Oikeusministeriö

EU:N YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET SUOMALAISIIN YRITYKSIIN

SISÄLTÖ

Oikeusministeriö

EU:N YLEISEN TIETOSUOJA-ASETUKSEN VAIKUTUKSET SUOMALAISIIN YRITYKSIIN

1 SELVITYKSEN KOHDE JA RAJAUKSET

Oikeusministeriö ("OM") on pyytänyt asianajaja Jukka Långia asianajotoimisto Dittmar & Indreniukselta ("D&I") tekemään vaikutustenarvioinnin EU:n yleisen tietosuoja-asetuksen (KOM(2012)11) ("Asetus") aiheuttamista muutoksista yksityisen sektorin rekisterinpitäjien toimintaan ja kustannuksiin, joita yrityksille muodostuu tietosuojavelvoitteiden huolehtimisesta.

Tämä muistio käsittää edellä kuvatun OM:n tilaaman vaikutusten- arviointiin kohdistuvan oikeudellisen selvitystehtävän ("selvitys") tulokset. Selvityksen tarkoituksena on toimia OM:n tausta-aineistona eduskunnalle annettavaan valtioneuvoston jatkokirjelmään, jolla eduskuntaa informoidaan EU-lainsäädäntöehdotuksista (U-kirjelmä U 21/2012).

Koska käytännössä kaikki suomalaiset ja Suomessa toimivat ulkomaiset yritykset käsittelevät liiketoiminnassaan tai muussa toiminnassaan henkilötietoina pidettävää dataa, yksityisen sektorin rekisterinpitäjiä koskevat tietosuojalainsäädäntöön perustuvat velvoitteet kohdistuvat käytännössä kaikkiin yrityksiin. Kyse on siis jo lähtökohdiltaan hyvin laajasti vaikuttavasta ja siten merkittävästä oikeudellisesta sääntelystä.

Selvityksen keskeisenä tarkoituksena on antaa yleiskäsitys siitä, miten tietosuojalainsäädännön muodostavat velvoitteet huomioidaan yritysten toiminnassa sekä mitkä niiden vaikutukset ovat yrityksiin kohdistuvien velvoitteiden myötä syntyvinä kustannuksina. Selvitys perustuu aiheesta yleisesti saatavilla oleviin tietoihin sekä D&I:lle yritysten neuvonantajaroolissa syntyneeseen kokemukseen ja markkinanäkemykseen.

Selvityksen pääkohde muodostuu Suomen voimassa olevan tietosuojalainsäädännön, erityisesti henkilötietolain (523/1999) ("HTL"), EU:n henkilötietodirektiivin (95/46/EY) ("Direktiivi") ja Asetuksen välisten keskeisten erojen erittelemisestä sekä näiden erojen vaikutuksen arvioimisesta suomalaisten yritysten näkökulmasta.

Tämän muistion laajuus on ollut saadun toimeksiannon perusteella rajoitettu. Selvitys ei käsittele kaikkia Asetuksen ja HTL:n tai muun

voimassa olevan tietosuojasäännöstön eroja tai säännöstön erojen vaikutuksia, vaan siinä keskitytään vaikutuksiltaan merkityksellisimpiin muutoksiin. Selvitys on valmisteltu tilanteessa, jossa Asetuksen lopullinen sisältö ei ole vielä varmistunut, joten asian arviointi on jouduttu perustamaan olettamille Asetuksen lopullisesta sisällöstä. Selvityksen tekemiseen käytettävissä oleva aika on rajoittunut marras-joulukuulle 2015. Muistion lopullinen versio on viimeistelty tammikuun 2016 alussa Asetuksesta käytyjen neuvotteluiden lopputulosten vahvistuttua.

Muistio ja selvityksen tulokset on laadittu yksinomaan OM:n käyttöön. Niiden sisältämien tulkintojen ei ole tarkoitettu toimivan yksittäisiin tapauksiin soveltuvina yleisinä oikeudellisina neuvoina eikä niitä voi tällaisessa tarkoituksessa käyttää.

Muistiossa on pyritty käyttämään lainsäädännössä määriteltyjä käsitteitä määritelmiä erikseen toistamatta. Viittauksissa artikla-numeroihin on käytetty sisällöltään hyväksyttyä uusinta tekstiversiota (EU-parlamentin LIBE-komitean 16.12.2015 julkistama versio), jonka artiklanumerointi tulee kuitenkin vielä lopullisessa asetusversiossa muuttumaan tässä muistiossa viitattavista neuvotteluissa käsitellyn version numeroinnista poikkeavaksi juoksevaksi numeroinniksi.

2 TIETOSUOJAVELVOITTEISTA HUOLEHTIMINEN YRITYKSISSÄ

2.1 Tietosuojasääntelyn merkitys yrityksille

Siinä, miten yritykset ottavat tietosuojan toiminnoissaan ja riskienhallinnassaan huomioon, on merkittäviä käytännön eroja.

Digitalisaation ja uusien teknologisten innovaatioiden kuten Big Datan ja teollisen internetin myötä tiedosta on tullut tai on tulossa huomattavalle osalle yrityksistä liiketoiminnan kannalta merkittävä tuotannontekijä. Tässä asetelmassa on luonnollista, että tietovarantoihin sisältyviin henkilötietoihin liittyvät tietosuojanäkökohdat ovat nousseet jo itsessään tärkeinä huomion kohteiksi.

Se mitä merkitystä yritykselle sisäisiä hallinnollisia velvoitteita luovalla oikeudellisella sääntelyllä on yrityksen käytännön toiminnan ja riskienhallinnan kannalta määräytyy erilaisten yleisten tekijöiden, kuten toimialan, koon, yhtiömuodon, omistusrakenteen ja kansainvälistymisen perusteella. Erityisen ilmeistä tämä on tietosuojasääntelyn suhteen.

Käytännössä isoilla yrityksillä on PK-yrityksiin verrattuna sekä erilaiset edellytykset että tosiasialliset intressit huolehtia tietosuojasääntelyn noudattamisesta.

Toisaalta myös liiketoiminnan luonne ja toimiala voivat vaikuttaa merkittävästi siihen, miten tietosuojavelvoitteet otetaan yrityksessä huomioon. PK-yritykseksi katsottavan tietointensiiviseen liiketoimintaan, kuten verkkokauppaan, suuntautuneen startup-yrityksen on jo liiketoiminnan edellytysten luomiseksi kiinnitettävä korostunutta huomiota tietosuojaan. Tällaiselle yritykselle tietosuoja on keskeisemmässä roolissa kuin esimerkiksi kymmenen kertaa suuremmalle metalliteollisuuden yritykselle, jolla ei ole kuluttaja-asiakkaita ja jonka valmistamiin tuotteisiin ei liity henkilötietojen käsittelyä.

Olennaista merkitystä on myös yrityksen käsittelemän datan luonteella. Kooltansa pieni terveydenhuoltoalan yritys saattaa käsitellä asiakkaidensa yksityisyyden suojan kannalta hyvin arkaluonteisia henkilötietoja, jolloin tietosuojan merkitys on toiminnan edellytysten luomisen ja riskienhallinnan kannalta ilmeinen.

Suurinta merkitystä tietosuojasääntelyllä on erityisesti kansainvälistä liiketoimintaa harjoittaville pörssiyhtiöille tai muuten suurille yrityksille, joiden liiketoimintaan liittyy toimialan perusteella laajamittaista yksityishenkilöasiakkaiden henkilötietojen käsittelyä (erityisesti vähittäiskaupan sekä finanssi-, media-, ja terveydenhuoltoalan yritykset sekä IT-palveluyritykset ja teleoperaattorit). Myös yrityskohtaisesti muotoutuneet riskienhallintakäytännöt korostavat tietosuojan merkitystä tämäntyyppisille yrityksille. Sääntelyn ja sen rikkomisesta seuraavien sanktioiden ohella tämäntyyppisten yritysten tietosuojakäytäntöjen järjestämiseen vaikuttavat olennaisesti tarve suojautua mahdolliseen tietosuojalaiminlöyntiin liittyvältä negatiiviselta julkisuudelta sekä asiakkaiden negatiivisilta reaktioilta.

Tietosuojan merkitys yrityksille määräytyy siis sääntelyn ohella olennaisesti sen mukaan, minkälaisen merkityksen yrityksen asiakkaat – ja osin myös työntekijät – omien tietojensa käsittelylle ja suojaamiselle antavat.

Tätä taustaa vasten on ilmeistä, että tietosuojalle yrityksissä annettu merkitys vaihtelee käytännössä hyvin paljon. Eri valtioita vertailtaessa merkitystä on myös historiallisilla ja kulttuurisilla syillä. Käytännössä tietosuojalla on Suomea keskeisempi merkitys monissa Keski- ja Etelä-Euroopan maissa, joissa yksilöt ovat lähtökohtaisesti suomalaisia tai muita pohjoismaalaisia huolestuneempia ja kiinnostuneempia henkilötietojensa käsittelystä.

