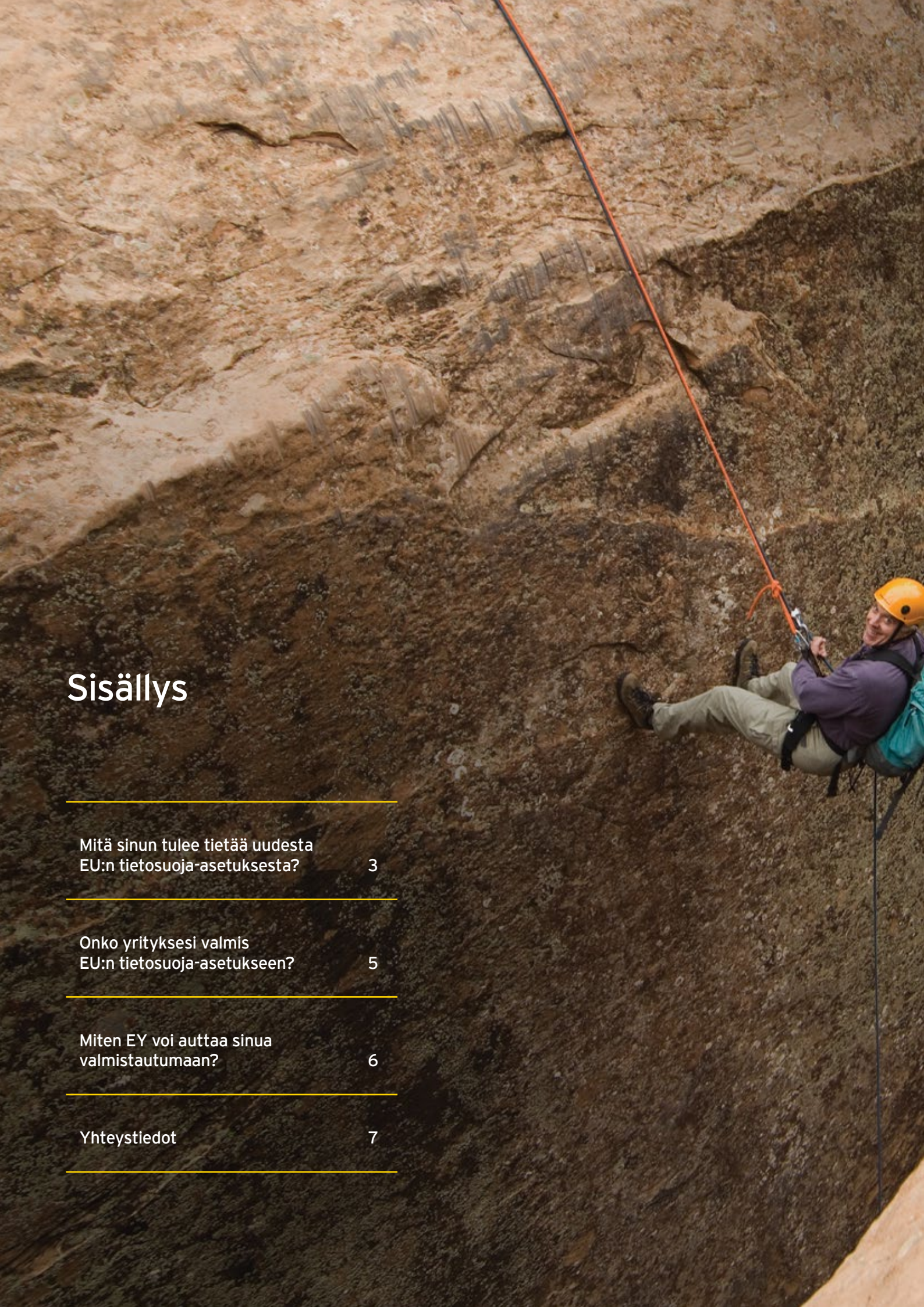
EU:n tietosuoja-asetus: oletko valmis?

Building a better working world



Sisällys

Mitä sinun tulee tietää uudesta EU:n tietosuoja-asetuksesta?

Elämme uutta tietosuojan aikakautta.

Muutokseen ovat vaikuttaneet seuraavat tekijät:

1

Mediassa on raportoitu kasvava määrä suuren luokan tietomurtoja. Kuluttajat ja lainsäätäjät ovat huolissaan henkilötietojen käsittelystä.

