Hvordan Blackboards GDPR-implementering støtter våre kunder

EUs General Data Protection Regulation (GDPR) er en total forandring. Blackboard ønsker endringen velkommen. Vi bryr oss om datavern og forstår at det er en menneskerett. GDPR styrker enkeltpersoners rettigheter og vil føre til bedre datavernpraksis. Dette vil være til fordel for enkeltpersoner og organisasjoner siden det vil øke tillit mellom dem.

Vi offentliggjør dette dokumentet for å gi våre kunder en oversikt over endringene og mytene omkring GDPR, for å omtalle i detaljer hvordan våre tiltak vil støtte din organisasjon. Vi fokuserer på informasjon som vi mener er mest nyttig for deg. Denne rapporten er derfor ikke ment som en omfattende veiledning til GDPR.[1]

Dette materialet er forberedt kun til informasjonsformål og er ikke juridiske råd. Søk råd fra din innomhus eller utenforstående advokat for implementeringen av GDPR i organisasjonen og tilknyttede juridiske spørsmål.

RGPD apporte des changements considérables, mais Blackboard peut compter sur des GDPR medfører betydelige endringer, men hos Blackboard kan vi bygge på vår eksisterende sterke praksis med hensyn til datavern (f.eks. vår EU-US Privacy Shield-sertifisering). Vi betrakter GDPR som en anledning til å viderestyrke vår praksis. Og vi vil fortsette å være kundeorientert og støtte deg med datavernoverholdelse.

INNHOLD

Blackboard er Privact Shiled-sertifisert, stolt underskriver av Student Privact Pledge og medlem av Future of Privact Forum.

GDPR - HVA DU TRENGER Å VITE

GDPR er den nye datavernlovgivningen for EU som vil erstatte det gjeldende EU Data Protection Directive 96/ 46 (direktivet) og implementere Data Protection Acts i medlemstater i EU (f.eks. UK Data Protection Act 1998).

GDPR trådde i kraft i mai 2016 med en overholdelsedato 25. mai 2018.

I avsnittene nedunder har vi gitt en svært kort (og langt fra omfattende) oversikt av GDPR-kravene. Du finner lenker til mer detaljert veiledning i avsnittet "Nyttige GDPR-ressurser".

Hvorfor ny lov?

Lovgivere og regulerende instanser i EU var overbevist om at direktivet trengte oppdatering for å ta opp mangelen på harmonisering og samfunns- og teknologisk utvikling i de 20 årene siden direktivet. Øverst på listen stod strengere håndheving, mer omfattende territorial rekkevidde og forbedrede rettigheter for enkeltpersoner.

Mange av de nye vedtektene (f.eks. ekstra-territorial virkning) er hovedsakelig siktet på sosiale medier og Internett-selskaper utenfor EU. EU-lovgivere og regulerende instanser mente at det eksistrende direktivet ikke tilstrekkelig beskyttet datavernrettighetene til enkeltpersoner i EU som bruker slike sosiale medier og Internett-tjenester.

Blackboard driver annerledes enn disse sosiale mediene og andre Internett-selskaper med modell bygd på å "monetisere" brukerdata. Vi samler inn og bruker personopplysninger2 om våre kunder etter deres anvisning og for å levere våre produkter og tjenester til dem og deres brukere. Vi samler ikke inn eller bruker personopplysninger for å selge denne informasjonen eller for å selge reklame. Vi forstår at personopplysninger blir betrodd oss og kommer med forpliktelser. Vi har derfor en delt interesse og et delt ansvar med våre kunder til å sikre denne informasjonen.

Hva er nytt?

Selv om den er basert på de eksisterende datavernprinsippene og konseptene til EU, medfører GDPR betydelige endringer til datavernregimet i EU, inkludert:

* Økt bøteleggingsmakt på opptil 4 % av global omsetning eller EUR 20 millioner (avhengig av hva som er størst)
* Utvidet territorialt omfang til organisasjoner utenfor EU som leverer produkter og tjenester til innbyggere i EU eller overvåker dem
* Obligatorisk underretning om brudd til overvåkende myndigheter innen 72 timer for datakontrollører[3]
* Strengere krav med hensyn til samtykke
* Forbedrede rettigheter for enkeltpersoner (inkludert retten til sletting og databærbarhet)

Noen av de aller viktigste endringene er imidlertid de nye prinsippene for ansvarlighet og Privacy by Design. Disse prinsippene krever effektiv datavernstyring og prosesser samt mer detaljerte og robust dokumentasjon om hvordan en organisasjon overholder GDPR-kravene.

Hva forblir det samme?

Mange av konseptene og definisjonene i GDPR forblir de samme eller lignende sammenlignet med direktivet.

* Definisjonen av "persondata" (eller personopplysning) forblir hovedsakelig den sammen, men inkluderer nå uttrykkelig IP-adresser, informasjonskapsler og enhetsidentifikatorer
* Konseptene "datakontrollør" og "databehandler" forblir de samme, men GDPR pålegger databehandlere mer direkt avsvar)[4]
* De etablerte prinsippene om behandling i direktivet (f.eks. lovlig og rettferdig behandling, formålsbegrensning, kun oppbevare persondata så lenge det er nødvendig) opprettholdes
* Dataoverføringskravene forblir hovedsakelig de samme: dataoverføringer utenfor EU/EØS er tillatt så lenge en godkjent dataoverføringsmekanisme brukes (f.eks. EU-US Privacy Shield eller "modellklausuler")[5]

Det høyere bøtenivå under GDPR betyr at ikke-overholdelse av eksisterende prinsipper og krav slik som å kun oppbevare personopplysninger så lenge det er nødvendig eller å ha egnede sikkerhetstiltak på plass, vil sannsynligvis medføre økt risiko.

Hva er virkningen av Brexit?

GDPR vil være direkte gjeldende i Storbritannia fra 25. mail 2018 til "Brexit" ved slutten av mars 2019. Selv etter Brexit vil imidlertid GDPR sette standarden for Storbritannia.

* Storbritannias regjering har offentliggjort UK Data Protection Bill 2017 (for tiden i lovgivningsprosessen) som implementerer GDPR før og etter Brexit[6]
* Etter Brexit gjelder GDPR direkte for organisasjoner i Storbritannia som tllbyr varer og tjenester til innbyggere i EU eller overvåker dem (f.eks. universiteter i Storbritannia som aktivt rekrutterer EU-studenter)

Innvirkning på dataoverføring fra og til Storbritannia:

* EU har klarifisert at etter Brexit vil Storbritannia bli ansett som et "tredje land" som betyr at det ikke lenger blir ansett som et "adekvat" (hvit-listet) land for dataoverføringer.
* Med mindre, og inntil Storbritannia blir erklært adekvat av EU-kommisjonen (f.eks. som del av en overgangsavtale), må dataoverføringsavtaler eller en annen datoverføringsmekanisme være på plass for overføring av data fra EU til Storbritannia.
* På den andre siden, må Strobritannia bestemme hvilke land det anser som adekvate (som sannsynligvis inkluderer EU-landene og landene hvit-listet av EU). For de landene som ikke blir ansett som adekvate, må overføringsmekanismer anerkjent av Storbritannia (sannsynligvis lignende EU-mekanismene) brukes for overføring av personopplysninger ut av Storbritannia.

