittelyn osapuolten rooleja, nousee keskeiseen osaan *rekisteröity* eli luonnollinen henkilö, jonka henkilötietoja käsitellään. Rekisteröidyllä tarkoitetaan siten henkilöä, jota henkilötieto koskee. On huomattava, että tietosuoja-asetus koskee lähtökohtaisesti kaikkea digitaalisessa muodossa olevaa henkilötietojen käsittelyä, eikä se siten rajoitu ainoastaan henkilörekisterissä olevien tietojen käsittelyyn⁵⁸.

Jokaisella on Euroopan unionin perusoikeuskirjan mukaan oikeus tutustua tietoihin, joita on kerätty sekä oikaista mahdolliset virheelliset tiedot. Rekisteröidyn oikeuksien taustalla on ajatus henkilötietojen oikeudettoman ja vahingollisen käytön suojaamisesta⁵⁹. Oikeuksia on tietosuoja-asetuksen nojalla pidetty rekisteröidyn työkalupakkina, jonka myötä rekisteröity voi vaikuttaa omien henkilötietojensa käsittelyyn. EU:n yleisessä tietosuoja-asetuksessa on määritelty rekisteröidylle kuuluvat oikeudet. Rekisteröidyn tietosuoja-asetuksen mukaisia oikeuksia ovat esimerkiksi oikeus tietojen tarkastamiseen, oikaisuun sekä poistamiseen. Euroopan unionin tuomioistuimen 14.12.2023 antamassa

⁵⁷ Lehtioksa ja muut, 2019, s. 867; Immonen, 2024, s. 57.

⁵⁸ Korpisaari ja muut, 2018, s. 28; Korpisaari ja muut, 2022, s. 34; K 13/2020 vp, s. 15.

⁵⁹ Aalto-Setälä & Viitaila, 2018, s. 19–20.

tuomiossa C-340/21 on arvioitu luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä. Tuomion kohdan 8 mukaan, jokaisella rekisteröidyllä on oikeus tehokkaiisiin oikeussuojakeinoihin, mikäli katsotaan, että asetukseen perustuvia oikeuksia on loukattu eikä henkilötietojen käsittelyssä ole noudatettu asetusta⁶⁰.

EU:n perusoikeuskirjan 8 artiklassa on vahvistettu rekisteröidyn oikeus tutustua tietoihinsa. Perusoikeuskirjan 8 artiklan 2 kohdan mukaan jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty sekä saada ne oikaistuksi. Rekisteröidyllä on oikeus saada rekisterinpitäjältä tietoja siitä mitä henkilötietoja käsitellään tai käsitelläänkö niitä. Tiedonsaantioikeuden tavoitteena on taata henkilölle riittävät, helposti saatavilla olevat ja läpinäkyvät tiedot henkilötietojen käsittelystä. Tämä mahdollistaa käsittelyn lainmukaisuuden ja käsiteltyjen tietojen täsmällisyyden varmistamisen. Oikeus määräytyy yleisen tietosuoja-asetuksen 4 artiklan 1 kohdassa määritellyn henkilötiedon käsitteen soveltamisalan mukaisesti⁶¹. Tiedot on oikeus saada yleisesti käytetyssä, jäsennellyssä sekä koneellisesti luettavassa muodossa. Rekisteröidyllä on oikeus siirtää saadut tiedot toiselle rekisterinpitäjälle edellyttäen, että käsittely perustuu sopimukseen tai suostumukseen ja se tehdään automatisoidusti⁶².

Rekisteröidyllä on tietosuoja-asetuksen mukainen oikeus vaatia rekisterinpitäjää rajoittamaan henkilötietojen käsittelyä tilanteissa, joissa: 1) rekisteröity kiistää tietojen oikeellisuuden, 2) käsittely on lainvastaista tai rekisteröity vastustaa poistamista ja vaatii käytön rajoittamista, 3) rekisterinpitäjä ei tarvitse henkilötietoja, mutta rekisteröity tarvitsee niitä oikeudelliseen vaateeseen sekä 4) rekisteröity vetoaa vastustamisoikeuteen. Mikäli henkilötietojen käsittelyä on rajoitettu, saa niitä käsitellä ainoastaan rekisteröidyn suostumuksella, toisen henkilön oikeuksien suojaamiseksi, oikeudellisen vaatimuksen esittämistä varten tai yleistä etua koskevista syistä⁶³.

⁶⁰ EUT C-340/21, VB v. Bulgarian kansallinen verohallinto, EU:C:2023:986; K 13/2020 vp, s. 13.

⁶¹ European Data Protection Board, 2023, s. 3.

⁶² Aalto-Setälä & Viitaila, 2018, s. 19–20.

⁶³ Aalto-Setälä & Viitaila, 2018, s. 22.

Luonnollisella henkilöllä eli rekisteröidyllä on tietosuoja-asetuksen mukaan oikeus tulla nohdetuksi sekä oikaista virheelliset henkilötiedot, mikäli tietojen säilyttäminen rikkoo rekisterinpitäjään sovellettavaa jäsenvaltion lainsäädäntöä tai unionin oikeutta taikka yleistä tietosuoja-asetusta. Erityisesti oikeus siihen, että henkilötiedot poistetaan, eikä niitä käsitellä alkuperäisen keräämistarkoituksen tai suostumuksen peruutuksen jälkeen tai henkilön ilmaiseman vastustamisen jälkeen, on tietosuoja-asetuksen mukaisesti varmistettava.

2.2.2 Rekisterinpitäjä ja henkilötietojen käsittelijä

Tietosuojan ja yksityisyyden toteutumisen ytimessä ovat rekisterinpitäjät sekä heidän tapansa käsitellä henkilötietoja⁶⁴. Rekisterinpitäjän ja henkilötietojen käsittelijän käsitteen keskinäisellä vuorovaikutuksella, täsmällisellä merkityksellä sekä oikean käytön kriteereillä on ratkaiseva merkitys yleisen tietosuoja-asetuksen soveltamisessa. Käsitteet nimittäin määrittelevät sen, kuka vastaa tietosuojasääntöjen noudattamisesta ja miten rekisteröidyt voivat käyttää oikeuksiaan⁶⁵.

Rekisterinpitäjä tarkoittaa osapuolta, jonka tarkoitusta varten henkilötietoja käsitellään ja joka tekee päätökset käsittelystä. Rekisterinpitäjä on siten elin, joka päättää käsittelyn keskeisistä tekijöistä ja vaikuttaa käsittelyyn päätöksentekovallan myötä. Tietosuoja-asetuksessa määritellyn mukaisesti rekisterinpitäjä on luonnollinen- tai oikeushenkilö, yritys, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisen kanssa määrittelee henkilötietojen käsittelyyn liittyvät keinot ja tarkoitukset⁶⁶. Rekisterinpitäjä voi olla esimerkiksi yritys, viranomainen, yhdistys, virasto tai jokin muu toimija⁶⁷. Henkilötietojen käsittelyn lainmukaisuuteen, oikeellisuuteen sekä rekisteröidyn oikeuksien kunnioittamiseen liittyvä viimesijainen vastuu on aina rekisterinpitäjällä, sillä rekisterinpitäjä määrittää kä-

⁶⁴ Andersson ja muut, 2023, s. 14.

⁶⁵ European Data Protection Board, Ohjeet 07/2020, s. 8.

⁶⁶ Hanninen ja muut, 2017, s. 25; Hietala ja muut, 2021, 11.29.1; Korpisaari ja muut, 2018, s. 28.

⁶⁷ Euroopan tietosuojaneuvosto. *Rekisterinpitäjä tai henkilötietojen käsittelijä*.

sittelyn tarkoitukset sekä keinot eli sen, miten ja miksi tietoja käsitellään. Rekisterinpitäjän on siten päätettävä henkilötietojen käsittelyn keinot ja tarkoitukset. Tarkoituksella viitataan odotettuun tulokseen, joka ohjaa suunniteltuja toimia, kun taas keino tarkoittaa sitä, miten päämäärä saavutetaan⁶⁸.

Yrityksen tulee asetuksen mukaisesti pystyä jälkikäteen osoittamaan toiminnan lainmukaisuus dokumentoimalla henkilötietojen käsittely. On syytä huomioida, että pelkkä vaatimuksenmukaisuus ei asetuksen mukaisesti riitä, vaan rekisterinpitäjän on pystyttävä osoittamaan, että tietosuojavelvollisuudet on varmistettu toiminnassa tarvittavin teknisillä, organisatorisilla ja hallinnollisilla toimenpiteillä. Velvollisuus koskee kerättyjen henkilötietojen määrää, laajuutta, saatavilla oloa sekä säilytysaikaa⁶⁹.

Rekisterinpitäjän tietosuoja-asetuksen mukaisen osoitusvelvollisuuden täyttääkseen, on seuraavat tiedot tultava ilmi: 1) tietosuojavastaava ja tietosuojaorganisaatio, 2) käsiteltävä tietoryhmä, 3) käsittelyn perusteet, 4) käsiteltävien henkilötietojen käyttötarkoitus sekä 5) tiedot henkilötietojen käsittelystä ja rekisteröityjen informoisesta. Dokumentaatioon tulisi myös tarkastella, mitkä tiedot ovat henkilötietojen käsittelyn ja yrityksen toiminnan kannalta tarpeellisia. Mikäli henkilötiedoissa on henkilötietotyyppisiä tai käsittelytapoja, joiden lainmukaisuutta ja tarpeellisuutta on jouduttu pohtimaan, suositeltavaa olisi esittää perustelut käsittelyn tarpeellisuudelle ja sallimiselle. Yritysten on arvioitava perusteellisesti jokaisen tiedon säilytysaikaa ja tuoda esiin perusteet, miten säilytysaikoihin on päädytty sekä käsiteltäessä tiettyjä henkilötietoja pidempään, perusteet poikkeaville käsittelyajoille⁷⁰.

Yleisen tietosuoja-asetuksen 32 artiklassa säädetään henkilötietojen käsittelyn turvallisuudesta. Henkilötietojen käsittelyn turvallisuuden varmistamiseksi on rekisterinpitäjän

⁶⁸ European Data Protection Board, Ohjeet 07/2020, s. 3, 12, 15.

⁶⁹ Hanninen ja muut, 2017, s. 15–16, 106–107; Korpisaari ja muut, 2022, s. 130.

⁷⁰ Hanninen ja muut, 2017, s. 52.

kyettävä tunnistamaan, mitkä tiedot liittyvät rekisteröityyn ja todentamaan kyseisen rekisteröidyn henkilöllisyys⁷¹. Unionin tuomioistuimen 14.12.2023 antaman tuomion C-340/21 kohdassa 7 on todettu, että ottaen huomioon toteuttamiskustannukset, käsittelyn luonne, laajuus, tarkoitukset, asiayhteys sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat vakavuudeltaan ja todennäköisyydeltään vaihtelevat riskit, mutta myös uusin teknologia, on rekisterinpitäjän ja henkilötietojen käsittelijän varmistukseen asianmukaiset tekniset ja organisatoriset toimenpiteet, toteutettava riskiä vastaava turvallisuustaso. Teknisinä ja organisatorisina toimenpiteinä tuomiossa on mainittu henkilötietojen salaus ja pseudonymisointi, käsittelyjärjestelmien luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden takaus, tietojen nopea saatavuus ja niihin pääsy sekä toimien tehokkuuden tutkiminen⁷².

Henkilötietoja rekisterinpitäjän lukuun käsittelee *henkilötietojen käsittelijä*. Henkilötietojen käsittelijä on siten taho, joka 1) auttaa henkilötietojen käsittelyssä tarjoamalla rekisterinpitäjälle esimerkiksi palvelualustan tai teknistä tietojärjestelmän ylläpitoa, 2) on rekisterinpitäjään nähden erillinen taho sekä 3) käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi virasto, yritys, viranomainen, yhdistys tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun annettujen dokumentoitujen ohjeiden mukaisesti⁷³. Henkilötietojen käsittelijän on käsiteltävä tietoja rekisterinpitäjän määräämin tavoin ja auttaa tätä noudattamaan yleistä tietosuojasetusta⁷⁴.

Henkilötietojen käsittelijän toimesta, rekisterinpitäjän lukuun, suorittamaan henkilötietojen käsittelyyn on sovellettava sopimusta tai muuta kirjallista ja sitovaa oikeudellista asiakirjaa. Henkilötietojen käsittelijän käsitellessä henkilötietoja rekisterinpitäjän lukuun tai sen puolesta, edellyttää tietosuojasetus tietojenkäsittelysopimuksen laatimista.

⁷¹ European Data Protection Board, 2023, s. 25.

⁷² EUT C-340/21, VB v. Bulgarian kansallinen verohallinto, EU:C:2023:986.

⁷³ Hanninen ja muut, 2017, s. 25, 83; Hietala ja muut, 2021, 11.29.1; Korpisaari ja muut, 2018, s. 29; Korpisaari ja muut, 2022, s. 342.

⁷⁴ Euroopan tietosuojaneuvosto. *Rekisterinpitäjä tai henkilötietojen käsittelijä*.

Henkilötietojen käsittelijän velvollisuudet sekä rekisterinpitäjän ja henkilötietojen käsittelijän välinen suhde määritellään käsittelysopimuksella, johon dokumentoidaan henkilötietojen käsittelyn keinot sekä käsittelytoimet. Sopimuksesta on tultava ilmi: 1) henkilötietojen käsittelyn kohde ja kesto, 2) käsittelyn tarkoitus ja luonne, 3) mitä henkilötietoja käsitellään, 4) rekisteröityjen ryhmät sekä 5) rekisterinpitäjän oikeudet ja velvollisuudet⁷⁵.

Henkilötietojen käsittelijällä ei ole henkilötietojen säilytyksen, keräämisen, käyttämisen tai muun käsittelyn suhteen päätösvaltaa. Arvioitaessa rajaa rekisterinpitäjän ja henkilötietojen käsittelijän välille on keskeistä arvioida, kumpi määrittelee sen, miten ja miksi henkilötietoja käsitellään. Rekisterinpitäjän ja käsittelijän vastuista tai rooleista ei voida lähtökohtaisesti neuvotella vaan ne määräytyvät tosiasiallisen toiminnan mukaisesti. Tietosuoja-asetuksen vaatimukset ja rekisteröityjen oikeuksien suojelun varmistamiseksi, on rekisterinpitäjän arvioitava ja osoitettava, että käsittelijä toteuttaa toiminnassaan tarvittavat suojatoimet sekä asetuksen mukaiset vaatimukset⁷⁶.

2.3 Oletusarvoinen ja sisäänrakennettu tietosuoja

Maailman digitalisoituessa on ensisijaisen tärkeää noudattaa oletusarvoista ja sisäänrakennettua tietosuojaa koskevia vaatimuksia. Henkilötietoja käsiteltäessä ja käsittelyä suunniteltaessa on lainsäädännön asettamat vastuut otettava vakavasti ja tietosuoja-asetuksessa asetetut velvollisuudet täytettävä, riippumatta siitä miten laajaa tai monimutkaista käsittely on. Jotta vaatimukset voidaan täyttää, on henkilötietoja käsittelevän ymmärrettävä yksilön oikeudet ja vapaudet sekä tietosuojaperiaatteet⁷⁷. Tietosuojan pääasiallisena tarkoituksena ei sananmukaisesti ole tiedon suojaaminen, vaan se pyrkii

⁷⁵ Hanninen ja muut, 2017, s. 83.

⁷⁶ Korpisaari ja muut, 2022, s. 342–343.

⁷⁷ Euroopan tietosuojaneuvoston ohje 4/2019, s. 4.

ohjaamaan henkilötietoja käsitteleviä toimijoita hyviin henkilötietojen käsittely- ja tietosuojakäytäntöihin, muodostaen asianmukaisen turvan tiedon kohteen eduille, oikeuksille, vapauksille ja yksityiselämälle⁷⁸.

Yleinen tietosuoja-asetus perustuu ennen kaikkea riskipohjaiseen lähestymistapaan. Toiminta, jolla katsotaan olevan vähäinen riski, ei aiheuta merkittävää uhkaa rekisteröidyn yksityisyyden suojalle, oikeuksille, eduille tai vapauksille. Korkeamman riskin henkilötietojen käsittely edellyttää asetuksen mukaan organisaatiolta hallinnollisiin sekä teknisiin toimenpiteisiin investoimista, jotta riittävä tietosuojan taso on mahdollista henkilöstön tietosuoja- ja käsittelykäytänteissä varmistaa⁷⁹. Tietosuoja-asetuksen mukaisen sisäänrakennetun ja oletusarvoisen tietosuojavaatimuksen toteuttaakseen, on rekisterinpitäjän tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä. Asetuksessa riskeiksi luokitellaan rekisteröidylle käsittelystä mahdollisesti aiheutuvat aineelliset tai aineettomat sekä fyysiset vahingot⁸⁰.

Merkitys riskien tunnistamiseen korostuu yrityksen määrittäessä, tietosuojan toteutusta henkilötietojen käsittelyssä. Yritysten velvollisuutena on huomioida harjoittamansa henkilötietojen käsittelyn laajuus, luonne, tarkoitukset, asiayhteydet sekä henkilöiden vapauksiin ja oikeuksiin kohdistuvat riskit. Tällaisen riskianalyysin avulla rekisterinpitäjä voi jo suunnitteluvaiheessa tunnistaa ne toimet, joihin asianmukaisen käsittelyn turvaamiseksi ja riskien hallitsemiseksi on ryhdyttävä. Tietosuojaperiaatteiden tehokas toteutuminen on rekisterinpitäjän toimesta varmistettava suhteessa käsittelyn liittyvään riskiin. Riskiarvio tulee tehdä rekisteröidyn näkökulmasta, joten rekisterinpitäjän on arvioitava millaisia rekisteröidyn oikeuksia ja vapauksia käsittely voi vaarantaa sekä millaisia vahinkoja rekisteröidylle voi suunnitellusta henkilötietojen käsittelystä aiheutua⁸¹.

⁷⁸ Andersson & Ylipartanen, 2022, s. 23.

⁷⁹ Andersson & Ylipartanen, 2022, s. 21–22.

⁸⁰ Talus ja muut, 2021, s. 16.

⁸¹ Tietosuojavaltuutetun toimisto. *Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.*

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa henkilötietojen asianmukainen turvallisuustaso, huomioiden uusimmat tekniikat ja toteuttamiskustannukset suhteessa suojeltavien henkilötietojen luonteeseen sekä tietojenkäsittelyn riskeihin. Tietojen suojaamisesta on huolehdittava käsittelyn jokaisessa vaiheessa, tietojen keräämisestä tietojen tuhoamiseen saakka. Yrityksen tulee varmistaa myös henkilötietojen käsittelyn turvallisuus. Henkilötietojen käsittelyn toteutustapaan vaikuttavat läheisesti henkilötietojen laatu sekä käsittelyyn liittyvät riskit⁸².



Kuvio 3. Rekisteröidyn oikeuksien ja vapauksien riskialueet⁸³.

Rekisterinpitäjän selkeä käsitys henkilötietojen käsittelystä luo pohjan riskiarviolle. Arvioidessa ja osoittaessa tietosuojasetuksen noudattamista, on rekisterinpitäjän otettava huomioon henkilötietojen laajuus (tiedon ja rekisteröityjen lukumäärä, säilytysaika ja maantieteellinen soveltamisala), luonne (uusi teknologia, erityiset henkilötietoryhmät, rekisteröidyn heikko asema ja vaikeus käyttää oikeuksiaan), asiayhteys (yksityisyyden turvaaminen, luottamuksellisuus ja eri yhteyksistä kerättyjen henkilötietojen yhdistely) sekä tarkoitus (automaattinen päätöksenteko, rekisteröityjen valvonta ja henkilöiden arviointi). Henkilötietojen käsittelylle asetetut suojatoimet on siten suhteutettava henkilötietojen käsittelystä rekisteröidyn vapauksille ja oikeuksille mahdollisesti aiheutuvaan

⁸² Hanninen ja muut, 2017, s. 106–107.

⁸³ Tietosuojavaltuutetun toimisto. *Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi*.

riskiin. Henkilötietojen huolimaton tai lainvastainen toiminta saattaa johtaa esimerkiksi identiteettivarkauteen, petokseen tai taloudellisiin menetyksiin⁸⁴.