Edellä kuvatuista syistä tietosuojasääntelyn taloudelliset vaikutukset yrityksiin vaihtelevat hyvin paljon yrityskohtaisesti.

2.2 Tietosuojasääntelyn lähtökohdat suhteessa erilaisiin yrityksiin

Sekä nykyisen Direktiiviin perustuvan tietosuojasääntelyn että Asetuksen lähtökohtana on samojen tietosuojaa koskevien velvoitteiden soveltaminen kaikkiin yrityksiin. Eroja yrityksille sääntelyn perusteella muodostuvien hallinnollisten velvoitteiden osalta voi kuitenkin syntyä siltä osin kuin säädösten on määritetty soveltuvan vain tietynlaisiin henkilötietoihin (esimerkiksi arkaluonteisiksi määritellyt henkilötiedot) tai tietynlaiseen toimintaan (esimerkiksi automaattinen päätöksenteko). Lisäksi Asetuksen sisältämä riskiarvioperusteinen velvoittavuus vaikuttaa siihen, miten sääntelyä on käytännössä erilaisissa yrityksissä noudatettava.

Asetus luo tietosuojasääntelyn soveltumiselle nykyistä Direktiiviä tai HTL:a selvemmin toiminnan erityispiirteistä tai kyseiseen toimintaan liittyvistä käytännön riskeistä lähtevät soveltamiskriteerit. Tietyiltä osin soveltamisen lähtökohdaksi on päätetty määrittää myös yrityksen koko (joko tietojen käsittelyn volyymin, työntekijämäärän tai vuotuisen liikevaihdon perusteella). Koska sääntely rakentuu kuitenkin tietojen käsittelyn kohteena olevien yksilöiden eikä tietoja käsittelevien yritysten lähtökohdista käsin, ei näille kriteereille muodostu keskeistä merkitystä, vaan jokaisen yrityksen on otettava tietosuojasääntely toiminnassaan huomioon.

2.3 Havaintoja nykykäytännöistä

Edellä kuvatulla tavoin tietosuojasääntely toisaalta näyttelee hyvin erilaista roolia yksittäisen yrityksen käytännön toiminnan näkökulmasta, mutta toisaalta lähtökohdiltaan soveltuu jokaiseen yritykseen. Koska tietosuojasääntely on luonteeltaan paikoin yleisluonteista, abstraktia ja tilannesidonnaista, on normiston käytännön huomioimisessa merkittäviä yrityskohtaisia eroja. Tällaisessa asetelmassa yhteneväiset käytännöt lainsäädännön noudattamisen suhteen olisi mahdollista – joskin ei välttämättä tarkoituksenmukaista – luoda tiukalla ja yhteneväisellä valvonnalla sekä ankaralla sanktioinnilla.

Tietosuojasääntelyn valvontaa voi kuitenkin Suomen tietosuojaviranomaisten – tietosuojavaltuutetun ja tietosuojalautakunnan – toimivaltuutuksien ja toimintakäytäntöjen perusteelta luonnehtia kansainvälisessä vertailussa varsin maltilliseksi. Se, että tietosuojalainsäädännön rikkomisesta ei voi ehdollisina tehostetarkoituksessa asetettavia ja

määrältään alhaisia uhkasakkoja lukuun ottamatta nykyisin seurata yritykselle muita taloudellisia sanktioita, on ollut myös omiaan vaikuttamaan siihen, että tietosuojasääntelyn huomioimista ei ole koettu kaikissa suomalaisyrityksissä yhtä keskeiseksi kuin samankaltaisissa toisissa EU-jäsenvaltioissa toimivissa yrityksissä. Yksikään iso suomalainen yritys ei ole myöskään toistaiseksi joutunut merkittävän tietosuojaskandaalin kohteeksi, millä on vaikutuksensa riskitietoisuuden muotoutumisen kannalta.

Käytännössä liiketoiminnan intressit ja esimerkiksi negatiivisen julkisen huomion kohteeksi joutumisen välttämiseen tai kuluttaja-asiakkaiden luottamuksen rakentamiseen liittyvät insentiivit ovat olleet lakia voimakkaammin määrääviä tekijöitä sen suhteen, miten yritys on tietosuojaan liittyvät toimintonsa järjestänyt. Tästä syystä suomalaisten yritysten tietosuojasääntelyn noudattamiseksi toistaiseksi tekemät taloudelliset panostukset sekä viime kädessä yritysjohdon asettamiin prioriteetteihin perustuvat käytännöt – ja näiden pohjalta kehittynyt tai kehittymättä jäänyt yleinen "tietosuojakulttuuri" – poikkeavat merkittävästi eri yritysten välillä.

Keskimäärin suomalaisyritysten tietosuojakulttuuri ja -käytännöt ovat kehittymättömämpiä samankokoisiin samalla toimialalla toimiviin ulkomaisiin, kuten esimerkiksi englantilaisiin, saksalaisiin tai ranskalaisiin, yrityksiin verrattuna. Myös tietosuojavelvoitteiden noudattamiseen kohdistetut taloudelliset panostukset ovat olleet suomalaisyrityksissä nykysääntelyn voimassa ollessa verrattain alhaisia, mistä ovat osoituksena muun muassa se, että tietosuojasääntelyn noudattamiseen liittyville kustannuksille ei ole juuri missään yrityksessä omaa kustannuspaikkaansa, koska tällaisten kustannusten erilliselle seuraamiselle ei ole niiden suhteellisen alhaisuuden vuoksi ollut tarvetta. Kustannukset ovat käytännössä jakautuneet muiden toimintojen, kuten tietohallinnon, tietoturvan tai lakiasiainpalveluiden kesken.

Myös se, että vain harvoissa ja lähinnä vain suurimmissa suomalaisyrityksissä on koettu tarpeelliseksi nimetä organisaatiolle oma tietosuojavastaava, kuvaa suomalaisyritysten tietosuojakulttuurin ja -käytäntöjen kehittymättömyyttä, minkä seurauksena voidaan perustellusti puhua tietosuojavaltuutettu Reijo Aarnion julkisuudessa usein toistamalla tavalla myös tietosuojaan liittyvästä osaamisvajeesta.

2.4 Yleisen tietosuoja-asetuksen säätämisen taustalla vaikuttavat tavoitteet ja tietosuojan merkityksen kasvu

EU:n tietosuojalainsäädännön uudistamisen taustalla vaikuttavat tavoitteet – nykysääntelyn päivittäminen vastaamaan muuttunutta toi-

mintaympäristöä, kansalaisten luottamuksen parantaminen verkossa tarjottaviin palveluihin sekä EU:n digitaalisten sisämarkkinoiden kehityksen tukeminen – pohjaavat keskeisellä tavalla taloudellisiin tavoitteisiin. Taustalla on ajatus siitä, että nykyistä laadukkaammalla tietosuojasääntelyllä voidaan saavuttaa EU:n mittakaavassa merkityksellisiä taloudellisia etuja, jotka kohdistuisivat myös eurooppalaisen elinkeinoelämän eduksi.

Taloudellisten tavoitteiden taustalla ovat digitalisaatiokehitykseen ja uuden teknologian synnyttämiin mahdollisuuksiin kytkeytyvät odotukset rajat ylittävän verkkokaupan mahdollistavasta taloudellisesta kasvusta sekä uuden digitaalisen liiketoiminnan synnystä.

Asetuksen säätämisen taloudelliset ulottuvuudet kytkeytyvät Asetuksen normisisällössä voimakkaasti yksilöiden tiedolliseen itsemääräämisoikeuteen ja korkean tietosuojan tason turvaamisen tavoitteeseen. Taustalla vaikuttavat Euroopan unionin perusoikeuskirjan 8 artiklassa turvattu henkilötietojen suoja sekä tarve vastata digitalisoituvan toimintaympäristön yksityisyyden suojaan kohdistaviin haasteisiin yksilöiden oikeudet riittävän tehokkaasti turvaavalla ja modernin toimintaympäristön huomioivalla sääntelyllä.

Edellä kuvatut Asetuksen säätämisen taustalla vaikuttavat tavoitteet ovat itsessään osoitus tietosuojan merkityksen kasvusta, mikä vääjäämättä myös käytännön syistä vaikuttaa yrityksiin kohdistuviin odotuksiin ja vaatimuksiin.

