Blackboardin

Miten GDPR-asetuksen toteutus Blackboardissa tukee asiakkaitamme

EU:n yleinen tietosuoja-asetus (GDPR) tuo mukanaan valtavasti muutoksia. Blackboard toivottaa omalta osaltaan nämä muutokset tervetulleiksi. Me välitämme tietosuojasta ja ymmärrämme sen olevan ihmisoikeus. GDPR vahvistaa yksilöiden oikeuksia ja johtaa tietosuojakäytäntöjen parantumiseen. Tämä puolestaan hyödyttää sekä yksilöitä että organisaatioita, sillä se lisää niiden välistä luottamusta.

Nämä materiaalit on laadittu vain tiedonantotarkoituksessa, eivätkä ne sisällä oikeudellisia neuvoja. Käänny organisaatiosi sisäisten tai ulkoisten asianajajien puoleen, mikäli sinulla on kysyttävää tai haluat lisätietoja GDPR-asetuksen toteuttamisesta organisaatiossasi tai siihen liittyvistä juridista seikoista ja kysymyksistä.

Julkaisemme ja jaamme asiakkaillemme tämän asiakirjan, jossa käsitellään GDPR-asetukseen liittyviä muutoksia ja myyttejä sekä selitetään lähestymistapamme GDPR-asetuksen toteuttamiseen ja se, miten toimemme tukevat organisaatiotasi. Tässä keskitytään pääasiassa tietoihin, joiden uskomme auttavan organisaatiotasi eniten. Siksi tätä valkoista paperia ei tule missään tapauksessa pitää kattavana GDPR-oppaana.[1]

GDPR aiheuttaa merkittäviä muutoksia, mutta me Blackboardilla käytämme jo valmiiksi erittäin toimivia tietosuojakäytäntöjä (esimerkiksi EU-US Privacy Shield -sertifiointimme). Me pidämme GDPR-asetusta mahdollisuutena käytäntöjemme vahvistamiseen. Toimimme jatkossakin asiakaskeskeisesti ja tarjoamme tukea tietosuojan vaatimustenmukaisuuden takaamisessa.

SISÄLLYSLUETTELO

GDPR – MITÄ SINUN ON TIEDETTÄVÄ

Blackboardilla on Privacy Shield -sertifiointi, ja se on ylpeä Student Privacy Pledge -sitoumuksen allekirjoittaja ja Future of Privacy Forum -tietosuojayhteisön jäsen.

GDPR on EU:n uusi tietosuojalainsäädäntö, joka korvaa nykyisen EU:n tietosuojadirektiivin 96/46 (direktiivi) ja sen täytäntöönpanevat tietosuojalait EU:n jäsenvaltioissa (esim. Yhdistyneen kuningaskunnan Data Protection Act 1998).

GDPR-asetus säädettiin vuoden 2016 toukokuussa, ja lain noudattamisvelvoite alkoi 25.5.2018.

Alla olevissa osioissa annamme erittäin lyhyen (eikä läheskään kattavan) GDPR-vaatimusten yleiskuvauksen. Linkkejä lisäohjeisiin on ”Hyödyllisiä GDPR-resursseja” -kohdassa.

Miksi uusi laki luotiin?

EU:n lainsäätäjät ja -valvojat olivat vakuuttuneita siitä, että direktiiviin olisi tehtävä päivityksiä sen harmonisoinnin puutteen sekä direktiivin voimaantulon jälkeisinä 20 vuotena tapahtuneiden yhteiskunnallisten ja teknologisten kehitysaskelten vuoksi. Lainsäädännön ensisijaisia tarpeita olivat voimakkaat täytäntöönpanovaltuudet, laajempi alueellinen kattavuus ja paremmat yksilöiden oikeudet.

Monet uusista määräyksistä (esimerkiksi alueen ulkopuolinen vaikutus) kohdistuvat pääasiassa yhteisöpalveluihin ja internetyrityksiin EU:n ulkopuolella. EU:n lainsäätäjät ja -valvojat katsoivat, että olemassa oleva direktiivi ei suojannut riittävällä tavalla yhteisöpalveluja ja internetpalveluja käyttävien EU-alueen henkilöiden tietosuojaoikeuksia.

Blackboardin toiminta eroaa yhteisöpalveluista ja muista internetyrityksistä, joiden toimintamalli perustuu käyttäjätietojen ”muuttamiseen rahaksi”. Me keräämme ja käytämme asiakkaidemme henkilötietoja[2] heidän ohjeistuksensa mukaan ja jotta voimme tarjota tuotteitamme ja palvelujamme heille ja heidän käyttäjilleen. Emme kerää tai käytä henkilötietoja myynti- tai mainontatarkoituksiin. Ymmärrämme, että henkilötiedot on annettu meidän hoidettaviksi ja että tähän liittyy velvoitteita. Tästä syystä meillä on asiakkaidemme kanssa yhteiset intressit ja vastuut näiden tietojen suojaamisen suhteen.

Mitä uutta asetus tuo mukanaan?

Vaikka GDPR perustuu olemassa oleviin EU:n tietosuojaperiaatteisiin ja -konsepteihin, se aiheuttaa huomattavia muutoksia EU:n tietosuojamenettelyissä, mukaan lukien seuraavat:

- laajemmat sakonmääräysoikeudet – sakon enimmäismäärä on nyt 4 % maailmanlaajuisesta liikevaihdosta tai 20 miljoonaan euroon (kumpi onkin suurempi)
- laajempi alueellinen kattavuus, joka koskee EU:n ulkopuolisia organisaatioita, jotka toimittavat tuotteita ja palveluja EU-maiden asukkaille tai jotka valvovat EU-alueen asukkaita
- rekisterinpitäjille määrätty velvoite antaa viranomaisille ilmoitus tietovuodosta 72 tunnin kuluessa[3]
- tiukemmat suostumusta koskevat vaatimukset
- paremmat yksilöiden oikeudet (mukana lukien oikeus poistattaa tiedot ja siirtää tiedot muualle).

Osa tärkeimmistä muutoksista koskee kuitenkin uusia sisäänrakennetun tilivelvollisuuden ja tietosuojan periaatteita. Nämä periaatteet edellyttävät tehokasta tietosuojan hallinnointia ja tietosuojaprosesseja sekä yksityiskohtaisempaa ja kattavampaa dokumentointia siitä, miten organisaatio noudattaa GDPR-vaatimuksia.

Mikä pysyy ennallaan?

Useat GDPR:n konsepteista ja määritelmistä pysyvät samoina tai ovat samankaltaisia kuin vanhassa direktiivissä:

- ”Henkilötietojen” (eli henkilökohtaisten tietojen) määritelmä pysyy pitkälti samana, mutta nyt henkilötiedoiksi katsotaan nimenomaisesti myös IP-osoitteet, evästeet ja laitetunnukset.
- ”Rekisterinpitäjän” ja ”tietojen käsittelijän” käsitteet pysyvät samoina (mutta GDPR asettaa suorempia vastuita tietojen käsittelijöille).[4]
- Direktiivissä säädetyt käsittelyä koskevat vakiintuneet periaatteet (esimerkiksi lainmukainen ja reilu käsittely, käsittelytarkoituksen rajoitus, henkilötietojen säilyttäminen vain niin pitkään kuin se on tarpeen) pysyvät ennallaan.
- Tiedonsiirtoa koskevat vaatimukset pysyvät pitkälti samoina: tiedonsiirrot EU:n ja ETA-alueen ulkopuolelle sallitaan, kunhan käytetään hyväksyttyä tiedonsiirtomekanismia (esimerkiksi EU-US Privacy Shield -tietosuojajärjestelyä tai ”mallilausekkeita”).[5]

Koska GDPR:n määräämät sakkosummat ovat suurempia, olemassa olevien periaatteiden ja vaatimusten (kuten henkilötietojen säilyttäminen vain niin pitkään kuin se on tarpeen tai asianmukaisten tietosuojatoimien toteuttaminen) noudattamatta jättämiseen liittyy todennäköisesti suurempi riski.

Mikä on Yhdistyneen kuningaskunnan EU-eron vaikutus?

GDPR-asetusta sovelletaan suoraan Yhdistyneessä kuningaskunnassa 25.5.2018 lähtien, kunnes Yhdistyneen kuningaskunnan EU-ero astuu voimaan vuoden 2019 maaliskuun lopussa. Myös EU-eron jälkeen GDPR toimii edelleen tietosuojastandardina Yhdistyneessä kuningaskunnassa:

- Yhdistyneen kuningaskunnan hallitus on julkaissut Data Protection Bill 2017 -lakiesityksen (tällä hetkellä lainsäädännöllisessä käsittelyssä), joka panee GDPR-asetuksen täytäntöön ennen EU-eroa ja sen jälkeen.[6]
- Yhdistyneen kuningaskunnan EU-eron jälkeen GDPR-asetusta sovelletaan suoraan niihin Yhdistyneen kuningaskunnan organisaatioihin, jotka tarjoavat tavaroita ja palveluja EU-maiden asukkaille tai jotka valvovat EU-maiden asukkaita (esimerkiksi Yhdistyneen kuningaskunnan yliopistoihin, jotka rekrytoivat aktiivisesti EU-alueen opiskelijoita).