Rekisterinpitäjän on tietosuojaperiaatteena säädetyn tiedon eheyden ja luottamuksellisuuden myötä suojattava henkilötiedot luvattomalta sekä lainvastaiselta käsittelyltä, mutta myös vahingossa tapahtuvalta tuhoutumiselta, vahingoittumiselta ja häviämiseltä. Rekisterinpitäjän tulee estää henkilötietojen ja aineistojen luvaton käyttö sekä ehkäistä luvattonta pääsyä henkilötietoihin tai niiden käsittelyssä käytettäviin laitteistoihin. Yrityksen tulee säännöllisesti tutkia, testata ja arvioida tietoturvan varmistamiseksi tehtyjen toimenpiteiden tehokkuutta, varmistaa rekisterinpitäjän ohjeiden mukainen henkilötietojen käsittely sekä luoda menettelytavat tietoturvan tason säännölliseen selvittämiseen⁸⁵.

Organisatoriset toimenpiteet muodostuvat yritysten asettamista toimintalinjauksista, henkilöstön vastuiden ja tehtävien määrittämisestä, ohjeistuksesta, valvonnasta, koulutuksesta sekä erilaisista periaatteista. Rekisterinpitäjän on varmistettava, että käyttäjän oikeudet ovat oikeassa suhteessa tälle asetettuihin asemiin ja vastuisiin. Henkilötietojen käyttöoikeuksien on oltava sitä rajatummat, mitä yksityisimmistä tiedoista on kyse. Järjestelmien ja laitteiden valvonta, tietojen luvattoman käytön estäminen sekä tietojen ja järjestelmien suojaaminen mahdollistetaan teknisiä toimenpiteitä hyödyntäen. Yrityskauppaprosessissa on tärkeää määrittellä teknisistä toimenpiteistä muodostuvat toimintatavat, joiden avulla yrityksellä on mahdollisuus seurata tietojenkäsittelyä⁸⁶. Asianmukaisen turvallisuustason arvioimisessa on tietosuoja-asetuksen 32 artiklan 2 kohdan mukaan kiinnitettävä huomiota erityisesti käsittelyn riskeihin, tallennettujen, siirrettyjen tai muutoin käsiteltyjen henkilötietojen laittoman tai vahingossa tapahtuvan häviämisen, tuhoutumisen, muuttumisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

⁸⁴ Hanninen ja muut, 2017, s. 26; Tietosuojavaltuutetun toimisto, *Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi*.

⁸⁵ Hanninen ja muut, 2017, s. 51, 108.

⁸⁶ Korpisaari ja muut, 2018, s. 272.

Organisatoristen toimenpiteiden tavoitteena on käyttäjien tietoisuuden lisääminen. Olennaisen tärkeää on, että henkilötietojen käsittelijät ovat tietoisia tietosuojaan liittyvistä riskeistä. Käsittelijöille tulee antaa tietoa mahdollisista, riskeistä aiheutuvista, seurauksista sekä niistä toimenpiteistä, joihin organisaatio on riskien torjumiseksi ryhtynyt. Tietoja käsittelevien henkilöiden ohjeistusta varten voidaan laatia sitova ja sisäisiä määräyksiä sisältävä asiakirja. Sisäisiin toimintaperiaatteisiin on sisällytettävä myös kuvaus turvallisuus- ja tietosuojasäännöistä. Tyypillinen organisatorinen toimenpide on myös sisällyttää henkilötietoja käsittelevien henkilöiden sopimukseen erityinen luottamuksellisuuslauseke sekä määrätä salassapitosopimuksen allekirjoittamisesta⁸⁷.

Tietoturvan tarkoituksen ollessa eheyden, luottamuksellisuuden ja käytettävyyden turvaaminen, on kyse tietoturvariskistä, mikäli oikeudettoman, tahallisen tai tahattoman teon seurauksena eheys, luottamuksellisuus tai käytettävyys ovat uhattuina. Riski on tietyn uhan aiheuttama vahingon tai menetyksen todennäköisyys. Riski tarkoittaa siten mitä tahansa kohtuullisesti tunnistettavissa olevaa tapahtumaa tai tilannetta, joka saattaa vaikuttaa haitallisesti tietojärjestelmien turvallisuuteen⁸⁸. Organisaation on arvioitava riskit seuraavien kohtien osalta, suojatakseen tietojen eheyden, luottamuksellisuuden sekä saatavuuden: 1) luvaton tai vahingossa tapahtuva pääsy tietoihin, 2) tietojen tahaton tai luvaton muuttaminen sekä 3) tietojen menettäminen tai tietojen käytettävyyden menetys⁸⁹.

⁸⁷ European Data Protection Board, *Huolehdi henkilötietojen turvallisesta käsittelystä*.

⁸⁸ Andersson, 2018, s. 2–3.

⁸⁹ European Data Protection Board, *Huolehdi henkilötietojen turvallisesta käsittelystä*.

3 Suunnittelu- ja valmisteluvaihe

Yrityskauppaprosessin toteuttaminen on monen erilaisen tekijän summa ja se vaatii merkittävän määrän suunnittelua. Rekisterinpitäjällä on ennen henkilötietojen keräämistä velvollisuus suunnitella henkilötietojen käsittely. Henkilötietojen käsittely oman toiminnan kannalta, tietojen hankinnan sekä luovutuksen määrittely tulee rekisterinpitäjän toimesta asiallisesti perustella⁹⁰. Suunnitteluvaiheen tarkoituksena on määrittellä yritystalon suuntaviivat sekä laatia ostostrategia seuraavien vaiheiden mukaisesti: identifiointi, ostokohteen kartoitus ja taloudellisen tilanteen määrittäminen. Yrityskauppojen ollessa monimutkaisia prosesseja, tulee niihin liittyvää epävarmuutta vähentää prosessin oltava hallittu sekä hyvin suunniteltu⁹¹.

Suunnittelu- ja valmisteluvaiheen toimilla on pyrittävä varmistamaan tietosuojan taso sekä tietosuoja-asetuksessa säädettyjen velvoitteiden myötä henkilötietojen asianmukainen luottamuksellisuus ja turvallisuus sekä käsittelyn lainmukaisuus, läpinäkyvyys ja asianmukaisuus koko yrityskauppaprosessin ajan. Arvioidessaan tietosuoja-asetuksen vaikutuksia, on yrityksen saatava kokonaiskuva henkilötietojen käsittelyn nykytilasta sekä arvioitava millaisia konkreettisia toimenpiteitä ja muutoksia tietosuoja-asetuksen sääntely sen suorittamalle henkilötietojen käsittelylle tosiasiaissa tarkoittaa. Toimenpiteiden laajuus ja laatu riippuvat organisaation nykyisistä käytännöistä, käsiteltävistä henkilötiedoista sekä käsittelyyn kohdistuvista riskeistä. On syytä korostaa, että erityisesti yrityksen johdon tulee olla tietoinen lainsäädännössä tapahtuvista muutoksista sekä niiden toimintaan liittyvistä vaikutuksista⁹².

Yleisen tietosuoja-asetusuudistuksen myötä tietosuojariskien arviointi muodostui osaksi organisaatioiden riskienhallintaa. Ostajalla on ennen yrityskauppaprosessin alkamista oltava ennakkonäkemyksensä kohdeyhtiön haltuunotosta kaupan jälkeen, kuten kohteen ja

⁹⁰ Korpisaari ja muut, 2018, s. 35.

⁹¹ Katramo ja muut, 2013, s. 39.

⁹² Talus ja muut, 2017, s. 11.

sen myötä henkilötietojen integroiminen osaksi kokonaisuutta. Tämä edellyttää suunnittelun ohessa tehtävää analyysia yhteisvaikutuksiin liittyvistä mahdollisuuksista ja riskeistä⁹³.

Yrityksen tulee jo varhaisessa vaiheessa ennen henkilötietojen käsittelyn aloittamista huomioida tietosuojaja sekä suorittaa vaikutustenarviointiprosessi (Data Protection Impact Assessment, DPIA). Henkilötietojen käsittelyn ollessa yrityksessä dynaamista, on vaikutustenarviointi jatkuva prosessi, joka pyrkii tietosuojan toteuttamiseksi sekä henkilöiden oikeuksille aiheutuvien riskien välttämiseksi tarkastelemaan suunniteltuja toimenpiteitä, mekanismeja sekä suojatoimia. Vaikutustenarvioinnin tarkoituksena on henkilötietojen käsittelyn havainnollistaminen ja käsittelyn tarpeen arvioiminen suhteessa riskeihin, tietosuojaja-asetusta noudattaen⁹⁴. DPIA-arviointi tulee rekisterinpitäjän toimesta tehdä, mikäli henkilötietojen käsittely, sen tarkoitukset, laajuus, luonne sekä asiayhteys huomioden, aiheuttaisi todennäköisiä riskejä henkilön oikeuksien kannalta. Tietosuojaja-asetuksessa todetaan, että arviointi velvoittaa rekisterinpitäjää, mikäli käsittely aiheuttaa henkilön oikeuksien ja vapauksien kannalta korkean riskin⁹⁵.

Jokaisen rekisterinpitäjän on arvioitava, tuleeko vaikutustenarviointi kyseeseen. Yrityksen käsitellessä laajamittaisesti arkaluontoisia henkilötietoja sekä käsittelyyn liittyessä henkilön oikeuksien sekä vapauksien kannalta suuri riski, on vaikutustenarviointi aina pakollinen. Vaikutustenarviointi on tehtävä, mikäli yritys ottaa käyttöön uusia tietojenkäsittelyteknologioita, henkilötietojen käsittely muuttuu tai käsittelyyn on arvioitu liittyvän tietosuojaja-asetuksen mukainen korkea riski. Huomioitavaa kuitenkin on, että rekisterinpitäjän on aina tarvittaessa eli henkilötietojen käsittelyyn sisältyvän riskin muuttuessa, tehtävä vaikutustenarviointi uudelleen. WP29-tietosuojaryhmän tulkinnan mukaan vain harva yritys välttyy vaikutustenarvioinnin tekemisvelvoitteelta, ollessa tulkinta sen

⁹³ Katramo ja muut, 2013, s. 44.

⁹⁴ Hanninen ja muut, 2017, s. 115–117; Euroopan tietosuojaneuvoston ohje 4/2019, s. 31.

⁹⁵ Andersson, 2018, s. 6.

tarpeellisuudesta varsin laaja. Tietosuojaryhmän suosituksen mukaan vaikutustenarviointi kannattaa tehdä tapauksissa, joissa ei ole täysin selvää, vaaditaanko tietosuojaan liittyvää vaikutustenarviointia⁹⁶.

Yrityskauppaprosessi alkaa yrityksen johdon tehdessä päätöksen yrityskaupan toteuttamisesta. Ennen yrityskaupan toteuttamista, kaupan kohteesta on tehtävä onnistuneelle yrityskaupalle edellytykset luova luottamuksellinen ennakkotarkastus eli *due diligence*-tarkastus, jossa kohdeyhtiöstä arvioidaan esimerkiksi oikeudelliset, verotukselliset sekä taloudelliset ominaisuudet. Käytännössä *due diligence*- tarkastus tehdään myytävän yrityksen riskien kartoittamiseksi ja arvon määrittelemisen perusteeksi. Ennakkotarkastuksen sananmukaisen määritelmän ollessa asianmukainen huolellisuus, voidaan sillä katsoa olevan kaksi erilaista pääfunktiota: ostajan taloudellisen riskin vähentäminen sekä juridinen virhevastuu⁹⁷. *Due diligence*-tarkastus merkitsee ennen kaikkea riskejä ja vastuita karttavaa asianmukaista huolellisuutta, joka mahdollistaa ostajalle kohteen tarkastamisen⁹⁸.

Due diligence- tarkastus pyrkii lisäämään ostajan tietoisuutta sekä kaventamaan myyjän virhevastuuta, mutta se toimii myös tuottamansa tiedon työkaluna yritysjärjestelyn jälkeisten asioiden haltuunotossa ja integraatiossa⁹⁹. Yleisesti se tehdään kohteen arvion määrittelemiseksi ja päätöksenteon tueksi. Tarkastusta pidetäänkin nykyään jo jonkinlaisena markkinastandardina, sillä mitä tarkempi tarkastus on, sitä vähäisemmät ovat jälkiselvittelyn riskit¹⁰⁰. *Due diligence*- tarkastuksen salliminen sekä toteuttaminen on usein hyvin monivaiheinen ja hienovarainen prosessi. Tarkastuksen alaa on perusteltua rajoittaa ja vaiheistaa tiedon herkkyysasteen mukaisesti. Tarkastuksella pyritään luomaan osapuolille selkeä kuva kohteesta ja sen arvosta sekä vähentämään ennalta arvaamattomia vastuisiin liittyviä riskejä. Lopulliseen päätökseen yrityskaupasta ja ehtojen

⁹⁶ Hanninen ja muut, 2017, s. 116–117.

⁹⁷ Immonen, 2022, s. 53; Katramo ja muut, 2013, s. 39; Vuola, 2009, s. 232.

⁹⁸ Katramo ja muut, 2013, s. 50–51.

⁹⁹ Blomquist ja muut, 2001, s. 23; Katramo ja muut, 2013, s. 52.

¹⁰⁰ Hietala ja muut, 2021, 5.8.5; Kaisko & Warma, 2007, s. 20.

toteuttamisesta vaikuttavat ostajan, due diligence- tarkastuksen myötä saadun tiedon perusteella tekemät oletukset ja johtopäätökset. Tämä vahvistaa sen roolia ennen kaikkea yritysjärjestelyn kohteen ennakkotarkastuksena sekä sensitiivisimmän tiedon edesauttajana¹⁰¹.

Yrityksen tulee due diligence-tarkastuksen aikana arvioida henkilötietoja sisältävien rekistereiden nykytila toteuttaakseen lainsäädännön asettamat velvoitteet. Henkilörekisteri tarkoittaa hallituksen esityksen (HE 75/2000 vp) mukaan henkilötietoja sisältävää rekisteriä, jota käsitellään ja ylläpidetään manuaalisten tai automaattisten tietojenkäsittelyjen avulla. Arvioinnin tarkoituksena on selvittää, mistä henkilötietoja hankitaan, mihin luovutetaan ja miten niitä käsitellään sekä sitä, millaisia muutoksia vuonna 2018 voimaan tulleen yleisen tietosuoja-asetuksen myötä yritysten toiminnassa on tehtävä¹⁰².

Due diligence- tarkastus pyrkii mahdollistamaan yritysjärjestelyllä sille ennalta asetetut tavoitteet. Prosessi toimii tuottamansa tiedon myötä työkaluna haltuunotossa ja integraatiossa, minkä vuoksi sitä toteutetaan päätöksenteon ja kohteen arvioinnin määrittämisen tueksi. On kuitenkin syytä todeta, että due diligence- tarkastusta suorittavan tahon tulisi tuntea ostajan liiketoiminta sekä sen taustalla vaikuttavat motiivit¹⁰³. Euroopan parlamentin ja direktiivin 95/46/EY johdanto-osan 25 kappaleen mukaan tietosuojan periaatteiden tulee ilmetä yksilöiden, yritysten, julkisten viranomaisten, virastojen tai muiden toimielinten velvoitteissa, jotka liittyvät tietojen laatuun, ilmoitusmenettelyyn, tekniseen turvallisuuteen, käsittelyn olosuhteisiin ja rekisteröidyn oikeuksiin¹⁰⁴. Toisin sanoen prosessin tarkoituksena on ennaltaehkäistä kaupan jälkeisiä yllätyksiä¹⁰⁵.

¹⁰¹ Katramo ja muut, 2013, s. 50–51, 409.

¹⁰² Andersson & Ylipartanen, 2022, s. 96; Hanninen ja muut, 2017, s. 15–16; HE 75/2000 vp, s. 14.

¹⁰³ Katramo ja muut, 2013, s. 52–53.

¹⁰⁴ Yksilöiden suojelua henkilötietojen käsittelyssä käsittelevä työryhmä, 2010, s. 4.

¹⁰⁵ Immonen, 2024, s. 56–57.

3.1 Käsittelyn suunnittelu ja tietojen määrittely

On luonnollista, että henkilöstöä koskevia tietoja luovutetaan jossain vaiheessa uudelle ostajalle. On kuitenkin huomioitava, että useinkaan yrityksen tilaa arvioidessa eli due diligence-tarkastuksen aikana, ei ole tarpeen tietää yksittäisten asiakkaiden tai työntekijöiden tietoja. Tämä tarkoittaa sitä, että työntekijöitä koskevia tietoja voidaan luovuttaa ryhmittäin, jolloin jaottelu on tehty koulutuksen, iän tai palkkauksen mukaan. Tällaisia tietoja voidaan pitää riittävänä due diligence-tarkastuksen aikana tehtävän analyysin laatimiseksi¹⁰⁶. Rekisterinpitäjän on ennen henkilötietojen käsittelyä valittava oletusarvoksi asetukset, joiden perusteella käsitellään ainoastaan sellaisia henkilötietoja, jotka ovat asetetun tavoitteen saavuttamisen kannalta välttämättömiä¹⁰⁷. Yrityskauppaprosessi ei siten saa olla kilpailukäyttämisen kannalta keinona arkaluontoisen tiedon vaihtamiseen, vaan prosessissa käsiteltävien tietojen on oltava kaupan kannalta merkityksellisiä eikä niiden säilytys ainoastaan kaupan toteuttamisen tarkoituksessa ole sallittua¹⁰⁸.

Tietosuoja-asetus velvoittaa yrityksiä henkilötietojen käsittelykäytänteiden sekä tietosuojan nykytilan kartoituksen tekoon sekä sen arviointiin suhteessa tavoitetaan. Voimassa oleva lainsäädäntö eli ennen kaikkea yleisen tietosuoja-asetuksen asianomaisen organisaation henkilötietojen käsittelyyn kohdistamat riskiperusteiset velvoitteet sekä vaatimukset määrittävät tavoitetilan¹⁰⁹. Yhä useampien yritysten toiminnan hoitaminen edellyttää henkilötietojen käsittelyä. Kuten jo edellä on todettu, ei olemassa ole yhtäkään organisaatiota, jossa ei käsiteltäisi tai kerättäisi henkilötietoja. Tämä on johtanut siihen, että henkilötiedoilla on monia käyttötarkoituksia ja rekisterien koot kasvavat tämän seurauksena¹¹⁰. Tietosuoja-asetuksen mukaan henkilötietojen on oltava täsmällisiä ja päivitettyjä. Yrityksen tulee yrityskauppaprosessin suunnitteluvaiheesta alkaen toteuttaa kaikki tarvittavat kohtuulliset toimenpiteet varmistaakseen, ettei prosessin aikana käsiteltävät henkilötiedot ole virheellisiä tai muuttuneita. Rekisterinpitäjän on

¹⁰⁶ Kaisko & Warma, 2007, s. 21.

¹⁰⁷ Korpisaari ja muut, 2022, s. 318.

¹⁰⁸ Vapaavuori, 2019, s. 636.

¹⁰⁹ Andersson ja muut, 2017, s. 14.

¹¹⁰ Andersson & Ylipartanen, 2022, s. 96; Hanninen ja muut, 2017, s. 15–16; HE 75/2000 vp, s. 14.

siten prosessin suunnitteluvaiheesta alkaen säännöllisesti käytävä henkilötiedot läpi ja varmistettava tietojen ajantasaisuus¹¹¹.

Yrityksen arvioidessa henkilötietojen käsittelytapoja eli rekisterinpitäjän päättäessä 1) miten käsittely toteutetaan, 2) tavoista, joilla käsittely tapahtuu sekä 3) mitä toimintaperiaatteita käsittelyyn käytetään, on sisäänrakennettu tietosuoja otettava käyttöön. Tietosuoja on huomioitava jo yrityskauppaprosessin suunnitteluvaiheessa ja tekniset sekä organisatoriset toimet toteuttaa siten, että rekisteröityjen lainsäädännössä turvatut oikeudet ja vapaudet toteutuvat. Yritysten tulee oletusarvoisesti käsitellä ainoastaan tarpeellisia tietoja. Käsittelytapojen määrittäminen ja henkilötietojen käsittely on toteutettava sisäänrakennettuna tietosuoja-asetuksen 5 artiklassa määriteltyjen tietosuojaperiaatteiden mukaisesti: lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Toimenpiteet eivät saa olla liian vähäisiä, mutta eivät myöskään ylikuormitettuja¹¹².



Kuvio 4. Henkilötietojen käsittelyn oikeusperusteet¹¹³.

¹¹¹ Korpisaari ja muut, 2022, s. 107.

¹¹² Andersson & Ylipartanen, 2022, s. 34; Korpisaari ja muut, 2022, s. 319.

¹¹³ Korpisaari ja muut, 2018, s. 267.