3 KESKEISET MUUTOKSET SÄÄNTELYYN

3.1 Lähtökohdat vaikuttavuuden arvioinnissa

Tietosuojasääntelyn yrityksille aiheuttamat kustannukset voidaan jaotella:

(a) sääntelyn noudattamisesta yrityksille aiheutuviin, hallinnollisten velvoitteiden muodossa välittömästi aktualisoituviin kustannuksiin ("*administrative costs*"); sekä

(b) sääntelyn sisältämien velvoitteiden tai sanktioiden muodostamien insentiivien mukaisesta toiminnasta aiheutuviin välillisiin kustannuksiin ("*compliance costs*").

Ensimmäisenä mainittujen välittömien kustannusten piiriin kuuluvat esimerkiksi tiettyä toimintaa harjoittavaa tai muutoin tietyt kriteerit

täyttävää yritystä sitovien hallinnollisten tietosuojavelvoitteiden täyttäminen. Tällaisten velvoitteiden, kuten esimerkiksi tietosuojavastaavan nimittämisvelvollisuuden, täyttäminen taikka tietystä Asetuksen määrittämästä tilanteesta, kuten esimerkiksi tietoturvaloukkauksesta ilmoittaminen, aiheuttaa yrityksille sisäisiä ja ulkoisia hallinnollisia kustannuksia muun muassa kasvavien palkkakustannusten sekä ulkoisten palveluntarjoajien palkkioiden muodossa.

Huomattavasti edellä todettuja hallinnollisia kustannuksia suurempi taloudellinen vaikutus on Asetuksen myötä syntyvillä compliance-velvoitteilla. Yrityksen compliance-velvoitteet perustuvat paljon laajempaan joukkoon yritykseen Asetuksen perusteella kohdistuvia velvoitteita kuin edellä mainitut hallinnolliset velvoitteet. Kasvavien compliance-kustannusten taustalla ovat ensisijaisesti Asetuksen myötä muuttuva yritysten riskiprofiili ja mahdollisuus joutua merkittävien, kilpailuoikeudellisesta sääntelystä kopioitujen hallinnollisten seuraamusmaksujen kohteeksi. Näiden tietosuojaviranomaisten langettamien sakkojen kohteeksi voi joutua sekä yritys, joka on jonkin Asetukseen perustuvan tietosuojavelvoitteen laiminlyönnillään aiheuttanut sakon langettamisen, mutta myös tällaisen yrityksen sopimuskumppani, jonka kannettavaksi sanktioriski on yksityisoikeudellisella sopimuksella siirretty.

Edellä kuvattu tilanne on markkinakäytäntöjä ajatellen tyypillisimmin käsillä tilanteissa, joissa tietojenkäsittelytoimintojaan ulkoistanut yritys käyttää palveluntarjoajaa, joka palvelusopimuksessa rajoittaa oman vastuunsa siten, että tietojenkäsittelyssä tapahtuvista Asetuksen näkökulmasta laiminlyönteinä pidettävistä sopimusrikkomuksista aiheutuva vastuu kanavoituukin laiminlyönnin aiheuttaneen tahon sijaan toiselle yritykselle.

On ilmeistä, että asetus tulee vaikuttamaan olennaisesti juuri yritysten sopimusriskien hallintaan ja riskienhallintakäytäntöihin.

Välillisesti vaikuttavia ja compliance-kustannuksia aiheuttavia Asetuksen uusia velvoitteita ovat sanktionormien ohella erityisesti yritykselle määritetystä tilivelvollisuudesta ("*accountability*") ja sisäänrakennetun tietosuojan vaatimuksesta ("*privacy by design*") aiheutuvat laajavaikutukselliset ja yleisellä tasolla varsin täsmentymättömät toimintavelvoitteet.

Compliance-kustannukset muodostuvat käytännössä muun muassa niistä uusista kustannuksista, jotka yrityksille välillisesti aiheutuvat nykytilannetta tarkemman ennakollisen riskienhallinnan seurauksena sekä kasvavina transaktiokustannuksina tilanteissa, joissa yritys neu-

vottelee tietosuojan ja tietoturvan toteuttamiseen liittyvien palveluiden hankinnasta.

Asetuksen myötä elinkeinoelämälle aiheutuvien hyötyjen voidaan katsoa realisoituvan niin ikään sekä välittöminä että välillisinä hyötyinä.

Yksi Asetuksen keskeisiä tarkoituksia on ollut alentaa yrityksille hallinnollisten velvoitteiden muodossa kohdistuvia välittömiä kustannuksia. Niiden EU-jäsenvaltioiden, joissa nykyinen Direktiivi on implementoitu laajoja ilmoitus- tai rekisteröitymisvelvollisuuksia luovalla tavalla, näkökulmasta näin myös tapahtuu. Sen sijaan esimerkiksi Suomessa, jossa yrityksiin kohdistuu HTL:n nojalla vain vähäisiä hallinnollisia ilmoitusvelvollisuuksia, jäävät tämän muutoksen hyödyt rajallisemmiksi.

Euroopan komissio on pääsääntöisesti perustanut julkaisemansa oman taloudellisten vaikutusten arviointinsa näille Asetuksen myötä osin ja erityisesti tietyissä suurissa jäsenvaltioissa, kuten Ranskassa ja Saksassa, olennaisestikin hallinnollisia velvoitteita vähentäville muutoksille. Tästä syystä Asetuksen myötä vähentyvät hallinnolliset ilmoitusvelvollisuudet ovat suomalaisten yritysten näkökulmasta positiivisilta vaikutuksiltaan rajatummat ja kohdistuvat merkittävinä ainoastaan niihin yrityksiin, joilla on liiketoimintaa lukuisissa EU-jäsenvaltioissa. Näin on siitä huolimatta, että Asetus vähentää kaikenlaisten yritysten hallinnollisia kustannuksia vähentämällä suomalaisille viranomaisille tehtäviä ilmoituksia ja poistamalla tarpeen tietosuojalautakunnalle esitettäville lupahakemuksille.

Keskeisin ja vaikeimmin arvioitavissa oleva kysymys Asetuksen taloudellisista vaikutuksista kiteytyy kysymykseen siitä, minkälaisiksi muotoutuvat Asetuksen välilliset positiiviset vaikutukset elinkeinoelämälle. Nämä edellä kohdassa 2.4 eritellyt Asetuksen säätämisen taustalla vaikuttavat keskeiset tavoitteet, sisämarkkinoiden nykyistä täysipainoisempi hyödyntäminen, digitalisaation etenemiseen ja sen mahdollistaviin uusiin innovaatioihin sekä niiden edellytyksenä olevaan kuluttajien ja palveluiden käyttäjien luottamuksen vahvistaminen ovat keskeisiä tavoitelluista positiivisista vaikutuksista. Jos nämä tavoitteet Asetuksen myötä toteutuvat, on mahdollista, että nämä Asetuksen välilliset positiiviset vaikutukset kumoavat merkitykseltään kaikkien yrityksille aiheutuvien välittömien ja välillisten kustannusten merkityksen.

3.2 Yrityksen kaikkeen tietojen käsittelyyn horisontaalisesti vaikuttavat uudistukset

3.2.1 Tietosuojasääntelyn harmonisointi

Henkilötietojen sääntelyä on Euroopan unionissa harmonisoitu 1990-luvulla henkilötietodirektiivillä, joka asettaa tietosuojan vähimmäistason unionin laajuisesti. Direktiivi on implementoitu osaksi kansallista lainsäädäntöä erikseen jokaisessa jäsenvaltiossa. Jäsenvaltioiden toisistaan poikkeavista tietosuojaperinteistä johtuen jäsenvaltioiden kansallinen sääntely poikkeaa käytännössä merkittävästi toisistaan Direktiivin implementoinnista huolimatta.

Useassa jäsenvaltiossa toimiva yritys on nykyisin velvollinen selvittämään jokaisen jäsenvaltion säädöksistä johtuvat toisistaan poikkeavat velvoitteet erikseen. Yritykseen kohdistuvista eri EU-jäsenvaltioiden välillä toisistaan poikkeavista velvoitteista aiheutuu merkittäviä kustannuksia erityisesti verkkokauppaa, verkon kautta toimitettavia palveluita, tietojenkäsittelypalveluita ja muuta sähköistä liiketoimintaa harjoittaville yrityksille. Lisäksi velvoitteista aiheutuvien muutosten huomioiminen itse palvelussa ja sen käyttöönotossa aiheuttaa merkittäviä kustannuksia erityisesti liiketoimintaa tai palvelun tarjoamista aloitettaessa, mutta myös säännöllisesti tämän jälkeen.

Tästä syystä harmonisoitu tietosuoja on perustellusti katsottu yhdeksi EU:n digitaalisten sisämarkkinoiden synnyn keskeiseksi edellytykseksi.