Lähes neljä vuotta käytyjen kovien neuvotteluiden ja useiden asetusluonnosten jälkeen Euroopan parlamentti ja Euroopan unionin neuvosto pääsivät sopuun tietosuojauudistuksesta 17. joulukuuta 2015. EU:n yleinen tietosuoja-asetus muuttaa yritysten maailmaa. Se tuo mukanaan tiukempia tietosuojavaatimuksia. Niiden noudattamatta jättämisestä voi seurata tuntuvia sakkoja, jotka voivat nousta jopa 20 miljoonaan euroon tai 4 prosenttiin yrityksen liikevaihdosta. Asetus korvaa EU:n henkilötietodirektiivin 95/46/EY, joka on ollut perustana eurooppalaiselle tietosuojasääntelylle sen voimaantulosta eli vuodesta 1995 lähtien.

2

Safe Harborin kuolema

Tietosuoja-asetuksella on merkittävä vaikutus yrityksiin kaikilla teollisuuden aloilla tuoden mukanaan sekä positiivisia että negatiivisia muutoksia liiketoiminnalle kustannusten ja työmäärän muodossa. Tietosuojalainsäädäntö harmonisoidaan kaikissa 28 EU:n jäsenvaltiossa, mikä tarkoittaa sitä, että ylikansallisten yritysten on helpompi navigoida vaikeaselkoisessa tietosuojaympäristössä. Uudet yritysten järjestelmiin rekisteröityjen henkilöiden oikeudet, kuten oikeus tulla unohdetuksi ja tietojen siirto-oikeus sekä pakollinen ilmoitusvelvollisuus tietoturvaloukkauksista, kasvattavat todennäköisesti yritysten sääntelytaakkaa.

3

Uusi EU:n tietosuoja-asetus – tietosuojan virstanpylväs

Yritysten tulee arvioida tämänhetkisen tietosuojansa nykytila suunnitellakseen seuraavat askeleet ja päättääkseen, mitä toimia niiden tulee tehdä ennen toukokuuta 2018.

Yritysten tulee toimia nyt varmistaakseen, että ne ovat valmiita noudattamaan uutta asetusta sen voimaanastumishetkellä 25. toukokuuta 2018.

EU:n tietosuoja-asetuksen keskeisimmät muutokset

Seuraamukset	Tietosuoja-asetuksen rikkomisesta aiheutuvat sakot ovat merkittäviä. Sakkoja voidaan määrätä jopa 4 % yrityksen koko vuotuisesta maailmanlaajuisesta liikevaihdosta tai korvaus voi nousta aina 20 miljoonaan euroon saakka.
Laajennettu soveltamisala	Uutta asetusta sovelletaan kaikkiin rekisterinpitäjiin ja henkilötietojen käsittelijöihin EU:n alueella ja yrityksiin, joiden kohderyhmänä ovat EU:n kansalaiset.
Tietosuojavastaava (Data Protection Officer, DPO)	Jos yrityksen ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa tai laajamittaista käsittelyä, joka kohdistuu arkaluonteisiin henkilötietoihin, sen tulee nimittää tietosuojavastaava.
Osoitusvelvollisuus	Yritysten tulee kyetä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä: ▸ Kartoittamalla tietojen käsittelyn nykytila ja ottamalla tietosuoja osaksi toimintojen suunnittelua ja mallinnusta. ▸ Dokumentoimalla tietosuojaperiaatteiden käytännön toteutusta, prosesseja ja menettelytapoja. Dokumentointi tulee pyydettäessä olla valvontaviranomaisen saatavilla. ▸ Varmistamalla sisäänrakennettu ja oletusarvoinen tietosuoja. ▸ Minimoimalla tietojen käsittelyä ja tietojen säilytystä.
Tietosuojaa koskeva vaikutustenarviointi (Privacy Impact Assessment, PIA)	Yritysten tulee tehdä tietosuojaa koskeva vaikutustenarviointi, kun ne suorittavat riskialtista tai laajamittaista henkilötietojen käsittelyä.
Suostumus	▸ Rekisteröidyn tulee voida vapaasti valita suostumuksensa henkilötietojen käsittelyyn ja antaa se tarkennetusti tiettyyn käyttötarkoitukseen. ▸ Rekisteröityjä tulee myös informoida heidän oikeudestaan peruuttaa suostumuksensa. ▸ Suostumuksen tulee olla täsmällinen, kun kyse on arkaluonteisista henkilötiedoista tai rajat ylittävästä tietojensiirrosta.
Tietoturvaloukkaukset ja ilmoitusvelvollisuus	▸ Rekisterinpitäjä; ilmoitus valvontaviranomaisille on tehtävä 72 tuntia loukkauksen ilmitulosta. Ilmoituksen voi jättää tekemättä ainoastaan, mikäli loukkauksesta ei todennäköisesti aiheudu henkilöiden oikeuksiin tai velvollisuuksiin kohdistuvaa riskiä. Yritysten tulee huolehtia dokumentoinnista. ▸ Mikäli vahingon riski henkilölle on korkea, myös henkilöä on informoitava.
Rekisteröidyn oikeudet	▸ Oikeus tulla unohdetuksi. ▸ Oikeus tietojen siirtämiseen. ▸ Oikeus vastustaa profilointia, eli esimerkiksi oikeus olla olematta automaattisen päätöksenteon kohteena.
Privacy by design - Sisäänrakennettu tietosuoja	Yrityksiä ohjaava periaate, jonka mukaan yritysten tulisi suunnitella ja rakentaa tietosuoja osaksi liiketoimintaprosessiensa ja uusien järjestelmiensä kehittämistä. Yksityisyysasetukset tulee asettaa oletusarvoisesti korkealle tasolle.
Käsittelijöiden velvollisuudet	Tietosuoja-asetus tuo mukanaan uusia velvollisuuksia henkilötietojen käsittelijöille. Seuraamuksia voidaan määrätä myös käsittelijöille.