Hallituksen esityksen (HE 75/2000 vp) sekä yksityisyyden suojasta työelämässä annetun lain 2 luvun 3 §:n mukaan työnantaja saa käsitellä työntekijän henkilötietoja ainoastaan työsuhteen kannalta välttämättömästi tarpeellisia henkilötietoja. Tällainen tarpeellisuusvaatimus on henkilön yksityisyyden kannalta keskeisessä roolissa. Työelämässä esiintyvät tilanteet ovat hallituksen esityksessä kuvastusti monimuotoisia. Kerättävien tietojen laatu ja määrä vaihtelevat työtehtävien ja työalojen mukaan. Henkilötietojen kerääminen on tosiallinen tarve organisaation toiminnan järjestämiseen tai sen kehittämiseen. Työnantajan on tästä syystä hallituksen esityksen mukaisesti voitava perustella kerättävien henkilötietojen tarpeellisuus¹¹⁴.

Tarpeellisuusvaatimusta korostava tietojen minimointi eli henkilötietojen käsittelyn tarkoituksen määrittäminen on lähtökohtana henkilötietojen käsittelylle yrityskauppaprosessin suunnitteluvaiheessa ja etenkin due diligence- tarkastuksessa. Henkilötietojen käsittely on minimointivaatimuksen edellyttämällä tavalla due diligence-tarkastuksessa rajoitettava ainoastaan siihen, mikä on tarkastuksen tekemisen kannalta tarpeen. Työntekijöitä koskevat rekisterit on aina oltava asiallisesti perusteltuja ja niiden tietosisällössä on huomioitava lainsäädännön asettamat edellytykset. Yritysten on määritettävä henkilötietoja kerätessä niiden tarpeellisuus ja arvioitava mahdollinen käyttötarkoitus tulevaisuudessa¹¹⁵.

Henkilötietoja on käsiteltävä asianmukaisesti, lainmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi. Henkilötiedot tulee kerätä tiettyä, nimenomaista sekä laillista tarkoitusta varten, eikä niitä saa käsitellä näiden tarkoitusten kanssa yhteensopimattomin tavoin. Käsiteltävänä olevien henkilötietojen on tietosuojasetuksen mukaisesti oltava riittäviä, mutta myös rajoitettava siihen, mikä tietojen käsittelyn tarkoituksen kannalta on välttämätöntä. Käyttötarkoitussidonnaisuus edellyttääkin henkilötietojen asianmukaisuutta,

¹¹⁴ HE 75/2000 vp, s. 15.

¹¹⁵ Hanninen ja muut, 2017, s. 49; Korpisaari ja muut, 2018, s. 24.

olennaisuutta sekä rajoituttavuutta ainoastaan siihen, mikä on tarpeen suhteessa tarkoituksiin, joita varten niitä käsitellään¹¹⁶. Sen periaatteena on siten rajoittaa tarkoituksia, joihin rekisterinpitäjä voi käyttää keräämiään henkilötietoja. On syytä korostaa, että mikäli toimenpide voidaan suorittaa ilman henkilötietojen erillistä käsittelyä, tulisi sitä lähtökohtaisesti välttää¹¹⁷.

Henkilötietojen käsittelyn on perustuttava läpinäkyvään käsittelyyn. Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY perustetun tietosuojaryhmän tietosuoja-asetuksen mukaista läpinäkyvyyttä koskevista suuntaviivoista laaditun ohjeen (WP29) mukaan luonnollisille henkilöille on oltava läpinäkyvää, miten henkilötietoja käytetään, kerätään tai käsitellään. Läpinäkyvyys ilmentää Euroopan perusoikeuskirjan 8 artiklan periaatetta henkilötietojen käsittelyn asianmukaisuudesta. WP29-ohjeen mukaan tietosuoja-asetuksen läpinäkyvyysvaatimusta tulee soveltaa koko tietojenkäsittelyn elinkaarajan ajan, käsittelyn oikeusperusteesta riippumatta. Tietosuoja-asetuksen 12 artiklasta ilmenee, että läpinäkyvyyden periaatetta sovelletaan: 1) ennen tietojen käsittelyn aloittamista eli henkilötietoja kerättäessä, 2) koko käsittelyn ajan eli rekisteröidyille oikeuksista viestimisessä, sekä 3) tietyissä tapauksissa käsittelyn aikana eli käsittelyn muuttuessa olennaisesti taikka tietoturvaloukkauksen sattuessa¹¹⁸.

Käsittelyn ei tule olla rekisteröidyn näkökulmasta odottamatonta tai ennakoimatonta, joten tietojen käsittelyssä on arvioitava vaikutukset rekisteröityyn. Henkilötietojen käsittelyn tosiasiallista vaikutusta on perusteltava rekisteröidyn näkökulmasta seuraavien kohtien mukaisesti: henkilötietojen luonne, käsittelytoimet ja tointen vaikutus rekisteröityyn. Mitä arkaluontoisempia käsiteltävät henkilötiedot ovat, sitä enemmän seurauksia käsittelystä voi rekisteröidylle olla. On huomioitava myös se, mitä epävarmempia ja kielteisempiä käsittelyn seuraukset ovat, sitä epätodennäköisimmin käsittelyä pidetään oikeutettuna¹¹⁹.

¹¹⁶ Aalto-Setälä & Viitala, 2018, s. 13–15; Hanninen ja muut, 2017, s. 48.

¹¹⁷ Hanninen ja muut, 2017, s. 49; Korpisaari ja muut, 2018, s. 24.

¹¹⁸ Tietosuojaryhmän (WP29) suuntaviivat, s. 5–7.

¹¹⁹ Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*.

Henkilötietoja käsiteltäessä rekisterinpitäjän on yrityskaupan toteutusvaiheessa varmistettava tietosuojaa-asetuksen mukainen reiluus. Rekisterinpitäjien tulee kohtuullisuusvaatimuksen mukaisesti ottaessaan henkilötietoja käsittelyyn, huomioida rekisteröidyn odotukset ja edut, käyttämättä tietoja väärin. Erilaiset tietoprosessit, kuten tiedon siirtäminen tai hyödyntäminen, ovat osa tieto- ja palveluyhteiskunnan rakennetta. Vuorovaikutuksen ollessa prosessien ydin, edellyttää se toimijoiden välistä luottamusta. Tietosuojaa ja etenkin ihmisten luottamus sen säilymisestä, luovat edellytykset kaikelle tietoon liittyvälle toiminnalle¹²⁰. Tietosuojassa ja henkilötietojen käsittelyssä on kyse paljon muustakin kuin tietojen salassapidosta. Tietosuojasta on kehittymässä yhä selkeämmin strategisen toiminnan keskeinen osa-alue, jolla on kokonaisvaltaisia vaikutuksia koko organisaation toimintaan. Se toimii luottamuksen rakentajana rekisterinpitäjän ja rekisteröidyn välillä, mutta myös onnistuneiden strategisten valintojen edellytyksenä¹²¹.

3.2 Perusteet henkilötietojen käsittelylle

Oikeudellinen due diligence- tarkastus keskittyy tyypillisesti yrityksen yhtiöoikeudellisiin sekä omaisuutta koskeviin asiakirjoihin, mutta myös työntekijöitä koskeviin henkilötietoihin. Yrityksen on arvioitava tarkat toimintaperiaatteet henkilötietojen käsittelylle. Myyjän pyrkimys due diligence- vaiheessa on usein rajata hyvin tarkasti myytävästä yrityksestä annettavan tiedot, etenkin kilpailijoille, joiden sitoumus mahdolliseen kauppaan voi olla epävarma. Huomioitavaa on, että yleensä yrityskaappaprosessin edetessä laajenee ostajalle yrityksestä luovutettavien tietojen määrä¹²². Henkilötietojen suojan ollessa perusoikeus, tulee henkilötietojen käsittely suunnitella siten, että se palvelee ihmisiä. Luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä koskevissa periaatteissa ja säännöissä on huomioitava ihmisten perusoikeudet- ja vapaudet, nimittäin oikeus henkilötietojen suojaan on oltava oikeassa suhteessa sille määriteltyyn tehtävään ja muihin asetettuihin perusoikeuksiin¹²³.

¹²⁰ Andersson, 2016, s. 9.

¹²¹ Korpisaari ja muut, 2018, s. 24.

¹²² Kaisko & Warma, 2007, s. 21.

¹²³ Korpisaari ja muut, 2018, s. 35

Arvioitaessa henkilötietojen käsittelylle tietosuoja-asetuksessa säädettyjä oikeusperusteita, voidaan due diligence- tarkastuksen todeta olevan kriittinen vaihe. Usein arvioitaessa henkilötietojen käsittelyyn sidoksissa olevien käytäntöjen lainmukaisuutta, on palattava periaatetasolle ja tarkasteltava, mikä on sallittua. Henkilötietoja käsiteltäessä onkin noudatettava tietosuoja-asetuksessa säädettyjä käsittelyä rajoittavia periaatteita, jotka ohjaavat rekisterinpitäjää käsittelemään henkilötietoja rekisteröidyn vapauksia ja oikeuksia kunnioittavalla tavalla¹²⁴.

Pohdittaessa yrityskauppojen suunnitteluvaiheeseen ja etenkin due diligence-tarkastukseen liittyvää henkilötietojen käsittelyä, on syytä hakea pohjaa ja arviota lainsäädännön asettamista lainmukaisista oikeusperusteista. Henkilötietojen käsittely on perustuttava lailliseen perusteeseen¹²⁵. Käsittelyperusteella on merkittäviä vaikutuksia rekisteröidyn oikeuksiin suhteessa rekisterinpitäjään. Rekisterinpitäjän on ennen yrityskaupan tekoa selvitettävä, vaikuttaako tietosuoja-asetus käytettäviin oikeusperusteisiin. Rekisterinpitäjän on siten tunnistettava laissa säädetyt perusteet henkilötietojen käsittelylle, sillä sidottaessa henkilötietojen käsittely tiettyyn käsittelyperusteeseen, ei perustetta voi myöhemmässä vaiheessa enää vaihtaa toiseen¹²⁶. Henkilötietojen käsittelyyn saattaa soveltua samanaikaisesti useampi käsittelyperuste. Huomioitavaa on siten, ettei käsittelyperusteilla ole keskinäistä etusijajärjestystä, jolloin mikään peruste ei toiseen nähden ole ensisijainen¹²⁷.

Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin, kun vähintään yksi seuraavista tietosuoja-asetuksessa säädetyistä edellytyksistä täyttyy: suostumus (a alakohta), laadittu sopimus (b alakohta), rekisterinpitäjän lakisääteinen velvoite (c alakohta), elintärkeiden etujen suojaaminen (d alakohta), julkinen valta tai yleistä etua koskeva tehtävä (e alakohta) sekä rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu (f alakohta). Mikäli käsittely ei perustu lakiin, rekisteröity ei ole antanut suostumusta käsittelylle tai se

¹²⁴ Aalto-Setälä & Viitala, 2018, s. 13–15; Hanninen ja muut, 2017, s. 20; Lehtioksa ja muut, 2019, s. 874.

¹²⁵ Hanninen ja muut, 2017, s. 48.

¹²⁶ Talus ja muut, 2017, s. 19.

¹²⁷ Korpisaari ja muut, 2018, s. 100.

perustuu johonkin muuhun tarkoitukseen, on rekisterinpitäjän varmistettava, että käsittely on yhteensopiva alkuperäisen käsittelytarkoituksen kanssa¹²⁸.



Kuvio 5. Henkilötietojen käsittelyperusteet¹²⁹.

Jotta tietosuoja-asetuksen mukainen laillisuus sekä asianmukaisuus henkilötietojen käsittelyssä voidaan taata, on sen perustuttava asianomaisen rekisteröidyn suostumukseen taikka muuhun oikeutettuun perusteeseen, josta on säädetty lainsäädännössä¹³⁰. Rekisterinpitäjän käyttäessä suostumusta henkilötietojen käsittelyperusteena, on varmistettava tietosuoja-asteuksessa säädetyt vapaaehtoisuus, yksilöitävyys, yksiselitteisyys sekä tietoisuus. Suostumus katsotaan tietosuoja-asetuksen mukaisesti tahdonilmaisuksi, jolla rekisteröity hyväksyy henkilötietojen käsittelyn, ilmaisevan lausunnon antamalla tai ilmaisevan toimen toteuttamalla.

¹²⁸ Aalto-Setälä & Viitaila, 2018, s. 16; Hietala ja muut, 2021, 11.29.1.

¹²⁹ Korpisaari ja muut, 2018, s. 101.

¹³⁰ Aalto-Setälä & Viitaila, 2018, s. 16.

Tietosuojasetuksen edellytykset täyttääkseen, on suostumuksen hankkimisessa huomioitava tietyt kriteerit. Pätevyyttä arvioidaan verrattain tiukasti, nimittäin suostumuksen on oltava 1) aidosti vapaaehtoinen ja 2) selkeästi yksilöitävissä. Rekisteröidyllä tulee tietosuojasetuksen mukaisesti olla tosiasiallinen mahdollisuus riittävän laisella yksilöllinällä valita, mihin käyttötarkoituksiin suostumus annetaan. Yksittäistä suostumusta ei siten voida laajentaa koskemaan muihin palveluihin liittymättömiä toimia. Tietojenkäsittelyn perustuessa rekisteröidyn suostumukseen, on rekisterinpitäjän tietosuojasetuksen kohdan 42 mukaisesti voitava osoittaa, että suostumus on annettu käsittelytoimiin, mutta myös siitä, että rekisteröity on ollut tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse. Suostumus edellyttää siten rekisteröidyn aktiivista toimintaa, kuten kirjallisen suostumuslomakkeen täyttö tai allekirjoitus. Huomioitavaa on kuitenkin se, että suostumusta ei voi antaa vaikenemalla tai jättämällä toimenpiteitä suorittamatta. Tietosuojasetuksessa onkin todettu, ettei suostumusta voida katsoa annetuksi valmiiksi rastitetuilla ruuduilla¹³¹.

Rekisteröityjen on aidosti ja vapaasti voitava valita, suostuvatko he henkilötietojen käsittelyyn. Jotta henkilöt voivat ymmärtää, mitä tietoja käsitellään, millä tavalla ja mihin tarkoitukseen, on heille tarjottava riittävä määrä tarvittavaa tietoa. Henkilöille on taattava vapaus suostumuksen peruutukseen ilman kielteisiä seuraamuksia. Mikäli yritys käsittelee henkilötietoja, mutta tosiasiallista mahdollisuutta suostumuksen peruutukseen ei voida taata, on se osoitus siitä, että asianmukainen peruste henkilötietojen käsittelylle puuttuu. Näissä tilanteissa yrityksen on sovellettava toista käsittelyperustetta¹³².

Edellytyksenä sille, että suostumus voisi olla tietoinen tahdonilmaisu, on katsottu olevan rekisteröidyn tietoisuus henkilötietoja käsittelevästä tahosta sekä siitä, mihin tarkoitukseen ja miten perusteellisesta käsittelystä on kyse. Suostumuksen vapaaehtoisuus perustuu rekisteröidyllä olevaan todelliseen valinnan vapauteen siitä, haluaako tämä henkilötietojaan käsiteltävän vai ei, mutta myös tosiasialliseen mahdollisuuteen kieltäytyä

¹³¹ Hanninen ja muut, 2017, s. 35–36; Lehtioksa ja muut, 2019, s. 875.

¹³² Aalto-Setälä & Viitaila, 2018, s. 16.

suostumuksen antamisesta. On todettava, että suostumusta ei voida katsoa annetuksi vapaaehtoisesti, mikäli palvelun tarjoamisen edellytyksenä on suostumuksen antaminen, vaikka henkilötietojen käsittely ei ole palvelun tarjoamisen kannalta tarpeellista. Huolimatta siitä, että henkilötietoja voidaan käsitellä ja kerätä myös henkilön suostumuksella, on syytä korostaa, että suostumuskaan ei oikeuta henkilötietojen tarpeettomaan käsittelyyn¹³³.

Rekisteröidyn ollessa osapuolena sopimuksessa, voidaan henkilötietoja käsitellä sopimuksen täytäntöön panemiseksi. Mikäli sopimussuhdetta osapuolten välillä ei voida täyttää henkilötietoja käsittelemättä, on oikeuskirjallisuudessa katsottu perusteen henkilötietojen käsittelylle täytyvän. On huomioitavaa, että vaatimus asettaa rajoituksia sen kannalta, mitä henkilötietoja perusteen nojalla voidaan käsitellä. Sopimusperuste voi tulla kyseeseen yrityskauppaprosessissa, sillä sopimukseen perustuvasta henkilötietojen käsittelystä on kyse palvelussuhteiden, kuten virka- ja työsuhteiden osalta. Työnantajalla on oikeus käsitellä henkilötietoja ilman työntekijän nimenomaista suostumusta, mikäli kyse on työ- ja virkasuhteen kannalta tarpeellisista henkilötiedoista¹³⁴.

Yrityksen on usein toimintaansa liittyviä toimenpiteitä suorittaakseen käsiteltävä henkilötietoja. Mikäli käsittelyä ei voida perustella suostumuksella tai sopimuksella, voi tällöin käsittely olla mahdollista oikeutetun edun perusteella. Henkilötietojen käsittely voidaan katsoa yrityskauppojen aikana rekisterinpitäjän oikeutetuksi eduksi, kun tämän ja rekisteröidyn välillä on merkityksellinen suhde. Tämä tarkoittaa, että rekisteröity voi olla esimerkiksi rekisterinpitäjän palveluksessa¹³⁵.

On syytä todeta, että yksityishenkilön oikeudet ja edut ovat lähtökohtaisesti rekisterinpitäjään nähden suojatumpia. Oikeudellisesta perusteesta riippumatta tulee ennen hen-

¹³³ Hanninen ja muut, 2017, s. 37, 49.

¹³⁴ Korpisaari ja muut, 2018, s. 103; Korpisaari ja muut, 2022, s. 118.

¹³⁵ Korpisaari, 2022, s. 132–133; Talus ja muut, 2017, s. 19; Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*.

kilötietojen käsittelyn aloittamista suorittaa oikeasuhtaisuuden arviointi, jossa rekisterinpitäjän tai kolmannen osapuolen etuja punnitaan rekisteröidyn oikeuksia ja etuja vasten. Henkilötietojen käsittely oikeutetun edun perusteella edellyttää, etteivät rekisteröidyn edut tai perusoikeudet- ja vapaudet syrjäytä rekisterinpitäjän oikeutettua etua. Yrityksen on säännöksen edellyttämällä tavalla suunnitteluvaiheessa suoritettava intressipunninta, jossa rekisterinpitäjän oikeutettua etua punnitaan käsittelyn edellyttämiin rekisteröidyn etuihin ja oikeuksiin. Intressipunninnassa on huomioitava henkilötietojen käsittelyn periaatteet, tietosuojalainsäädäntö sekä suhteellisuusperiaate. Lopputulos määrittää voidaanko käsittely oikeutetun edun perusteen nojalla arvioida lainmukaiseksi¹³⁶.

Tietosuoja-asetuksen 6 artiklan f kohdan perusteella henkilötietojen käsittely on lainmukaista, mikäli se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Huomioitavaa on kuitenkin, että henkilötietojen suoja edellyttävät perusoikeudet- ja vapaudet sekä rekisteröidyn edut syrjäyttävät kyseiset edut. Rekisterinpitäjän oikeutettujen etujen vaikutukset rekisteröidyn oikeuksiin ja etuihin muodostavat muuttuvan skaalan. Due diligence-prosessin aikana on yrityksen syytä arvioida, voidaanko oikeutetuksi käsittelyperusteeksi katsoa rekisterinpitäjän oikeutettu etu. Intressit, jotka liittyvät oikeutettuun etuun, saattavat vaihdella merkityksettömistä melko tärkeisiin tai jopa pakottaviin. Vaikutukset rekisteröidyn oikeuksiin ja etuihin voivat muuttua huomattavista vakaviin. Oikeutettu etu käsittelyperusteena edellyttää rekisteröidyn oikeuksien ja etujen erityisen tarkkaa huomioimista¹³⁷.

Asianomaisen rekisterinpitäjän oikeutetun edun mukainen henkilötietojen käsittely on tietosuoja-asetuksen mukaan rajattava siihen, mikä on oikeasuhtaista ja ehdottoman välttämätöntä. Tietosuojavaltuutetun toimisto on kiteyttänyt 6.4.2018 antamassa oh-

¹³⁶ Korpisaari ja muut, 2018, s. 119–120; Korpisaari ja muut, 2022, s. 132; Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*.