Asetus vähentää merkittävästi tietosuojasääntelyyn liittyviä kansallisia erityispiirteitä ja poistaa ne yksityisellä sektorilla keskeisimmiltä osiltaan kokonaan. Yksityiskohtaisempaa kansallista sääntelyä tulee jäämään yritystoiminnan kannalta merkityksellisestä näkökulmasta lähinnä työelämän tietosuojan sääntelyyn.

Erityispiirteiden vähentäminen nopeuttaa unionin laajuisen liiketoiminnan aloittamista sekä vähentää rajat ylittävän liiketoiminnan kustannuksia. Yhdenmukainen sääntely myös lisää pitkän aikavälin oikeusvarmuutta, sillä se vähentää eri maiden säännöstöjen välisten ristiriitojen aiheuttamia ongelmia.

Toisaalta uuden säännöstön käyttöönoton myötä syntyvät tulkintaepäselvyydet ja uusien normien tulkintaan liittyvän oikeuskäytännön puute heikentävät oikeusvarmuutta ja ennakoitavuutta erityisesti säännöstön voimassaolon ensimmäisinä vuosina.

3.2.2 Yhdenmukaistettu valvontamekanismi

Henkilötietodirektiiviin ja sen implementoineisiin lakeihin perustuva valvonta on järjestetty kansallisesti. Valvonnasta säädetään henkilötietolain 9 luvussa. Asetuksessa tietosuojaviranomaisten toiminnasta ja heidän toteuttamastaan valvonnasta on säädetty erityisesti luvuissa VI–VII. Asetuksen valvonta pohjautuu kansallisten tietosuojaviranomaisten toimintaan, ylikansalliseen yhteistyöhön ja Asetuksen myötä perustettavaan uuteen toimielimeen.

Asetuksen VII luvussa säädetään tietosuojaviranomaisten yhdenmukaistetusta valvonnasta. Yhdenmukaistetun valvonnan voidaan olettaa keventävän yritysten hallinnollisia velvoitteita, sillä se vähentää yritysten tarvetta ja velvollisuutta asioida usean eri jäsenvaltion tietosuojaviranomaisen kanssa.

Toisaalta Asetuksen myötä kasvavat yritysten hallinnolliset velvoitteet ja niiden taloudellinen sanktiointi tekee tietosuojaan liittyvistä hallintoprosesseista nykyistä selvästi todennäköisempiä. Jos tietosuojalaiminlyönnin seuraamuksena yritykseen uhkaa kohdistua nykyisin käytössä olevan huomautuksen tai vastaisuudessa tapahtuvaan toimintaan kohdistuvan kiellon sijaan jopa miljoonien eurojen suuruinen hallinnollinen sanktiomaksu, on huomattavan paljon todennäköisempää, että yritys haluaa valittaa tällaisesta viranomaispäätöksestä.

Vastaavasti, jos tietyn jäsenvaltion tietosuojaviranomaisen langettamaa sanktiota koskeva päätös poikkeaa siitä, mitä vastaavan tilanteen osalta olisi todennäköisesti jossain muussa EU-jäsenvaltiossa toimittu, muodostuu yritykselle nykyistä herkemmin intressi viedä asian käsittely ylikansalliselle EU-valituselimelle. Tästä syystä yhdenmukaistetun valvontamekanismin vaikutukset muodostuvat todennäköisesti hyvin merkityksellisiksi ja muuttavat nykyisiä valvontakäytäntöjä olennaisesti.

Yhdenmukaistettu valvonta edellyttää tietosuojaviranomaisten välistä yhteistyötä. Väärin tai liian vähin resurssein toteutettuna yksittäisen tapauksen käsittely voi yhteistyön johdosta pitkittyä nykyisiin käsittelyaikoihin nähden.

Valvonnan yhdenmukaistaminen myös lisää Suomen tietosuojaviranomaisen tehtäviä ja työmäärää. Suomalaisten yritysten tehokkaan liiketoiminnan mahdollistamiseksi on ensisijaisen tärkeää, että työmäärän kasvu otetaan huomioon tietosuojaviranomaisen resursoinnissa. Liian vähäinen viranomaisresursointi voisi merkittävästi heikentää oikeus-

varmuutta vähentämällä viranomaisen kykyä antaa ennakoivaa ohjausta sekä riittävästi perehtyä yksittäisiin tapauksiin. Vähäinen resursointi voisi myös pitkittää käsittelyaikoja, mikä haittaisi yritysten toiminta-edellytyksiä ja heikentäisi suomalaisten yritysten kilpailukykyä.

3.2.3 Yrityksen tilivelvollisuus ("Accountability-periaate")

Asetuksen 5(2) artiklan mukainen tilivelvollisuuden ("*accountability*") periaate on henkilötietolain säännöksiin nähden uusi. Periaatteen mukaan rekisterinpitäjä vastaa siitä, että se pystyy osoittamaan noudattaneensa henkilötietojen käsittelyyn liittyviä 5(1) artiklan mukaisia periaatteita, kuten laillisuus-, avoimuus-, käyttötarkoitussidonnaisuus- ja salassapitoperiaatteita. Yritykset ovat siten velvollisia sekä noudattamaan niihin soveltuvia säännöksiä että varmistamaan, että ne pystyvät myöhemmin osoittamaan toteuttaneensa säännösten mukaiset velvoitteensa.

Prosessuaalisesta näkökulmasta Accountability-periaate muodostaa nykylainsäädäntöön nähden merkittävän muutoksen näyttötaakan osalta. Muutoksen seurauksena rekisterinpitäjän on tarvittaessa itse kyettävä osoittamaan, että se on noudattanut sääntelyä.

Henkilötietolain mukainen viranomaisvalvonta on ensisijaisesti ennakkovalvontaa, joka perustuu yritysten tekemiin tietojenkäsittelyilmoituksiin. Tilivelvollisuuden periaate vähentää ennakkovalvonnalle tyypillisiä hallinnollisia velvoitteita mahdollistamalla viranomaisen toteuttaman jälkikäteisen valvonnan nykyistä tehokkaammin. Ennakkovalvonnan väheneminen mahdollistaa myös viranomaisten resurssien kohdistamisen merkittävään ja korkeariskiseen käsittelyyn.

Hallinnollisten velvoitteiden vähenemisen vastapainona on kuitenkin merkittävä compliance-kustannusten, kuten yrityksen sisäisen hallinnon ja riskienhallintaan liittyvien toimenpiteiden, lisääntyminen. Näitä kustannuksia syntyy erityisesti sisäisen hallinnon organisatorisesta ja teknisestä uudelleenjärjestämisestä, tietosuojavelvoitteiden toteutumisen kirjaamisesta, palveluiden ulkoistamisen kuvaamisesta ja menettelyiden kirjaamisesta sekä syntyvän asiakirja-aineiston tallentamisesta ja saatavilla pidosta.

3.2.4 Riskiarvioperusteinen velvoittavuus

Henkilötietolain säännösten soveltuminen tai soveltumatta jääminen ei riipu tietojenkäsittelyyn liittyvistä riskeistä. HTL:n sääntelyn vaikutukset ja velvoitteiden laajuus saattavat kuitenkin vaihdella käsittelyn ris-

keistä johtuen. Esimerkiksi säännösten edellyttämien tietoturvatoimenpiteiden laatu ja laajuus riippuvat muun muassa tietojenkäsittelyn ja käsiteltävien tietojen ominaispiirteistä.

Henkilötietolaista poiketen Asetus sisältää säännöksiä, jotka soveltuvat vain riskitasoltaan korkeaan tietojenkäsittelyyn. Tällaisia velvoitteita sisältyy tietosuojavaikutusten ennakkoarviointiin (33 artikla), ja viranomaisten ennakkokuulemiseen (34 artikla).

Riskiarvioperusteisen velvoittavuuden tarkoituksena on edistää sekä rekisterinpitäjien ja käsittelijöiden että valvovien viranomaisten tietosuojaresurssien tehokasta kohdentamista. Säännösten kohdentaminen vain korkean riskin käsittelyyn vähentää tietosuojavelvoitteista aiheutuvia kustannuksia. Ne on myös kirjoitettu tavalla, joka mahdollistaa tietoteknisen kehityksen ja muiden käsittelyn ominaispiirteiden huomioimisen.

Velvoitteiden tehokas toteutuminen edellyttää unioninlaajuisesti yhtenäistä tulkintakäytäntöä siitä, minkälainen toiminta katsotaan kussakin tilanteessa säännöksen mukaiseksi korkean riskin käsittelyksi. Jäsenvaltioiden viranomaisten väliset tulkintaerot voivat pahimmillaan johtaa merkittävään forum shopping -ilmiöön, jossa yritykset hakeutuvat niiden viranomaisten valvonnan piiriin, jotka tulkitsevat säännöstöä kaikista yritysmyönteisimmin. Toisaalta myös tulkinnanvaraisuus on omiaan lisäämään hallintoprosesseja Asetuksen voimassaolon ensimmäisinä vuosina.