Onko yrityksesi valmis EU:n tietosuoja-asetukseen?

Nyt on aika aloittaa valmistautuminen. Kiinnitä huomiota seuraaviin osa-alueisiin:

Laajennettu soveltamisala
Oletko henkilötietojen käsittelijä tai rekisterinpitäjä ja käsittelet henkilötietoja EU:n alueella tai käsittelet EU-kansalaisten henkilötietoja?

Tietosuojavastaavat
Suoritatko laajaa systemaattista valvontaa (mukaan lukien työntekijöiden henkilötiedot) tai käsitteletkö suurta määrää arkaluonteisia henkilötietoja?

Uudet oikeudet
Tiedätkö kuinka noudatat uusia oikeuksia: oikeutta tulla unohdetuksi, oikeutta siirtää tiedot ja oikeutta vastustaa profilointia?

Osoitusvelvollisuus
Onko tietosuojan hallinnointi varmistettu ja oletko valmis osoittamaan, kuinka noudatat yleisen tietosuoja-asetuksen vaatimuksia?

Sisäänrakennettu tietosuoja
Suunnitteletko ja rakennatko tietosuojan osaksi liiketoimintojesi ja uusien järjestelmiesi kehitystä?

Ilmoitusvelvollisuus
Pystytkö ilmoittamaan valvontaviranomaisille tietoturvaloukkauksesta 72 tunnin kuluessa?

Miten EY voi auttaa sinua valmistautumaan?