Avmystifiere GDPR

Ett mål for GDPR var å gi mer klarhet gjennom mer detaljerte forskrifter. Det er imidlertid fremdeles mange aspekter av GDPR som er åpne for fortolkning. I tillegg har kompleksiteten til GDPR ført til en mangel på forståelse samt overdrevne uttalelser. Dette har skap mange myter. Vi skal avkrefte noen få av dem nedunder:[7]

Myte 1: Det trengs samtykke for all behandling av personopplysninger

Faktum: Samtykke er bare én av en rekke juridiske grunnlag som tillater at personopplysninger blir behandlet (f.eks. behandling som kreves for utførelsen av en kontrakt eller for den "legitime interessen" til en organisasjon). Grensen for samtykke er blitt svært høy. For eksempel, med mindre enkeltpersonene har et virkelig fritt valg og kan trekke tilbake sitt samtykke når som helst uten problemer, vil det ikke bli ansett som gyldig samtykke. I mange databehandlingscenarioer vil andre juridiske grunnlag være mer egnet.[8]

Myte 2: 72 timersperiode for underretning om brudd gjelder for hele forsyningskjeden (dvs. fra det øyeblikk en (under)behandler blir klar over bruddet)

Faktum: GDPR krever at databehandlere skal underrette sine datakontrollører "uten unødvendig forsinkelse" i tilfelle et persondatabrudd. Bare etter at databehandleren har underrettet kontrolløren, starter 72-timers underretningsperioden for datakontrolløren. Article 29 Working Party (WP29), gruppen av datavernmyndigheter i EU, har klarifisert i sine endelige retningslinjer at "uten unødvendig forsinkelse" betyr "prompt" underretning (ikke "umiddelbar" underretning som antydet i et tidligere utkast.

Myte 3: Dataoverføringer utenfor EU/EØS er ikke tillatt eller bare med kundens samtykke for hver dataoverføring

Faktum: GDPR beholder hovedsakelig de eksisterende reglene for dataoverføring. Som sådan er dataoverføring tillatt hvis en dataoverføringsmekanisme godkjent av EU slik som EU-US Privacy Shield eller de EU-godkjente modellklausulene (dataoverføringsavtaler) er på plass. Blackboard har begge disse mekanismene på plass for å overføre kunders personopplysninger i overholdelse.[10] Siden Blackboard opptrer som databehandler, kreves det en generell instruks for dataoverføringer fra kunden (som er inkludert i vår standard databehandlingsavtale), men kundesamtykker for hver dataoverføring er ikke nødvendig.

Myte 4: Retten til sletting krever at organisasjoner skal slette alle data om en enkeltperson

Faktum: Den nye retten til sletting er ikke en absolutt "rett til å bli glemt". Det er isteden en rett til å få slettet data hvis data ikke lenger kreves og under andre omstendigheter hvor organisasjonen ikke oppfyller GDPR-kravene. Hvis en organisasjon fremdeles legitimt trenger å holde tilbake data (f.eks. på grunn av krav om tilbakeholdelse av registreringer), trenger disse personopplysningene ikke å bli slettet.

Myte 5: GDPR gjelder for alle universiteter som har EU-studenter

Faktum: Bare det å ha studenter fra EU-land innrullert er ikke nok for at GDPR gjelder. GDPR gjelder vanligvis for instituasjoner som er etablert i EU. Det gjelder også for universiteter utenfor EU, men bare hvis de tilbyr varer og tjenester til enkeltpersoner i EU eller overvåker oppførselen til enkeltpersoner i EU. For å bli ansett som å "tilby tjenester" kreves det en viss grad av målsetting. Bare det faktum at EU-studenter er innrullert, er ikke tilstrekkelig. GDPR kan imidlertid gjelde når universiteter aktivt har EU-innbyggere som mål (f.eks. for kurs online) eller aktivt rekrutterer studenter i EU-land. Disse kritereiene er åpne for fortolkning. Vi anbefaler at kunder får sine egne juridiske råd.

IMPLEMENTERE GDPR

Hvorfor det er viktig å gjøre datavern og GDPR på riktig måte

Risikoen for bøter på 4 % av global omsetning er absolutt en grunn til at mange organisasjoner har begynt å ta datavern mer alvorlig. Vi mener imidlertid at det positive ved god datavernpraksis er minst like viktig fordi datavern er en menneskerett, og det å ha sterke datavernpraksiser skaper tillit.

I dagens samfunn er personopplysninger over alt. Personopplysningen blir ofte kalt den nye oljen til økonomien. Vi bruker alle online tjenester og oppgir våre personopplysninger. Studie etter studie viser imidlertid at organisasjoner ikke er til å stole på når det gjelder personopplysninger. Det er en følelse av at enkeltpersoner har mistet kontroll over sine data. Lovgivere og regulerende enheter reagerer på dette. GDPR er antagelig det mest prominente eksempel på dette. Organisasjoner trenger å (gjen)vinne enkeltpersoners tiltro. God datavernpraksis er nøkkelen til å bygge opp denne tiltroen. Det er også en konkurransemessig fordel. Og endelig, det hjelper organisasjoner med innovasjon. Hvis studenter (og stab) stoler på institusjonen, er det mer sannsynlig at de vil dele sine opplysninger og bruke nye verktøy.

Det kan være en katastrofe å ikke gjøre datavern på riktig måte. Databrudd er stadig i nyhetene. Det som følger er skade på anseelse, tap av tillit fra enkeltpersoner og risiko for erstatningskrav fra de med data som er blitt misbrukt. Datavernmyndighetene bruker kanskje ikke bøter på 4 % av global omsetning fra begynnelsen, men de har mange andre håndhevelsesmidler til anvendelse og kan tvinge institusjoner til å endre sin datapraksis og implementere datvernprogrammer med regelmessige eksterne revisjoner.

Vår og din organisasjons rolle under GDPR

GDPR opprettholder konseptet med "datakontrollør" og "databehandler". Dette konseptet er av avgjørende betydning siden det bestemmer ansvaret og forpliktelsene til organisasjoner og deres tjenesteleverandører.

En organisasjon blir ansett som datakontrollør hvis den bestemmer "midlene og formålene" for behandlingen av personopplysninger, dvs. hvorfor og hvordan personopplysninger blir brukt. Databehandlerer er derimot organisasjonen som opptrer på vegne av datakontrolløren og under kontrollørens ledelse.

For de fleste av Blackboards produkter og tjenester (f.eks. Learn, Collaborate, Open LMS blir Blackboatd ansett som databehandler og våre kunder som datakontrolløren.