3.3 Keskeisimmät yksittäiset uudet tai muuttuvat velvoitteet

3.3.1 Henkilötietojen käsittelyn aloittaminen ja hyväksyttävinä pidettävät käsittelyperusteet

Henkilötietojen käsittelyn aloittamiseen liittyvistä velvoitteista ja hyväksyttävistä käsittelyperusteista säädetään erityisesti henkilötietolain 5–8 §:ssä ja 3 luvussa. Lisäksi henkilötietolain 8 luvussa säädetään käsittelyä edeltävistä viranomaisilmoituksista. Aihepiiriltään näitä vastaavat säännökset on sisällytetty muun muassa Asetuksen II lukuun sekä artikloihin 33 ja 34.

HTL:n ja Asetuksen sääntelyn taustalla vaikuttavat periaatteet ovat pitkälti samoja. Säännösten keskeisinä eroina ovat kuitenkin yrityksen viranomaisilmoituksiin liittyvien hallinnollisten velvoitteiden rajoittuminen aiempaa tiiviimpään tietojenkäsittelyyn sekä yrityksen sisäisen hallinnon kasvu.

Käsittelyperusteet. Henkilötietolain 8 § ja 3–4 luvut luettelevat tyhjentävästi ne käsittelyperusteet, joihin henkilötietojen käsittely voi hyväksyttävästi perustua. Henkilötietolain mukaiset käsittelyperusteet ovat Direktiiviin ja Asetukseen nähden hyvin tarkkarajaiset ja jättävät rekisterinpitäjälle suhteellisen vähän harkintavaltaa.

Oikeutettu etu. HTL:n 8 §:n 1 momentin 5–9 kohtien mukaiset tarkkarajaiset käsittelyperusteet ja tietosuojalautakunnan lupaan perustuva käsittely on sekä Direktiivissä että Asetuksessa korvattu oikeutetun edun hyväksi tapahtuvan käsittelyn käsittelyperusteella. Direktiivin 7(1)(f) artiklassa ja Asetuksen 6(1)(f) artiklassa kuvattu käsittely "*rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun edun toteuttamiseksi*" antaa rekisterinpitäjälle merkittävän mahdollisuuden itsenäisesti arvioida ja osoittaa käsittelyn hyväksyttävyys ja lainmukaisuus. Ellei henkilötietolaissa ole käsittelyperusteesta erikseen säädetty, tällainen käsittely on nykyisin mahdollista vain tietosuojalautakunnan luvalla.

Yritykset kokevat tietosuojalautakunnan lupakäsittelyn hitaaksi ja epäkäytännölliseksi. Käsittelylupia on tämän vuoksi haettu varsin vähän. Tämä on johtanut yksittäistapauksissa jopa käsittelyn epätarkoituksenmukaiseen rajoittamiseen ja yrityksen tietojenkäsittelyyn liittyvien kustannusten kasvuun. "Oikeutetun edun hyväksi" -käsittelyperusteeseen liittyvän harkintavallan siirtäminen Asetuksen myötä tietosuojalautakunnalta yrityksille vähentää teknologisen kehityksen aikaansaamiin uusiin liiketoimintamuotoihin liittyviä hallinnollisia velvoitteita, nopeuttaa käsittelyn aloittamista ja voi edistää suomalaisten yritysten kilpailukykyä.

Tietosuoja-arviointi. Asetuksen 33 artikla täsmentää henkilötietolain 6 §:n mukaista suunnitteluvelvoitetta asettamalla rekisterinpitäjälle velvollisuuden arvioida tietojenkäsittelyn vaikutuksia tietosuojaan ja yksityisyydensuojaan (Asetuksessa "*Data Protection Impact Assessment*", yleisesti käytetty myös "*Privacy Impact Assessment*" tai "*PIA*"), jos tietyn tyyppisestä käsittelystä todennäköisesti aiheutuu korkea riski yksilöiden oikeuksille. Arvioinnin vähimmäissisältö on asetettu yksityiskohtaisesti artiklassa 33(3). Tietosuoja-arvioinnin tarkoituksena on toteuttaa selvityksen kohdassa 3.3.5 esitettyjä oletusarvoisen ja sisäänrakennetun tietosuojan periaatteita.

Tietosuojaviranomaisen kuuleminen. Henkilötietolain 36 § asettaa rekisterinpitäjille ja käsittelijöille oletusarvoisesti velvollisuuden ilmoittaa tietosuojavaltuutetulle kaikesta henkilötietojen käsittelystä ennen käsittelyn aloittamista. Laki kuitenkin rajoittaa tätä pääsääntöä merkittävästi, minkä johdosta ilmoitus käytännössä kohdistuu vain osaan käsittelyä.

Ennakkoilmoituksen tarkoituksena on ehkäistä tietojenkäsittelystä aiheutuvia haittoja antamalla viranomaiselle mahdollisuus vaikuttaa henkilötietojen käsittelyyn ennen sen aloittamista. Yritykset ovat kuitenkin pitäneet ilmoitusvelvollisuutta epätarkoituksenmukaisena sillä velvollisuus tehdä ilmoitus ei käytännössä riipu käsittelyyn liittyvistä riskeistä. Ilmoitusvelvollisuus kohdistuu siten myös yksityisyydensuojan kannalta vähäiseen käsittelyyn ja lisää merkittävästi siihen liittyviä hallinnollisia rasitteita. Merkitykseltään vähäistä tietojenkäsittelyä koskevat ilmoitukset myös sitovat valvovan viranomaisen resursseja vaikuttavuudeltaan vähäiseen toimintaan. Asetuksen 34 artikla poikkeaa tästä lähtökohdasta.

Asetuksen mukainen tietosuoja-arviointi ja kuulemisvelvollisuus korvaavat yhdessä henkilötietolain 36 §:n mukaisen ennakkoilmoituksen tietosuojavaltuutetulle. Asetuksen ennakkokuulemisvelvollisuuden mukaan yrityksellä on velvollisuus kuulla tietosuojaviranomaista vain, jos se arvioi käsittelyyn liittyvän riskin olevan korkea. Koska sekä arviointi että kuuleminen tulee toteuttaa vain korkean riskin tietojenkäsittelyssä, niiden tarkoituksena on keskittää yritysten ja viranomaisten hallinnollisiin menettelyihin käyttämiä resursseja suunnittelua eniten tarvitseviin käsittelymuotoihin. Siten ne ovat kohdassa 3.2.4 kuvatulla tavalla riskiperusteisesti velvoittavia säännöksiä.

Viranomaiskuulemisen rajoittamisen voidaan olettaa nopeuttavan erityisesti henkilötietojen käsittelyn tavanomaista ulkoistamista, sillä henkilötietolain mukaan kaikki henkilötietojen käsittelyn ulkoistaminen on ilmoitusvelvollisuuden alaista toimintaa. Korkean riskin tietojenkäsittelyn osalta Asetus saattaa kuitenkin merkittävästi viivyttää käsittelyn aloittamista, sillä henkilötietolain 30 päivän sijaan Asetus antaa viranomaisille 8 viikkoa – tai monimutkaisissa asioissa jopa 14 viikkoa – aikaa käsitellä sille tehty ilmoitus.

Ei velvollisuutta käsitellä tietoja sääntelyn toteuttamista varten. Sekä henkilötietolaki että Asetus sisältävät säännöksiä, joiden voidaan katsoa aikaansaavan henkilötietojen käsittelyä, joka ei olisi muutoin tarpeen. Tällaisen käsittelyn vähentämiseksi Asetus sisältää henkilötietolakiin nähden uuden täsmentävän säännöksen, 10 artiklan, jonka mukaan rekisterinpitäjällä ei ole velvollisuutta käsitellä henkilötietoja tai tunnistaa rekisteröityä vain Asetuksen velvollisuuksien noudattamiseksi. Säännös rajoittaa rekisterinpitäjien vastuuta käytännössä ja suojaa rekisteröityjä tarpeettomalta tietojenkäsittelyltä. Säännös on erityisen merkittävä toteutettaessa lapsiin kohdistuvaan tietojenkäsittelyyn liittyviä säännöksiä. Ilman säännöstä yritysten voitaisiin katsoa olevan velvollisia keräämään tarpeettoman laajasti henkilötietoja vain osoittaakseen, että rekisteröity on tai ei ole lapsi.

Yritysten velvollisuutta arvioida tietojen käsittelyn vaikutuksia ja kuulla tietosuojaviranomaisia tietojen käsittelystä Asetuksen voimaantulon myötä on rajoitettu Asetuksen 134 resitaalissa. Arviointi- ja kuulemisvelvoitteet eivät resitaalin mukaan sovellu Direktiivin mukaiseen käsittelyyn, joka on aloitettu ennen Asetuksen voimaantuloa.