Vaikutus tiedonsiirtoihin Yhdistyneestä kuningaskunnasta ja Yhdistyneeseen kuningaskuntaan:

- EU on selventänyt, että Yhdistyneen kuningaskunnan EU-eron jälkeen Yhdistynyttä kuningaskuntaa pidetään ”kolmantena maana”, mikä tarkoittaa sitä, että sitä ei pidetä enää ”riittävän” tietosuojatason (hyväksyttynä) maana tiedonsiirron osalta.
- Ellei EU:n komissio julista Yhdistynyttä kuningaskuntaa riittävän tietosuojatason maaksi ja kunnes tällainen julistus tehdään (esimerkiksi osana siirtymäsopimusta), henkilötietojen siirtoon EU:sta Yhdistyneeseen kuningaskuntaan pitää soveltaa tiedonsiirtosopimuksia tai muuta tiedonsiirtomekanismia.
- Sitä vastoin Yhdistyneen kuningaskunnan pitää määrittää, mitkä maat se katsoo riittäviksi tietosuojatason suhteen (näitä maita olisivat todennäköisesti EU-maat ja EU:n hyväksymien maiden luetteloon kuuluvat maat). Maissa, joiden tietosuojatasoa ei katsota riittäväksi, Yhdistyneen kuningaskunnan tunnustamia tiedonsiirtomekanismeja (todennäköisesti samankaltaisia kuin EU:n mekanismit) pitää soveltaa henkilötietojen siirrossa Yhdistyneen kuningaskunnan ulkopuolelle.

GDPR-asetukseen liittyviä vääriä uskomuksia

Yksi GDPR-asetuksen tavoitteista oli tarjota lisäselkeyttä yksityiskohtaisemman määritelmän avulla. Monet GDPR:ään liittyvät osa-alueet ovat silti edelleen tulkinnanvaraisia. Lisäksi GDPR-asetuksen monimutkaisuus on johtanut ymmärryksen puutteeseen sekä liioiteltuihin lausuntoihin. Tästä on syntynyt useita myyttejä, joista muutamat kumoamme seuraavassa:[7]

Uskomus 1: Kaikki henkilötietojen käsittely edellyttää suostumusta

Fakta: Suostumus on yksi lukuisista oikeusperusteista, jotka sallivat henkilötietojen käsittelyn (esimerkiksi sopimuksen täytäntöönpanon edellyttämän käsittelyn tai organisaation ”laillisten intressien” toteuttamiseksi tehdyn käsittelyn). Suostumuksen rima on nostettu erittäin korkealle. Jos esimerkiksi henkilöllä on aidosti vapaus valita ja hän voi perua suostumuksensa milloin tahansa ilman mitään haittaa, tilannetta ei katsota kelvolliseksi suostumukseksi. Monissa tiedonkäsittelytilanteissa muut oikeusperusteet ovat sopivampia.[8]

Uskomus 2: 72 tunnin ilmoitusaika tietovuototapauksissa koskee koko toimitusketjua (eli siitä hetkestä, kun (ali)käsittelijä tulee tietoiseksi tietovuodosta)

Fakta: GDPR edellyttää, että tietojen käsittelijät ilmoittavat rekisterinpitäjilleen tietovuodoista ”ilman kohtuutonta viivettä”. Todellisuudessa rekisterinpitäjää koskeva 72 tunnin ilmoitusaika alkaa vasta sitten, kun tietojen käsittelijä on ilmoittanut rekisterinpitäjälle loukkauksesta. Artiklan 29 mukainen EU:n tietosuojaviranomaisten yhteistyöelin (”Working Party” eli ”WP29”) on selventänyt lopullisissa ohjeissaan[9], että ”ilman kohtuutonta viivettä” tarkoittaa ”mahdollisimman nopeaa” ilmoitusta (eikä ”välitöntä” ilmoitusta, kuten edellisessä versiossa ehdotettiin).

Uskomus 3: Tiedonsiirtoja EU:n ja ETA-alueen ulkopuolelle ei sallita, tai ne sallitaan vain silloin, kun asiakas on hyväksynyt kunkin tiedonsiirron

Fakta: GDPR ei muuta oleellisesti olemassa olevia tiedonsiirtovaatimuksia. Tiedonsiirrot sallitaan sellaisinaan, jos käytetään EU:n hyväksymää tiedonsiirtomekanismia, kuten EU-US Privacy Shield -tietosuojajärjestelyä tai EU:n hyväksymiä mallilausekkeita (tiedonsiirtosopimuksia). Blackboard toteuttaa toiminnassaan kumpaakin näistä mekanismeista, jotta sen asiakastietojen siirrot tapahtuvat määräysten mukaisesti.[10] Koska Blackboard toimii tietojen käsittelijänä, se tarvitsee asiakkaalta tiedonsiirtoja koskevan yleisohjeistuksen (joka sisältyy vakiomalliseen tiedonkäsittelysopimukseemme), mutta asiakkaalta ei tarvita erikseen suostumusta jokaiselle siirrolle.

Uskomus 4: Poistattamisoikeus tarkoittaa, että organisaatioiden pitää poistaa kaikkia henkilöä koskevat tiedot

Fakta: Uusi tietojen poistattamisoikeus ei ole absoluuttinen ”oikeus tulla unohdetuksi”. Sen sijaan se tarkoittaa oikeutta poistattaa tiedot, jos tietoja ei enää tarvita, sekä muissa tilanteissa, joissa organisaatio ei täytä GDPR-asetuksen vaatimuksia. Jos organisaation on edelleen lain nojalla säilytettävä tiedot (esimerkiksi tietojen säilyttämisvaatimusten vuoksi), näitä henkilötietoja ei tarvitse poistaa.

Uskomus 5: GDPR koskee kaikkia yliopistoja, joissa on EU-maiden opiskelijoita

Fakta: GDPR-asetuksen soveltamiseen ei riitä pelkästään se, että yliopiston kirjoilla on EU-maiden opiskelijoita. GDPR-asetusta sovelletaan yleisesti EU-alueella toimiviin laitoksiin. Sitä sovelletaan myös EU-alueen ulkopuolisiin yliopistoihin, mutta vain siinä tapauksessa, että ne tarjoavat tavaraa ja palveluja EU-alueen henkilöille tai valvovat EU-alueen henkilöiden käyttäytymistä. ”Palvelujen tarjoamisen” katsotaan edellyttävän jonkinasteista kohdentamista. Pelkästään kirjoilla olevat EU-maiden opiskelijat eivät riitä asetuksen soveltamiseen. GDPR-asetusta voidaan kuitenkin soveltaa, kun yliopistot kohdentavat mainontansa aktiivisesti EU-maiden asukkaisiin (esimerkiksi verkkokursseilla) tai rekrytoivat aktiivisesti EU-maiden opiskelijoita. Nämä ehdot ovat tulkinnanvaraisia. Suosittelemme asiakkaita pyytämään tarvittaessa neuvoja omalta lakiasiainneuvojaltaan.

GDPR-ASETUKSEN TOTEUTTAMINEN

Miksi on tärkeää hoitaa tietosuoja-asiat ja GDRP-asetuksen soveltaminen kunnolla

4 %:n sakko maailmanlaajuisesta liikevaihdosta on varmasti riittävä syy siihen, että monet organisaatiot ovat alkaneet suhtautua tietosuojaan vakavammin. Me kuitenkin uskomme, että hyvät tietosuojakäytännöt itsessään ovat vähintään yhtä houkuttava syy tietosuoja-asioiden kunnioittamiseen, sillä tietosuoja on ihmisoikeus ja toimivat tietosuojakäytännöt parantavat luottamusta.

Nykyajan yhteiskunnassa henkilötietoja käytetään kaikkialla. Henkilötietoja kutsutaankin usein talouden ”uudeksi öljyksi”. Me kaikki käytämme verkkopalveluja ja luovutamme henkilötietojamme. Tutkimus tutkimuksen jälkeen kuitenkin on osoittanut, että organisaatioihin ei luoteta henkilötietojen suhteen. Ihmiset tuntevat menettäneensä tietojensa hallinnan. Lainsäätäjät
ja -valvojat ovat myös reagoimassa tähän. GDPR on todennäköisesti silmiinpistävin esimerkki tästä. Organisaatioiden täytyy saada (uudelleen) ihmisten luottamus. Hyvät tietosuojakäytännöt ovat keskeinen osa tätä luottamusta. Lisäksi ne tarjoavat kilpailuetua. Tietenkin ne myös auttavat organisaatioita innovoinnissa. Jos opiskelijat (ja henkilökunta) luottavat laitokseesi, he jakavat todennäköisemmin tietonsa ja käyttävät todennäköisemmin uusia työkaluja.

Tietosuoja-asioiden epäasianmukainen hoitaminen voi aiheuttaa katastrofaalisia seuraamuksia. Tietovuodoista uutisoidaan jatkuvasti. Niistä aiheutuu mainehaittaa, ihmisten luottamuksen menetystä ja oikeusvaateita niiden taholta, joiden tietoja on joutunut vääriin käsiin. Tietosuojaviranomaiset eivät välttämättä määrää 4% prosenttiin maailmanlaajuisesta liikevaihdosta yltäviä sakkoja heti alusta alkaen, mutta viranomaisilla on käytettävissään monia muitakin täytäntöönpanovälineitä. Viranomaiset voivat muun muassa pakottaa laitokset muuttamaan tietokäytäntöjään ja ottamaan käyttöön tietosuojaohjelmia, joihin kuuluvat säännölliset ulkoiset tarkastukset.

Meidän ja organisaatiosi rooli GDPR-asetuksen mukaisesti

GDPR pitää ”rekisterinpitäjän” ja ”tietojen käsittelijän” käsitteen ennallaan. Tämä käsite on ratkaisevan tärkeä, sillä se määrittää organisaatioiden ja niiden palveluntarjoajien vastuut ja velvollisuudet.

Organisaatiota pidetään rekisterinpitäjänä, jos se määrittää henkilötietojen käsittelyn ”keinot ja tarkoitukset” eli sen, miksi ja miten henkilötietoja käytetään. Tietojen käsittelijä on puolestaan organisaatio, joka toimii rekisterinpitäjän puolesta ja sen ohjeiden mukaisesti.