GDPR pålegger databehandlere slik som Blackboard flere direkte krav. Majoriteten av GDPR-kravene gjelder imidlertid fremdeles for datakontrollører (f.eks. ansvaret for å informere enkeltpersoner om hvordan deres data blir brukt, etterkomme enkeltpersoners anmodning om tilgang til sine data, obligatorisk underretning om brudd til datavernmyndigheter og enkeltpersoner).

Hva kan du gjøre for å forberede deg til GDPR?

Alle organisasjoner innen omfanget til GDPR må være klar innen 25. mai 2018. Her er noen få ting kunder kan gjøre for å forberede seg. Denne listen med trinn er basert på vår egen erfaring og er på ingen måte ment som altomfattende. Vær sikker på at du engasjerer dataverneksperter for å hjelpe deg med implementering. Mange datavernmyndigheter har også opprettet sin egen veiledning om hvordan man implementerer GDPR.[11]

Forhåpentligvis har du allerede trinn 1–6 bak deg og er midt i å implementere handlingsplaner. Det er imidlertid aldri for sent å begynne. Selv om du akkurat har begynt, kan du implementere de mest kritiske endringene. Det betyr også at du kan vise datavernmyndighetene at du arbeider med en plan. Ignorere GDPR er ikke en mulighet.

1. **Sjekk om GDPR gjelder for din organisasjonen**

   Hvis din organisasjonen er etablert i EU, gjelder GDPR. GDPR kan imidlertid også gjelde for organisasjoner utenfor EU.

2. **Opprette et GDPR-prosjekt**

   Utform og implementer et dedikert GDPR-prosjekt. Ideelt sett skal du ha støtte fra ledelsen for prosjektet og utnevnte kontakter som kan støtte deg i hver avdeling. Dette prosjektet vil gjelde alle avdelingene i institusjonen, og du trenger hjelp.

3. **Utnevne en erfaren GDPR-leder til å lede prosjektet**

   Lederen skal ikke bare være en erfaren datavernleder, men skal også ha tilstrekkelig tid og ressurser samt tilgang til ekstren støtte (f.eks. advokatfirma). Hvis organisasjonen er en offentlig myndighet etablert i EU, trenger du også utnevne en datavernleder.

4. **Sikre at toppledelsen er ombord og har overoppsyn**

   Det er vanskelig å implementere et GDPR-prosjekt uten støtte, veiledning og overvåking fra toppledelsen.

5. **Gjennomgå bruken av personopplysning og utføre gapanalyse**

   Å forstå hvor og hvordan personopplysninger brukes og hvor det kreves GDPR-forbedringer, er den første viktige fasen i GDPR-prosjektet.

6. **Utvikle handlingsplaner for å lukke gap**

   Dette er kanskje den vanskeligste delen av GDPR siden det krever å oversette GDPR-kravene som ofte er på et høyt nivå, til spesifikke handlinger som kan utføres for alle de forskjellige prosessene og systemene.

7. **Implementere handlingsplaner**

   Tiltro er bra, men kontroll er bedre i dette tilfellet. Denne fasen krever sporing av andres handlingsplaner for å være sikker på at de oppfyller frister.

8. **Gjennomgå leverandørene**

   Under er du ansvarlig for dine leverandører. Det er viktig å ha de riktige kontraktsmessige bestemmelser på plass, men det er ikke nok. Du må være sikker på at leverandørene oppfyller GDPR-krav og kan støtte deg i overholdelsen. Spør dem hvordan de implementerer GDPR.

9. **Hold deg ajour med juridiske/forskriftsmessige utviklinger (Art. 29 Working Party-retningslinjer, medlemstaters implementeringslover)**

   Det er nok å kjenne til GDPR, ikke sant? Feil! Mens GDPR gjelder direkte, implementerer alle medlemstater i EU supplementerende datavernlover.

   Disse kreves for å regulere områder der medlemstater har lovgivningsmyndighet (f.eks. datavern for ansatte) eller der GDPR tillater videre lovgivning (f.eks. kriterier for DPO-er og DPIA-er). I tillegg offentliggjør W29 viktig veiledning. Å holde seg oppdatert er utfordrende, men viktig.[13]