3.3.2 Rajoitukset henkilötietojen tulevien käsittelytarkoitusten laventamiselle

Käyttötarkoitussidonnaisuudesta on säädetty henkilötietolain 7 §:ssä ja Asetuksen 5(1)(b)–(c) ja 6(3a) artikloissa. Henkilötietolain sääntelyyn nähden Asetus pyrkii selventämään ja asettamaan yksityiskohtaiset kriteerit sen arvioinnille, millä perusteella yrityksillä on oikeus käyttää käsittelemiään henkilötietoja muuhun kuin sen ennalta määrittämiin käsittelytarkoituksiin.

Käyttötarkoitussidonnaisuuden periaate rajoittaa merkittävästi yritysten mahdollisuutta muuttaa käsittelemiensä henkilötietojen käyttötarkoitusta vastaamaan muuttuvan liiketoimintansa tai teknologisen kehityksen vaatimuksia. Tämä käy erityisen selvästi ilmi massaluonteisen tietojen keräämisen ja käsittelyn ("*Big Data*") sekä data-analytiikkaan liittyvän yritystoiminnan yhteydessä. Käyttötarkoitussidonnaisuus rajoittaa yritysten mahdollisuuksia hyödyntää sillä olevaa tietoa, mikä saa aikaan toteutumatta jäävää voittoa ja heikentää suomalaisten yritysten kansainvälistä kilpailukykyä.

Asetuksen sisältämät täsmennykset selventävät yritysten oikeutta käyttää käsittelemiään tietoja uuteen käyttötarkoitukseen, minkä voi katsoa selventävän nykyistä oikeustilaa ja luovan tietojen käyttömahdollisuuden tilanteissa, joissa se on henkilötietolain voimassa ollessa ollut epävarma. Täsmennysten voidaan myös katsoa toteuttavat Euroopan unionin perusoikeuskirjan 8 artiklan mukaista henkilötietojen suojaa rajaamalla käsittelyn koskemaan vain tiettyä tarkoitusta.

Toisaalta Asetus vahvistaa elinkeinoelämän ongelmallisena pitämän tiukan henkilötietojen käyttötarkoitussidonnaisuuden periaatteen ja mahdollistaa laajamittaisen ja kontrolloimattoman data-analytiikan lähinnä vain yksinomaan anonymisoidun tiedon osalta. Käyttötarkoitussidonnaisuuden tiukkuudella voi katsoa olevan teknisiä innovaatioita ja datan taloudellisia hyödyntämismahdollisuuksia rajoittava vaikutus.

3.3.3 Velvollisuus päivittää nykyistä asiakirja-aineistoa sekä dokumentoida ja uudistaa prosesseja

Asetus sisältää monia velvoitteita, jotka saavat aikaan velvollisuuden laatia ja ylläpitää asiakirja-aineistoa. Ensinnäkin, sekä henkilötietolain

10 että 24–25 §:ssä sekä Asetuksen 14 ja 14a artikloissa säädetään rekisterinpitäjän tiedonantovelvollisuudesta. Toiseksi, Asetuksen 28 artikla velvoittaa rekisterinpitäjän ylläpitämään käsittelyä koskevaa kuvausta. Kolmanneksi, Asetuksen 7 artiklassa määritellään ne tiedot, jotka yrityksen tulee antaa rekisteröidylle pyytäessään häneltä suostumusta henkilötietojen käsittelyyn.

Mainitut säädökset velvoittavat rekisterinpitäjän antamaan rekisteröidylle tietyt tiedot henkilötietojen käsittelystä sekä ylläpitämään käsittelyä koskevaa kuvausta. Siinä missä henkilötietolain 10 § mukainen velvoite on rekisterikohtainen, Asetuksen velvoitteet koskevat toteutettua käsittelyä kokonaisuudessaan. Rekisterikohtaisuudesta luopuminen vähentää yritysten tietojenantoon liittyviä pitkän aikavälin kustannuksia.

Asetus laajentaa tiedonantovelvollisuutta sisällöllisesti henkilötietolakiin nähden. Rekisterinpitäjän tulee muun muassa antaa tietoa henkilötietojen säilytysajoista ja tietojen vastaanottajista tai vastaanottajaryhmistä. Vastaavia tiedonantovelvollisuuksia ei sellaisenaan sisälly henkilötietolakiin, vaikka rekisterinpitäjällä voidaan HTL:n perusteella katsoa olevan velvollisuus määrittää säilytysajat ja pitää kirjaa vastaanottajaryhmistä. Asetuksen myötä yritysten tulee siten päivittää kaikki rekisteriselosteensa. Tästä aiheutuva työmäärä riippuu yrityksellä olevien henkilörekisterien määrästä. Päivittäminen johtaa merkittävään työmäärään yrityksissä, jotka ylläpitävät laajaa joukkoa eri henkilörekistereitä.

Rekisteröidyille annettavien tietojen lisäksi yli 250 henkilöä työllistävien rekisterinpitäjien ja käsittelijöiden tulee ylläpitää 28 artiklan mukaista kuvausta tietojen käsittelystä. Kuvauksen sisältö poikkeaa hieman 14 ja 14a artikloista. Yrityksille aiheutuu siten lisätyötä joko kaksinkertaisen asiakirja-aineiston ylläpidosta tai sen varmistamisesta, että yksi kuvaus täyttää molempien säännösten toisistaan poikkeavat vaatimuksen.

Suostumus. Sekä henkilötietolain 3 § että Asetuksen 7 artikla sekä sitä täydentävät resitaalit asettavat pätevälle suostumukselle pitkälle vietyjä vaatimuksia. Asetuksen säännös on kuitenkin henkilötietolain säännöstä yksityiskohtaisempi. Yritysten tulee siten varmistua, että niiden pyytämät suostumukset täyttävät Asetuksen muotovaatimukset sekä tarvittaessa päivittää suostumukseen liittyvät asiakirjat. Asetuksen muotovaatimukset eivät kuitenkaan vaikuta ennen sen voimaantuloa pyydettyjen suostumusten pätevyyteen.

3.3.4 Rekisteröidyn uusien oikeuksien toteuttaminen

Rekisteröidyn oikeuksista säädetään erityisesti henkilötietolain 6 luvussa ja Asetuksen III luvussa. Asetus antaa rekisteröidyille nykyistä laajemmat oikeudet vaikuttaa omien tietojensa käsittelyyn sekä hyödyntää näitä tietoja itse.

Artikla 18 laajentaa rekisteröidyn henkilötietolain 26–28 § mukaisia mahdollisuuksia hyödyntää itsestään käsiteltyjä tietoja antamalla hänelle tietyin edellytyksin oikeuden saada nämä tiedot koneluettavassa muodossa sekä siirtää ne edelleen toiselle rekisterinpitäjälle. Jo nykyinen laki antaa rekisteröidylle oikeuden saada kopiot itseään koskevista tiedoista. Henkilötietolakiin verrattuna artiklan säännös laajentaa rekisteröidyn mahdollisuutta hyödyntää itseään koskevia tietoja määrittelemällä tietojen luovutusmuodon rekisteröidylle edullisella tavalla. Muutos saattaa lisätä yritysten IT-hankintoihin liittyviä kustannuksia sillä niiden tulee ylläpitää sellaisia järjestelmiä, jotka mahdollistavat yhtä henkilöä koskevien tietojen konekielisen erottamisen ja ulosviennin järjestelmästä. Kaikki nykyisin käytössä olevat vanhat tietojärjestelmät eivät sisällä tällaista toiminnallisuutta.

Lisäksi Asetus laajentaa henkilötietolain 29 ja 30 § mukaisia rekisteröidyn oikeuksia vastustaa henkilötietojensa käsittelyä sekä saada tietonsa poistettua rekisterinpitäjän henkilörekisteristä ("*right to be forgotten*"). Oikeuksien laajenemisesta huolimatta niiden toteuttaminen ei todennäköisesti edellytä nykyiseen lakiin verrattuna merkittäviä uusia teknisiä tai hallinnollisia rakenteita. Rekisteröityjen pyyntöjen käsittelyn voidaan kuitenkin olettaa lisäävän rekisterinpitäjän tietojenkäsittelykustannuksia. Kustannusten tosiasiallinen kasvu riippuu käytännössä siitä, kuinka laajasti rekisteröidyt vetoavat oikeuksiinsa.