¹³⁷ Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*.

jeessaan oikeutetun etuun vaadittavan harkinnan. Yrityksen on arvioitava, onko oikeutettu etu 1) sopivin käsittelyperuste, 2) täyttääkö se seuraavat edellytykset: lainmukaisuus, todellinen ja välitön tarve sekä tasapaino rekisteröidyn etuihin sekä oikeuksiin arvioitu ja ilmaistu selkeästi, 3) onko käsittely edun saavuttamiseksi tarpeen sekä 4) syrjäyttääkö etu rekisteröidyn oikeudet ja edut. Edun ollessa oikeutettu, on tietojen käsittelyn oltava tarpeen esimerkiksi perusoikeuksien toteuttamiseksi ja oikeassa suhteessa siihen nähden. Merkitystä on myös sillä, tunnistetaanko EU:n tai kansallisessa lainsäädännössä taikka muussa sääntelyvälineessä rekisterinpitäjän oikeus henkilötietojen käsittelyyn oikeutetun edun toteuttamiseksi. Tietosuoja-asetuksen mukaista oikeutetun edun myötä tulee yrityksen arvioida henkilötietoja kerätessä sitä, voiko rekisteröity kohtuudella odottaa, että henkilötietoja käytetään, käyttötarkoitussidonnaisuus huomioon otettuna, tiettyä tarkoitusta varten. Yrityksen harkitessa oikeutetun edun käyttöä käsittelyperusteena, on otettava huomioon tietosuoja-asetuksen 5 artikla mukaiset käsittelyä rajoittavat perusteet, kuten läpinäkyvyys, lainmukaisuus, käyttötarkoitussidonnaisuus, täsmällisyys sekä tietojen minimoinnin periaate¹³⁸.

Yrityksen on tietosuoja-asetuksen tietosuojaperiaatteiden sekä rekisteröidyn oikeuksien turvaamiseksi suoritettava rekisteröidyn etuja koskeva punninta eli tasapainotesti. Testin lopputulos riippuu saadusta kokonaisarviosta: mitä huomattavampi vaikutus rekisteröidyn kannalta käsittelyllä on, sitä enemmän rekisterinpitäjältä edellytetään tietosuojaan liittyviä asianmukaisia takeita, joiden on vähennettävä merkittävästi rekisteröityihin kohdistuvia vaikutuksia. Lisätoimenpiteitä voivat olla esimerkiksi henkilötietojen salaus, tekniset ja organisatoriset toimenpiteet tai anonymisointitekniikoiden käyttö. Mikäli rekisteröidyn oikeudet tai edut syrjäyttävät rekisterinpitäjän edun, ei henkilötietoja saa käsitellä¹³⁹. Oikeutettu etu edellyttää asianmukaista ja lainmukaista käsittelyä. Henkilötietojen käsittelyn on siten, oikeutettua etua oikeusperusteena käytettäessä, tapahduttava

¹³⁸ Korpisaari ja muut, 2018, s. 118–119, 121–122.

¹³⁹ Korpisaari ja muut, 2018, s. 117–118; Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*.

lainmukaisten intressien suojaamiseksi. Asianmukaisuus kattaa vaatimukset oikeutetun edun tarkasta määrittelemisestä sekä sen ajankohtaisuudesta ja tosiasiallisuudesta¹⁴⁰.

Tietosuoja-asetuksen mukaista oikeutetun edun myötä tulee yrityksen arvioida henkilötietoja kerätessä sitä, voiko rekisteröity kohtuudella odottaa, että henkilötietoja käytetään, käyttötarkoitussidonnaisuus huomioiden, tiettyä tarkoitusta varten. Yrityksen harjoittamassa oikeutetun edun käyttöä käsittelyperusteena, on otettava huomioon tietosuoja-asetuksen 5 artikla mukaiset käsittelyä rajoittavat perusteet, kuten läpinäkyvyys, lainmukaisuus, käyttötarkoitussidonnaisuus, täsmällisyys sekä tietojen minimoinnin periaate. Jotta etua voidaan pitää oikeutettuna, on sen täytettävä tietyt edellytykset: 1) edun on oltava lainmukainen eli sovellettavan EU:n tai kansallisen lainsäädännön mukainen, 2) edun on oltava selkeästi ilmaistu, jotta tasapainoa suhteessa rekisteröidyn oikeuksiin ja etuihin on mahdollista arvioida ja 3) edun edustettava välitöntä ja todellista intressiä. Mikäli nämä edellytykset täyttyvät, on rekisterinpitäjän harkittava voiko samaan lopputulokseen päästä keinoilla, joilla puututaan vähemmän rekisteröidyn yksityisyyteen¹⁴¹.

3.3 Tietojen anonymisointi ja salassapitosopimus

Yrityskaupan ollessa osapuolten välinen hyvin luottamuksellinen sopimus, on jo pelkkä hankkeen vireilläolo varjeltu liikesalaisuus, osapuolten luovuttaessa toisilleen luottamuksellisia tietoja. Osapuolet solmivat usein tiukkoja salassapitosopimuksia ja yritys-kauppasopimus sisältää erinäisiä salassapitoehtoja. Tietoyhteiskunnan kehityksen myötä viimeisten vuosikymmenten aikana liike-elämässä on koettu salassapitosopimusten eli NDA (Non-Disclosure Agreement) vallankumous. Ryhdyttäessä mihin tahansa merkittävään yhteistyösuhteeseen, vaaditaan usein toinen osapuoli sitoutumaan luottamuksellista aineistoa koskeviin salassapitovelvoitteisiin. Salassapitosopimuksen myötä liikesuhteessa voidaan täsmentää tai laajentaa lakisääteistä luottamuksellisen tiedon

¹⁴⁰ Korpisaari ja muut, 2022, s. 134.

¹⁴¹ Korpisaari ja muut, 2018, s. 118–119.

suoja. Suurin merkitys salassapitosopimuksessa onkin preventiivinen eli ennaltaehkäisevä, sen korostaessa tietoa luovuttavan osapuolen salassapidon tärkeyttä ja salassapito-intressiä sekä osoittaessa liikesalaisuudesta huolehtimisen säilymisen. On syytä huomioida, että salassapitosopimus vaikuttaa merkittävästi tietoa luovuttavan, että vastaanottavan osapuolen liiketoimintamahdollisuuksiin¹⁴².

Salassapitosopimus mahdollistaa tietojen luovutuksen ostajalle, joten erityisen tärkeää on määritellä sopimuksessa sitoumuksen kohde sekä laajuus, mutta erityisesti myös tietojen tarkoitettu sekä sallittu käyttötarkoitus. Salassapitosopimuksen lähtökohtana voidaan siten pitää sitä, että kaikki kohdeyhtiötä tai myyjää koskevat tiedot ovat luottamuksellista, myös tilanteissa, joissa tiedot on määritelty sopimuksessa. Osapuolten tulee salassapitosopimuksen solmittuaan ymmärtää, mihin salassapito, johon ostaja sitoutuu, on kohdistettu. On kuitenkin epätarkoituksenmukaista edellyttää, että jokainen henkilö, joka käsittelee luottamuksellisia tietoja ostajan puolesta, allekirjoittaa salassapitosopimuksen¹⁴³.

Yrityskaupprosessin suunnitteluvaiheeseen, etenkin due diligence-tarkastukseen, vaikuttavat lainsäädännön asettamat rajat salassapito- ja vaitiolovelvollisuudelle¹⁴⁴. Käikentyyppisten yrityskaupprosessien alkuvaiheisiin liittyy useimmiten myyjän puolesta vaadittu salassapitosopimus, joka solmitaan ennen arkaluontoisten tietojen luovuttamista ostajaehdokkaalle. Salassapitosopimuksen keskeisin tarkoitus on mahdollistaa kaupan kohteen tutkiminen, myyjän salassapitotarpeet suojaten¹⁴⁵. Salassapitosopimuksen allekirjoitettuaan, ostajan neuvonantajilla sekä edustajilla on mahdollisuus tutustua kohdeyrityksen hallussa olevaan materiaaliin. Kohdeyrityksen asiakirja-aineiston sisältäessä tyypillisesti erilaisia liikesalaisuuksia sekä arkaluontoisia tietoja, kerätään ne yleensä datahuoneeseen. Ostaja sitoutuu allekirjoittamallaan salassapitosopimuk-

¹⁴² Vapaavuori, 2019, s. 453–455, 637.

¹⁴³ Katramo ja muut, 2013, s. 347.

¹⁴⁴ Immonen, 2024, s. 57.

¹⁴⁵ Katramo ja muut, 2013, s. 345, 513.

sella käyttämään asiakirja-aineistoissa olevia tietoja ainoastaan yrityskauppaa palvele-
viin sekä edistäviin tarkoituksiin, mutta myös rajaamaan niiden henkilöiden määrää,
joille tiedot näytetään¹⁴⁶.

Tietosuoja-asetuksen 6 artiklan 1 kohta painottaa käsittelyn lainmukaisuutta ainoastaan
siltä osin, kun jokin mainituista oikeusperusteista täyttyy. On syytä huomioida, että jotkin
henkilötiedot on katsottu yksityisyyden kannalta riskialttiiksi. Tietosuoja-asetuksen mu-
kaisesti erityisiä henkilötietoryhmiä koskevien henkilötietojen käsittely on lähtökohtai-
sesti kiellettyä. Erityisiin henkilötietoryhmiin katsotaan asetuksen mukaisesti kuuluvaksi:
rotu tai etninen alkuperä, uskonnollinen tai filosofinen vakaumus, poliittiset mielipiteet,
ammattiliiton jäsenyys, tervettä koskevat tiedot, geneettiset tai biometriset tiedot ja sek-
suaalinen suuntautuminen.

Henkilötiedot, jotka on luokiteltu erityisen arkaluontoisiksi henkilön vapauksien- ja pe-
rusoikeuksien kannalta, tulee suojata yrityskaupprosessin eri vaiheissa erityisen tar-
kasti, sillä tietosuoja-asetuksen mukaan niiden käsittelyn asiayhteys voi aiheuttaa huo-
mattavia riskejä perusoikeuksille- ja vapauksille. Tietosuoja-asetuksen 9 artiklassa on
säädetty edellytyksistä, joiden tulee täytyä erityisiä henkilötietoryhmiä koskevien tieto-
jen käsittelyn sallimiseksi: 1) rekisteröidyn suostumus, 2) rekisterinpitäjän tai rekiste-
roidyn velvoitteiden ja erityisten oikeuksien noudattaminen 3) rekisteröidyn tai toisen
luonnollisen henkilön elintärkeiden etujen suoja, 4) poliittinen, uskonnollinen, filosofi-
nen tai ammattiliittotoimintaan liittyvän yhdistyksen, säätiön tai voittoa tavoittelemat-
toman yhteisön toiminta, 5) rekisteröity saattanut julkisiksi, 6) oikeusvaade, 7) yleinen
etu, 8) ennalta ehkäisevää tai työterveyshuoltoa koskeva tarkoitus, 9) kansanterveyden
yleinen etu ja 10) arkistointitarkoitus.

Varmuus tietoturvajärjestelmien luotettavuudesta organisaatioissa on keskeistä ja sitä
voidaan toteuttaa asianmukaisilla turvatoimilla. Jokaisen yrityskaupprosessin suunnit-
teluvaiheessa on mahdollisuuksien mukaan varmistettava tietojen anonymisointi ja

¹⁴⁶ Kaisko & Warma, 2007, s. 21.

pseudonymisointi. Puhuttaessa anonymisoinnista, tarkoitetaan sillä henkilötietojen käsittelyä, jossa henkilöä ei voida tunnistaa. Tiedot karkeistetaan yleiselle tasolle tai muutetaan sellaiseen muotoon, josta yksittäistä henkilöä koskevat tiedot eivät ole tunnistettavissa. Huomioon on kuitenkin otettava se, että anonymisoituihin tietoihin ei sovelleta tietosuojasäännöksiä, sillä niitä ei luokitella henkilötiedoiksi¹⁴⁷. Pseudonymisointi on henkilötietojen käsittelyä, jossa henkilötietoja ei ilman lisätietoja voida yhdistää tiettyyn henkilöön. Käytännössä pseudonymisointi tarkoittaa suorien tunnistetietojen, kuten henkilötunnus, korvaamista epäsuorasti tunnistettavilla tiedoilla, kuten järjestysnumero¹⁴⁸. Tietosuoja-asetuksen kohdan 28 mukaisesti pseudonymisoinnin soveltaminen henkilötietoihin voi auttaa rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan tietosuojavelvoitteita, mutta myös vähentää asianomaisiin rekisteröityihin kohdistuvia riskejä.

¹⁴⁷ Tietosuojavaltuutetun toimisto, *Pseudonymisoidut ja anonymisoidut tiedot*.

¹⁴⁸ European Data Protection Board, *Huolehdi henkilötietojen turvallisesta käsittelystä*.

4 Kaupan toteutusvaihe

Yrityskauppaprosessin toteutusvaiheen tavoitteena on neuvotella lopulliset ehdot sekä toteuttaa kauppasopimus. Ammattitaitoisesti luodut toteutussuunnitelmat ovat kriittisiä tekijöitä onnistuneessa yrityskaupassa. Keskeisenä onnistuneen yrityskaupan merkinä pidetäänkin kokemusta, ammattitaitoista sekä sitoutunutta projektinjohtoa, joka omaa tiedot kaikista yrityskauppaan liittyvistä seikoista¹⁴⁹. Perustellut, avoimet sekä läpinäkyvät toimet parantavat yrityksissä tapahtuvaa tietojen hyödyntämistä, mutta erityisesti lisäävät rekisteröityjen luottamusta henkilötietojen käsittelytoimiin¹⁵⁰. Yrityskaupan toteutuessa, siirtyvät henkilötiedot ostajalle osana kaupan kohdetta. Huomattavaa on, että tällöin salassapitosopimukset menettävät merkityksensä¹⁵¹.

Yrityskaupan toteuduttua, tulee ostajan informoida rekisteröityjä omistajan- ja rekisterinpitäjän vaihdoksesta riippumatta siitä, aiheuttaako vaihdos muutoksia rekisteröidyn ja rekisterinpitäjän väliseen suhteeseen¹⁵². Tietosuoja-asetuksessa säädetyn läpinäkyvän ja asianmukaisen käsittelyn periaatteiden mukaisesti, rekisteröidylle tulee ilmoittaa henkilötietojen käsittelystä ja sen tarkoituksista. Tietosuojavaikuttettu on kiinnittänyt erityistä huomioita 14.9.2009 antamassa ratkaisussaan (1467/44/2009) henkilötietojen käsittelyä koskevaan informointiin ja erityisesti siihen, että rekisterinpitäjänä työnantajalle säädetyt velvoitteet henkilötietojen käsittelyn informoinnista tulee toteutua¹⁵³.

Yrityksen kartoitettua yrityskauppaprosessin suunnitteluvaiheessa ja due diligence- tarkastuksen aikana henkilötietojen käsittelyn nykytilan, tulee sen toteutusvaiheessa selvittää, millaisia konkreettisia toimenpiteitä ja muutoksia tietosuoja-asetuksen sääntelytoiminnassa ja henkilötietojen käsittelyssä aiheuttaa. Toteutusvaiheen aikana yritykselle

¹⁴⁹ Katramo ja muut, 2013, s. 57, 67.

¹⁵⁰ Korpisaari ja muut, 2018, s. 648.

¹⁵¹ Vapaavuori, 2019, s. 637–638.

¹⁵² Kaisko & Warmo, 2007, s. 21.

¹⁵³ Tietosuojavaikuttettu 14.9.2009, 1467/44/2009.

tuleekin arvioitavaksi, ovatko tekniset ja organisatoriset toimenpiteet toteutuneet lainsäädännössä edellytetyin tavoin. Yrityksen on siten arvioitava myös henkilötietojen käsittelyn lainmukaisuus, luottamuksellisuus, eheys sekä läpinäkyvyys. Tietosuojatyön organisointi ja sen toteuttaminen tietosuoja-asetuksen vaatimusten täyttämiseksi sekä merkittävien sanktioiden välttämiseksi edellyttää yrityksiltä huolellista suunnittelua. Ei riitä, että noudatetaan tietosuojakysymyksissä lakia, vaan yrityksen ja etenkin rekisterinpitäjän on pystyttävä osoittamaan, miten lainsäädäntöä on organisaation toiminnan toteutuksessa ja suunnittelussa noudatettu. Tietosuoja-asetuksen myötä yritysten on myös varauduttava ongelmatilanteisiin, varmistamalla tietoturvasojen riittävyys¹⁵⁴.

Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY perustetun tietosuojaryhmän tietosuoja-asetuksen mukaista läpinäkyvyyttä koskevista suuntaviivoista laaditussa WP29-ohjeessa on todettu, että rekisterinpitäjän on kohtuullisuuden ja osoitusvelvollisuuden periaatteiden myötä huomioitava muutosten sekä kohtuullisten odotusten vaikutukset rekisteröityyn. Mikäli henkilötietoihin liittyvät muutokset johtavat käsittelyn luonteen perustavanlaatuisen muutokseen, kuten siirto kolmansiin maihin, tai sellaista muutosta, joka ei käsittelytoimen kannalta ole perustavanlaatuinen, mutta voi vaikuttaa rekisteröityyn tai olla tämän kannalta olennainen, on tiedot toimitettava tehokkaasti ja yksiselitteisesti asianmukaisen sekä kohtuullisen kohtelun periaatteita noudattaen, rekisteröidylle hyvissä ajoin ennen muutosten voimaantuloa. Tarkoituksena on varmistaa, ettei muutos jää rekisteröidyn toimesta huomaamatta sekä se, että rekisteröidyllä on kohtuullisesti aikaa käyttää tietosuoja-asetuksessa säädettyjä oikeuksiaan, kuten suostumuksen peruutus tai käsittelyn vastustaminen, sekä arvioida muutoksen vaikutuksia ja luonnetta¹⁵⁵.

Jotta henkilötietojen käsittelyn läpinäkyvyysvaatimus täyttyy, on henkilötietojen käsittelystä viestittävä rekisteröidylle selkeällä ja ymmärrettävällä tavalla sekä yksinkertaista

¹⁵⁴ Andersson & Ylipartanen, 2022, s. 45, 47.

¹⁵⁵ Tietosuojaryhmän (WP29) ohje, s. 16–17.

kieltä käyttäen niin, että tiedot ovat helposti rekisteröidyn saatavilla. Henkilötietojen lähde sekä niiden oikeusperuste vaikuttavat informoinnin tietosisältöön, rajoitusperusteisiin ja ajankohtaan. Läpinäkyvyyden periaate edellyttää myös rekisteröidyn oikeutta saada tieto, kuka toimii rekisterinpitäjänä ja mikä tarkoitus henkilötietojen käsittelyllä tosiasiallisesti on. Käsittelyn tarkoitukset tulee siten määrittellä ja ilmoittaa yksiselitteisesti henkilötietoja kerätessä. Läpinäkyvyys velvoittaa ilmoittamaan rekisteröidylle, jonka henkilötietoja käsitellään, riskeistä ja suojatoimista sekä tälle kuuluvista oikeuksista. Rekisterinpitäjän on näyttövelvollisuuden nojalla osoitettava, että rekisteröity on tullut tietoiseksi informaatiosta eikä annettu informaatio ole muuttunut¹⁵⁶.

Jotta henkilön oikeus tulla unohdetuksi sekä oikeus tietojen poistamiseen toteutuvat yrityskauppaprosessin toteutusvaiheessa, on rekisterinpitäjä tietosuoja-asetuksen mukaisesti velvollinen ilmaisemaan sen selkeästi henkilötietoja käsitteleville rekisterinpitäjille. Toteutusvaiheessa on siten arvioitava henkilötietojen käsittelyä tietosuoja-asetuksessa määriteltyjä rajoittavia menetelmiä, kuten tietojen siirtäminen toiseen järjestelmään ja käyttäjien pääsyn estäminen kyseisiin henkilötietoihin. Tietosuoja-asetuksen mukaan rekisterinpitäjän on toiminnallaan toteutettava kohtuulliset toimenpiteet, huomioiden käytettävissä olevat keinot ja teknologia.

Yleisessä tietosuoja-asetuksessa säädettyä henkilötietojen täsmällisyyttä sekä ajantasaisuutta korostaa yrityskauppaprosessin toteutusvaiheessa tietojen minimointivaatimus. Yrityksen tulee kaupan toteutusvaiheessa tietosuoja-asetuksessa tietosuojaperiaatteena säädetyn tietojen minimoinnin myötä arvioida ja tarkastaa, onko yrityksen keräämät tiedot tarpeellisia määritellyn käyttötarkoituksen kannalta. Jotta henkilötietojen käsittelyn eheys, luottamuksellisuus ja käytettävyys voidaan toteutusvaiheessa ja siirrossa taata tietosuoja-asetuksen edellyttämin tavoin, on tietojen oltava tarpeellisia tarkoitettuun käyttötarkoitukseen eikä muita tietoja tule yrityksen toimesta käsitellä tai luovuttaa¹⁵⁷.