BLACKBOARDS PLAN OG FREMGANGSMÅTE

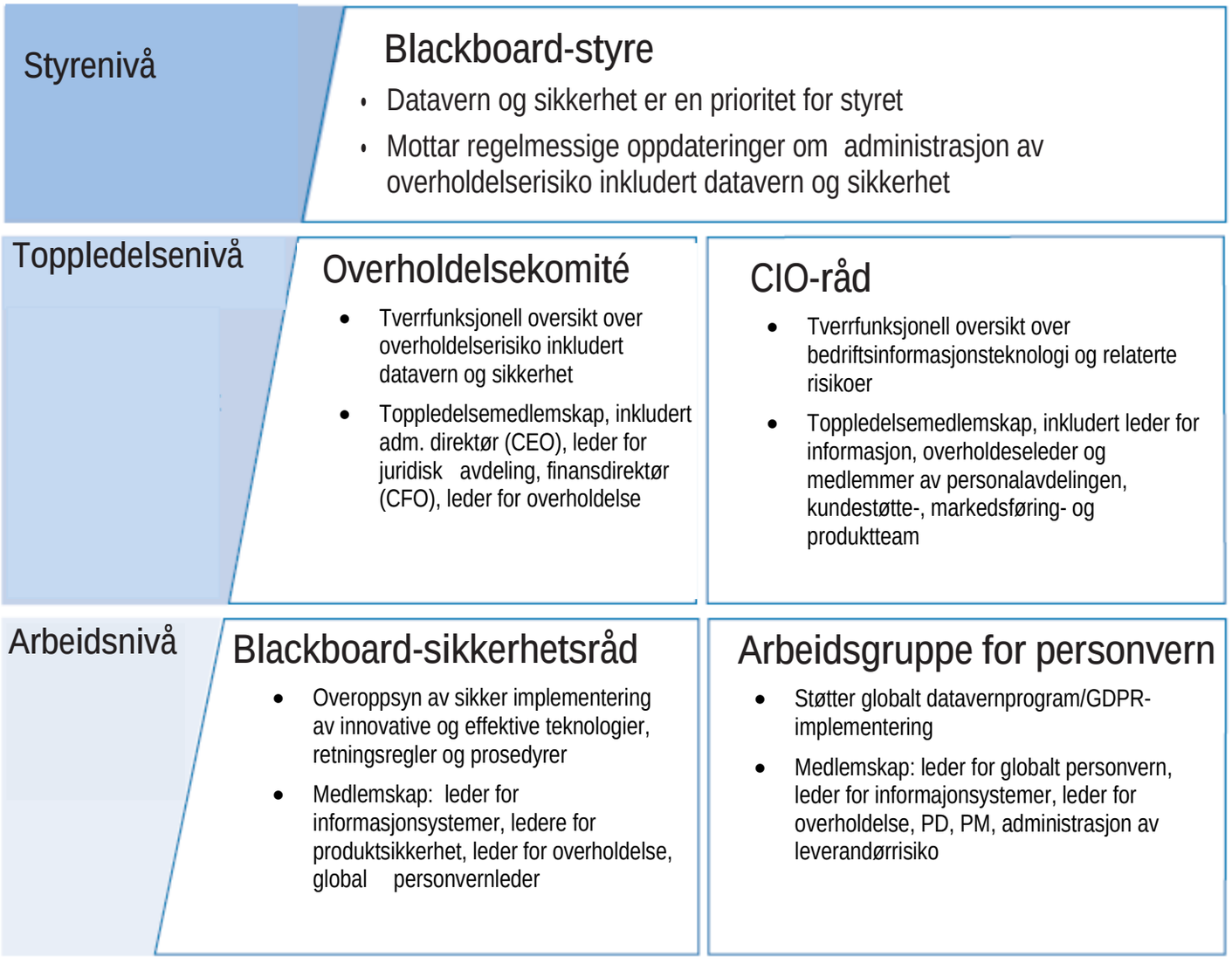
Datavern og sikkerhet hos Blackboard

Datavern og sikkerhet har lenge vært en viktig prioritet hos Blackboard. For oss er GDPR en mulighet til å viderestyrke vår eksistrende datavernpraksis.

Vår fremgangsmåte med hensyn til datavern har alltid vært kundeorientert. Vi forstår utfordringene kundene står overfor og vil hjelpe deg med dem.

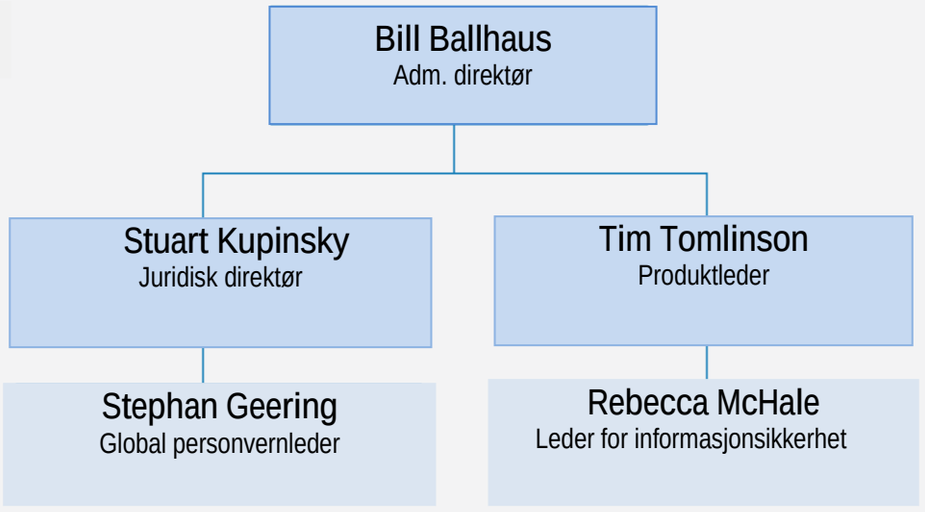
God datavernpraksis krever en solid styringsmodell. Hos Blackboard er datavern og sikkerhet en prioritet for styret, og vår styringsmodell (se nedunder) sikrer at toppledelsen overvåker og støtter våre tiltak for datavern og sikkerhet.

Vekten som Blackboard legger på datavern og sikkerhet understrekes også av det faktum at vår globale personvernleder og leder for informasjonsikkerhet [14] rapporterer til adm. direktørs lederteam (se organisasjonsdiagram nedunder).



Personvern og sikkerhet

Vekten som Blackboard legger på datavern og sikkerhet, understrekes også av det faktum at vår globale personvernleder og leder for informasjonsikkerhet rapporterer til adm. direktørs lederteam



Blackboards fremgangsmåte med hensyn til GDPR

Vi har etablert et omfattende prosjekt for å implementere kravene til GDPR med følgende fremgangsmåte:

* GDPR-implementeringen bygger på Blackboards eksisterende datavernerfaring og overholdelsemekanisme
* GDPR-implementeringen ledes av lederen for globalt datavern og støttes av en egen prosjektleder og "GDPR-leder" i hvert funksjonsområde
* Det velkjente advokatfirma Bristows LLP, bl. a. har blitt engasjert for å støtte GDPR-implementeringen
* GDPR-inmplementeringen blir overvåket av Blackboards Overholdelsekomité som inkluderer selskapets adm. direktør, juridisk direktør og andre toppledere

GDPR er en mulighet

Vi tenker på GDPR-implementeringen ikke bare som et tiltak for å overholde nye EU-krav om datavern, men også som en mulighet. Som sådan tar vi sikte på å bruke GDPR-implementeringen for å oppnå følgende:

* Styrke global datavernpraksis - vi vil bruke GDPR-prosjektet til å forbedre vårt globale datavernprogram i og utenfor EU
* Utvikle personvern ved å utforme prosesser som videre bygger inn datavernoverholdelse i våre daglige prosesser
* Støtte våre kunder med deres GDPR-overholdelsetiltak
* Posisjonere Balckboard som den anerkjente lederen i utdanningsteknologi

Vår implementeringsplan

Vi følger Bristow LLPs etablerte 3-fase metodologi for å implementere vårt Globale datavern-/GDPR-program. Denne metodologien brukes av en rekke andre selskaper, inkludert ledende teknologiselskaper. De tre hovedfasene er følgende:

* **FASE 1 - Innsamling av informasjon**
* **FASE 2 - Utvikling av løsninger**
* **FASE 3 - Implementering av arbeidsflyt**

Vi har brukt denne 3-fase metodologien for å utvikle programmet med følgende fire hovedstadier:

Igangsetting av prosjekt

igangsettingstadiet av prosjektet inkluderer følgende aktiviteter:

* Briefing av og godkjennelse fra toppledelsen
* Ansette en global personvernsleder med ansvar for å lede GDPR-prosjektet
* Utvikling av prosjektplan og prosjektstyring
* Opprinnelig innsamling av informasjon og vurdering av gjeldende overholdelseaktiviterer for områder som krever forbedring under GDPR

FASE 1 - Innsamling av informasjon (Seminarer)

I løpet av den første fasen ledet vi strukturerete samtaler/seminarer med viktige inreressenter fra Blackboards funksjonsområder og produktgrupper for å få detaljert informasjon om databehandlingspraksis innen disse områdene.

Resultatet av seminarene ble brukt til å utføre gapanalysen og utvikle løsningene og implementeringsplanene i fase 2.

FASE 2 - Utvikling av løsninger

Basert på onformasjonen fra seminarene, utviklet vi følgende løsninger og dokumentasjon:

* Forbedret intern dataverndokumentasjon (retningslinjer og detaljerte driftstandarder) som avspeiler GDPR-kravene og forklarer hvordan GDPR-kravene må bli oppfylt for forskjellige databehandlingsaktiviteter (f.eks. krav for behandling av kundedata, Privacy by Design-prosess)
* Produktkrav
* Implementeringsplaner for funksjonsområdene og for tiltak som kreves sentralt.