3.3.5 Vaatimus sisäänrakennetusta tietosuojasta ja oletusarvoisesta tietosuojasta

Artikla 23 asettaa rekisterinpitäjälle velvoitteita sisäänrakennetusta tietosuojasta ("*privacy by design*") sekä oletusarvoisesta tietosuojasta ("*privacy by default*"). Vastaavia velvollisuuksia ei sellaisenaan sisälly henkilötietolakiin, vaikka niiden mukaisia tavoitteita voidaan katsoa sisältyvän henkilötietolain 5 §:n huolellisuusvelvoitteeseen.

Privacy by Design -periaatteen tavoitteena on edistää Asetuksessa säädettyjen yleisten tietosuojaperiaatteiden toteutumista. Säännös velvoittaa rekisterinpitäjän järjestämään tietojenkäsittelynsä tavalla, jonka avulla Asetus, tietosuojaperiaatteet ja rekisteröidyn oikeudet tulevat tehokkaasti huomioiduiksi kaikessa tietojenkäsittelyssä.

Privacy by Default -periaate puolestaan vahvistaa sisäänrakennetun tietosuojan periaatetta velvoittamalla rekisterinpitäjän järjestämään varsinaisen tietojenkäsittelynsä niin, että se käsittelee henkilötietoja vain siinä määrin kuin on tarpeen kussakin yksittäistapauksessa.

Periaatteet edistävät siten tehokasta tietojen käsittelyä sekä ehkäisevät tarpeetonta ja virheellistä tietojenkäsittelyä. Toteuttamiseen liittyvän laaja-alaisen suunnittelun ja edellä kuvatun tilivelvollisuuden periaatteen vuoksi niiden toteuttamisen voidaan kuitenkin olettaa lisäävän yritysten sisäisen hallinnon kustannuksia.

Privacy by Design -periaate voi myös vaikuttaa ennakoimattomalla tavalla tietynlaisten liiketoimintamuotojen toteuttamiseen ja niihin kohdistuviin riskeihin. Esimerkiksi ohjelmistoliiketoiminnassa uusi yleinen velvollisuus voi muuttaa myyjän ja ostajan välisen vastuunjaon lähtökohtia, sillä uuteen ohjelmistotuotteeseen tai tietojärjestelmään tehtävään räätälöintiin kohdistuu asetusperusteinen vaatimus, jonka mukaan sen on – nimenomaisten sopimuksellisten vaatimusten lisäksi – täytettävä myös yleiset tietosuojavaatimukset. Vaatimuksen täyttymisestä vastaa rekisterinpitäjän roolissa oleva yritys (tyypillisesti asiakas), mutta osapuolet saattavat myös huomaamattaan siirtää vastuun velvoitteen noudattamisesta soveltamissaan sopimusehdoissa (esimerkiksi ottamalla sopimukseen yleisluonteisen ehdon siitä, että myyjä vastaa sopimuksen kohteen täyttävän kaikki siihen kohdistuvat lainsäädäntöperusteiset vaatimukset).

3.3.6 Käsittelijän roolissa olevan palveluntarjoajayrityksen velvollisuudet ja vastuut

Pääosa henkilötietolain vaatimuksista kohdistuu yksinomaan rekisterinpitäjään. Vain 5, 32, 33 ja 36 pykälät asettavat välittömiä velvoitteita käsittelijöille. Näin ollen, rekisterinpitäjän käyttäessä palveluntarjoajia kohdistuu vastuu tietojen käsittelystä henkilötietolain nojalla käsittelyn toteuttavan palveluntarjoajan sijaan lähes yksinomaan henkilötietojenkäsittelypalveluita hankkiviin rekisterinpitäjän roolissa oleviin yrityksiin.

Asetus muuttaa osapuolten välistä vastuunjakoa henkilötietolakiin nähden. Erityisesti Asetuksen 26 artikla laajentaa käsittelijöiden vastuuta sekä tietojen käsittelyn ulkoistamiseen liittyviä velvoitteita. Artikla muun muassa velvoittaa rekisterinpitäjän ja käsittelijät laatimaan tarkkojen edellytysten mukaisen kirjallisen sopimuksen käsittelystä.

Tietojärjestelmien hallinnointipalveluita tai muita IT-alan palveluita käsittelijän roolissa tarjoavat IT-palveluyritykset joutuvat lain nojalla

ensimmäistä kertaa tilanteeseen, jossa tietosuojaa koskevat velvoitteet on välttämätöntä ottaa osaksi palveluiden tarjoamista koskevaa sopimusta. Tämä johtaa käytännössä tietosuojavelvoitteisiin liittyvien vastuiden nousua neuvotteluiden kohteeksi.

Samalla Asetuksen artiklat 77 ja 78 kohdistavat käsittelijään taloudellisen sanktioriskin, mikä muuttaa olennaisesti käsittelijöiden riskiprofiilia nykyasetelmasta. Riskien kasvu tulee todennäköisesti nostamaan henkilötietojen käsittelyä sisältävien palveluiden hintoja käsittelijöiden siirtäessä kasvaviin taloudellisiin vastuisiinsa liittyvän riskin palveluidensa hintoihin.

3.3.7 Tietoturvan toteuttaminen ja henkilötietojen suojaaminen

Tietoturvasta säädetään henkilötietolain 5 ja 32–33 §:ssä sekä Asetuksen 30 artiklassa.

Säännökset ovat luonteeltaan hyvin samanlaisia. Asetus kuitenkin sisältää esimerkinomaisena esitettävän luettelon toimenpiteistä, joita voidaan pitää tarpeellisina riittävän tietotuvan toteuttamiseksi. Näitä ovat esimerkiksi tietojen pseudonyymisointi sekä tietojenkäsittely toimenpiteiden säännöllinen testaaminen ja tarkastaminen. Lista on ohjeellinen, mutta käytännössä merkityksellinen, sillä se osoittaa, mitä toimenpiteitä voidaan pitää riittävän tietoturvallisuuden tason edellytyksenä.

Henkilötietolaki ei sisällä ohjausta siitä, miten saavuttaa riittävä tietoturvan taso. Lain mukaan tietoturvan riittävä taso arvioidaan kunkin yksityistapauksen erityispiirteistä lähtöisin ottaen huomioon muun muassa käsittelyyn liittyvät riskit ja suojattava intressi. Yritykset ovat siten voineet valita hyödyntämänsä toimenpiteet vapaasti. Tämä on johtanut hyvin erilaiseen käytännön toteutukseen. Ohjeellisesta luonteestaan huolimatta monien yritysten voidaan olettaa muuttavan toimintaansa Asetuksen toimenpiteitä vastaavaksi. Muutostöiden johdosta Asetuksen toimenpidelistaus aiheuttaa käytännössä monille yrityksille kustannuksia. Myös toteutettavien menetelmien säännöllinen tarkastaminen ja testaus lisäävät tietoturvan toteutuksen kustannuksia.

3.3.8 Velvollisuudet ilmoittaa tietoturvaloukkauksista viranomaisille ja rekisteröidyille

Asetuksen 31 artikla velvoittaa rekisterinpitäjät kertomaan tietomurroista sekä viranomaisille että rekisteröidyille. Henkilötietolaki ei sisällä vastaavanlaista nimenomaista velvollisuutta ilmoittaa tietomurroista viranomaisille, rekisteröidyille tai muutoin. Suomen lainsäädännössä

velvollisuus kertoa tietomurrosta on asetettu toimialakohtaisesti tietoyhteiskuntakaaren (917/2014) 275 §:n mukaisesti vain teleyrityksille.

Asetus asettaa tietomurtoilmoitukselle hyvin alhaisen kynnyksen, lyhyen toteutusajan ja laajan tietosisällön. Nämä velvollisuudet voivat aiheuttaa merkittäviä kustannuksia yrityksille, sillä teknologisen kehityksen johdosta yritysten on lähes mahdotonta täysin torjua tietomurtoja. Siten myös huolellisesti toimiva yritys voi joutua tietomurron kohteeksi.

Tietomurtoilmoituksesta syntyy välittömiä kustannuksia erityisesti ilmoituksen tekemiseen liittyvien käytäntöjen laatimisesta ja ilmoituksen tekemisestä yksittäistapauksessa. Sekä käytäntöjen laatiminen että ilmoituksen tekeminen edellyttävät todennäköisesti yrityksen ulkopuolisten tietoturva- ja tietosuoja-asiantuntijoiden käyttämistä.

Välittömien kustannusten lisäksi velvollisuus ilmoittaa tietomurroista voi aiheuttaa yrityksille merkittävää mainehaittaa, sillä laaja joukko yksityishenkilöitä ja yhtiöitä saa tiedon murrosta joko suoraan tai epäsuorasti ilmoituksen kautta. Tämä mainehaitta voi merkittävästi heikentää yrityksen tulevaa liiketoimintaa.