Valtaosan Blackboardin tuotteista ja palveluista (esimerkiksi Learn, Collaborate, Open LMS) osalta Blackboardia pidetään tietojen käsittelijänä ja sen asiakkaita rekisterinpitäjänä.

GDPR asettaa suorempia vaatimuksia tietojen käsittelijöille, kuten Blackboardille. Suurin osa GDPR-asetuksen vaatimuksista koskee kuitenkin edelleen rekisterinpitäjiä (esimerkiksi vastuu tietojen käyttötapojen ilmoittamisesta henkilöille, vastuu henkilöiden tiedonsaantipyyntöjen noudattamisesta, velvollisuus ilmoittaa tietovuodosta tietosuojaviranomaisille ja asiaankuuluville henkilöille).

Miten voit valmistautua GDPR-asetuksen voimaantuloon?

Kaikkien GDPR-asetuksen piiriin kuuluvien organisaatioiden tuli olla valmiina asetuksen voimaantuloon 25.5.2018. Seuraavassa kuvataan muutama seikka, jotka toteuttamalla asiakkaat voivat valmistautua asetuksen käyttöönottoon. Tämä vaiheiden luettelo perustuu omaan kokemukseemme, eikä sen ole mitenkään tarkoitus olla kattava. Muista pyytää tietosuoja-asiantuntijoita
avuksi asetuksen toteuttamisessa omassa organisaatiossasi. Monet tietosuojaviranomaiset ovat myös laatineet omat ohjeensa GDPR-asetuksen toteuttamisesta.[11]

Toivottavasti organisaationne on jo toteuttanut vaiheet 1–6 ja olette ottamassa käyttöön toimintasuunnitelmianne. Koskaan ei ole kuitenkaan liian myöhäistä aloittaa. Vaikka olisitte vasta aloittamassa, voitte edelleen toteuttaa kriittisimmät muutokset. Se tarkoittaa myös, että pystytte osoittamaan tietosuojaviranomaiselle, että olette laatimassa suunnitelmaa. GDPR-asetuksen huomiotta jättäminen ei ole vaihtoehto.

1 Tarkista, sovelletaanko GDPR-asetusta organisaatioosi

Jos organisaatiosi toimii EU-alueella, siihen sovelletaan GDPR-asetusta. GDPR-asetus voi koskea kuitenkin myös EU-alueen ulkopuolisia organisaatioita.[12]

2 GDPR-hankkeen luominen

Suunnittele ja toteuta GDPR-asetusta koskeva hanke. Ihanteellisessa tilanteessa hankkeelle on johdon tuki ja sille on nimetty yhteyshenkilöt, jotka voivat antaa tukea kullakin osastolla. Tämä hanke kattaa kaikki laitoksen osastot, ja tulette tarvitsemaan apua sen toteuttamisessa.

3 Nimitä kokenut GDPR-vastaava johtamaan hanketta

Vastaavan henkilön pitää olla kokenut tietosuojapäällikkö, mutta hänellä on oltava myös riittävästi aikaa ja resursseja sekä mahdollisuus ulkoiseen tukeen (esimerkiksi lakiasiaintoimiston palveluksille). Jos organisaatiosi on EU-alueen julkinen viranomainen, organisaatiosi on myös nimitettävä tietosuojavaltuutettu.

4 Varmista, että ylempi johto sitoutuu hankkeeseen ja valvoo sitä

GDPR-hankkeen toteuttaminen ilman ylemmän johdon tukea, ohjeistusta ja valvontaa on vaikeaa.

5 Tarkista organisaatiosi henkilötietojen käyttö ja suorita puutteiden analyysi

Sen ymmärtäminen, missä ja miten henkilötietoja käytetään ja missä tarvitaan GDPR-asetukseen liittyviä parannuksia, on ensimmäinen GDPR-hankkeen vaihe.

6 Kehitä toimintasuunnitelmat puutteiden korjaamiseksi Tämä on todennäköisesti vaikein GDPR-asetuksen osa, sillä se edellyttää usein erittäin tiukkojen GDPR-vaatimusten muuttamista nimenomaisiksi ja käytännöllisiksi toimiksi kaikkien erilaisten prosessien ja järjestelmien osalta.

7 Toteuta toimintasuunnitelmat

Luottamus on tärkeää, mutta hallinta on tässä tapauksessa vieläkin tärkeämpää. Tämä vaihe edellyttää muiden tahojen toimintasuunnitelmien seuraamista, jotta voidaan varmistaa, että he täyttävät määräajat.

8 Tarkista toimittajat

GDPR-asetuksen nojalla organisaatiot ovat itse vastuussa toimittajistaan. Oikeiden sopimusvelvoitteiden käyttäminen on tärkeää, mutta se ei yksinään riitä. Sinun on oltava varma siitä, että toimittajat täyttävät GDPR-asetuksen vaatimukset ja voivat tukea organisaatiotasi sen noudattamisessa. Kysy, miten ne toteuttavat GDPR-asetuksen omassa organisaatiossaan.

9 Pysy ajan tasalla lakien ja määräysten kehittymisestä (artiklan 29 mukaiset tietosuojaryhmän ohjeet, jäsenvaltioiden asetuksen täytäntöönpanevat lait)

GDPR-asetuksen tunteminen riittää, eikö niin? Väärin! Vaikka GDPR-asetusta sovelletaan suoraan, kaikki EU:n jäsenvaltiot panevat täytäntöön sitä täydentäviä kansallisia tietosuojalakeja.
Nämä vaaditaan sellaisten osa-alueiden sääntelyyn, joilla jäsenvaltioilla on lainsäädäntövaltaa (esimerkiksi työntekijöiden tietosuoja) tai joiden osalta GDPR mahdollistaa lisäsäätelyn (esimerkiksi tietosuojavaltuutettuja ja tietoturvavaikutusten arviointia koskevat ehdot). Lisäksi WP29 eli tietosuojaviranomaisten yhteistyöelin julkaisee tärkeitä ohjeita. Ajan tasalla pysyminen on haastavaa mutta tärkeää.[13]

BLACKBOARDIN SUUNNITELMA JA LÄHESTYMISTAPA

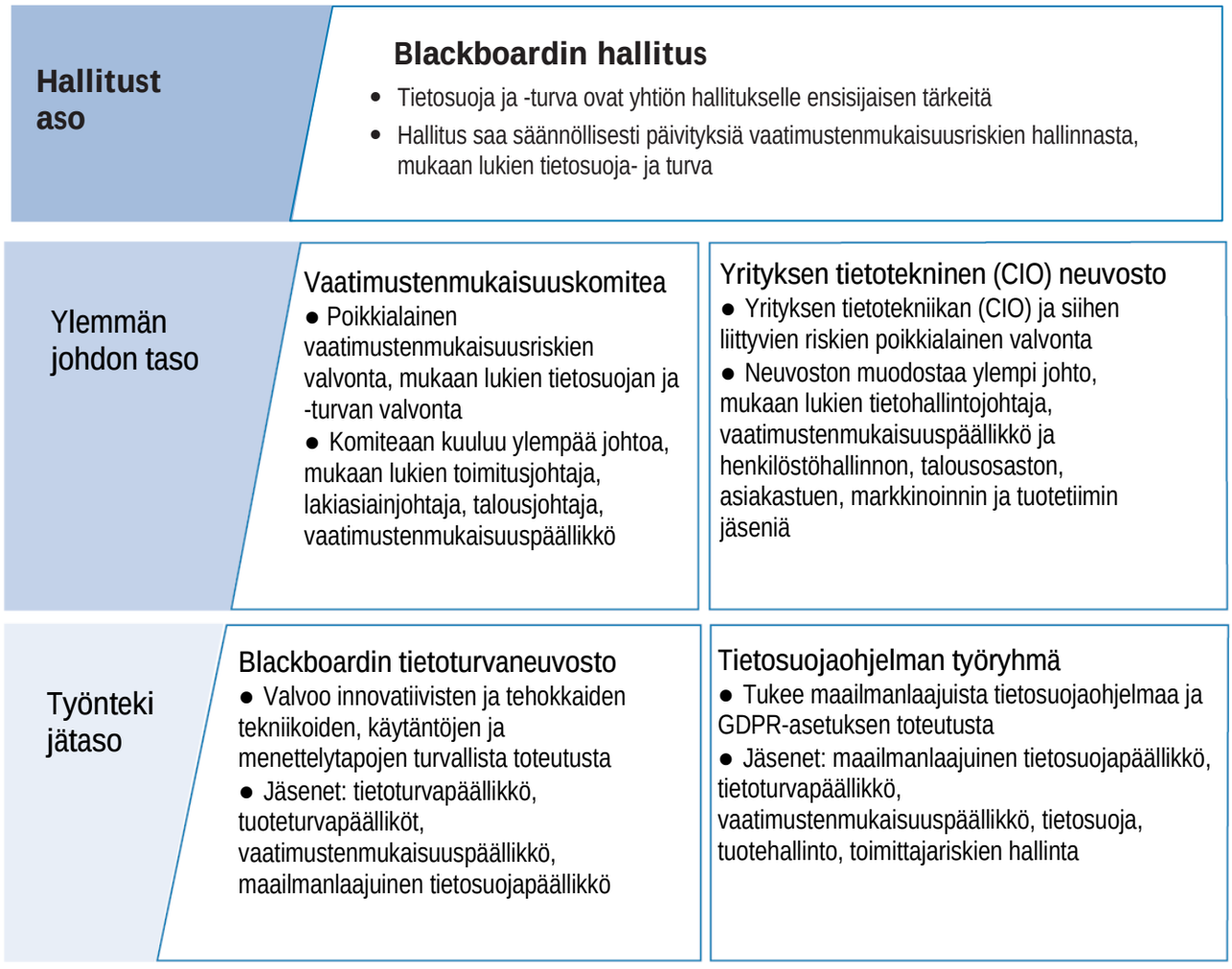
Tietosuoja ja -turva Blackboardilla

Tietosuoja- ja turva ovat olleet pitkään ensisijaisen tärkeitä Blackboardille. Meille GDPR on mahdollisuus vahvistaa entisestään olemassa olevia tietosuojakäytäntöjämme.