Toimenpide	Kohde	Kuvaus	Aikataulu
Tietosuojan pikakartoitus	Korkean tason arvio tietosuojan nykytilasta	▸ Korkean tason arvio yrityksen tietosuojan nykytilasta ja valmiuksista suhteessa tietosuoja-asetuksen uusiin vaatimuksiin	1 päivä
Tietosuojan nykytilan arviointi	Kokonaisvaltainen arvio tietosuojan nykytilasta GAP- ja riskianalyysi Kehityssuunnitelman laatiminen	▸ Nykyisten henkilötietojen käsittelytoimien ja -prosessien kartoittaminen ▸ Henkilötietokartoitus ▸ Henkilötietovirrat ml. siirrot ETA-alueen ulkopuolelle ▸ Liiketoiminnan kannalta kriittisten osa-alueiden tunnistaminen ▸ Konkreettiset toimenpiteet puutteiden korjaamiseksi ▸ Toimenpiteiden aikataulutus ja priorisointi ▸ Tarvittaessa avustaminen kehityssuunnitelman käytännön toteutuksessa	2–4 viikkoa riippuen yrityksen koosta ja moni-mutkaisuudesta
Tietosuojan kehitysohjelma	Kokonaisvaltainen arvio tietosuojan nykytilasta Kehitysohjelman suunnittelu ja implementointi Kehitysohjelman jatkuva tuki Vaatimustenmukai-suuden kehittäminen ja jatkuvuus	Tietosuojan kehitysohjelma sisältää seuraavien asioiden suunnittelun ja toteutuksen ▸ Kokonaisvaltainen arvio tietosuojan nykytilasta ▸ GAP- ja riskianalyysi ▸ Konkreettiset toimenpiteet puutteiden korjaamiseksi ▸ Kehitysohjelman jatkuva tuki ▸ Tietosuojan hallinnointi, roolit ja vastuut ▸ Henkilöstön ohjaus ja neuvonta ▸ Henkilötietojen elinkaaren hallinta ▸ Hallintaprosessit ▸ Toimittajien hallinta ▸ Pääsyhallinta ▸ Raportointi ja seuranta ▸ Vaatimustenmukaisuuden kehittäminen ja jatkuvuus	3–12 kuukautta riippuen tietosuojan nykytilasta ja yrityksen koosta
Muut tietosuojapalvelut	Koulutukset Vaikutusten arvioinnit (PIA) Hallintaprosessien laadinta Juridinen analyysi Juridisten dokumenttien laadinta	▸ Tietosuojakoulutukset ▸ Henkilöstön ohjaus ja neuvonta ▸ Tietosuojaa koskevan vaikutustenarviointien suorittaminen (PIA) järjestelmille ja projekteille ▸ Rekisteröityjen oikeuksia ja tietoturvaloukkauksia koskevien hallintaprosessien määritteleminen ▸ Avustaminen tietojen siirrossa ulkomaille ▸ Tietosuojapolitiikoiden tarkastaminen ja laatiminen ▸ Rekisterinpitäjän ja henkilötietojen käsittelijän sopimusten tarkastaminen ja muotoilu tietosuojanäkökulmat huomioiden ▸ Rekisteri- ja tietosuojaselosteiden laatiminen ▸ Binding Corporate Rules (BCRS) laatiminen	Arvioidaan tapaus-kohtaisesti, riippuen toimeksiannon laajuudesta

EY:n yhteyshenkilöt

Lisätietoja antavat:

Kaakkois-Suomi ja Pirkanmaa

Senior Legal Counsel
Teemu Summanen

p. +358 50 324 9086
teemu.summanen@fi.ey.com

Lounais-Suomi

Senior Legal Counsel
Tom Edelman

p. +358 400 979 067
tom.edelman@fi.ey.com

Pohjanmaa

Legal Counsel
Joe Gummerus

p. +358 40 350 7334
joe.gummerus@fi.ey.com

Legal Counsel
Ilkka Puikkonen

p. +358 40 834 6648
ilkka.puikkonen@fi.ey.com

Pohjois-Suomi ja Itä-Suomi

Partner, Legal Services
Kirsi Putkonen

p. +358 50 548 0730
kirsi.putkonen@fi.ey.com

Legal Intern
Jari Piittinen

p. +358 40 162 4687
jari.piittinen@fi.ey.com

Uusimaa

Partner, Legal Services
Riitta Sedig

p. +358 40 555 1687
riitta.sedig@fi.ey.com

Legal Counsel
Silja Järvinen

p. +358 50 406 8650
Silja.jarvinen@fi.ey.com

EY | Assurance | Tax | Transactions | Advisory

EY lyhyesti
EY on globaali tilintarkastuksen, verotuksen, liikejuridiikan, ja yritysjärjestelyiden asiantuntija ja liikkeenjohdon konsultti. Näkemyksemme ja korkealaatuiset palvelumme vahvistavat luottamusta pääomamarkkinoiden ja talouden toimintaan kaikkialla maailmassa. Kasvatamme huippuosaajia, joiden yhteistyöllä lunastamme lupauksemme ja rakennamme parempaa työ- ja liike-elämää sekä toimivampaa maailmaa asiakkaillemme, omalle henkilöstöllemme ja yhteisöille, joissa toimimme. Lisätietoja löydät internetistä www.ey.com/fi. Voit myös seurata meitä twitterissä: @EY_Suomi.

EY viittaa globaaliin organisaatioomme ja saattaa viitata yhteen tai useampaan Ernst & Young Global Limitedin jäsenyhtiöön, joista kukin on erillinen oikeushenkilö. Ernst & Young Global Limited, joka on Yhdistyneen kuningaskunnan lakien mukainen yhtiö (company limited by guarantee), ei tarjoa palveluja asiakkaille. Lisätietoja organisaatiostamme löytyy osoitteesta ey.com.

ey.com/fi

ey.com/fi/gdpr

B17012fi