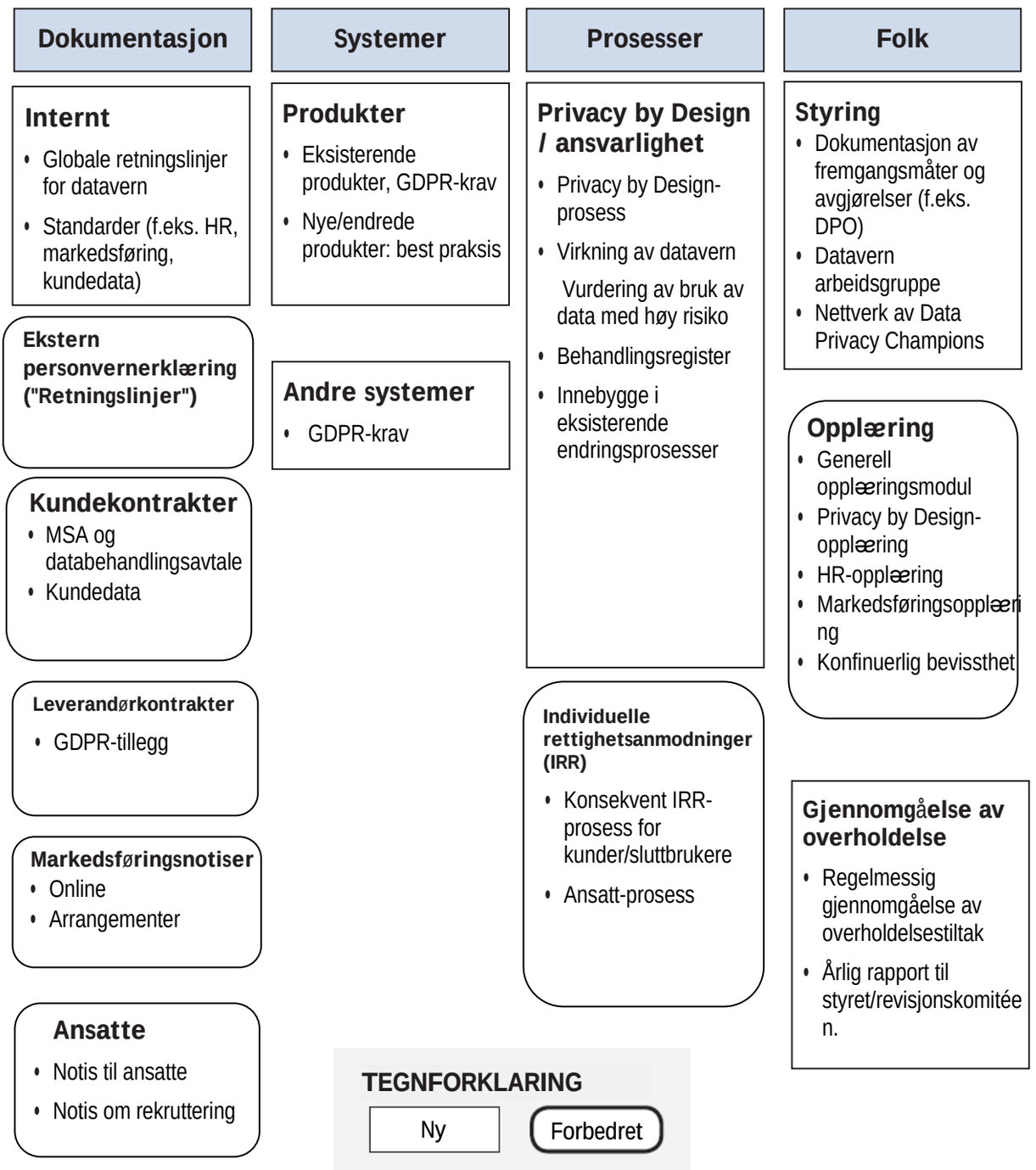
FASE 3 - Implementering av arbeidsflyt

I løpet av den siste fasen implementerer vi den utviklede datverndokumentasjonen og utfører implementeringsplanene:

1. Utføre inplementeringsplanene for funksjonsområdene og produktgruppene
2. Gjennomgå og oppdatere rettningslinjer, underretninger of samtykker til offentligheten.
3. Forbedre styring (roller, opplæring, Privacy by Design osv.)
4. Gjennomgå og oppdatere leverandørkontrakter (der det er nødvendig)15
5. Endringer av IT-systemer, (der det er nødvendig)
6. Opprette databehandlingsregister

Oversikt over endringer

Skjemaet nedunder viser hvordan vi tenker oss endestadiet for GDPR/datavernprogrammet etter implementeringsaktivitetene. Etter GDPR-implementeringen vil vi fortsette å innovere og tilpasse for å videremodne vår datavernprosess.



HVORDAN VIL GDPR-PROGRAMMET VÅRT HJELPE DEG?

Balckboards Global Data Privacy / GDPR-implementeringsprogram fokuserer på å støtte din organisasjon med implementeringen av GDPR. Følgende avsnitt vil gi flere detaljer, men i sammedrag er de 7 hovedpunktene:

1. **GDPR-klare produkter:** Vi implementerer produktkrav for å støtte kunder med forespørsler om åpenhet, forespørsler om individuelle rettigheter osv.
2. **Privacy by Design:** Vi implementerer en Privacy by Design- og Data Protection Impact Assessment (DPIA)-prosess for å lette dokumentasjon av overholdelse
3. **Dataoverføringer:** Vi vil fortsette vår flerlags fremgangsmåte: Regionalisering, EU-US Privacy Shield og EU-autoriserte modellklausuler
4. **Kontrakt med kunder:** Vi har et GDPR-klart databehandlingstillegg til vår standard masteravtale
5. **Våre leverandører:** Vi har sterke kontrakter og et rammeverk for administrasjon av kunderisiko på plass
6. **Sikkerhet:** Vi har etablerte retningslinger, prosedyrer og styring som blir forbedret kontinuerlig for å sikre sikkerheten av kundedata
7. **Underretning om brudd:** Vi har dokumentert og testet Security Incident Respons-prosessen

1. GDPR-klare produkter

Å støtte kundene ved å gjøre produktene våre GDPR-klare er ett av hovedaspektene av implementeringsarbeidsflyt. I den hensikt utarbeidet vi minimums GDPR/datavernkrav for våre produkter. På linje med fremgangsmåten for å styrke vår datavernpraksis globalt, gjelder de fleste av disse kravene for alle våre produkter, ikke bare de produktene vi gjør tilgjengelige i EU. Dette støtter også våre kunder utenfor EU som kan falle inn under omfanget av GDPR.

Vi utviklet våre GDPR/datavernproduktkrav gjennom en sterk og intensiv prosess. Vi laget et utkast til en fø rste versjon med en utenforstående advokat. I løpet av flere arbeidsøkter og revisjoner med viktige interessenter fra våre produktutviklings- og produktadministrasjonsteam finpusset vi versjonen til spesifikke og brukbare generelle produktkrav med detaljert veiledning. GDPR/datavernproduktkravene ble deretter oversatt til produktspesifikke handlinger i produktimplementeringsplanene for hver produktgruppe.