¹⁵⁶ Hanninen ja muut, 2017, s. 48; Korpisaari ja muut, 2022, s. 181–182.

¹⁵⁷ Hanninen ja muut, 2017, s. 49–50.

Henkilötietoja käsiteltäessä ja luovuttaessa on syytä harkita tietojen tarkoitusta, alkuhetkeä sekä sitä, milloin käsittelylle ei ole enää tarvetta. Henkilötietoja voidaan pitää tarpeellisina silloin, kun ne ovat olennaisia ja asianmukaisia eivätkä liian laajoja käsittelyn tarkoitukseen nähden. Tietosuojalain 5 artiklan d kohta sisältää säädöksen henkilötietojen käsittelyn täsmällisyydestä. Periaatteen mukaisesti henkilötietojen tulee olla täsmällisiä, ajantasaista ja tarvittaessa päivitettyjä. Ennen henkilötietojen luovuttamista uudelle yritykselle, on tietosuojavaltuutetun 14.9.2009 antaman ratkaisun (1467/44/2009) mukaisesti käytävä läpi henkilörekisterissä olevien tietojen ajantasaisuus tarpeellisuusvaatimuksen mukaisesti. Rekisterinpitäjän tulee huolehtia, että tarpeettomia, epätäydellisiä, virheellisiä tai vanhentuneita henkilötietoja ei käsitellä¹⁵⁸.

Henkilötietojen käsittelijän tulee täsmällisyysperiaatteen ja virheettömyysvaatimuksen mukaisesti toteuttaa kaikki kohtuulliset tekniset ja organisatoriset toimenpiteet varmistukseen, että käsittelyn tarkoituksiin nähden virheelliset ja epätarkat tiedot oikaistaan tai poistetaan viipymättä¹⁵⁹. Tarpeellisuusvaatimuksen arviointiin liittyy hallituksen esityksen (HE 75/2000 vp) mukaisesti henkilörekisteriin talletettujen tietojen sekä rekisterin asianmukainen hävittäminen. Arvioidessa henkilötietojen käsittelyn tarpeellisuutta yrityskaupprosessin toteutusvaiheessa, on siten otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelystä rekisteröidyn yksityisyyden suojalle aiheutuva merkitys. Rekisterinpitäjän on ilman aiheetonta viivytystä poistettava tarpeeton tai vanhentunut tieto¹⁶⁰.

4.1 Tietojen siirto ja luovutus

Rekisterinpitäjä voi siirtää rekisteröityjen eli työntekijöiden henkilötietoja kolmansille osapuolille käsiteltäväksi tai siten, että vastaanottaneesta osapuolesta tulee tietojen re-

¹⁵⁸ Korpisaari ja muut, 2018, s. 93, 113; Tietosuojavaltuutettu 14.9.2009, 1467/44/2009.

¹⁵⁹ Krakau & Haapalehto, 2020, s. 198.

¹⁶⁰ HE 75/2000 vp, s. 17–18.

kisterinpitäjä. Kyseessä on tällöin henkilötietojen luovuttaminen, kun tiedot vastaanotaneesta yrityksestä tulee siirron jälkeen rekisterinpitäjä¹⁶¹. Henkilötietojen siirto tulee kyseeseen henkilötietojen käsittelyn ulkoistamisessa, kun henkilötietoja siirretään rekisterinpitäjän lukuun käsiteltäväksi käsittelijälle. Henkilötietojen käyttöä on valvottava koko siirtoprosessin ajan sekä varmistuttava siitä, etteivät tiedot ole ulkopuolisten saatavilla. Henkilötietojen luovuttamispäätöksen tai luovuttajan on varmistuttava siitä, että tietojen saajalla on oikeus luovutettavien henkilötietojen käsittelyyn. Sisäänrakennettu ja oletusarvoinen tietosuojaja edellyttää henkilötietojen luovutuksessa ja siirrossa ymmärrystä eri tietosuojaperiaatteista¹⁶².

Tietosuojavaltuutettu on 14.9.2009 antamassaan ratkaisussa (1467/44/2009) todennut, että ennen yritysjärjestelyn toteuttamista tulee yrityksille harkittavaksi yksityisyyden suojasta työelämässä annetun lain mukaisesti työsuhteen etujen, oikeuksien, velvollisuuksien sekä työtehtävien erityisluonteen kannalta välittömästi tarpeellisten tietojen luovuttaminen. On syytä kuitenkin korostaa, että työntekijöiden henkilötietoja voidaan tietosuojavaltuutetun ratkaisun mukaan luovuttaa ainoastaan sellaiseen tarkoitukseen, joka on yhteensopiva henkilörekisterille määritellyn käyttötarkoituksen kannalta, mikäli voidaan olettaa työntekijöiden tietävän tällaisesta henkilötietojen luovutuksesta¹⁶³.

Tietosuojavaltuutetun 14.9.2009 antaman ratkaisun mukaan liiketoiminnan siirron, liikkeen luovutuksen, sulautumisen tai muun yritysjärjestelyä suunnitellessa on tarkoin harkittava millä perusteilla ja millä hetkellä henkilötietoja voidaan luovuttaa uudelle omistajalle. Henkilötietojen muodostaessa henkilöstöhallinnon käyttöön tarkoitettun henkilörekisterin, ovat ne kokonaisuutena luovutettavissa vasta yrityskaupan tai muun yritysjärjestelyn toteutuessa tosiasiallisesti, esimerkiksi sopimuksella. On kuitenkin todettava,

¹⁶¹ Hanninen ja muut, 2017, s. 94–95.

¹⁶² Korpisaari ja muut, 2022, s. 320, 467, 693.

¹⁶³ Tietosuojavaltuutettu 14.9.2020, 1467/44/2009.

että henkilötietojen luovuttaminen on tarpeellisuusvaatimuksen täytyessä tietosuojavaltuutetun mukaan mahdollista myös suostumuksella. Tietosuojavaltuutetun käsityksen mukaisesti onkin tarkoituksenmukaista, että kaikkien työntekijöiden nimiluettelo yksityiskohtineen ei luovuteta uudelle yritykselle ennen yritysjärjestelyn toteutumista. Siitä huolimatta, etteivät kaikki henkilötiedot sisällä arkaluontoisia henkilötietoja, on niiden luonne pääsääntöisesti luottamuksellinen¹⁶⁴.

Yritys voi luovuttaa henkilötietoja ainoastaan, mikäli luovuttajalla sekä luovutuksensaajalla on laillinen peruste henkilötietojen käsittelyyn. Laillisenä perusteena voidaan tietosuojasetuksen mukaan pitää suostumusta, sopimusta, lakisääteistä velvoitetta, elintärkeää etua, yleistä etua tai julkisen vallan käyttöä sekä oikeutettua etua. Yrityksen luovuttaessa henkilötietoja toiselle yritykselle laaditaan usein kirjallinen luovutussopimus, johon sisällytetään tietojen luovutukseen liittyvät ehdot. Tietosuojasetuksessa ei ole säädöstä luovutussopimuksen laatimisvelvollisuudesta, mutta sen tekeminen on asianmukaista henkilötietojen luovuttamiseen liittyvien vaatimusten täyttymiseksi. Luovutussopimuksesta tulee ilmetä: 1) kohde eli henkilötietojen luovuttaminen, 2) perusteet luovuttamiselle, 3) tietosuojasetuksen mukaiset luovutukseen liittyvät velvollisuudet sekä 4) käytännön järjestelyt henkilötietojen luovutukselle eli mitä tietoja luovutetaan, miten luovutetaan turvallisesti, milloin tiedot luovutetaan sekä sopimuksen voimassaoloaika¹⁶⁵.

Yrityksen siirtäessä henkilötietoja on erityisin toimenpitein varmistettava, ettei siirron yhteydessä häviä henkilötietoja eikä siirto aiheuta muutoksia tietojen sisällössä¹⁶⁶. Tietosuojasetuksen 5 artiklan 1 kohdassa on säädetty tietojen eheydestä eli oikeellisuudesta. Yrityskauppaprosessissa säilytetyt tiedot tulee säilyä muuttumattomina. Yritysten tulee siten varmistaa, että yrityskaupan toteutusvaiheessa uudelle ostajalle siirtyvät tiedot ovat ajantasaisia eivätkä sisällä virheellisiä tai muuttuneita tietoja.

¹⁶⁴ Tietosuojavaltuutettu 14.9.2009, 1467/44/2009.

¹⁶⁵ Hanninen ja muut, 2017, s. 95.

¹⁶⁶ Korpisaari ja muut, 2018, 274.

Suosittelusten mukaisesti yrityksen tulee listata kaikki ne tahot, joilta henkilötietoja saadaan tai joille niitä luovutetaan. Esiin on myös tuotava, mikäli tietoja siirretään EU:n ulkopuolelle. Erityisen tärkeää osoitusvelvollisuuden kannalta on kirjata ylös henkilöiden annetut suostumukset ja mahdolliset peruutukset sekä se, miten varmistutaan, että suostumuksen peruutus otetaan huomioon käytännön toiminnassa¹⁶⁷. Henkilötietojen käsittelyn jatkuessa yrityskaupprosessin toteutusvaiheessa ja ostajan muuttuessa tosiasialliseksi rekisterinpitäjäksi tulee yrityksen siten arvioida, tarvitaanko käsittelyn toteuttamiseksi uusi oikeusperuste tai suostumus. Suostumuksen ollessa käsittelyn oikeusperuste, tarvitaan henkilötietojen siirron myötä usein uusi, yhteensopiviin käyttötarkoituksiin soveltuva, suostumus käsittelyn oikeudenmukaisuuden ja laillisuuden varmistamiseksi¹⁶⁸.

4.2 Kansainväliset tiedonsiirrot

Yleistä tietosuojasetusta sovelletaan Euroopan talousalueella (ETA). Tietosuojavaltuutetun ohjeiden mukaan tietosuojalainsäädännön keskeisin tavoite on henkilötietojen vapaan liikkuvuuden takaaminen ETA-alueilla. On kuitenkin syytä korostaa, että soveltaminen ulottuu henkilötietojen käsittelyyn, jota suoritetaan rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa unionin alueella, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei¹⁶⁹.

Liiketoiminnan tarpeet vaativat entistä yleisemmin henkilötietojen siirtoa, mitä erilaisimmissa tilanteissa, Euroopan unionin ulkopuolelle eli kolmansiin maihin. Tietosuojasetuksen keskeisenä periaatteena on, että tietoja voidaan siirtää ainoastaan asetuksen mukaisia edellytyksiä noudattaen. Vastaanottavan kolmannen maan on edellytysten mukaisesti komission päätöksellä katsottu tavoin varmistettava riittävä tietosuojan taso

¹⁶⁷ Hanninen ja muut, 2017, s. 53.

¹⁶⁸ Tietosuojavaltuutetun toimisto, *Käyttötarkoitussidonnaisuus*.

¹⁶⁹ Tietosuojavaltuutetun toimisto, *Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle*.

sekä se, että siirto toteutetaan asianmukaisia suojatoimia soveltaen¹⁷⁰. Tietojen luovuttajan ja siirtäjän on osoitusvelvollisuuden periaatteen mukaisesti kartoitettava tekemänsä tiedonsiirrot. Jotta tietosuojan tasosta voidaan varmistua, on siirrettävien tietojen tarpeellisuus, asianmukaisuus ja olennaisuus arvioitava aina erikseen¹⁷¹.

Euroopan unionin tuomioistuimen 6.10.2015 annetun tuomion (C-362/14) mukaan henkilötietojen käsittelyä koskevien kansallisten lainsäädäntöjen tavoitteena on varmistaa perusoikeuksien- sekä vapauksien kunnioittaminen. Henkilötietojen kansainvälinen siirto voidaan katsoa olevan tarpeen kansainvälisen kaupan kehittämiseksi. Tuomiossa on todettu, että henkilötietojen siirto on sallittua sellaisiin kolmansiin maihin, jotka voivat taata tietosuojan riittävän tason ja sen on säilyttävä kaikissa siirron vaiheissa riittävänä. Mikäli tietosuojan tasoa ei kolmannessa maassa voida pitää riittävän laisena, henkilötietojen siirto kyseiseen maahan tulee kieltää¹⁷².

Yleinen tietosuojasetus ei sisällä suoraa määritelmää henkilötietojen siirrolle. Tietosuojaneuvosto on määrännyt ETA-maiden ulkopuolelle tehtävien siirtojen tunnistamiseksi seuraavat kriteerit: 1) rekisterinpitäjän tai henkilötietojen käsittelijän toimintaan sovelletaan yleistä tietosuojasetusta käsittelyn osalta, 2) rekisterinpitäjä tai henkilötietojen käsittelijä luovuttaa tietoja siirtämällä tai muulla tavoin saattamalla toiselle organisaatiolle ja 3) organisaatio, joka vastaanottaa tiedot, sijaitsee ETA:n ulkopuolisessa maassa¹⁷³. Rajat ylittävä käsittely tarkoittaa tietosuojavaltuutetun toimiston vuoden 2019 toimintakertomuksen mukaisesti henkilötietojen käsittelyä, joka suoritetaan useammassa kuin yhdessä Euroopan unionin jäsenvaltiossa sijaitsevassa toimipaikassa, jonne rekisterinpitäjä tai henkilötietojen käsittelijä on sijoittautunut sekä käsittelyä, joka vaikuttaa merkittävästi useammassa kuin yhdessä jäsenvaltiossa oleviin rekisteröityihin,

¹⁷⁰ Hanninen ja muut, 2017, s. 97–98.

¹⁷¹ Korpisaari, 2022, s. 491.

¹⁷² EUT C-362/14, Schrems. v. Data Protection Commissioner, EU:C:2015:650.

¹⁷³ Euroopan tietosuojaneuvosto. Kansainväliset tiedonsiirrot.

mutta käsittely suoritetaan Euroopan unionissa rekisterinpitäjän tai henkilötietojen käsitteijän ainoassa toimipaikassa¹⁷⁴.

Tietosuoja-asetus asettaa kaksi pääsääntöistä perustetta henkilötietojen siirrolle ETA-alueiden ulkopuolelle: 1) tietosuojan riittävyttä koskeva päätös ja 2) jos päätöstä ei ole, asianmukaiset suojatoimet. Asetuksen 44 artikla sisältää säädökset henkilötietojen siirrostä kolmansiin maihin. Artiklan mukaan sellaisten henkilötietojen siirto, joita käsitellään tai on tarkoitus käsitellä kolmanteen maahan siirtämisen jälkeen, toteutetaan vain, mikäli rekisterinpitäjä sekä henkilötietojen käsitteijä noudattavat tietosuoja-asetuksessa vahvistettuja edellytyksiä. Henkilötietojen siirto kolmanteen maahan voidaan toteuttaa, mikäli komissio on päätöksellään arvioinut, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori varmistaa riittävän tietosuojan ta-son.

Henkilötietoja siirrettäessä Euroopan unionin jäsenvaltioiden tai Euroopan talousalueen ulkopuolelle tulee rekisterinpitäjän aina varmistua tiedon riittävästä tasossa kohdevaltiossa sekä tarvittaessa tehdä ilmoitus tietosuojavaltuutetulle henkilötietojen siirrosta¹⁷⁵. Yleinen tietosuoja-asetus asettaa rajoitukset henkilötietojen siirrolle ETA:n ulkopuolisiin maihin. Tietosuoja-asetuksen mukaan henkilötietoja voidaan siirtää poikkeustapauksissa ETA-alueiden ulkopuolelle ainoastaan sen 49 artiklan luvussa säädettyjen siirtope- rusteiden mukaisesti:

- Henkilön nimenomainen suostumus
- Henkilön ja organisaation välisen sopimuksen täytäntöönpano tai sopimusta edeltävien toimenpiteiden teko
- Rekisterinpitäjän ja toisen henkilön välisen sopimuksen täytäntöönpano
- Yleistä etua koskeva syyt
- Oikeusvaateen laatiminen, estäminen tai puolustaminen
- Elintärkeiden etujen suojaaminen

¹⁷⁴ K 13/2020 vp, s. 18.

¹⁷⁵ Kaisko & Warma, 2007, s. 20.

- Rekisteri

Tilanteissa, joissa mikään tietosuoja-asetuksen 49 artiklan mukainen peruste ei täyty, on tietoja mahdollista siirtää rekisterinpitäjän pakottavien oikeutettujen etujen vuoksi. Jotta voidaan arvioida, ovatko siirrot tarpeellisia, on suoritettava tarpeellisuustesti, jolla arvioidaan, onko henkilötietojen siirtoa pidettävä tarpeellisena. Tietoja siirtävän organisaation tulee tietosuoja-asetuksen 49 artiklan mukaisesti noudattaa myös muita säännöksiä, kuten asianmukaisen oikeusperusteen määrittäminen, tarvittavien turvatoimien toteuttaminen sekä tietojen minimointi¹⁷⁶.

Yleisessä tietosuoja-asetuksessa on säädetty yritystä koskevien sitovien sääntöjen eli BCR-sääntöjen käytöstä yhteistä taloudellista toimintaa harjoittavissa yritysryhmissä tapahtuvissa kansainvälisissä tietojensiirroissa. Yritystä koskevat BCR-säännöt tarkoittavat tietosuoja-asetuksen mukaan sellaisia henkilötietojen suojeluperiaatteita, joita jäsenvaltion alueelle sijoittunut rekisterinpitäjä tai henkilötietojen käsittelijä on sitoutunut noudattamaan henkilötietojen siirtoja tehdessään. Säännöt ovat sitovia ja niitä sovelletaan tietosuoja-asetuksessa säädetyn mukaisesti kaikkiin asianomaisiin yritysryhmän jäseniin, jotka harjoittavat yhteistä taloudellista toimintaa.

Unionin tuomioistuin on tulkinnut valtion valvonnalle asetettuja rajoituksia 16.7.2020 antamassaan päätöksessä C-311/18 tietosuojavaikuttettu vastaan Facebook Irlanti ja Maximilian Schrems. Tuomioistuin on katsonut, että unionin oikeutta, erityisesti yleistä tietosuoja-asetusta, sovelletaan henkilötietojen siirtoon, jonka jäsenvaltioon sijoittautunut toimija toteuttaa siirtämällä tiedot kolmanteen maahan sijoittautuneelle toimijalle kaupallisessa tarkoituksessa. Ratkaisussa unionin tuomioistuin on todennut, että tietosuojaan ja yksityisyyden suojaan liittyvien perusoikeuksien rajoittaminen tai niihin puuttuminen, (esimerkiksi henkilötietojen kerääminen, käyttö, tallentaminen tai levittäminen tarkoituksiin, joita varten niitä ei alkuperäisen tarkoituksen vuoksi siirretty, vaan kansallisen turvallisuuden tai tiedustelun tarkoituksiin) voidaan perustella ainoastaan,

¹⁷⁶ Euroopan tietosuojaneuvosto. *Kansainväliset tiedonsiirrot*.

mikäli se on ehdottoman välttämätöntä demokraattisessa yhteiskunnassa. Tuomioistuinten mukaan kaikki toimenpiteet on toteutettava lain mukaisesti ja niiden tarjottava väärinkäyttöä vastaan tarpeelliset toimet¹⁷⁷.

Euroopan tietosuojaneuvosto on vuonna 2021 antanut suositukset EU:ssa taatun henkilötietojen suojan noudattamisesta kansainvälisissä tietojen siirroissa. Jotta voidaan varmistaa henkilötietojen unionissa taattu suojan taso niitä käsiteltäessä, on tietojen viejien Euroopan tietosuojaneuvoston mukaan tunnistettava tiedonsiirtonsa eli siirrettävien henkilötietojen määränpää. Tiedon siirtäjien on varmistuttava siitä, että tiedot ovat olennaisia, asianmukaisia ja rajoittuvat ainoastaan siihen tarkoitukseen, mikä on käsittelyn kannalta tarpeen¹⁷⁸. Henkilötietojen siirtäminen unionista kolmansissa maissa oleville rekisterinpitäjille, henkilötietojen käsittelijöille tai muille vastaanottajille ei saisi tietosuojasetuksen mukaan vaarantaa luonnollisten henkilöiden tietosuojan tasoa. Siirto voidaan siten asetuksessa säädetyllä tavalla toteuttaa ainoastaan, jos rekisterinpitäjä tai henkilötietojen käsittelijä noudattaa yleisen tietosuojasetuksen säännöksissä vahvistettuja edellytyksiä.