On todennäköistä, että monet yritykset pyrkivät rajoittamaan tietomurron seurauksista aiheutuvia vahinkojaan käyttämällä ulkopuolisten konsulttien, kuten viestintätoimistojen ja tietoturvayhtiöiden sekä asianajotoimistojen palveluita tietomurrosta viestiessään ja varautuessaan sopimuskumppaniensa ja asiakkaidensa reaktioihin. Tämä puolestaan lisää tietomurtoilmoituksesta aiheutuvia välittömiä kustannuksia.

Tietomurtojen julkiseksi tuleminen lisäävät todennäköisyyttä siitä, että rekisteröidyt sekä yrityksen sopimuskumppanit esittävät yritykselle vahingonkorvausvaatimuksia tietomurron seurauksena.

3.3.9 Velvollisuus nimittää tietosuojavastaava

Asetuksen 4 osassa säädetään tietosuojavastaavista. Siihen sisältyvä 35 artikla velvoittaa yritykset nimittämään tietosuojavastaavan. Henkilötietolaki ei sisällä vastaavaa velvollisuutta nimittää tietosuojasta vastaavaa henkilöä. Sen sijaan velvollisuus nimittää tietosuojavastaava on nykyisin asetettu toimialakohtaisesti sähköisistä lääkemääräyksistä annetussa laissa (61/2007) ja sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007). Lakien mukainen velvollisuus koskee muun muassa apteekkeja, terveydenhuollon palveluiden antajia ja Kansaneläkelaitosta.

Velvollisuus nimittää tietosuojavastaava koskee sekä rekisterinpitäjiä että käsittelijöitä. Velvollisuus ei kuitenkaan koske kaikkia yrityksiä, vaan se on rajoitettu kattamaan vain luonteeltaan erityisen merkityksellinen käsittely. Velvollisuus nimittää tietosuojavastaava koskee ensinnäkin yrityksiä, joiden liiketoiminnan keskeisenä osana on käsitellä henkilötietoja tavalla, joka edellyttää rekisteröityjen säännöllistä ja systemaattista valvontaa. Lisäksi velvollisuus koskee yrityksiä, jotka keskeisenä osana liiketoimintaansa käsittelevät laajoja määriä arkaluonteisia tai rikosoikeudellisiin sanktioihin liittyviä tietoja.

Tietosuojavastaavan on Asetuksen mukaan tarkoitus toimia itsenäisesti ja vastata toiminnastaan suoraan yrityksen korkeimmalle johdolle. Asetuksen mukaan hänen tehtäviensä tulee käsittää ainakin tietoja käsittelevien työntekijöiden ohjeistamisen, tietosuojalainsäädännön noudattamisen valvonnan, vaikutustenarvioinnin toteuttamisen ohjeistamisen sekä toimimisen yhteyshenkilönä tietosuojaviranomaiseen nähden. Tietosuojavastaava saa hoitaa myös muita tehtäviä Asetuksen mukaisten tehtäviensä ohessa.

Velvollisuus nimittää tietosuojavastaava lisää yritysten sisäisen hallinnon kustannuksia. Kustannusten lisäys voi kuitenkin jäädä suhteellisen vähäiseksi kolmesta eri syystä: Ensinnäkin, velvollisuus nimittää tietosuojavastaava koskee erityisesti arkaluonteisia tietoja kuten terveydentilatietoja käsitteleviä yrityksiä. Monet tällaiset yritykset ovat jo nykylainsäädännön perusteella velvollisia nimeämään tietosuojavastaavan. Asetuksen velvoitteet eivät siten merkittävästi lisää yritysten velvollisuuksia.

Toiseksi, vaikka henkilötietolaki ei velvoita yrityksiä nimeämään tietosuojavastaavaa, erityisesti monet suuret ja keskisuuret yritykset ovat sisäisen hallinnon järjestämiseen ja/tai riskienhallintaan liittyvistä syistä nimittäneet tietosuojavastaavan jo nyt tai osoittaneet sitä vastaavat työtehtävät yhdelle tai useammalle yrityksen työntekijälle. Tämä pitää erityisesti paikkansa yrityksissä, joissa tietojenkäsittely muodostaa merkittävän osan liiketoimintaa.

Kolmanneksi, tehokkaasti toteutettuna tietosuojaan liittyvien tehtävien keskittäminen edistää Asetusten mukaisten velvollisuuksien tehokasta toteutumista. Siten tietosuojavastaavan nimittäminen saattaa välillisesti vähentää tietojenkäsittelystä aiheutuvia välillisiä ja välittömiä kustannuksia pitkällä aikavälillä verrattuna siihen, että yritys toteuttaa Asetuksen mukaiset velvoitteensa keskittämättä tietosuojaan liittyviä tehtäviä yhdelle tai useammalle henkilölle.

3.3.10
Käytännesäännöt ja sertifioinnit

Asetuksen 38 ja 39 artikloissa säädetään käytännesääntöjen ("*codes of conduct*") ja sertifiointijärjestelmien käyttöönotosta. Toimialakohtaiset yksityisen sektorin ja tietosuojaviranomaisten yhteistoiminnassa syntyvät Asetuksen normisisältöä täydentämään tai tulkitsemaan tarkoitetut käytännesäännöt saattavat vaikuttaa kyseisen toimialan yritysten velvollisuuksiin ja riskeihin joko kustannuksia korottavasti tai toisaalta oikeusvarmuuden lisääntymisen seurauksena kustannuksia alentavasti.

Sertifiointijärjestelmien tarkoituksena on asetetut kriteerit täyttävien yritysten käyttöön saatettavin erilaisin sertifikaatein tehdä sääntelyn noudattamiseen liittyvien, riippumattoman ulkopuolisen tahon tarkastamien käytäntöjensä osoittaminen yritykselle mahdollisimman yksinkertaiseksi ja siten lisästä yritykseen kohdistuvaa luottamusta ja alentaa transaktiokustannuksia. Sertifiointijärjestelmien perustamismahdollisuudet luovat edellytyksiä uudenlaisen liiketoiminnan synnyttämiselle.

3.3.11
Henkilötietojen käsittelystä sääntelyn perusteella aiheutuvat vastuut ja niiden jakaantuminen

Asetuksen 79 ja 79a artikloissa säädetään hallinnollisista sakoista ja 79b artiklassa jäsenvaltioiden oikeudesta säätää rangaistussäännöksiä muista kuin hallinnollisen sakon kattavista rikkomuksista. Henkilötietolaki ei tunnista hallinnollisia sakkoja tai yhteisösakkorangaistusta, vaan sen 10 luvussa ja rikoslain 38 luvussa säädetyt rangaistussäännökset luovat ainoastaan yrityksen vastuullisille henkilöille rikosoikeudellisen vastuun.

Hallinnolliset sakot on määrätty Asetuksessa liiketaloudellisesti hyvin merkittävälle tasolle, sillä ne voivat enimmillään olla jopa 4 % yrityksen edellisen vuoden maailmanlaajuisesta liikevaihdosta tai 20 000 000 euroa, kumpi johtaa korkeampaan summaan. Näin suuret summat mahdollistavat tuntuvan sanktion määräämisen, minkä myötä tietosuojasäännösten noudattamatta jättämisen potentiaaliset seuraamukset muodostuisivat niin merkittäviksi, että yritysten kannattaa lähtökohtaisesti aina pyrkiä huolehtimaan velvoitteistaan ennaltaehkäisevästi laiminlyöntiin perustuvan taloudellisen sanktion riskin kannettavaksi ottamisen sijaan.

Taloudellinen sanktiouhka tulee määrittämään yrityksen hyväksyttävinä pitämien compliance-kustannusten tasoa, joten suurempi taloudellinen sanktiouhka johtaa todennäköisesti suurempiin panostuksiin ennaltaehkäisevään riskienhallintaan.

Sanktiotason kasvu lisää samalla yritysten tietojenkäsittelyn yleisiä riskejä. Näiden riskien merkitys on erityisen keskeinen laajoja tietojenkäsittelypalveluita tarjoaville käsittelijöille, joiden vastuu nykyisen lainsäädännön perusteella on hyvin rajattu. Tämän voidaan olettaa nostavan palveluiden ulkoistamisen kustannuksia, sillä käsittelijät pyrkivät todennäköisesti siirtämään kantamaansa riskiä palvelusopimusten kautta rekisterinpitäjien kannettavaksi sekä palvelun ehtojen että hintojen kautta.

Asetuksen mukainen sanktiojärjestelmä synnyttää myös uutta liiketoimintaa erityisesti vakuutusyhtiöille, sillä se synnyttää aiempaa merkittävämmän tarpeen varautua tietojenkäsittelystä aiheutuviin riskeihin myös uudenlaisin vaikutustuottein.

8.12.2015, täydennetty ja viimeistelty 15.1.2016
JULÅ