Våre produktkrav[16] kan kategoriseres som følger:

Åpenhet

* Kunders muliighet til å lenke til sine personvernsregler/underretninger
* Skaffe informasjon om hvordan personopplysninger genrelt brukes i et produkt

Dataminimalisering/-sletting

* Gjennomgåelse av produkter for unnødvendige/valgfrie felter
* Gjennomgåelse av produkter for muligheter til å bruke pseudonym eller anonyme data istedenfor personopplysninger
* Mulighet til å slette personopplysninger når anmodet av kunder (når kunder/brukere ikke selv kan slette data)

Generelle individuelle rettigheter

* Mulighet til å skaffe tilgang til og rette personopplysninger når anmodet om dette av en enkeltperson
* Mulighet til å slette personopplysninger når anmodet om dette av en enkeltperson

Individuelle EU-rettigheter

* Mulighet til å ta seg av anmodninger om databærbarhet (enkeltpersoners rett til å motta data i maskinlesbart format under visse omstendigheter
* Mulighet til å slutte og bruke personopplysninger (rett til å nekte / rett til å begrense under visse omstendigheter)

Blackboard har allerede definerte programmer for våre produkter som tar GDPR i betraktning. Vi definerte derfor ikke ytterligere spesifikke GDPR-sikkerhetskrav,[17]

2. Privacy by Design

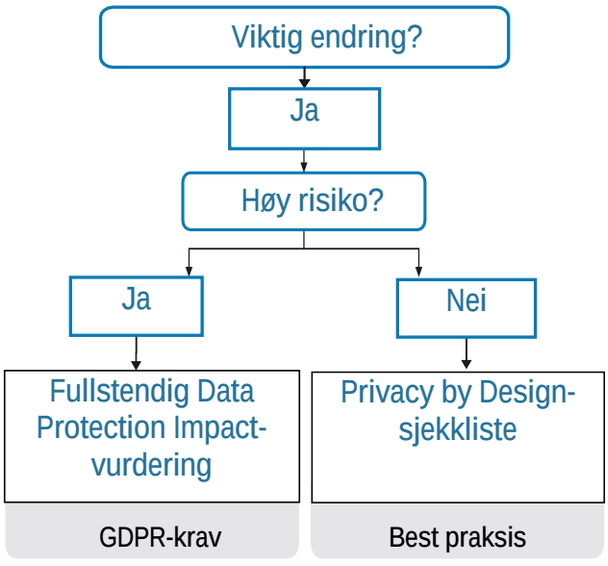
Ettersom det blir mer og mer utfordrende i dagens verden for enkeltpersoner å beholde kontroll over sin informasjon (se vår personvernsblogg om dette emnet), har Privacy by Design og ansvarlighet blitt stadig viktigere for å beholde tilliten til enkeltpersoner, kunder og regulerende enheter, og å dokumentere hvordan en organisasjon overholder GDPR. Vi setter derfor vår Privacy by Design-fremgangsmåte som selve midtpunket for vårt Global Data Privacy/GDPR-program.

For Blackboard er dette heller en evolusjon enn en revolusjon. Vi har alltid utført juridiske gjennomgåelser av nye produkter og praksis. Med vår Privacy by Design-fremgangsmåte har vi formalisert og bedre dokumentert disse gjennomgåelsene.

Fremgangsmåte

* Vi skapte en dokumentert Privacy by Design-prosess og sjekkliste
* Funksjonsområder og produktgrupper onkluderer Privacy by Design-sjekklisten i sine endringsprosesser
* Hver betydelige endring i hvordan personopplysninger brukes krever utfylling av Privacy by Design-sjekklisten. Mens det ikke kreves spesielt av GDPR, er dette beste praksis.
* Sjekklisten vil utløse den mer detaljerte Data Protection Impact Assessment (DPIA) for høy-risiko bruk av personopplysninger (GDPR-krav)

Flytdiagrammet nedunder visualiserer fremgangsmåten:



3. Dataoverføringer

GDPR medfører ikke noen betrydelige endringer av hvordan personopplysninger kan overføres utenfor EU/EØS. De gjeldende begrensningene og dataoverføringsmekanismer blir værende. Dette betyr at dataoverføringer er tillatt hvis en EU-godkjent dataoverføringsmekanisme slik som EU-US Privacy Shield

eller de EU-godkjente modellklausulene (dataoverføringsavtaler) er på plass. Disse mekanismene sikrer at personopplysninger blir tilstrekkelig beskytte selv når de forlater EU.

Vi vil fortsette vår flerlags- og overflødige fremgangsmåte for dataoverføringsoverholdelse. Dette betyr at vi håndterer dataoverføring på flere måter for å sikre at riktige sikringstiltak er på plass for dine opplysninger.

- Regional vert: Vi har en regional vertstrategi med nesten alle produkter med vert i EU, og det er planlagt å flytte andre produkter for regionale vertløsninger. Selv om regional lagring ikke kreves av GDPR og vi ikke tror at datalokalisering fører til bedre datavern eller sikkerhet,[18] forstår vi at mange EU-kunder foretrekker at deres data blir lagret i EU.

* Privacy Shield: Blackboard er EU-US Privacy Shield-sertifisert som lar oss overføre data til USA på lovlig måte.
* Modell klausuler: Vi bruker også EU-godkjente "modellklausul"-avtaler som tillater oss å i overholdelse overføre personopplysninger utenfor EØS innen Blackoard-konsernet ("Customer Data Transfer Agreement")
* Leverandører: Sterke kontrakter er på plass med leverandører og partnere (f.eks. IBM, Amazon Web Services) for å sikre at dataoverføringskrav (og andre datavernforpliktelser) blir sendt videre til våre leverandører og partnere.

Vi har for tiden[19] flere regionale datasentre for å støtte datahåndtering i EU for våre EU-kunder:

* Administrert vert (Blackboard datasentre): Datasentre i Amsterdam (Nederland) og Frankfurt (Tyskland)
* Skyvert (AWS datasenter): AWS-region Frankfurt, Tyskland (eu-cental-1)

AWS-datasentre oppfyller en lang rekke sertifiseringer og krav fra ISO 27001 og ISO 27018, til SOC2, og til overholdelse av GDPR samt overholdelse av lokale krav slik som tysk C5 og IT-Grundschutz.[20]

Der er viktig å forstå at mens personopplysningene til kundene er lagret i disse datasentrene for de fleste av produktene (inkludert Learn 9.1, Lern SaaS, Open LMS og Collaborate) for EU-kunder, kan tilgang til disse data fra utenfor EU/EØS kreves for å levere produkter og tjenester, f.eks. for 24/7-støtte. Slike dataoverføringer er tillatt takket være den nevnte EU-US Privacy Shield-sertifiseringen og modellklausulene.