Henkilötietojen suojaaminen on tapahduttava kaikkialla Euroopan unionissa tehokkaasti. Tämä edellyttää tietosuojasetuksen 11 kohdan mukaisesti rekisteröityjen henkilötietoja ja oikeuksia käsittelevien ja käsittelystä päättävien velvollisuuksien täsmentämistä ja vahvistamista, mutta myös valtuuksia valvoa henkilötietojen suojaan koskevien sääntöjen noudattamista. Huomioitavaa on kuitenkin se, että jäsenvaltioiden väliset eroavaisuudet henkilötietojen käsittelyssä suhteessa henkilöiden vapauksien ja oikeuksien suojeeluun, erityisesti henkilötietojen suojaan, voivat tietosuojasetuksen mukaan estää henkilötietojen vapaan liikkuvuuden Euroopan unionin alueella.

¹⁷⁷ Article 29 Data Protection Working Party, 2018, s. 5; EUT C-311/18, Tietosuojavaltuutettu v. Facebook Irlanti ja Maximillian Schrems, EU:C:2020:559.

¹⁷⁸ European Data Protection Board, Suositukset 1/2020, s. 3.

5 Integraatiovaihe ja jälkitoimet

Yrityskauppojen sopeuttamis- eli integraatiovaiheessa ostettu yritys integroidaan osaksi ostajayritystä kaupan vahvistamisen jälkeen. Integrointi on todettu olevan yrityskaupan kannalta vaikea ja hyvin herkkä vaihe. Tapauksesta riippuen tilanteisiin liittyy monenlaisia- ja tasoisia kysymyksiä, jotka on pystyttävä ratkaisemaan liiketoiminnalliset edellytykset varmistaen. Yrityskaupan kohteen integraatio eli yhdistäminen on tärkeässä roolissa yrityskaupan strategisten tavoitteiden saavuttamisessa, kun ostettu yritys yhteensoviteetaan ostavaan yritykseen. Huomioitavaa on, että menestyksen määrittely on aina syytä pitää tapauskohtaisena¹⁷⁹.

Yritysten yhdistäminen tuo organisaatioihin haasteita ja siinä onnistuminen vaatii huolellista suunnittelua. Integraatioprosessiin liittyy vahvasti ennen kaupan lopullista allekirjoitusta tapahtuva suunnittelu. Jotta kaupan vahvistumisen jälkeen suunnittelua ja toteutusta voidaan jatkaa, tulee suunnitteluvaiheessa luoda perusta integroinnille. Yleensä integroinnin suunnittelu kannattaa aloittaa, kun kaupan varmistuminen arvioidaan todennäköiseksi, esimerkiksi yhtäaikaisesti due diligence-prosessin kanssa. Tämä luo mahdollisuuden integraatioprosessissa mukana oleville henkilöille perehtyä kohdeyritykseen. Yrityskaupassa ostajalla intressinä on saada mahdollisimman täsmälliset ja virheettömät tiedot varmistaakseen kaupan jälkeisten henkilötietojen lainmukainen ja asianmukainen käsittely. Täsmälliset tiedot edesauttavat tunnistamaan ostajan oikeudelliseen turvallisuuden liittyvät riskit. Kaupan kohteen tarkistaminen on kuitenkin erilaisten seikkojen vuoksi enemmän tai vähemmän puutteellista. Myyjän intressissä ei ole pantata tietoa vaan antaa valmisteluvaiheessa ostajalle kaupan kohteesta oikeat ja mahdollisimman laajat ennakkotiedot¹⁸⁰.

Yrityskaupprosessin integraatiovaiheessa korostuu tietosuoja-asetuksessa säädetty läpinäkyvän informoinnin vaatimus, nimittäin merkittävin syy integraation

¹⁷⁹ Immonen, 2024, s. 55; Katramo ja muut, 2013, s. 443.

¹⁸⁰ Katramo ja muut, 2013, s. 420, 443–444; Yksilöiden suojelua henkilötietojen käsittelyssä käsittelevä työryhmä, 2010, s. 4.

epäonnistumiselle on arvioitu olevan epäselvät tavoitteet, vaativien johtamistaitojen puuttuminen sekä puutteelliset tiedonjako ja viestintätaidot¹⁸¹. Rekisteröidyn informointi on osa tietosuojan takaamista. Yrityskaupan vahvistamisen jälkeen tulee yrityksen informoida läpinäkyvin tavoin rekisteröidyille henkilötietojen käsittelyn nykytilasta, toimista joihin ollaan ryhtymässä sekä varmistettava asianmukaisten tointen kautta rekisteröidyn oikeuksien säilyminen. Erityisen tärkeää on huomioida se, että rekisteröity ymmärtää, miten tämän henkilötietoja yrityskaupan aikana ja sen jälkeen tullaan käsittelemään¹⁸².

Tietosuoja-asetuksen 5 artiklan 1 kohdassa on säädetty henkilötietojen käsittelyn laillisuudesta, kohtuullisuudesta sekä läpinäkyvyydestä. Henkilötietojen siirtyessä yrityskaupan yhteydessä uudelle ostajayritykselle, on prosessissa ja etenkin uuden käsittelyperusteen kannalta varmistettava tietosuojaperiaatteina säädetty lainmukaisuus, olennaisuus sekä käyttötarkoitussidonnaisuus. Tietosuoja-asetuksen mukaan henkilötietojen käsittelyn on oltava käyttötarkoitussidonnaista ja lähtökohtaisesti aina palveltava käsittelyn ensisijaista tarkoitusta. Käsittely katsotaan olevan ristiriidassa alkuperäisen käyttötarkoituksen kanssa, mikäli: 1) käsittely on odottamatonta, 2) käyttötarkoitus muuttuu olennaisesti sekä 3) käsittelystä aiheutuu epäoikeudenmukaisia seurauksia. Tietosuojaperiaatteena säädetyn käytettävyyden myötä, tulee yrityskauppaprosessin integraatovaiheessa varmistaa, että pääsy henkilötietoihin ja niiden käyttämiseen on rajoitettu ainoastaan käsittelyyn oikeutetuille henkilöille. Yritysten on kerättävä ainoastaan sellaisia tietoja, joiden tarpeellisuus on määritelty jo tietoja kerättäessä. Muita, kuin käyttötarkoitukseen tarkoitettuja henkilötietoja ei siten tule käsitellä eikä kerääminen voi perustua arvioon tietojen tarpeellisuudesta mahdollisesti myöhemmässä vaiheessa¹⁸³.

¹⁸¹ Katramo ja muut, 2013, s. 443–444.

¹⁸² Korpisaari ja muut, 2018, s. 174.

¹⁸³ Hanninen ja muut, 2017, s. 37, 49, 107; Tietosuojavaltuutetun toimisto, *Käyttötarkoitussidonnaisuus*.

Henkilötietojen käsittely yrityskauppaprosessin integraatiovaiheessa tulee perustua nimenomaiseen, tiettyyn ja lailliseen tarkoitukseen, eikä tietoja saa käyttötarkoitussidonnaisuuden myötä käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla¹⁸⁴. Henkilötietojen käsittely alkuperäisestä käyttötarkoituksesta poikkeavaan tarkoitukseen on tietosuojavaltuutetun mukaan mahdollista, mikäli suunniteltu käyttötarkoitus noudattaa tietosuojasäännöksiä. Vaatimuksena uudelle käyttötarkoitukselle on säännösten lisäksi ennen käsittelyn aloittamista saatava rekisteröidyn suostumus sekä laillinen käsittelyperuste¹⁸⁵.

Henkilötietojen käsittely muita, kuin niitä tarkoituksia varten, johon ne on kerätty, katsotaan tietosuoja-asteuksen mukaan sallituksi ainoastaan, jos käsittely sopii yhteen niiden alkuperäisen keräämistarkoituksen kanssa. Huomioon on kuitenkin otettava tietosuoja-asetuksen kohta 50, jonka mukaan rekisteröidyn antaessa suostumuksensa tai käsittelyn perustuessa unionin oikeuteen tai jäsenvaltion lainsäädäntöön, tulee rekisterinpitäjälle sallia henkilötietojen myöhempi käsittely riippumatta tarkoituksen yhteensopivuudesta. Kaikissa tilanteissa on kuitenkin varmistettava tietosuoja-asetuksen periaatteiden noudattaminen sekä ilmoitettava rekisteröidylle muista tarkoituksista sekä erityisesti tämän oikeuksista.

Yrityksen käsiteltäessä tietoja muuta, kuin sitä tarkoitusta varten, johon henkilötiedot on kerätty eikä käsittely perustu soveltuvaan lainsäädäntöön tai rekisteröidyn suostumukseen, on yrityksen huomioitava seuraavat asiat varmistaakseen, että käsittely on yhteensopivaa alkuperäisen tarkoituksen kanssa: 1) henkilötietojen keräämisen ja myöhemmän käsittelyn tarkoituksen yhteys, 2) henkilötietojen keräämisen asiayhteys, 3) henkilötietojen luonne, 4) mahdollisen myöhemmän käsittelyn seuraukset rekisteröidylle sekä 5) asianmukaisten suojatointen, kuten salaaminen ja pseudonymisointi olemassaolo¹⁸⁶.

¹⁸⁴ Korpisaari ja muut, 2018, s. 113; Krakau & Haapalehto, 2020, s. 198.

¹⁸⁵ Tietosuojavaltuutetun toimisto, *Käyttötarkoitussidonnaisuus*.

¹⁸⁶ Hanninen ja muut, 2017, s. 33.

5.1 Tietosuoja kaupan jälkeen

Lainsäädäntö sisältää vaatimuksen henkilötietojen käsittelyn oikeasuhtaisuudesta sekä tarpeellisuudesta. Yritysten on arvioitava säilytettävien henkilötietojen suhdetta yleisen edun mukaiseen arkistointitarpeeseen. Harkinnassa on huomioitava tietosuoja-asetuksen mukaiset tietosuojaperiaatteet, erityisesti tietojen minimoinnin periaate. Henkilötietojen on säilyttävä yrityskauppojen jälkeen asianmukaisena, olennaisina sekä rajoitettava ainoastaan siihen käyttötarkoitukseen, mikä on arvioitu tarpeelliseksi käsittelyn tarkoitukseen nähden¹⁸⁷.

Tietosuoja-asetuksen 5 artiklan 1 kohdassa on säädetty tietosuojaperiaatteena säilytyksen rajoittamisesta. Artiklan mukaan henkilötiedot tulee säilyttää muodossa, josta rekisteröity on tunnistettavissa vain siihen asti, kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. Henkilötietoja voidaan tietosuoja-asetuksen 5 artiklan e kohdan mukaisesti säilyttää pidempiä aikoja ainoastaan, jos henkilötietoja käsitellään yleisen edun mukaisia arkistointitarkoituksia tai historiallista tai tieteellistä tutkimustarkoitusta tai sellaisia tilastollisia tarkoituksia varten edellyttäen 89 artiklan 1 kohdan mukaisesti, että tietosuoja-asetuksessa vaaditut tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn vapauksien ja oikeuksien turvaamiseksi.

Rekisterinpitäjä ei oletusarvoisuuden nojalla saa säilyttää kerättyjä henkilötietoja kauempaa, kuin on välttämätöntä. Tietosuoja-asetuksen mukaisten henkilötietojen käsitelyä koskevien periaatteiden myötä rekisterinpitäjällä on oikeus säilyttää rekisterissä tunnistettavassa muodossa olevia henkilötietoja niin kauan kuin tietojenkäsittelyn tarkoituksen toteuttamista varten on tarpeen. Rekisterinpitäjän päättäessä henkilötietojen käsittelyn keinoista ja tarkoituksesta, on sen varmistettava yksilöiden henkilötietojen suojaus. Tämän varmistamiseksi, on rekisterinpitäjän tehtävä toimenpiteitä henkilötietojen

¹⁸⁷ Korpisaari ja muut, 2018, s. 114.

suojaamiseksi ja mahdollistettava yksilöiden oikeuksien käyttö¹⁸⁸. Suojatoimien ja toimenpiteiden, joilla periaate säilytyksen rajoittamisesta pannaan käytäntöön, on täydennettävä rekisteröityjen oikeuksia ja vapauksia. Henkilötietoja käsiteltäessä on määriteltävä ne tiedot, jotka ovat tarpeen tarkoituksen kannalta ja miten kauan niitä on säilytettävä. Rekisterinpitäjällä on oltava sellaiset sisäiset toiminnot ja menettelyt, jotka takaavat selkeän henkilötietojen anonymisoinnin ja/tai poistamisen. Rekisterinpitäjän on varmistuttava siitä, ettei poistettuja tietoja voida palauttaa tai anonymisoiduista tiedoista tunnistaa henkilöitä uudelleen¹⁸⁹.

Henkilötietojen käsittelyn tarpeen päätyttyä, tulee tietojen käsittely lopettaa ja mahdollisuuksien mukaan tiedot poistaa käytetyistä henkilötietorekistereistä. Rekisterinpitäjällä on velvollisuus antaa tiedot tällaisista, ei-lainmukaisista, tietojenkäsittelyistä ja virheellisistä tiedoista¹⁹⁰. Tarpeellisuusvaatimuksen tavoite on aiheuttaa tarpeen harkita henkilötietojen käsittelyä sekä tietojen tarpeellisuutta¹⁹¹. Tietojen ollessa tarpeettomia, tulee ne oletusarvoisesti poistaa tai anonymisoida¹⁹². Henkilötietojen käsittelyn perusteissa sopimussuhteeseen, tulee henkilötiedot sopimussuhteen tarkoituksen täytyttyä rekisterinpitäjän toimesta poistaa rekisteristä, ellei niiden käsittelylle löydy muuta perustetta¹⁹³.

Tietosuoja-asetus ei määrittele tarkkoja aikoja henkilötietojen säilytykselle, mutta minimoinnin periaate edellyttää mahdollisimman lyhyitä säilytysaikoja. Yrityskaupan toteutumisen jälkeen, on rekisterinpitäjän arvioitava henkilötietojen tarpeellisuutta ja säilytysaikaa kysymyksessä olevaa käyttötarkoitusta vasten. Rekisterinpitäjän on pystyttävä perustelemaan tarkoitus, arvioimaan, kuinka pitkään henkilötietojen säilyttäminen on asiakassuhteen päättymisen jälkeen tarpeen sekä esittämään syyt ja lailliset perusteet

¹⁸⁸ Euroopan tietosuojaneuvosto. *Rekisterinpitäjä tai henkilötietojen käsittelijä*.

¹⁸⁹ Euroopan tietosuojaneuvoston ohje 4/2019, s. 26.

¹⁹⁰ European Data Protection Board, 2023, s. 18; Neuvonen, 2014, s. 62.

¹⁹¹ Neuvonen, 2014, s. 62.

¹⁹² Korpisaari, 2022, s. 319.

¹⁹³ Korpisaari ja muut, 2018, s. 103.

henkilötietojen käsittelylle¹⁹⁴. Henkilötiedot tulee säilyttää muodossa, josta rekisteröity on tunnistettavissa niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten. Rekisterinpitäjän on säännöllisin väliajoin tarkasteltava, onko henkilötietojen säilyttäminen tarpeen vai tuleeko ne poistaa. Henkilötietoja on mahdollista säilyttää pidempiä aikoja, mikäli käsittely ulottuu ainoastaan yleisen edun mukaisiin tarkoituksiin. Henkilötiedot on kuitenkin säilytettävä sellaisessa muodossa, josta rekisteröity ei ole tunnistettavissa¹⁹⁵.

Rekisterinpitäjän on tiedettävä tarkasti, mitä henkilötietoja yritys käsittelee ja miksi. Tietosuojan säilytyksen rajoittamista koskevat seuraavat keskeiset tekijät: 1) anonymisointi sekä poistaminen ja niiden tehokkuus, 2) automatisointi, 3) säilytyskriteerit, 4) perustelut, 5) säilytyskantojen valvonta, 6) varmuuskopiot sekä 7) tiedon kulku¹⁹⁶. On huomiotava, että henkilötietoja ei saa käsitellä, mikäli tarkoitukset on mahdollista toteuttaa anonymoimalla tiedoilla. Rekisterinpitäjän on varmistettava käytössä olevien tietojärjestelmien ja muiden käsittelyprosessien säilytysaikojen säännöllisen arvioimisen sekä noudattamisen tukeminen¹⁹⁷.

5.2 Vastuiden jakautuminen

Yrityskauppaprosessin integraatiovaiheessa osapuolten on tarkoin arvioitava ja tiedostettava velvollisuudet ja vastuut välttääkseen lainsäädännössä turvattujen rekisteröidyn oikeuksien oikeudettoman vahingoittumisen. Tämä on huomiotava etenkin yrityskauppaprosessin jälkeen tehtävien toimien osalta. Myyjä ja ostaja ovat molemmat osaltaan vastuussa henkilötietojen lainmukaisesta käsittelystä, siirrosta sekä luovuttamisesta. Usein yrityskauppojen jälkeisissä riitatilanteissa on kyse lähes aina ostajan tarkastusvelvollisuudesta, myyjän tiedonantovelvollisuudesta tai myyjän antamista kaupan kohteen ominaisuuksien vaikutuksista¹⁹⁸.

¹⁹⁴ Tietosuojavaltuutetun toimisto. *Säilytyksen rajoittaminen*.

¹⁹⁵ Aalto-Setälä & Viitala, 2018, s. 13–15; Hanninen ja muut, 2017, s. 50.

¹⁹⁶ Euroopan tietosuojaneuvoston ohje 4/2019, s. 26–27.

¹⁹⁷ Tietosuojavaltuutetun toimisto. *Säilytyksen rajoittaminen*.

¹⁹⁸ Katramo ja muut, 2013, s. 420.

On huomattavaa, että henkilötietojen käsittelyyn liittyvät osapuolet eivät voi sopia vapaasti, kuka on käsittelijä, vaan roolit määräytyvät sen perusteella, kuka tosiasiallisesti käyttää päätösvaltaa henkilötietojen osalta ja kenen tarkoituksia varten käsittely tapahtuu¹⁹⁹. Voidaan kuitenkin todeta, että rekisterinpitäjä on vastuussa siitä, että toiminnassa noudatetaan yleistä tietosuojaa-asetusta. On henkilötietojen käsittelijän ja rekisterinpitäjän edun mukaista, että osapuolet sitoutuvat noudattamaan sopimusta ja ovat tietoisia sen tosiasiallisesta sisällöstä²⁰⁰. Henkilötietojen luovutustilanteissa tiedon luovuttanut yritys sekä tiedon vastaanottanut yritys vastaavat itsenäisesti tietosuojaa-asetuksen noudattamisesta henkilötietojen käsittelyssä. Tiedot luovuttaneella yrityksellä on velvollisuus rekisteröidyn pyynnöstä ilmoittaa käsittelyn rajoitukset, tehdyt oikaisut tai poistot²⁰¹.

Yleisen tietosuojaa-asetuksen 5 artikla sisältää henkilötietojen käsittelyä koskevat periaatteet. Rekisterinpitäjän tulee vastata 5 artiklassa säädetyistä henkilötietojen käsittelyä koskevista periaatteista, nimittäin tietosuojaperiaatteita noudatettaessa jokaisessa henkilötietojen käsittelyn vaiheessa, tulee rekisterinpitäjän pystyä osoittamaan, että näin on toimittu. Osoitusvelvollisuuden täyttääkseen on rekisterinpitäjän arvioitava, mitä tietosuojaperiaatteet tarkoittavat käytännössä ja miten ne ilmenevät toiminnassa. Rekisterinpitäjän ja henkilötietojen käsittelijän on tietosuojaa-asetuksen mukaan suojattava henkilötiedot sellaisilla suojaustoimenpiteillä, jotka vastaavat henkilötietojen käsittelyyn liittyviä riskejä. Yrityksen on pystyttävä tietosuojaa-asetuksessa säädetyllä tavalla osoittamaan, että toiminta täyttää asteuksessa sovellettavat velvoitteet sekä laadittava ja säännöllisesti päivitettävä kirjallisesti laadittuja ohjeita ja menettelytapoja. Yrityksen on siten kuvattava henkilötietojen käsittelyyn liittyvät prosessit sekä dokumentoitava tietosuojaa-periaatteiden noudattaminen. Tämä edellyttää yrityksiltä suunnittelua, dokumentaatiota sekä varautumista²⁰².

¹⁹⁹ Korpisaari ja muut, 2018, s. 296.

²⁰⁰ Euroopan tietosuojaneuvosto. *Rekisterinpitäjä tai henkilötiedon käsittelijä*.

²⁰¹ Hanninen ja muut, 2017, s. 94–95.

²⁰² European Data Protection Board, 2020, s. 3; Hanninen ja muut, 2017, s. 51–52; Korpisaari ja muut, 2018, s. 28.