Lähestymistapamme tietosuoja-asioihin on aina ollut asiakaskeskeinen. Ymmärrämme haasteet, joita asiakkaillamme on, ja haluamme auttaa sinua niiden kanssa.

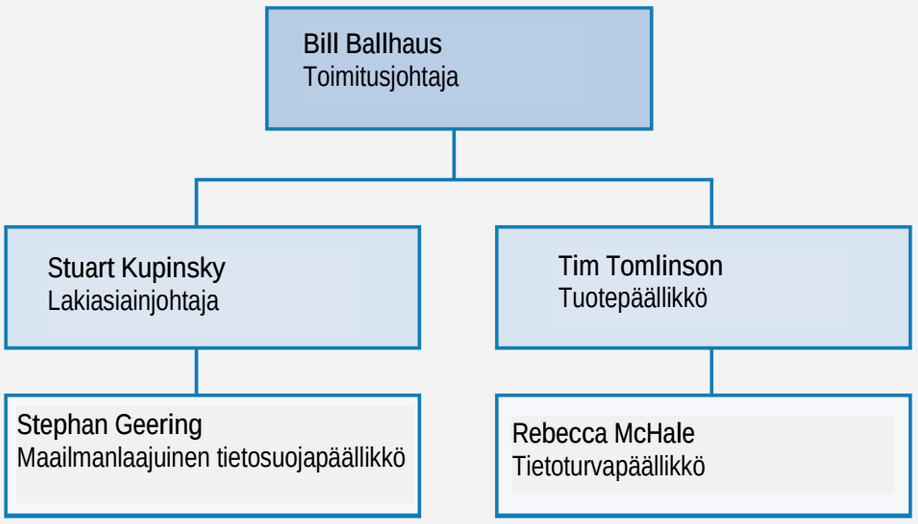
Hyvät tietosuojakäytännöt edellyttävät luotettavaa hallintomallia. Meillä Blackboardilla tietosuoja ja -turva ovat yhtiön hallitukselle prioriteetteja, ja hallintomallimme (katso alla) takaa, että ylempi johto valvoo ja tukee tietosuojaan ja -turvaan liittyviä toimiamme.

Maailmanlaajuinen tietosuojapäällikkömme (Global Privacy Officer) ja tietoturvapäällikkömme (Chief Information Security Officer)[14] raportoivat toimitusjohtajan johtoryhmälle (katso alla oleva organisaatiokaavio). Tämä korostaa entisestään sitä, miten paljon Blackboard arvostaa tietosuojaa ja -turvaa.



Tietosuoja ja -turva

Maailmanlaajuinen tietosuojapäällikkömme (Global Privacy Officer) ja tietoturvapäällikkömme (Chief Information Security Officer) raportoivat toimitusjohtajan johtoryhmälle, mikä korostaa entisestään sitä, miten paljon Blackboard arvostaa tietosuojaa ja -turvaa.



Blackboardin lähestymistapa GDPR-asioihin

Olemme luoneet kattavan hankkeen, jonka avulla toteutamme GDPR-asetuksen vaatimukset seuraavaa lähestymistapaa käyttäen:

- GDPR-asetuksen toteuttaminen perustuu Blackboardin olemassa olevaan kokemukseen tietosuoja-asioista sekä vaatimustenmukaisuusmekanismeihin.
- GDPR-asetuksen toteutusta johtaa maailmanlaajuinen tietosuojapäällikkö, ja sitä tukevat GDPR-hankejohtaja ja kunkin toiminta-alueen ”GDPR-vastaavat”.
- Muun muassa kuuluisa lakiasiaintoimisto Bristows LLP on palkattu tukemaan GDPR-asetuksen toteutusta.
- GDPR-asetuksen toteutusta valvoo Blackboardin vaatimustenmukaisuuskomitea, johon kuuluvat yhtiön toimitusjohtaja, lakiasiainjohtaja ja muita ylempiä toimihenkilöitä.

GDPR mahdollisuutena

Me uskomme, että GDPR-asetuksen toteutus ei ole pelkästään hanke, jolla pyritään täyttämään EU:n uudet tietosuojavaatimukset, vaan myös mahdollisuus. Pyrimme soveltamaan GDPR-asetusta sellaisenaan seuraavien tavoitteiden saavuttamiseen:

- maailmanlaajuisten tietosuojakäytäntöjen vahvistaminen – käytämme GDPR-hanketta maailmanlaajuisen tietosuojaohjelman parantamiseen EU-alueella ja muualla
- sellaisten sisäänrakennettujen tietosuojan prosessien kehittäminen, jotka tekevät tietosuojavaatimusten noudattamisesta osan päivittäisiä prosessejamme
- asiakkaidemme tukeminen niiden GDPR-vaatimustenmukaisuustoimissa
- Blackboardin asemointi tunnustetusti johtavana toimijana tietosuoja-asioiden parissa koulutustekniikan alalla.

Toteutussuunnitelmamme

Noudatamme Bristow LLP:n määrittämää kolmevaiheista menetelmää maailmanlaajuisen tietosuoja- ja GDPR-ohjelmamme toteuttamisessa. Tätä menetelmää käyttävät myös lukuisat muut yritykset, mukaan lukien johtavat teknologia-alan yritykset. Sen kolme keskeistä vaihetta ovat seuraavat:

- **1. VAIHE: tiedonkeruu**
- **2. VAIHE: ratkaisujen kehitys**
- **3. VAIHE: toteutuksen työvirrat**

Olemme käyttäneet tätä kolmevaiheista menetelmää ohjelmamme kehittämiseen seuraavia neljää keskeistä porrasta käyttäen:

Hankkeen aloitus

Hankkeen aloitusvaiheessa tehtiin seuraavat toimet:

- tiedottaminen ylemmälle johdolle ja sen sitouttaminen
- maailmanlaajuisen tietosuojapäällikön palkkaaminen; hänen vastuullaan on johtaa GDPR-hanketta
- hankesuunnitelman kehitys ja hankkeen hallinnointi
- alustava tiedonkeruu ja nykyisten vaatimustenmukaisuustoimien arviointi GDPR-asetuksen nojalla parannusta kaipaavilla osa-alueilla.

1. VAIHE: tiedonkeruu (työpajat)

Tämän alkuvaiheen aikana kävimme jäsennettyjä keskusteluja ja työpajoja Blackboardin toiminta-alueiden ja tuoteryhmien keskeisten sidosryhmien kanssa tarkoituksenamme saada yksityiskohtaisia tietoja näiden alueiden tiedonkäsittelykäytännöistä.

Työpajoista saatua palautetta käytettiin puutteiden analysoinnissa ja 2. vaiheen ratkaisujen ja toteutussuunnitelmien kehittämisessä.

2. VAIHE: ratkaisujen kehitys

Kehitimme seuraavat ratkaisut ja ohjeet työpajoista saatujen tietojen perusteella:

- paremmat sisäiset tietosuojaohjeet (käytäntö ja yksityiskohtaiset toimintanormit), jotka vastaavat GDPR-asetuksia ja joissa selitetään, miten GDPR-asetuksen vaatimukset on täytettävä erilaissa tiedonkäsittelytoimissa (esimerkiksi asiakastietojen käsittelyvaatimukset, sisäänrakennetun tietosuojan prosessi)
- tuotevaatimukset
- toiminta-alueiden ja keskitetysti toteuttavien toimien toteutussuunnitelmat.