4. Kontrakter med kunder

Det gjeldende direktivet krever at en datakontrollør har på plass en kontrakt med leverandøren (databehandler), men foreskriver ikke innholdet av kontrakten i detaljer. GDPR er mer foreskrivende og inkluderer en liste med påbudt innhold.[21]

Vårt gjeldende standard databehandlingstillegg inkluderer alle de påbudte punktene nedenunder. Det blir automatisk inkludert for kunder med våre standard avtaler som er innenfor omfanget av GDPR.

- ✓ Bare bruke personopplysninger som instruert
- ✓ Stab må undertegne konfidensialitetavtaler
- ✓ Egnede sikkerhetstiltak må være på plass
- ✓ Bare engasjere leverandører (underbehandlere) . . .

- som godkjent av datakontrollør (kan være en generell godkjenning)

- som ifølge kontrakt er pålagt å følge de samme forpliktelser til datavern

- ✓ Assistere kontrollør med å svare på anmodninger om individuelle rettigheter
- ✓ Assistere kontrollør med sikkerhetstiltak, underretninger om brudd og vurderinger av datavernvirkning
- ✓ Returnere eller slette data ved slutten av en kontrakt
- ✓ Skaffe informasjon som er nødvendig for at datakontrolløren kan vise overholdelse
- ✓ Øyeblikkelig informere datakontrolløren hvis noen instruksjoner fra datakontrolløren er brudd på GDPR

5. Administrere våre leverandører

Blackboard bruker leverandører (f.eks. IBM, Amazon Web Services) til å hjelpe oss levere våre produkter og tjenester til våre kunder. Der hvor dette krever tilgang til våre kunders personopplysninger, er Blackboard ansvarlig for leverandørenes retningslinjer for datavern.

Som en del av vårt GDPR-program knytter vi Privacy by Design-fremgangsmåten nært sammen med de eksistrende Vendor Risk Management- og Procurement-prosessene. Dette resulterer i følgende hovedkontroller:

* Sterke kontrakter med et personvern- og GDPR-tillegg på plass med tredjeparter som pålegger hovedsakelig tilsvarende bestemmelser som vi har på plass med våre kunder
* "Modellklausul"-avtaler og/eller GDPR og Privacy Shiled Assendum for å muliggjøre lovlig dataoverføringer til våre leverandører
* Dokumentert Vendor Risk Management-retningslinjer og rammeverk
* Nye leverandører må fylle ut et Vendor Security Assessment Questionaire med spørsmål om datavernoverholdelse
* Leverandører med tilgang til Blackboard-administrerte systemer må følge Blackboads interne retningslinjer for tilgangskontroll , identitet og godkjenning, som inkluderer kontogjennomgåelser etter som det er aktuelt
* Leverandører trenger å ha tilgang til Blackboards ressurser gjennom godkjente mekanismer (f.eks. VPN)
* Leverandører har begrensede tilgangskontroller for trafikk, brukere og eiendeler

6. Sikkerhet

GDPR endrer ikke vesentlig de tekniske og driftsmessige tiltakene ("TOM-er") for sikkerheten av personopplysninger. Slike tiltak må være "passende" for risikoen involvert som under det gjeldende direktivet. Derfor fortsetter vi å stole på våre etablerte informasjonsikkerhetsprogrammer.

Styre informasjonsikkerhetrisiko

Vi har opprettet retningslinjer, prosedyrer, styring og tekniske krav for å administrere IT-sikkerhetsrisiko for hele virksomheten.

Fra første dag må Blackboard-stab forstå sitt ansvar for å beskytte kunders personopplysninger:

* Anerkjenne retningslinjer for å beskytte sensitiv informasjon
* Årlig opplæring i brukersikkerhet og datavern
* Nettfiskingsøvelser
* Oppmerksomhetsnotiser

Følgende krav er på plass for beskyttelse av data av staben:

* Dataklassifiseringer blir definert med krav for å beskytte hver datatype. Våre kunders data - dataene til institusjonene og deres elever - er de mest sensitive.
* Tekniske kontroller er på plass for å sikre data, f.eks.:
  - bruk av kryptering
  - umiddelbare sikkerhetsoppdateringer
  - forbedrede autentifiseringskontroller
  - beskyttelse mot ondsinnet e-post og nettrafikk
  - teknologier for endepunkbeskyttelse
  - tilgang begrenset basert på behov-for-å-vite

Der er ikke bare GDPR ...

Som et globalt selskap som betjener utdanningssamfunnet, overvåker vi nøye relevante geografiske og utdanningsektorspesifikke datavern-og sikkerhetslover og vedtekter.

Listen nedenunder er bare noen eksempler på sikkerhet- og datavernvedtekter, standarder og rammeverk som Blackboard tar i betraktning i tillegg til GDPR når vi utvikler våre retningslinjer for sikkerhet, prosesser og tekniske kontroller.

* US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
* US Children's Online Privacy Protection Act (COPPA)
* Amerikanske delstatslover (eksisterende og kommende 50-delstats lappverk)
* Amerikanske føderale standarder - FedRAMP
* PCI Data Security Standards, der det gjelder
* ISO/IEC, OWASP, NIST
* Internasjonale standarder (MTCS, IRAP)

Sikkerhetsmodenhetsvurdering og veikart

Vi arbeider hardt for å kontinuerlig forbedre våre tekniske og driftsmessige sikkerhetstiltak. Diagrammet på neste side visualiserer våre kontinuerlige moddenhetsvurderinger og veikart.

Adoptere rammeverk: Sikkerhetsmodningsvurderinger og veikart

7. Underretning om brudd

En av de viktigste endringene i GDPR er den nye obligatoriske underretning om brudd på persondata til den pågjeldende datavernmyndigheten og (i noen tilfeller) til enkeltpersonene det gjelder.[22]

For de fleste av våre produkter og tjenester er Blackboard databehandler[23] ifølge GDPR. Forpliktelsen til å underrette datavernmyndigheter og enkeltpersoner i tilfelle av et brudd som involverer Blackboard, vil derfor hvile på våre kunder. GDPR krever imidlertid at databehandlere slik som Blackboard underretter sine kunder (datakontrollører) uten unødvendig forsinkelse (dvs. "imiddelbart") i et slikt tilfelle.

Vi har følgende tiltak på plass som støtter våre kunder i å oppfylle sine forpliktelser i tilfelle av et databrudd hos Blackboard som gjelder en kunde:

* Blackboards Security Incident Response (SIR)-prosess
  - Dokumentert og testet på regelmessig basis
  - Muliggjør rask identifisering, etterforskning og utbedring i tilfelle en hendelse
  - Tillater imiddelbar underretning til kunder
  - Stoler på det etablerte responsteamet for sikkerhetshendelser (som inkluderer lederen for informasjonssikkerhet og lederen for globalt personvern)
* Vår forpliktelse til å umiddelbart underrette kunder er uttrykkelig fremsatt i vår gjeldende masteravtale og dataverntillegg[25]

KONKLUSJON

GDPR krever betydelige endringer med virkning langt etter overholdelsesdatoen 25. mai 2018.