Henkilötietojen käsittelyyn liittyvät vastuut ovat Euroopan yleisen tietosuoja-asetuksen ja muun tietosuojasääntelyn seurauksena muodostuneet hyvin moniulotteisiksi. Tietosuojavastuun kohdentumisen lähtökohdaksi nousee rekisterinpitäjän tai henkilötietojen käsittelijänä toimivan oikeushenkilön tai luonnollisen henkilön vastuu. Pääsääntöisesti vastuu henkilötietojen käsittelystä kiinnittyy oikeushenkilöön, joka on toiminut rikkomuksen aikana rekisterinpitäjänä tai käsittelijänä. Tietosuoja-asetuksen seuraamusmekanismien perusteella yksittäisestä rikkomuksesta johtuva vastuu sekä siihen liittyvät hallinnolliset seuraamukset tulisi arvioida tietosuojaviranomaisen toimesta erillisesti ja itsenäisesti²⁰³.

Rekisterinpitäjällä sekä henkilötietojen käsittelijällä on oltava ajantasainen tieto henkilötietojen käsittelyyn liittyvistä vastuista. Tietosuoja-asetuksen 30 artikla asettaa rekisterinpitäjälle veloitteen käsittelytoimiin liittyvän selosteen ylläpidosta. Artiklan mukaan jokaisen rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan on ylläpidettava vastuullaan olevista käsittelytoimista selostetta. Käsittelyseloste toimii yrityksen sisäisenä asiakirjana, joka pyrkii ohjaamaan henkilötietojen käsittelyn suunnittelua sekä tietosuojalainsäädännön mukaisen toiminnan toteutumisen osoittamista. Henkilötietojen käsittelijällä on velvoite laatia käsittelytoimistaan seloste, mikäli: 1) organisaatiossa on yli 250 työntekijää, 2) käsittely aiheuttaa todennäköisen riskin rekisteröidyn vapauksille ja oikeuksille, 3) käsittely ei ole satunnaista sekä 4) henkilötiedot sisältävät erityisiin tietoryhmiin liittyviä tietoja²⁰⁴. Tietosuojavaltuutettu on 18.5.2020 antamassaan ratkaisussa (137/161/2020) todennut, että rekisterinpitäjän palveluksessa ollessa alle 250 työntekijää, tulee sen laatia ja ylläpitää selostetta käsittelytoimista, mikäli työntekijöiden henkilöiden käsittely kohdistuu erityisiin henkilötietoryhmiin ja on säännöllistä²⁰⁵.

²⁰³ Lång ja muut, 2022, s. 175.

²⁰⁴ Andersson & Ylipartanen, 2022, s. 188; Korpisaari ja muut, 2018, s. 299; Tietosuojavaltuutetun toimisto, *Henkilötietojen käsittelijän seloste käsittelytoimista*.

²⁰⁵ Tietosuojavaltuutettu 18.5.2020, 137/161/2020.

Tietosuoja-asetuksesta ilmenee, että vastuussa henkilötiedoista ja niiden käsittelystä ovat yrityskaupan toimijat. Organisaatioilla on vastuu heidän hallussaan olevista henkilötiedoista. Vastuun alaan voivat sisältyä asianmukaisten vastuuvollisuusstoimenpiteiden käyttöönotto tai asianmukaisen due diligence-tarkastuksen suorittaminen yrityskauppoja tehtäessä, sen arvioimiseksi, miten henkilötietoja on hankittu tai miten niitä suojataan. Henkilötiedoilla on todellinen arvo, joten organisaatioilla on lakisääteinen velvollisuus varmistaa niiden turvallisuus²⁰⁶. Huomioitavaa on, että mikäli tietoihin ja niiden käsittelyyn on kytköksissä rekisterinpitäjää koskevia erityisiä vaatimuksia tai rajoituksia, siirtyvät ne tietojen vastaanottajaa velvoittaviksi²⁰⁷.

Yleisen tietosuoja-asetuksen mukaan kyseessä on tietoturvaloukkaus, mikäli yrityksen vastuulla olevia tietoja on luovutettu, laittomasti tai vahingossa, valtuuttamattomille vastaanottajille tai kun tietoja on muutettu tai niihin pääsy tilapäisesti estetty. Mikäli tietoturvaloukkaus tapahtuu ja aiheuttaa riskin henkilön vapauksille ja oikeuksille, tulee siitä ilmoittaa tietosuojaviranomaiselle. Yritys voidaan myös velvoittaa ilmoittamaan tietoturvaloukkauksesta asiaan kuuluville tahoille, riskin suuruudesta riippuen. Tietosuoja-vastuun lähtökohdat rakentuvat ajatuksen ympärille siitä, että vastuun tietosuojarikkomuksesta kantavat rekisterinpitäjänä tai henkilötietojen käsittelijänä toimiva oikeushenkilö tai luonnollinen henkilö taikka molemmat yhdessä tai erikseen. Pääsäännön mukaan, mikäli kyseessä on oikeushenkilö, kohdentuu organisatorisissa ja oikeudellisissa muutostilanteissa vastuu ensisijaisesti oikeudellisen seurannon mukaan. Vastuu kiinnittyy siten oikeushenkilöön, joka on toiminut rekisterinpitäjänä tai käsittelijänä rikkomuksen aikaan²⁰⁸.

Tietosuoja-asetuksen ja muun tietosuojasäätelyn myötä henkilötietojen käsittelyyn liittyvät vastuut ovat muodostuneet hyvin moniulotteisiksi. Ennen tietosuoja-asetuksen soveltamista, perustuivat tietosuojavelvoitteiden rikkomisesta aiheutuvat seuraamukset

²⁰⁶ European Data Protection Board, 2019.

²⁰⁷ Korpisaari ja muut, 2018, s. 420.

²⁰⁸ Lång ja muut, 2022, s. 174.

pääsääntöisesti yksittäisten tietojenkäsittelystä vastuussa olleen henkilön rikosoikeudelliselle vastuulle. Oikeushenkilön, kuten yritys tai organisaatio, rangaistusvastuusta ei ollut säädetty, joten rikosvastuun kohteena saattoi olla ainoastaan luonnollinen henkilö. Tietosuoja-asetuksen myötä henkilötietojen käsittelyyn liitettävä rikosoikeudellinen vastuu voidaan kytkeä ainoastaan sellaisiin tilanteisiin, joissa asetuksen nojalla lainvastainen käsittely ei ole hallinnollisten seuraamusmaksujen piirissä. Muutoksen myötä, tietosuojarikoksen mukainen rangaistussäännös tulee sovellettavaksi vain tilanteissa, joissa menettelyyn syyllistyneen henkilön ei voida katsoa toimineen tietosuoja-asetuksen määrittelemän henkilötietojen käsittelijän tai rekisterinpitäjän ominaisuudessa²⁰⁹.

Laiminlyöntien ja niistä aiheutuvien vahinkojen ilmeneminen pitkänkin ajan kuluttua, on katsottu olevan henkilötietojen käsittelyn erityispiirre. Tietosuojarikkomukseen syyllistyneen tahon liiketoiminnan siirtyessä uudelle rekisterinpitäjälle tai uusille omistajille kokonaisuudessaan, on tietosuojavaaluttetun toimisto linjauksessaan katsonut, että vastuu seuraa mukana. Vaikeasti tunnistettuihin laiminlyönteihin liittyy erinäisiä riskejä taloudellisista seuraamuksista, mutta miten ostajalla on mahdollisuus varautua tietosuojavaaluttuuseen, jonka olemassaoloa ei ole tunnistettu²¹⁰?

Henkilötietojen tietoturvaloukkauksesta on tietosuojavaaluttetun toimiston vuonna 2019 toimintakertomuksen mukaisesti ilmoitettava tietosuojavaaluttetun toimistolle, mikäli loukkauksesta voi aiheutua riskejä luonnollisten henkilöiden vapauksille ja oikeuksille²¹¹. Tietosuoja-asetuksen 6 artiklan e kohta sisältää säädöksen yleistä etua koskevan tehtävän suorittamisperusteen lainmukaisuudesta. Asetuksen mukaan henkilötietojen käsittely katsotaan täyttävän lainmukaisuuden, mikäli käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttä-

²⁰⁹ Lång ja muut, 2022, s. 173.

²¹⁰ Renko, 2022.

²¹¹ K 13/2020 vp, s. 17.

miseksi. Rekisterinpitäjän on tietosuojasetuksessa säädetyn oikeutetun edun mukaisesti ilmoitettava mahdollisista rikollisista teoista tai yleiseen turvallisuuteen kohdistuvista uhista sekä toimitettava olennaiset henkilötiedot toimivaltaiselle viranomaiselle.

Esimerkkinä yrityskaupan jälkeisten toimenpiteiden merkityksestä tietosuojariskien hallinnassa toimii worst case scenario-tyyppisenä varoittavana esimerkkinä tietosuojan ja tietoturvan laiminlyönnistä tunnettu tapaus Psykoterapiakeskus Vastaamo. Lokakuussa 2020 paljastunut tietomurto sekä sitä seurannut kiristys havahduttivat niin yrittäjät, kansalaiset sekä päättäjät tietosuojan merkityksestä. Psykoterapiakeskus Vastaamon toimintaan lukeutuu lukemattomien, erittäin luottamuksellisten, asiakastietojen käsittely ja hallinnointi. Psykoterapiakeskuksen palomuriin tehdyn muutoksen myötä, avautui internettiin potilastietokanta. Tähän erittäin luottamuksellisia tietoja sisältävään asiakastietokantaan murtauduttiin vuonna 2018 sekä toistamiseen vuonna 2019²¹².

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä tietosuojavaltuutetun toimistolle. Psykoterapiakeskus Vastaamon tapauksessa näin ei kuitenkaan toimittu, vaan yritys vaikeneti tapahtuneesta. Tietosuojavaltuutetun toimiston tekemän tutkimuksen mukaan yhtiön katsottiin lainvastaisella toiminnalla laiminlyöneen velvollisuutensa henkilötietojen käsittelyn turvallisuudesta huolehtimiseen. Mikäli katsotaan, että henkilötietojen tietoturvaloukkauksesta aiheutuu korkea riski henkilön oikeuksille ja vapauksille, tulee siitä ilmoittaa rekisteröidylle ilman aiheetonta viivytystä. Psykoterapiakeskus Vastaamo laiminlöi velvollisuuksiaan, jättäessään ilmoittamatta rekisteröidylle tapahtuneesta heti²¹³.

²¹² Keller, 2023, s. 21.

²¹³ Järvinen, 2022, s. 29; Tietosuojavaltuutetun toimisto. *Tietoturvaloukkaukset*.

6 Johtopäätökset

Tämän tutkimuksen tavoitteena oli selvittää, miten Euroopan unionin yleinen tietosuojasetus (GDPR), tietosuojalaki sekä yksityisyyden suojasta työelämässä annettu laki, Euroopan perusoikeuskirja, kansalliset sopimukset sekä tietosuojavaltuutetun ja tietosuojatyöryhmän ohjeet vaikuttavat henkilötietojen käsittelyyn ja millaisia rajoja ne asettavat yrityskauppojen osalta. Tutkimuksessa tutkittiin lainsäädännön asettamia oikeusperusteita sekä velvollisuuksia henkilötietojen käsittelylle, yrityskaupprosessille ominaisten vaiheiden kautta. Tutkimuksessa tarkasteltiin myös henkilötietojen käsittelyn ytimen eli luottamuksellisuuden, eheyden sekä lainmukaisuuden säilymistä yrityskaupprosessin eri vaiheissa.

Teknologian kehittyessä, sääntelyn lisääntyessä ja tietomäärien kasvaessa ovat ihmiset entistä kiinnostuneempia omien henkilötietojen käsittelystä sekä tietosuojan tasosta. Henkilötietojen tärkeys organisaatioiden toiminnassa onkin tunnistettu kasvavissa määrin. Erilaisten yritysjärjestelyiden käsittelyyn liittyvät vaatimustenmukaisuudet sekä erilaiset toiminnot ovat olleet selvitysten keskiössä. Organisaatiot ovat tämän myötä ryhtyneet arvioimaan tarkemmin omien henkilötietojen käsittelytehtäviensä sekä toimintojensa läpikäyntiä. Oikeuksia käyttäessä on aina syytä muistaa vastuu, nimittäin henkilötietojen käsittelyssä ei ole varaa väärinkäytöksille tai asiattomille tiedusteluille²¹⁴.

Ensimmäisenä tutkimuskysymyksenä oli selvittää, miten henkilötietojen suoja ja yleisen tietosuojasetuksen mukainen käsittely voidaan turvata yrityskaupoissa, erityisesti due diligence-prosessissa. Tietosuojassa on kyse paljon suuremmasta, kuin tietojen panttaamisesta, salaamisesta tai kätkemisestä²¹⁵. Henkilötiedot muodostavat osan perusoikeutena suojattua yksityisyyden suojaa, liittyessään kiinteästi henkilöiden identiteettiin²¹⁶. Yrityksellä ollessa velvollisuus yrityskaupprosessissa huomioida harjoittamansa henki-

²¹⁴ Korpisaari ja muut, 2022, s. 755.

²¹⁵ Andersson & Ylipartanen, 2022, s. 13.

²¹⁶ Lehtioksa ja muut, 2019, s. 865.

lötietojen käsittelyn laajuus, asiayhteys, luonne sekä rekisteröidyn oikeuksiin ja vapauksiin kohdistuvat riskit, on käsittelyn oltava suunnitelmallista sekä dokumentoitavissa²¹⁷. Henkilötietojen suoja sekä yleisen tietosuoja-asetuksen mukainen käsittely voidaan yrityskaupan aikana varmistaa seuraavat kohdat toteuttamalla: 1) henkilötietojen kartoitus, 2) käyttötarkoituksen selvittäminen ja tietojen järjestäminen, 3) riskiarvion tekeminen, 4) toimintatapojen suunnittelu sekä 5) dokumentaatio²¹⁸.

Perustuslakivaliokunta on lausunnossaan (PeVL 14/2018 vp – HE 9/2018 vp) todennut, että Euroopan unionin perusoikeuskirjassa turvattuihin oikeuksiin sovellettava ja tulkittava tietosuoja-asetus, muodostaa yksityiskohtaisella sääntelyllään riittävän säännöspohjan perustuslain 10 §:ssä turvatun henkilötietojen- ja yksityiselämän suojan kannalta. Tietosuoja-asetuksen sääntely vastaa valiokunnan käsityksen mukaisesti asianmukaisella tavalla sovellettuna ja tulkittuna myös Euroopan ihmisoikeussopimuksessa määrättyä henkilötietojen suojan tasoa. Henkilötietojen suojan taso on perustuslakivaliokunnan mukaisesti turvattava kansallisen yleislainsäädännön sekä yleisen tietosuoja-asetuksen nojalla²¹⁹.

Henkilötietojen turvallinen käsittely on osa henkilötietojen suojaa. Tietojen, järjestelmien sekä palvelujen suojaaminen toteutetaan osana tietoturvaa. Se takaa tietojen eheyden, luottamuksellisuuden ja käytettävyyden teknisten ja organisatoristen toimenpiteiden avulla. Siten henkilötiedot ovat ainoastaan niiden käyttöön oikeutettujen henkilöiden saatavilla eikä tietoja voida ulkopuolisten toimesta hyödyntää tai toisin muuttaa. Luottamuksellisuus turvaa tietojen salassapidon, eheys turvaa luotettavuuden sekä virheettömyyden ja saatavuus turvaavat sen, että henkilötiedot ovat ainoastaan niiden käyttöön oikeutettujen hyödynnettävissä²²⁰.

²¹⁷ Hanninen ja muut, 2017, s. 16.

²¹⁸ Korpisaari ja muut, 2018, s. XVII.

²¹⁹ PeVL 14/2018 vp – HE 9/2018 vp.

²²⁰ Korpisaari ja muut, 2018, s. 306–307.

Rekisterinpitäjän toiminnan ollessa läpinäkyvää, on ihmisen helpompi rakentaa luottamusta ja hyväksyä erilaiset henkilötietojen käsittelytilanteet²²¹. Luottamuksella on merkittävä vaikutus henkilötietojen käsittelylle yrityskauppaprosessin aikana. Yrityskaupan eri vaiheissa on erityisen tärkeää varmistaa lainsäädännön mukainen rekisteröidyn oikeus valvoa omien henkilötietojen käsittelyä, mutta myös vahvistaa oikeusvarmuutta sekä luottamusta henkilötietojen käsittelyssä²²². Yrityskauppaprosessin eri vaiheissa säilyvä avoimuus lisää uskottavuutta sekä luotettavuutta. Mitä enemmän informaatiota prosessin aikana on saatavilla, sitä nopeammin osapuolten näkemykset yhtenevät ja prosessin tehokkuus kasvaa²²³.

Due diligence-prosessin pyrkiessä ostajan tietoisuuden lisäämiseen sekä virhevastuun kaventamiseen, arvioi se myös henkilötietoja sisältävien rekisterien nykytilaa. Due diligence-prosessilla ollessa merkittävä rooli henkilötietojen suojan toteutumisessa ja käsittelyn suunnittelemisessa, on sen huolellinen toteuttaminen yksi tietosuoja-asetuksen mukaisen käsittelyn kulmakivistä. Due diligence-tarkastuksen myötä suoritettavassa arvioinnissa selvitetään henkilötietojen käsittelyyn vahvasti vaikuttavat tietosuoja-asetuksen asettamat velvoitteet ja etenkin se, mistä henkilötietoja hankitaan, miten niitä käsitellään ja mihin niitä voidaan lain puitteissa luovuttaa²²⁴.

Yrityskauppoihin vaikuttavat lainsäädännön asettamat rajat vaitiolo- ja salassapitovelvollisuudesta²²⁵. Tietosuoja-asetuksen 32 artiklassa on säädetty teknisten ja organisatoristen toimien toteuttamisesta henkilötietojen turvallisuustason varmistamisessa. Toimenpiteet on suhteutettava käsittelyn laajuuteen, luonteeseen, tarkoitukseen, asiayhteyteen sekä uusimpaan tekniikkaan. Tietoturvallisuuden tavoitteiden asettamiseksi ja niiden saavuttamiseksi tarvittavat tekniset ja organisatoriset toimet on arvioitava riskienhallinnan perusteella. Tietosuoja-asetuksen säännösten vastaisen käsittelyn estämiseksi

²²¹ Korpisaari ja muut, 2022, s. 755.

²²² Korpisaari ja muut, 2018, s. 37.

²²³ Katramo ja muut, 2013, s. 48.

²²⁴ Andersson & Ylipartanen, 2022, s. 96; Hanninen ja muut, 2017, s. 15–16; HE 75/2000 vp, s. 14; Katramo ja muut, 2013, s. 50–51, 409.

²²⁵ Immonen, 2024, s. 58.

sekä henkilötietojen käsittelyn turvallisuuden ylläpitämiseksi, on rekisterinpitäjän ja henkilötietojen käsittelijän arvioitava käsittelyyn olennaisesti liittyvät riskit ja toteutettava tarvittavat toimenpiteet niiden estämiseksi. Organisaation on jatkuvalla menettelyllä tutkittava, arvioitava sekä testattava teknisten ja organisatoristen toimien tehokkuutta sekä tarvittaessa salattava sekä pseudonymisoitava henkilötiedot eli käsiteltävä niitä siten, ettei tietoja voida yhdistää tiettyyn rekisteröityyn²²⁶.

Toisena tutkimuskysymyksenä oli selvittää tietosuojaan vaikutuksista tietojen siirtoihin ja luovutuksiin eri osapuolten välillä. Henkilötietojen luonne on luottamuksellinen. Tietosuoja asettaa rajat sille, millä perusteilla ja millä hetkellä henkilötietoja voidaan luovuttaa uudelle ostajalle. Sisäänrakennettu tietosuoja edellyttää henkilötietojen siirrossa ja luovutuksessa tietosuojaperiaatteiden vahvaa ymmärrystä sekä henkilötietojen käytön valvontaa koko yrityskauppaprosessin ajan. Henkilötietojen siirto on tietosuojaan myötä mahdollista, mikäli se perustuu asianmukaisten suojatoimien soveltamiseen, yritystä velvoittavien sitovien sääntöjen noudattamiseen, tietosuojaan riittävyttä koskevaan päätökseen tai erityistilanteita koskevaan poikkeukseen²²⁷.