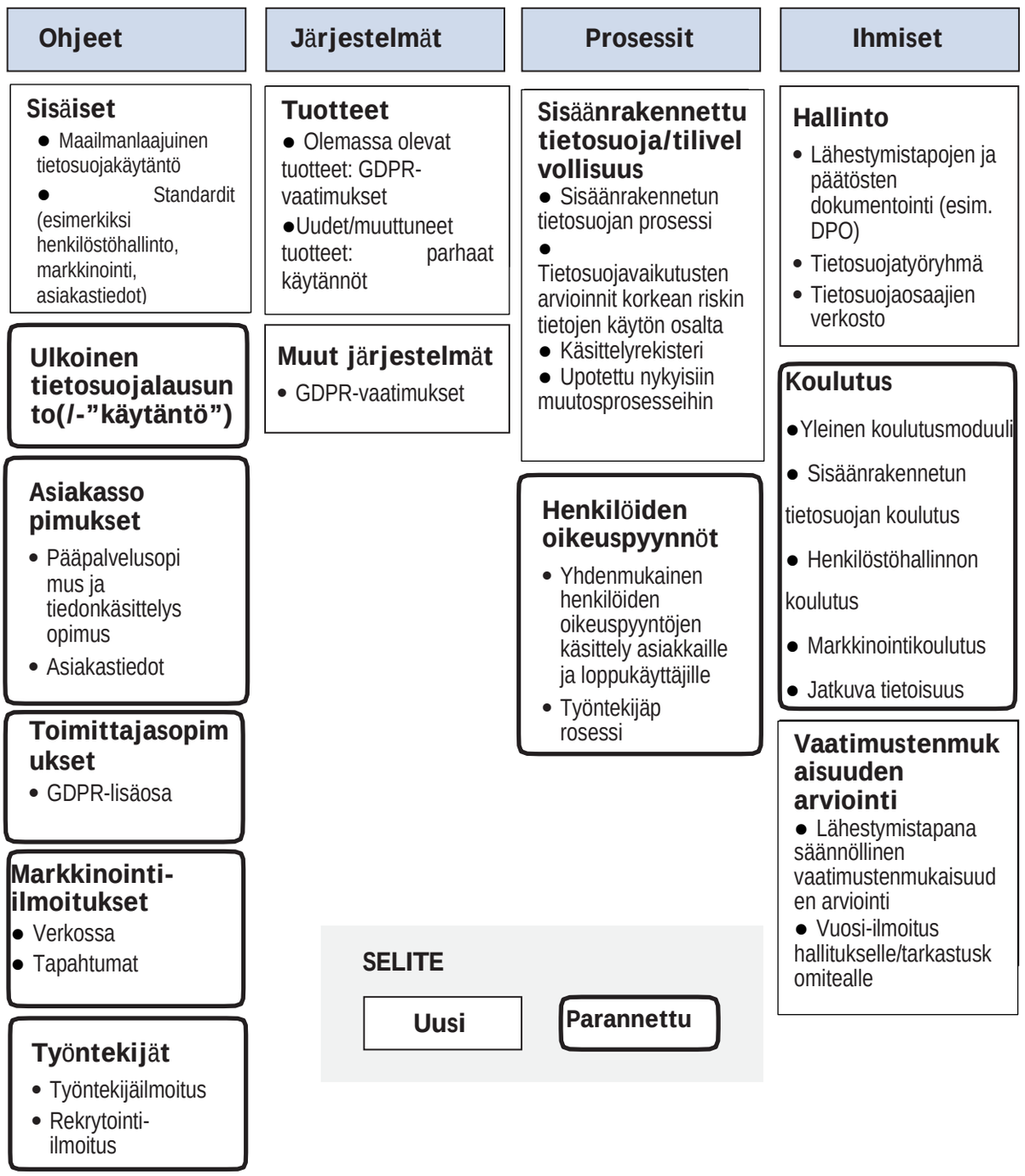
3. VAIHE: toteutuksen työvirrat

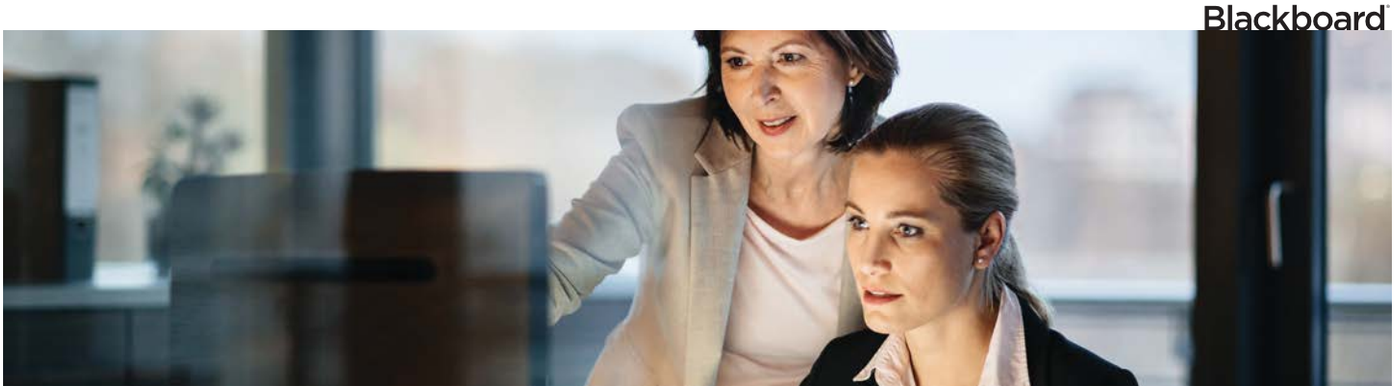
Loppuvaiheessa otamme käyttöön kehitetyt tietosuojaohjeet ja panemme toteutussuunnitelmat täytäntöön. Toteutuksen saavuttamiseen käytetään kuutta päätyövirtaa:

1. toiminta-alueiden ja tuoteryhmien toteutussuunnitelmien täytäntöönpano
2. suurta yleisöä koskevien käytäntöjen, ilmoitusten ja suostumusten tarkastus ja päivitys
3. hallinnoinnin parantaminen (roolit ja vastuualueet, koulutus, sisäänrakennettu tietosuoja jne.)
4. toimittajasopimusten tarkastus ja päivitys (tarvittaessa)[15]
5. IT-järjestelmän muutokset (tarvittaessa)
6. tiedonkäsittelyrekisterin luonti.

Muutosten yleiskuvaus

Alla olevassa kaaviossa esitetään, miten näemme GDPR- ja tietosuojaohjelmamme lopputilan toteutustoimien jälkeen. GDPR-asetuksen toteutuksen jälkeen jatkamme edelleen innovointia ja sopeutumista ja pyrimme siten tekemään tietosuojakäytännöistämme entistäkin kypsempiä.





MITEN GDPR-OHJELMAMME AUTTAA SINUA?

Blackboardin maailmanlaajuinen tietosuoja- ja GDPR-toteutusohjelma keskittyy organisaatiosi tukemiseen GDPR-asetuksen toteutuksessa. Seuraavissa osioissa annetaan aiheesta lisätietoja. Toteutuksen keskeiset seitsemän avainkohtaa ovat pääpiirteissään seuraavat:

1. **GDPR-yhteensopivat tuotteet:** otamme käyttöön tuotevaatimukset tukeaksemme asiakkaitamme läpinäkyvyysvaatimusten, henkilöiden oikeuspyyntöjen jne. osalta.
2. **Sisäänrakennettu tietosuoja:** toteutamme sisäänrakennetun tietosuojan ja tietosuojavaikutusten arvioinnin (DPIA) prosessin vaatimustenmukaisuuden dokumentoinnin edistämiseksi.
3. **Tiedonsiirrot:** Jatkamme monitasoista lähestymistapaamme: alueellistaminen, EU-US Privacy Shield ja EU:n hyväksymät mallilausekkeet.
4. **Sopimukset asiakkaiden kanssa:** meillä on GDPR-yhteensopiva tiedonkäsittelylisäosa, joka lisätään vakiomalliseen pääsopimukseemme.
5. **Toimittajillemme:** käytämme kattavia sopimuksia ja sovellamme toimittajien riskienhallinnan puitekehystä.
6. **Tietoturva:** olemme määrittäneet käytännön, menettelytavat ja hallintotavat, joita parannetaan jatkuvasti asiakastietojen tietoturvan suojaamiseksi.
7. **Tietovuodoista ilmoittaminen:** olemme dokumentoineet ja testanneet tietoturvahäiriöiden toimintaprosessin.

1. GDPR-yhteensopivat tuotteet

Yksi tärkeimmistä toteutuksen työvirtamme osa-alueista on asiakkaidemme tukeminen tekemällä tuotteistamme GDPR-yhteensopivia. Tätä varten olemme määritelleet tuotteillemme GDPR-asetuksen ja tietosuojan vähimmäisvaatimukset. Pyrimme vahvistamaan tietosuojakäytäntöjämme maailmanlaajuisesti, ja tämän mukaisesti suurin osa näistä vaatimuksista koskee kaikkia tuotteitamme eikä vain EU-alueella tarjoamiamme tuotteita. Tämä tukee myös EU-alueen ulkopuolisia asiakkaitamme, jotka voivat kuulua GDPR-asetuksen piiriin.

Olemme kehittäneet GDPR-asetuksen ja tietosuojan tuotevaatimuksemme pitkällisen ja kattavan prosessin seurauksena. Laadimme alustavan version ulkopuolisen lainopillisen neuvojan kanssa. Käsittelimme vaatimuksia useissa käsittelyistunnoissa tuotekehitys- ja tuotehallintatiimiemme keskeisten sidosryhmien kanssa ja teimme niihin useita muutoksia. Näin saimme hiottua vaatimukset täsmällisiksi ja toteuttamiskelpoisiksi yleisiksi tuotevaatimuksiksi ja niihin liittyviksi yksityiskohtaisiksi ohjeiksi. GDPR-asetukseen ja tietosuojaan liittyvät tuotevaatimuksemme on myöhemmin muunnettu tuotekohtaisiksi toimiksi kunkin tuoteryhmän tuotteiden toteutussuunnitelmissa.