Vi håper at denne meldingen kan bidra til din vellykkede implementering av GDPR og har vist hvor alvorlig Blackboard tar GDPR og overholdelse av datavern.

De neste avsnittene gir mer nyttig informasjon og lister vår e-postkontakt hvis du har spørsmål eller tilbakemelding om denne meldingen.

NYTTIGE GDPR-RESSURSER

Ressurlenkene nedenunder er bare et lite utvalg av nyttig materiale som er tilgjengelig online. Det er ikke ment som å være en altomfattende liste.

For en detaljert analyse av hvordan GDPR gjelder for deg bør du også søke råd fra spesialister. Det er viktig å stole på erfarne datevernekseperter (f.eks. advokatfirmaet du velger).

Offisielle EU-ressurser

- GDPR-tekst
- Article 29 Working Party-retningslinjer
- EU kommisjonens GDPR-nettsted

Materiale fra EU Data Protection Authority

- Strobritannias Information Commissioner's Office (ICD) hare et utmerket GDPR-nettsted med nyttig materiale på et enkelt språk som konstant oppdateres
- Den irske Data Protection Commissioner (DPC) har en dedikert GDPR-side for organisasjoner
- Den franske CNIL har noe materiale på engelsk, inkludert en Privacy Impact Assesment-programvare (og mye mer materiale på fransk)
- Den spanske AEPO produserte en guide for utdanningsinstitusjoner (PDF, på spansk)

Veiledninger fra advokatfirmaer

- Bird & Bird's veiledning for GDPR
- Bird & Bird's sporer av medlemstaters lover (sporer nasjonale GDPR-variasjoner)
- Linklater's GDPR-overlevelsesveiledning (PDF)
- White & Case GDPR-håndbok

Andre organisasjoner

- JISC i Storbritannia har nyttige ressurser, arrangementer og bloggoppdateringer om GDPR
- UCISA har offentliggjort et GDPR-best praksis-dokument med praktiske trinn og kasusstudier
- International Association if Privacy Professionals (IAPP) har et godt (gratis) ukentlig nyhetsbrev om utviklinger i europeisk personvern
- IAPP har også en nyttig oversikt over leverandører av datavernverktøy (PDF)
- Amazon Web Services har et dedikert GDPR Centre

BIBLIOGRAFIER

Stephan Geering

Global leder for personvern

- Globalt ansvar for overholdelse av datavern- og sikkerhetslover
- Leder Global Data protection / GDPR Implementation-programmet
- Rapporterer til juridisk direktør,
- medlem av Blackboards juridiske team

Stephans bakgrunn:

- Jurist / Deputy Data Protection Commisssioner i en datavernmyndighet i en sveitsisk kanton (2002–2008)
- LLM ved University College London (2008–2009)
- Assisterende direktør, Group Privacy hos Barclays (2010–2012)
- EMEA regional leder av Data Protection Operations hos Citigroup (2012–2014)
- EMEA og APAC leder for privatvern hos Citigroup (2014–2017)
- CIPP/E-sertifisert

Rebecca McHale

Leder for informasjonsikkerhet

- Leder sikkerhetstrategi for produkter og infrastruktur
- Overvåker Blackboards kybersikkerhetstyring
- Rapporterer til leder for produksjon
- Basert i Washington, D.C.

Rebeccas bakgrunn:

- Kom til Blackboard i 2016; kombinerte nylig sikkerhetsteam og eleverte rollen til sikkerhetsorganisasjon innen selskapet
- MS Discrete Mathematics and Computing application fra Royal Holloway, University of London
- Tidligere senorleder av kyberprogram his Novetta og CSRA og betjente amerikanske offentlige og kommersielle kunder - f.eks. Department of State, Transportation Security Administration (TSA) og Federal Deposit Insurance Corporation (FDIC)

MER INFORMASJON

Du kan finne mer informasjon på vår dedikerte Data Privacy and Security Community-side.

Vi har også et Data Privacy Newsletter. Hvis du vil motta nyhetsbrevet eller har spørsmål eller tilbakemelding om denne meldingen, kan du kontakte oss på privacy@blackboard.com.

Kilder

1 Se avsnittet "Nyttige GDPR-ressurser" ved slutten for mer detaljert veiledning om GDPR.

2 Vi foretrekker uttrykket "personopplysninger" fremfor "personlige data", men bruker det med den samme betydning og omfang som "personlige data".

3 Datakontrolløren er organisasjonen som bestemmer midlene og formålene for databehandling (hvordan og hvorfor personopplysninger blir brukt).

4 Se avsnittet "Vår og din organisasjons rolle under GDPR."

5 Se avsnittet "Avmystifisere GDPR" nedenunder for flere detaljer om dataoverføringer.

6 Se ICOs "An introduction to the Data Protection Bill" for en nyttig oversikt av loven.

7 Se bloggpostene til Storbritannias ICO om GDPR-myter.

8 Se også WP 29 (utkast) Guidelines on Consent under Regulation 2016/679 (WP259) og retningslinjene til ICO for samtykke.

9 WP29 Guidelines on Personal Data Breach Notification under Regulation 2016/679 (WP250 rev.01)

10 Se også avsnittet "Dataoverføringer".

11 Se f.eks. Storbritannias ICO Preparing for the GDPR - 12 steps to take now (PDF)

12 Se også avsnittet "Avmystifisere GDPR".

13 Se avsnittet "Nyttige GDPR-ressurser".

14 For mer informasjon om lederen for globalt personvern og lederen for informasjonsikkerhet se avsnitter "Bibliografi".

15 Som en del av EU-US Privacy Shield-sertifiseringsprosjektet, har vi allerede inkludert de nødvendige GDPR-kontraktbestemmelser i mange av kontraktsvilkårene med våre leverandører (underbehandlere) som har tilgang til personopplysninger i EU.

16 Merk at ikke alle produktkrav gjelder for alle produkter. For eksempel, noen produkter har ikke et brukergrensesnitt som lar kunder lenke til sine personvernsretningslinjer/notiser.

17 Se avsnittet "Sikkerhet" for flere detaljer.

18 Etter at et nettverk eller system er koblet til Internett, har det fysiske stedet liten eller ingen innflytelse på sikkerhetstrusler. Se Amazon Web Services (AWS)-meldingen "Data Residency AWS Policy Perspective" (spesielt side 2 og 3) for overbevisende argumenter mot datalokalisering.

19 Fra og med datoen for dette dokumentet.

20 Se AWS Compliance Programs for den fullstendige listen med sertifiseringer og juridisk overholdelse.

21 Art. 28(2)-(4) GDPR.

22 Art. 33 og 34 GDPR.

23 For en forklaring på rollen til databehandleren se avsnittet "Vår og din organisasjons rolle under GDPR".

24 Se avsnittet "Avmystifisere GDPR" for mer detaljer om timingen og behandlingen av underretning om brudd på personopplysninger.

25 Se avsnittet "Kontrakter med kunder".