Tiedon kansainvälinen siirto edellyttää tietosuoja-asetuksen mukaisesti riittävän tietosuojatason täyttymistä. Mikäli asetuksessa säädetyt edellytykset eivät täyty, on henkilötietojen siirto tietosuoja-asetuksen kohdan 107 mukaan kielletty. Yritys voi luovuttaa henkilötietoja ainoastaan laillisen perusteen täytyessä ja yritysjärjestelyn tosiasiallisesti toteutuessa. Tietosuojaan myötä yritysten on kaupan toteutuessa arvioitava ja tarkastettava kerättyjen henkilötietojen tarpeellisuus määriteltyyn käyttötarkoitukseen nähden²²⁸. Tietosuojaan pyrkiessä estämään henkilötietojen saavutettavuuden ulkopuolisille, tulee henkilötietojen käsittelijän koko yrityskauppaprosessin ajan, erityisesti luovutus ja siirtotilanteissa, varmistaa tietojen saajan oikeus siirrettävien tai luovutettavien henkilötietojen käsittelyyn²²⁹.

²²⁶ Korpisaari ja muut, 2018, s. 309–311; Hanninen ja muut, 2017, s. 107.

²²⁷ Korpisaari ja muut, 2022, s. 320, 465; Tietosuojavaltuutettu 14.9.2009, 1467/44/2009.

²²⁸ Hanninen ja muut, 2017, s. 49–50; Tietosuojavaltuutettu 14.9.2009, 1467/44/2009.

²²⁹ Korpisaari, 2022, s. 693.

Kolmantena tutkimuskysymyksenä oli selvittää, millaisia ongelmia tai riskejä henkilötietojen käsittelyyn yrityskauppaprosessissa liittyy. Yrityskauppojen toteuttamiseen sisältyy yleensä merkittäviä riskitekijöitä, joiden on arvioitu pohjautuvan järjestelyn kohteeseen, toteuttamiseen tai osapuoliin liittyvään epävarmuuteen. Hyvin suunniteltu ja toteutettu yrityskauppa ei kuitenkaan poista epävarmuustekijöitä, sillä osa tekijöistä on aina yrityksen oman kontrollin ulottumattomissa. Onnistuessaan yritysjärjestelyt ovat paras keino omistaja-arvon kasvattamiseen, mutta usein se nähdään ongelmatilanteita sisältävänä epäjatkumona. Merkittävimmät epävarmuudet liittyvät yrityskauppojen kohteeseen, osapuoliin sekä järjestelyn toteuttamiseen. Prosessin aikana voi ilmetä toisen osapuolen vilpillinen toiminta tai epäluotettavan tiedon antaminen. Kohteeseen ja osapuoliin liittyvät epävarmuustekijät ovat sidonnaisia onnistuneeseen integraatioprosessiin, arvostuksen löytymiseen sekä sidosryhmien tarpeiden huomioimiseen. Kohteeseen liittyvistä epävarmuuksista voidaan kuitenkin saada ennen prosessia hyvin rajallisesti tietoa²³⁰.

Henkilötietojen suojan lainsäädännön on arvioitu olevan sirpaleista. Yleisen tietosuojasetuksen 6 perustelukappaleessa on todettu, että globalisaatio ja teknologian nopea kehitys ovat lisänneet henkilötietojen käsittelyyn liittyviä riskejä ja haasteita. Teknologian mahdollistaessa yrityksille ja viranomaisille henkilötietojen ennennäkemättömän laajan käytön toiminnassaan, lisääntyy tietosuojasetuksen mukaan henkilötietojen kerääminen ja jakaminen merkittävästi. Oikeuskirjallisuudessa onkin nostettu esiin kysymys siitä, voidaanko teknologian kehityksen myötä henkilötietojen käsittelyyn liittyviä mahdollisia uhkia hallita lainsäädännöllä.²³¹ Tietosuojasetuksessa on todettu, että henkilötietojen käsittelyyn liittyvien vakavien riskien välttämiseksi, tulisi luonnollisten henkilöiden suojelun olla teknologianeutraalia eikä se saisi riippua käytetystä tekniikasta.

Tietosuojan monimutkaistumisen myötä henkilötiedon määritelmä eli se, mitä lainsäädännöllä suojataan, on muuttanut vuosien kuluessa muotoaan laajemmaksi. Tämä on puolestaan vaikuttanut lainsäädännön vaatimusten kasvuun, epä johdonmukaisuuteen,

²³⁰ Katramo ja muut, 2013, s. 59–60.

²³¹ Korpisaari ja muut, 2018, s. 3.

epäyhtenäisyyteen sekä lainsäädännön ymmärrettävyyden heikkenemiseen²³². Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY perustetun yksilöiden suojelua henkilötietojen käsittelyssä käsittelevän työryhmän mukaan henkilötietojen käsittelyssä vastuut tulee määritellä selvästi ja tehdä niiden soveltamisesta tehokasta. Työryhmä on todennut, että ei ole riittävää selvyyttä, keneltä mitään odotetaan, jolloin on olemassa riski, että säännökset jäävät tehottomiksi. Ratkaisevaksi haasteeksi nousee siten se, miten saadaan aikaan riittävän lainen selkeys siihen, miten tehokas käytännön soveltaminen ja toteuttaminen kyetään varmistamaan tai toteuttamaan. Työryhmän päätelmän mukaan, vastuussa tietosuojan rikkomisesta on kuitenkin aina rekisterinpitäjä eli oikeushenkilö (yritys) tai luonnollinen henkilö²³³.

Tietosuoja-asetuksen mukaan kansainvälinen kauppa sekä yhteistyön kehittäminen vaativat henkilötietojen rajat ylittävää siirtoa unionin ulkopuolisiin maihin sekä kansainvälisiin järjestöihin. Siirtojen lisääntyminen on kuitenkin luonut huolenaiheita ja haasteita. Henkilötietojen siirtäminen unionista kolmansissa maissa tai kansainvälisissä järjestöissä toimiville rekisterinpitäjille ei saa vaarantaa henkilöiden henkilötietojen suojan tasoa. Tietoturvaloukkauksista voidaan tunnistaa tiettyjä yhteisiä piirteitä. Tästä huolimatta tietosuojavaltuutetun toimiston vuoden 2019 toimintakertomuksessa on havaittu, että rekisterinpitäjien on vaikea todentaa ja yksilöidä ne henkilötiedot, jotka on päätyneet ulkopuolisille. Toimintakertomuksen mukaan kehitettävää on myös siinä, miten nopeasti rekisterinpitäjä havaitsee mahdolliset tietoturvaloukkaukset. Erityisesti pienten organisaatioiden kohdalla, voi yleisissä tietoteknisissä kyvyissä olla puutteita²³⁴.

²³² Keller, 2023, s. 211.

²³³ Yksilöiden suojelua henkilötietojen käsittelyssä käsittelevä työryhmä, 2010, s. 4–7.

²³⁴ K 13/2020 vp, s. 17.

Lähteet

Kirjallisuuslähteet

- Aalto-Setälä, M. & Viitaila, M. (2018). *Tietosuoja pähkinänkuoressa – Tietosuojaopas yrityksille*. Kauppakamari. Helsinki. Noudettu 9.2.2026 osoitteesta <https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf>
- Aarnio, A. (1989). *Laintulkinnan teoria: yleisen oikeustieteen oppikirja*. WSOY.
- Andersson, A., Koivisto, J. & Ylipartanen, A. (2016). *Tietosuojakäsikirja johdolle* (kolmas, uudistettu painos). Tietosanoma Oy.
- Andersson, A., Oravala, J. & Toivonen, M. (2023). *Tietosuoja ja yksityisyys – opas jokaiselle*. Tietosanoma Oy.
- Andersson, A. & Ylipartanen, A. (2022). *Osaava tietosuojavastaava ja EU:n yleinen tietosuoja asetetus (GDPR)* (toinen, uudistettu painos). Tietosanoma.
- Andersson, A., Riikonen, J. & Ylipartanen, A. (2017). *Osaava tietosuojavastaava*. Tietosanoma Oy.
- Andersson, J. (2024). *Organisaation hyvä tietoturvan sääntelyjärjestelmä*. Acta Wasaensia 536. Vaasan Yliopisto. Noudettu 19.3.2026 osoitteesta <https://osuva.uwasa.fi/server/api/core/bitstreams/c8164e24-6384-4352-ba90-56da7d703f5d/content>
- Andersson, J. (2018). *Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset*. Edilex. Noudettu 19.3.2026 osoitteesta <https://www-edilex-fi.proxy.uwasa.fi/artikkelit/18528.pdf>
- Blomquist, L., Blummé, N., Lumme, E., Pitkänen, T. & Simonsen, L. (2001). *Due Diligence osana yrityskauppaa*. KHT-Media Oy.
- Gustafsson, L. (2001). *Due diligence – Observations on Pre-Contractual Investigations in National and International Transactions*. Teoksessa Asianajotoimisto Borenius & Kempainen 90 vuotta. Gummerus kirjapaino Oy.

- Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. (2017). *Henkilötietojen käsittely – EU-tietosuoja-asetuksen vaatimukset*. Kauppakamari.
- Hietala, H., Järvensivu, P., Kaivanto, K. & Kyläkallio, K. (2021). *Yrityksen asiakirja- ja sopimusopas*. Alma Media Finland Oy.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. (2018). *Tutki ja kirjoita*. Tammi.
- Hirvonen, A. (2011.) *Mikä menet? Opas oikeustieteen metodologiaan*. Helsinki. Noudettu 23.10.2025 osoitteesta <https://helda.helsinki.fi/server/api/core/bitstreams/20149471-38b2-4cc8-94b7-2f6b3feed81d/content>
- Husa, J., Mutanen, A. & Pohjolainen, T. (2008). *Kirjoitetaan juridiikkaa: ohjeita oikeustieteellisten kirjallisten töiden laatijoille*. Talentum.
- Immonen, R. (2018). *Yritysjärjestelyt* (seitsemäs, uudistettu painos). Alma Talent Oy.
- Immonen, R. (2022). *Yritysjärjestelyt* (kahdeksas, uudistettu painos). Alma Talent Oy.
- Immonen, R. (2024). *Yritysjärjestelyt* (kymmenes, uudistettu painos). Alma Insights.
- Järvinen, P. (2022). *Yrityksen tietoturvaopas*. Kauppakamari.
- Kaisko, A. & Warma, E. (2007). Teoksessa: Tietosuoja. *Henkilötietojen käsittely yrityskaupoissa*. Tietoturvan ja tietosuojan erikoislehti.
- Katramo, M., Lauriala, J., Matinlauri, I., Niemelä, J., Svensas, K. & Wilkman, N. (2013.) *Yrityskauppa* (toinen, uudistettu painos). Alma Talent Oy. ISBN 978-952-63-1747-2
- Keller, M. (2023). *Mitä on tietosuoja*. Alma Talent Oy.
- Koskinen, S., Alapuranen, L., Heino, A-M. & Lehtonen, L. (2012). *Henkilötietojen käsittely työelämässä* (toinen, uudistettu painos). Edita.
- Korja, J. (2016). *Biometrinen tunnistaminen ja henkilötietojen suoja. Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta*. Acta Universitatis Lapponiensis 325. Hansaprint Oy. Noudettu 16.4.2026 osoitteesta https://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja_Juhani_ActaE_193_pdfA.pdf?sequence=2&isAllowed=y

- Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2018). *Uusi tietosuojalainsäädäntö*. Alma Talent.
- Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2022). *Tietosuoja* (toinen, uudistettu painos). Alma Talent.
- Krakau, T. & Haapalehto, S. (2020). *Tietopyynnöt ja henkilötietojen luovuttaminen: opas julkisuuslain mukaisten tietopyyntöjen ja tietosuoja-asetuksen mukaisten henkilötietojen tarkastuspyyntöjen käsittelyyn sekä muihin tietojen luovutuksiin*. Alma Talent Oy.
- Kurkela, M. & Ståhlberg, K. (1997). "*Due diligence*" yrityskaupassa ja osakkeenomistajan oikeus saada tietoa julkisesta osakeyhtiöstä. Defensor legis 1/1997. Edilex. Noudettu 8.3.2026 osoitteesta <https://www-edilex-fi.proxy.uwasa.fi/defensor legis/1001300081.pdf>
- Lehtioksa, J., Ljungman, J. & Vainio, S. (2019). *Tieto on valtaa – tietosuojalainsäädännön vastainen henkilötietojen käsittely määräävän markkina-aseman väärinkäytönä*. Defensor Legis N:o 6/2019. Edilex. Noudettu 20.1.2026 osoitteesta <https://www-edilex-fi.proxy.uwasa.fi/defensor legis/202690006.pdf>
- Lång, J., Kalliokoski, T. & El Asry, E. (2022). *Tietosuojavastuun kohdentuminen*. Defensor Legis 1/2022. Edilex. Noudettu 7.3.2026 osoitteesta <https://www-edilex-fi.proxy.uwasa.fi/defensor legis/1000490011.pdf>
- Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa*. Helsingin Kamari Oy. ISBN 978-952-246-230-5
- Raatikainen, A. (2002). *Yksityisyyden suoja työelämässä*. Edita Publishing Oy.
- Renko, A-K. (2022). *Yrityskaupat ja tietosuojavastuu*. Keski-Suomen kauppakamari. Noudettu 17.2.2026 osoitteesta <https://kskauppakamari.fi/fi-fi/article/blogi/yrityskaupat-ja-tietosuojavastuu/3702/>
- Tall, J. (2014). *Yrityskauppa ja strateginen uudistuminen*. Acta Wasaensia 536. Vaasan yliopisto. Noudettu 1.4.2026 osoitteesta <https://osuva.uwasa.fi/server/api/core/bitstreams/a57be31a-1d09-4a54-abea-a53ddb06759/content>

- Talus, A., Autio, E., Hänninen, A., Pihamaa, H-T. & Kantonen, S. (2017). *Miten valmistautua EU:n tietosuojasetukseen?* Oikeusministeriö. Noudettu 13.3.2026 osoitteesta <https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/>
- Vapaavuori, J. (2019). *Liikesalaisuudet ja salassapitosopimukset* (kolmas, uudistettu painos). Alma Talent.
- Voutilainen, T. (2012). *Oikeus tietoon. Informaatio-oikeuden perusteet*. Edita Publishing Oy.
- Vuola, L. (2009). *Environmental due diligence viranomaisen neuvonnan, salassapidon ja vastuun kannalta*. Edilex. Noudettu 7.3.2026 osoitteesta: https://www-edilex-fi.proxy.uwasa.fi/ymparistopolitiikka_ja_oikeus/177570006.pdf

Virallislähteet

European Data Protection Board (EDPB). *Huolehdi henkilötietojen turvallisesta käsittelystä*. Noudettu 4.4.2026 osoitteesta https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_fi

European Data Protection Board (EDPB). (2019). *ICO statement: Intention to fine the Marriot International, Inc more than 99 million under GDPR for data breach*. Noudettu 5.4.2026 osoitteesta https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-marriott-international-inc-more-ps99-million_en

European Data Protection Board (EDPB). (2021). *Suosituksset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan noudattamiseksi*. Versio 2.0. Noudettu 9.3.2026 osoitteesta https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fi.pdf

European Data Protection Board (EDPB). (2023). *Ohjeet 1/2022 rekisteröityjen oikeuksista – oikeus tutustua tietoihin*. Versio 2.1. Noudettu 31.3.2026 osoitteesta https://www.edpb.europa.eu/system/files/2024-04/edpb_guidelines_202201_data_subject_rights_access_v2_fi.pdf

European Data Protection Board (EDPB). (2021). *Suuntaviivat 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuojaa-asetuksessa*. Versio 2.0. Noudettu 25.3.2026 osoitteesta https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fi.pdf

Euroopan tietosuojaneuvosto. *Kansainväliset tiedonsiirrot*. Noudettu 14.2.2026 osoitteesta https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_fi

Euroopan tietosuojaneuvoston (EDPB) ohje 4/2019. *Ohjeet 4/2019 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta*. Versio 2.0, 20.10.2020.

Euroopan tietosuojaneuvosto. *Rekisterinpitäjä tai henkilötiedon käsittelijä*. Noudettu 14.2.2026 osoitteesta https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_fi

Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY perustetun tietosuojatyöryhmän ohje WP29. (2017). *Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat*. Noudettu 3.4.2026 osoitteesta <https://tietosuoja.fi/documents/6927448/8316711/Läpinäkyvyys+fi/c102605b-e386-4661-9b51-bf427875c8db?t=1535696089000>

Euroopan unionin tuomioistuin. (2024). *Aiheenmukainen muistio: henkilötietojen suoja*. Noudettu 31.1.2026 osoitteesta https://curia.europa.eu/site/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_fi.pdf

HE 75/2000 vp. *Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräksi siihen liittyviksi laeiksi*. Finlex. Noudettu 1.4.2026 osoitteesta <https://www.finlex.fi/fi/hallituksen-esitykset/2000/75>

HE 125/2003 vp. *Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräksi siihen liittyviksi laeiksi*. Finlex. Noudettu 13.3.2026 osoitteesta <https://www.finlex.fi/fi/hallituksen-esitykset/2003/125>

K 13/2020 vp. *Tietosuojavaltuutetun toimiston toimintakertomus 2019*. Tietosuojavaltuutetun toimisto. Noudettu 13.2.2026 osoitteesta <https://tietosuoja.fi/documents/6927448/10717840/Tietosuojavaltuutetun+toimiston+toimintakertomus+2019.pdf/a62e42ed-9fee-9bc4-7d74-ebf74c75173d/Tietosuojavaltuutetun+toimiston+toimintakertomus+2019.pdf?t=1608209826788>

PeVL 14/2018 vp – HE 9/2018 vp. *Hallituksen esitys eduskunnalle EU:n yleistä tietosuojasetusta täydentäväksi lainsäädännöksi*. Eduskunta. Noudettu 6.4.2026 osoitteesta https://www2.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_14+2018.aspx?TSPD_101_R0=0814c91602ab2000df69011d5c8762dbe4b0daeed4db2499fb4d9eb4be80fa0c00eed2aa14bf98dc08d86534501430002

07d12764734bcd2ec992783229be965a44a112aa41ef8b01b7aa1732e9838640a
02621b05945d78622f722aab6c0f7f

Tietosuojavaltuutettu 14.9.2009. Diaarinumero 1467/44/2009. *Henkilötietojen luovuttaminen yritysjärjestelyn yhteydessä*. Finlex. Noudettu 18.2.2026 osoitteesta <https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2009/88>

Tietosuojavaltuutettu 18.5.2020. Diaarinumero 137/161/2020. *Työnhakijoiden henkilötietojen kerääminen tarpeettomasti*. Finlex. Noudettu 6.4.2026 osoitteesta <https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2020/583>

Tietosuojavaltuutetun toimisto. *Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi*. Noudettu 12.3.2026 osoitteesta <https://tietosuoja.fi/arvioi-riskit>

Tietosuojavaltuutetun toimisto. *Henkilötietojen käsittelijän seloste käsittelytoimista*. Noudettu 1.4.2026 osoitteesta <https://tietosuoja.fi/henkilotietojen-kasittelijan-seloste-kasittelytoimista>

Tietosuojavaltuutetun toimisto. *Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle*. Noudettu 3.4.2026 osoitteesta <https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle>

Tietosuojavaltuutetun toimisto. *Käyttötarkoitussidonnaisuus*. Noudettu 16.4.2026 osoitteesta <https://tietosuoja.fi/kayttotarkoitussidonnaisuus>

Tietosuojavaltuutetun toimisto. *Pseudonymisoidut ja anonymisoidut tiedot*. Noudettu 1.4.2026 osoitteesta <https://tietosuoja.fi/pseudonymisointi-anonymisointi>

Tietosuojavaltuutetun toimisto. *Rekisterinpitäjän oikeutettu etu*. Noudettu 14.2.2026 osoitteesta <https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu>

Tietosuojavaltuutetun toimisto. *Säilytyksen rajoittaminen*. Noudettu 16.4.2026 osoitteesta <https://tietosuoja.fi/sailytyksen-rajoittaminen>

Tietosuojavaltuutetun toimisto. *Tietoturvaloukkaukset*. Noudettu 19.3.2026 osoitteesta <https://tietosuoja.fi/tietoturvaloukkaukset>

Yksilöiden suojelua henkilötietojen käsittelyssä käsittelevä työryhmä. (2010). *Lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*. Noudettu 17.2.2026 osoitteesta https://ec.europa.eu/justice/article-29/documenta-tion/opinion-recommendation/files/2010/wp169_fi.pdf

Oikeustapausluettelo

EU-tuomioistuin

Schrems. v. Data Protection Comissioner (6.10.2015). C-362/14, EU:C:2015:650. 62.

Data Protection Comissioner v. Facebook Ireland Ltd ja Maximillian Schrems (16.7.2020).
C-311/18. EU:C:2020:559. 64–65.

VB v. Bulgarian kansallinen verohallinto (14.12.2023). C-340/21. EU:C:2023:986. 27, 30.