Tuotevaatimuksemme[16] voidaan luokitella seuraavasti:

Läpinäkyvyys

- Asiakkaat voivat linkittää tietosuojakäytäntöihinsä ja -ilmoituksiinsa
- Annamme tietoja siitä, miten henkilötietoja yleensä käytetään tuotteessa

Tietojen vähentäminen tai poistaminen

- Tuotteiden tarkastaminen tarpeettomien/valinnaisten kenttien suhteen
- Tuotteiden tarkastaminen sen suhteen, onko niissä mahdollista käyttää pseudonymisoituja tai anonyymejä tietoja henkilötietojen sijaan
- Mahdollisuus poistaa henkilötiedot, kun asiakkaat sitä pyytävät (jos asiakkaat/käyttäjät eivät voi poistaa tietoja itse)

Yleiset yksilön oikeudet

- Mahdollisuus päästä käsiksi henkilötietoihin ja korjata ne, jos kyseinen henkilö sitä pyytää
- Mahdollisuus poistaa henkilötiedot, jos kyseinen henkilö sitä pyytää

Yksilön oikeudet EU:ssa

- Mahdollisuus käsitellä tietojen siirrettävyyteen liittyvät pyynnöt (yksilöiden oikeus saada tiedot konekielisessä muodossa tietyissä olosuhteissa)
- Mahdollisuus lopettaa henkilötietojen käyttö (oikeus kieltää käyttö tai oikeus rajoittaa käyttöä tietyissä olosuhteissa)

Blackboard on jo määrittänyt tuotteiden tietoturvaohjelmat, joissa huomioidaan GDPR-asetus. Tästä syystä emme ole määrittäneet mitään muita GDPR-asetusta koskevia tietoturvavaatimuksia.[17]

2. Sisäänrakennettu tietosuoja

Koska yksittäisten ihmisten on nykypäivän maailmassa koko ajan vaikeampi hallita omia tietojaan (katso tietosuojapäivän blogissamme julkaistu kirjoitus tästä aiheesta), sisäänrakennettu tietosuoja ja tilivelvollisuus nousevat koko ajan tärkeämpään rooliin yksilöiden, asiakkaiden ja sääntelyviranomaisten luottamuksen säilyttämisen sekä organisaation GDPR-vaatimustenmukaisuuden dokumentoinnin kannalta. Tästä syystä teemme sisäänrakennetun tietosuojan lähestymistavastamme keskeisen osan maailmanlaajuista tietosuoja- ja GDPR-ohjelmaamme.

Blackboardin kannalta tämä on osa kehitystä eikä suinkaan vallankumous. Olemme aina tehneet oikeudellisia arviointeja uusille tuotteillemme ja käytännöillemme. Sisäänrakennetun tietosuojan lähestymistapamme ansiosta virallistamme ja dokumentoimme nämä arvioinnit paremmin.

Lähestymistapa

- Olemme luoneet dokumentoidun sisäänrakennetun tietosuojan prosessin ja tarkistuslistan.
- Toiminta-alueet ja tuoteryhmät lisäävät sisäänrakennetun tietosuojan tarkistuslistan osaksi muutosprosessejaan.
- Jokainen keskeinen henkilötietojen käyttöön liittyvä muutos edellyttää sisäänrakennetun tietosuojan tarkistuslistan täyttämistä. Vaikka GDPR ei nimenomaisesti tätä edellytä, se on paras käytäntö.
- Tarkistuslista aikaansaa yksityiskohtaisemman tietosuojavaikutusten arvioinnin (DPIA) henkilötietojen korkean riskin käytön osalta (mikä on GDPR-asetuksen vaatimus).

Alla olevassa vuokaaviossa havainnollistetaan tätä lähestymistapaa:

3. Tiedonsiirrot

GDPR ei aiheuta huomattavia muutoksia siihen, miten henkilötietoja voidaan siirtää EU- ja ETA-alueen ulkopuolelle. Nykyiset rajoitukset ja tiedonsiirtomekanismit pysyvät ennallaan. Tämä tarkoittaa sitä, että tiedonsiirrot sallitaan sellaisinaan, jos käytetään EU:n hyväksymää tiedonsiirtomekanismia, kuten EU-US Privacy Shield -tietosuojajärjestelyä tai EU:n hyväksymiä mallilausekkeita (tiedonsiirtosopimuksia). Näillä mekanismeilla taataan henkilötietojen riittävä suojaus myös silloin, kun tietoja siirretään EU- ja ETA-alueen ulkopuolelle.

Jatkamme monitasoista ja varmentavaa lähestymistapaamme tiedonsiirron vaatimustenmukaisuuteen. Tämä tarkoittaa sitä, että paneudumme tiedonsiirron vaatimuksiin useilla tavoilla ja varmistamme näin, että tietosi on suojattu asianmukaisin suojaustoimin:

- **Alueellinen isännöinti:** Meillä on alueellinen isännöintistrategia lähes kaikille EU-alueella isännöidyille tuotteillemme ja muille tuotteillemme, jotka aiotaan siirtää alueellisiin isännöintiratkaisuihin. Vaikka GDPR ei edellytä alueellista säilytystä emmekä me usko, että tietojen lokalisointi parantaa tietosuojaa tai -turvaa,[18] ymmärrämme myös, että monet EU-asiakkaat haluavat tietojaan säilytettävän EU-alueella.
- **Privacy Shield:** Blackboard on EU-US Privacy Shield -sertifioitu yritys, minkä ansiosta voimme siirtää henkilötietoja laillisesti Yhdysvaltoihin.
- **Mallilausekkeet:** Käytämme myös EU:n hyväksymiä ”mallilausekesopimuksia”, joiden ansiosta voimme siirtää henkilötietoja ETA-alueen ulkopuolelle lakien mukaisesti Blackboard-konsernin sisällä (”asiakastietojen siirtosopimus”).
- **Toimittajat:** Olemme solmineet kattavia sopimuksia toimittajien ja kumppanien (esimerkiksi IBM, Amazon Web Services) kanssa sen varmistamiseksi, että tiedonsiirtovaatimukset (ja muut tietosuojaa koskevat velvoitteet) välitetään toimittajillemme ja kumppaneillemme.

Meillä on tällä hetkellä[19] EU-asiakkaillemme useita alueellisia konesaleja, jotka tukevat tiedonkäsittelyä EU-alueella:

- hallinnoitu isännöinti (Blackboardin konesalit) – konesalit Amsterdamissa (Hollannissa) ja Frankfurtissa (Saksassa).
- pilvi-isännöinti (AWS-konesali) – AWS-alue Frankfurt, Saksa (eu-keskus-1).

AWS-konesalit vastaavat lukuisia sertifiointeja ja vaatimuksia, joita ovat mm. ISO 27001 ja ISO 27018 sekä SOC2. Lisäksi ne vastaavat GDPR-asetuksen vaatimuksia sekä paikallisia vaatimuksia, kuten Saksan C5- ja IT-Grundschutz-vaatimuksia.[20]

On tärkeää ymmärtää, että vaikka näissä konesaleissa säilytetään useimpien EU-alueen asiakastuotteiden sisältämiä asiakkaiden henkilötietoja (mukaan lukien Learn 9.1, Learn SaaS, Open LMS ja Collaborate), näihin tietoihin voidaan tarvita pääsyä EU- ja ETA-alueen ulkopuolelta tuotteiden ja palvelujen (esimerkiksi ympärivuorokautisen, joka viikonpäivä toimivan asiakastuen) tarjoamiseksi. Tällaiset tiedonsiirrot sallitaan edellä mainitun EU-US Privacy Shield -sertifioinnin ja mallilausekkeiden ansiosta.

4. Sopimukset asiakkaiden kanssa

Vanha direktiivi edellyttää, että rekisterinpitäjä on solminut toimittajan (tietojen käsittelijän) kanssa sopimuksen, mutta siinä ei määritellä yksityiskohtaisesti sopimuksen sisältöä. GDPR on tarkempi ja sisältää luettelon vaaditusta sisällöstä.[21]

Nykyinen vakiomallinen tiedonkäsittelylisäosamme sisältää kaikki vaaditut alla esitetyt seikat. Se lisätään automaattisesti niiden asiakkaidemme vakiomallisiin pääsopimuksiin, jotka kuuluvat GDPR-asetuksen piiriin.

- ✓ Henkilötietoja saa käyttää vain asiakkaan ohjeistuksen mukaan.
- ✓ Henkilöstön pitää allekirjoittaa luottamuksellisuussopimus.
- ✓ Asianmukaiset tietoturvatoimet pitää ottaa käyttöön.
- ✓ Tiedonkäsittelyyn saa käyttää vain toimittajia (alikäsittelijöitä)...
  - jotka rekisterinpitäjä on valtuuttanut (voi olla yleinen valtuutus)
  - joiden on sopimuksen velvoittamana noudatettava samoja tietosuojavelvoitteita.
- ✓ Rekisterinpitäjää on autettava yksilön oikeuspyyntöihin vastaamisessa.
- ✓ Rekisterinpitäjää pitää auttaa tietoturvatoimissa, tietovuodoista ilmoittamisessa ja tietosuojavaikutusten arvioinnissa.
- ✓ Tiedot on palautettava tai poistettava sopimuksen rauetessa.
- ✓ Rekisterinpitäjälle on annettava tiedot, joita se tarvitsee vaatimustenmukaisuuden osoittamiseen.
- ✓ Rekisterinpitäjälle on ilmoitettava välittömästi, jos jokin rekisterinpitäjän ohje on GDPR-asetuksen vastainen.

5. Toimittajien hallinta

Blackboard käyttää toimittajia (joita ovat esim. IBM, Amazon Web Services) tuotteiden ja palvelujen toimittamiseen asiakkaillemme. Jos tämä edellyttää pääsyä asiakkaidemme henkilötietoihin, Blackboard on vastuussa toimittajien tietosuojakäytännöistä.

Osana GDPR-ohjelmaamme yhdistämme tietosuojan sisäänrakennetusti olemassa oleviin toimittajien riskienhallinta- ja hankintaprosesseihin. Tästä seuraavat keskeiset valvontatoimet:

- Solmimme kolmansien osapuolten kanssa kattavat sopimukset ja tietosuoja- ja GDPR-lisäosan, jotka asettavat olennaisesti vastaavat määräykset kuin meillä on asiakkaidemme kanssa.
- ”Mallilausekesopimukset” ja/tai GDPR- ja Privacy Shield -lisäosat mahdollistavat lailliset tiedonsiirrot toimittajillemme.
- Dokumentoitu toimittajien riskinhallintakäytäntö- ja puitekehys.
- Uusien toimittajien, jotka tarvitsevat pääsyn henkilötietoihin, pitää täyttää toimittajien tietoturva-arviointikysely, jossa on tietosuojan vaatimustenmukaisuutta koskevia kysymyksiä.
- Toimittajien, joilla on pääsy Blackboardin hallinnoimiin järjestelmiin, pitää noudattaa Blackboardin sisäistä käyttöoikeusvalvontaa ja identiteetti- ja valtuutuskäytäntöjä, joihin kuuluu tarpeen mukaan tilien tarkastuksia.
- Toimittajat tarvitset pääsyn Blackboardin resursseihin hyväksytyillä mekanismeilla (esim. VPN-yhteydellä).
- Toimittajilla on rajoitettu käyttöoikeusvalvonta liikenteelle, käyttäjille ja resursseille.

6. Tietoturva

GDPR ei muuta oleellisesti henkilötietojen tietoturvan teknisiä ja toiminnallisia toimia (”TOM”). Näiden toimien pitää olla ”sopivia” niihin liittyvän riskin suhteen, kuten vanhassakin direktiivissä määriteltiin. Tästä syystä luotamme kehittämiimme tietoturvaohjelmiin jatkossakin.

Tietosuojariskien hallinnointi

Olemme määrittäneet käytäntö-, toimenpide-, hallinnointi- ja tekniset vaatimukset, jotka koskevat IT-tietoturvariskien hallintaa koko yrityksessä.

Blackboardin henkilöstön pitää alusta alkaen ja aina ymmärtää vastuunsa asiakkaiden henkilötietojen suojaamisessa:

- hyväksyttävä arkaluonteisten tietojen suojaamista koskeva käytäntö
- vuosittainen käyttäjien tietoturvaa ja -suojaa koskeva koulutus
- tiedonkalasteluharjoituksia
- tiedotelehtisiä.

Sovellamme seuraavia henkilöstömme tietosuojaa koskevia käytäntöjä:

- Tietojen luokittelu määritetään kunkin tietotyypin suojaamisvaatimusten mukaan. Kaikkein arkaluonteisimpia tietoja ovat asiakkaidemme tiedot – tiedot laitoksista ja niiden opiskelijoista.
- Tietoja suojataan teknisin toimin, joita ovat esimerkiksi
  - salauksen käyttö
  - mahdollisimman nopeat tietoturvapäivitykset
  - parannettu todennuksen valvonta
  - haittasähköposteilta ja haitalliselta verkkoliikenteeltä suojautuminen
  - päätepisteiden suojaustekniikat
  - käyttöoikeuksien rajoitus tiedonsaantitarpeen mukaan.

Kyse ei ole vain GDPR-asetuksesta…

Maailmanlaajuisesti toimivana koulutusyhteisöä palvelevana yhtiönä seuraamme tarkasti oleellisia alue- ja koulutussektorikohtaisia tietosuojaa ja -turvaa koskevia lakeja ja määräyksiä.

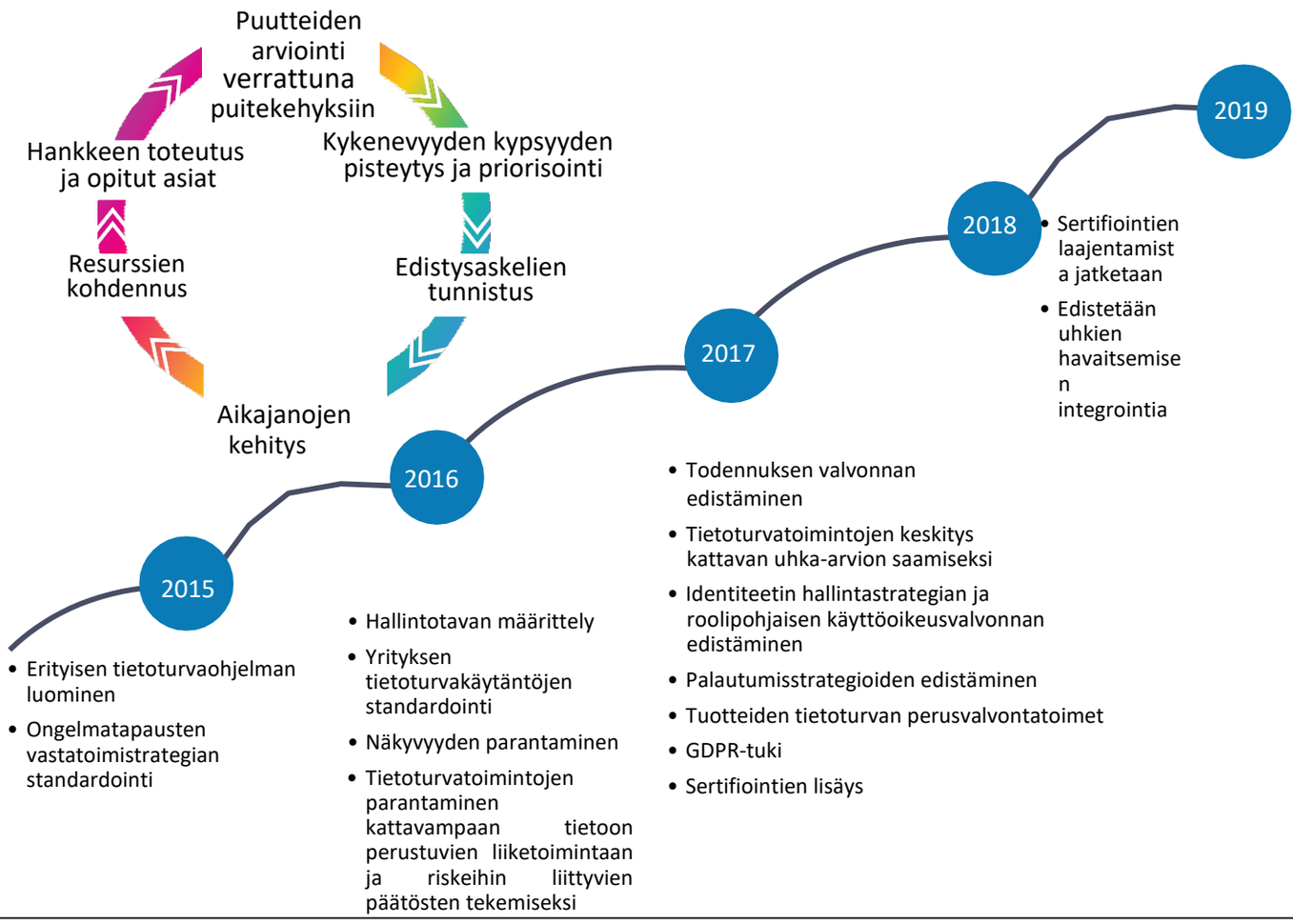
Alla luetellaan muutamia esimerkkejä tietoturvaa ja -suojaa koskevista määräyksistä, standardeista ja puitekehyksistä, jotka Blackboard huomioi GDPR-asetuksen lisäksi kehittäessään tietoturvakäytäntöjään, -prosessejaan ja teknisiä valvontatoimiaan.

- US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
- US Children’s Online Privacy Protection Act (COPPA)
- Yhdysvaltain osavaltioiden lait (olemassa olevat ja vireillä olevat 50 osavaltion lait)
- Yhdysvaltion valtionhallinnon standardit – FedRAMP
- PCI-tietoturvastandardit, jos tarpeen
- ISO/IEC, OWASP, NIST
- kansainväliset standardit (MTCS, IRAP).

Tietoturvan kypsyysarvioinnit ja toimintasuunnitelmat

Pyrimme koko ajan parantamaan teknisiä ja toiminnallisia tietoturvatoimiamme. Seuraavan sivun kaavio havainnollistaa jatkuvia kypsyysarviointejamme ja toimintasuunnitelmiamme.

Puitekehysten käyttöönotto: tietoturvan kypsyysarvioinnit ja toimintasuunnitelmat



7. Tietovuodoista ilmoittaminen

Yksi keskeisistä GDPR-asetusten mukanaan tuomista muutoksista on velvollisuus ilmoittaa tietovuodoista toimivaltaiselle tietosuojaviranomaiselle ja (joissain tapauksissa) henkilöille, joita tietovuoto koskee.[22]

Valtaosan Blackboardin tuotteista ja palveluista osalta Blackboard on GDPR-asetuksen mukaan tietojen käsittelijä.[23] Blackboardia koskevan tietovuodon tapauksessa asiakkaillamme on siis velvollisuus ilmoittaa tietovuodosta tietosuojaviranomaisille ja asiaankuuluville henkilöille. GDPR-asetus kuitenkin edellyttää, että tietojen käsittelijät, kuten Blackboard, ilmoittavat asiakkailleen (rekisterinpitäjilleen) tietovuodoista ilman kohtuutonta viivettä (eli mahdollisimman pian).[24]

Me sovellamme seuraavia toimia, jotka tukevat asiakkaitamme heidän velvollisuuksiensa täyttämisessä, jos Blackboardilla tapahtuu asiakkaaseen liittyvä tietovuoto:

- Blackboardin tietoturvahäiriöiden vastatoimi (SIR) -prosessi
  - dokumentoitu ja säännöllisesti testattava
  - helpottaa tietoturvahäiriön ilmetessä nopeaa tunnistusta, tutkintaa ja tilanteen korjaamista
  - mahdollistaa mahdollisimman nopeat ilmoitukset asiakkaille
  - pohjautuu määriteltyyn tietoturvahäiriöiden vastatoimitiimiin (johon kuuluvat tietoturvapäällikkö ja maailmanlaajuinen tietosuojapäällikkö).
- Meillä on velvollisuus ilmoittaa asiakkaille mahdollisimman pian, kuten vakiomallisessa pääsopimuksessamme ja tietosuojalisäosassamme nimenomaisesti on mainittu.[25]

YHTEENVETO

GDPR edellyttää huomattavia muutoksia, joiden vaikutukset jatkuvat asetuksen voimaantulopäivämäärän (25.5.2018) jälkeenkin. Toivomme, että tämä valkoinen paperi voi auttaa organisaatiotasi toteuttamaan GDPR-asetuksen vaatimat muutokset. Lisäksi toivomme tämän valkoisen paperin osoittavan, miten vakavasti Blackboard suhtautuu GDPR-asetuksen ja tietosuojavaatimusten noudattamiseen.

Seuraavassa on hyödyllisiä lisätietoja sekä sähköpostiosoite yhteydenottoja varten, jos sinulla on jotain kysyttävää tai palautetta tästä valkoisesta paperista.

HYÖDYLLISIÄ GDPR-RESURSSEJA

Alla linkitetyt resurssit ovat vain pieni valikoima verkossa saatavissa olevasta hyödyllisestä materiaalista. Tämän ei ole tarkoitus olla kattava luettelo.

Jos haluat yksityiskohtaisempaa analyysiä GDPR-asetuksen vaikutuksesta organisaatioosi, pyydä neuvoja asiantuntijoilta. On tärkeää luottaa kokeneisiin tietosuoja-asiantuntijoihin (esimerkiksi lakiasiaintoimiston asiantuntijoihin).

Viralliset EU-resurssit

- GDPR-teksti
- Artikla 29, tietosuojatyöryhmän ohjeet
- EU-komission GDPR-verkkosivusto

EU:n tietosuojaviranomaisten materiaalit

- Yhdistyneen kuningaskunnan tietosuojavirastolla (ICO) on erinomainen GDPR-verkkosivusto, jossa on hyödyllistä, yksinkertaisesti muotoiltua aineistoa, jota päivitetään jatkuvasti.
- Irlannin tietosuojakomissaarilla (DPC) on oma GDPR-sivunsa organisaatioita varten.
- Ranskan CNIL-viranomainen tarjoaa jonkin verran sisältöä englanniksi, mm. ilmaisen tietosuojavaikutusten arviointiohjelmiston (ja paljon muuta sisältöä ranskaksi).
- Espanjan AEPD on laatinut koulutuslaitoksille tarkoitetun oppaan (PDF, espanjaksi)

Lakiasiaintoimistojen oppaat

- Bird & Birdin GDPR-ohje
- Bird & Birdin jäsenvaltioiden lakien seurantaopas
  (luettelee kansalliset GDPR-vaihtelut)
- Linklatersin GDPR-eloonjääntiopas (PDF)
- White & Casen GDPR-käsikirja

Muut organisaatiot

- JISC UK:lla on hyödyllisiä resursseja, tapahtumia ja blogipäivityksiä GDPR-asetukseen liittyen.
- UCISA on julkaissut GDPR:n parhaan käytännön asiakirjan, jossa esitetään käytännön vaiheita ja tapaustutkimuksia.
- International Association of Privacy Professionals (IAPP) -järjestöllä on hyvä (ilmainen) viikoittainen uutiskirje Euroopan tietosuoja-asioiden kehittymisestä.
- IAPP:llä on myös hyödyllinen tietosuojatyökalujen yleiskuvaus (PDF).
- Amazon Web Servicesillä on oma GDPR-keskuksensa.

HENKILÖKUVAUKSET

Stephan Geering

Maailmanlaajuinen tietosuojapäällikkö

- Maailmanlaajuinen vastuu tietosuojaan ja -turvaan liittyvien lakien noudattamisesta
- Johtaa maailmanlaajuista tietosuoja- ja GDPR-toteutusohjelmaa
- Raportoi lakiasiainjohtajalle; kuuluu Blackboardin lakiasiaintiimiin
- Toimii Lontoosta käsin

Stephanin tausta:

- lakimies / apulaistietosuojakomissaari Sveitsin kantonien tietosuojavirastossa (2002–2008)
- OTK, University College London (2008–2009)
- Apulaisjohtaja, konsernin tietosuojaosasto Barclaysilla (2010–2012)
- EMEA-alueen alueellinen tietosuojatoimintojen johtaja Citigroupissa (2012–2014)
- EMEA- ja APAC-alueiden tietosuojajohtaja Citigroupissa (2014–2017)
- CIPP/E-sertifioitu

Rebecca McHale

Tietoturvapäällikkö

- Johtaa tuotteiden ja infrastruktuurin tietoturvastrategiaa
- Valvoo Blackboardin kyberturvallisuushallintoa
- Raportoi tuotepäällikölle
- Toimii Washington, D.C:stä käsin

Rebeccan tausta:

- Liittyi Blackboardin palvelukseen vuonna 2016. Yhdisti äskettäin tietoturvatiimit ja sai ylennyksen yhtiön tietoturvaorganisaatiossa.
- Suorittanut maisterin tutkinnon diskreeteistä matemaattisista ja tiedonkäsittelysovelluksista Royal Hollowayssä (University of London).
- Toimi aiemmin kyberohjelmien ylijohtajana Novettalla ja CSRA:lla, joissa palveli Yhdysvaltain valtionhallintoa ja kaupallisia asiakkaita, esim. Yhdysvaltain ulkoministeriötä, kuljetusturvallisuusvirastoa (TSA) ja liittovaltion luottovakuutusyhtiötä (FDIC).

MORE INFORMATION

You can find more information on our dedicated Data Privacy and Security Community page.

We also have a Data Privacy Newsletter. If you would like to receive our newsletter or have any questions or feedback regarding this white paper, please contact us at privacy@blackboard.com.

Lähteet

1 Tarkemmat GDPR-asetusta koskevat ohjeet löytyvät lopussa olevasta ”Hyödyllisiä GDPR-resursseja” -kohdasta.

2 Käytämme mieluummin ”henkilötieto”-termiä ”henkilökohtaisten tietojen” sijaan, mutta kummallakin termillä on sama merkitys ja laajuus.

3 Rekisterinpitäjä on se organisaatio, joka määrittää tiedonkäsittelyn keinot ja tarkoitukset (miten ja miksi henkilötietoja käytetään).

4 Katso ”Meidän ja organisaatiosi rooli GDPR-asetuksen mukaisesti” -kohta.

5 Katso ”GDPR-asetukseen liittyviä vääriä uskomuksia” -kohdasta lisätietoja tiedonsiirroista.

6 ICO:n ”An introduction to the Data Protection Bill” (Johdanto tietosuojalakiin) -julkaisussa on kätevä yhteenveto tietosuojalaista.

7 Katso myös Yhdistyneen kuningaskunnan ICO-viranomaisen blogikirjoitukset GDPR-asetusta koskevista uskomuksista.

8 Katso myös WP29 (luonnos) -ohjeet, jotka koskevat asetuksen 2016/679 (WP259) mukaista suostumusta, sekä ICO:n suostumusta koskevat ohjeet.

9 WP29-ohjeet henkilötietovuodoista ilmoittamisesta asetuksen 2016/679 (WP250, versio 01) mukaisesti.

10 Katso myös ”Tiedonsiirrot”-kohta.

11 Katso esimerkiksi Yhdistyneen kuningaskunnan ICO:n ”Preparing for the GDPR - 12 steps to take now” (GDPR-asetukseen valmistautuminen – 12 toimenpidettä, joihin pitää ryhtyä nyt) -julkaisu (PDF).

12 Katso myös ”GDPR-asetukseen liittyviä vääriä uskomuksia” -kohta.

13 Katso ”Hyödyllisiä GDPR-resursseja” -kohta.

14 Lisätietoja maailmanlaajuisesta tietosuojapäälliköstä ja tietoturvapäälliköstä on Henkilökuvaukset-kohdassa.

15 Osana EU-US Privacy Shield -sertifiointihanketta olemme jo sisällyttäneet tarvittavat GDPR-sopimusehdot moniin sopimuksiimme, jotka olemme solmineet sellaisten toimittajiemme (alikäsittelijöiden) kanssa, joilla on pääsy EU:n henkilötietoihin.

16 Huomaa, että kaikki tuotevaatimukset eivät koske kaikkia tuotteita. Esimerkiksi osassa tuotteista ei ole käyttöliittymää, jonka kautta asiakkaat voivat linkittää omiin tietosuojakäytäntöihinsä ja -ilmoituksiinsa.

17 Katso lisätietoja ”Tietoturva”-kohdasta.

18 Kun verkko tai järjestelmä on yhdistetty internetiin, tietojen fyysisellä sijainnilla on vähäinen tai olematon vaikutus tietoturvauhkiin. Katso Amazon Web Servicesin (AWS) valkoinen paperi ”Data Residency AWS Policy Perspective” (AWS:n näkemys tietojen säilyttämisestä) ja erityisesti sen sivut 2 ja 3, sillä siinä on vakuuttavia argumentteja tietojen lokalisointia vastaan.

19 Tämän asiakirjan päivämäärällä.

20 Katso AWS Compliance Programs (AWS:n vaatimustenmukaisuusohjelmat) -julkaisusta täydellinen luettelo sertifioinneista ja lakien noudattamisesta.

21 GDPR-asetuksen artikla 28(2)–(4).

22 GDPR-asetuksen artiklat 33 ja 34.

23 Jos haluat selvityksen tietojen käsittelijän roolista, katso ”Meidän ja organisaatiosi rooli GDPR-asetuksen mukaisesti” -kohta.

24 Katso ”GDPR-asetukseen liittyviä vääriä uskomuksia” -kohdasta lisätietoja henkilötietovuodoista ilmoittamisen ajankohdasta ja prosessista.

25 Katso myös ”Sopimukset asiakkaiden kanssa” -kohta.

Blackboard.com