Hur Blackboards GDPR-implementering stöder våra kunder

EU:s Allmänna Dataskyddsreglering (GDPR) är ett paradigmskifte. Blackboard välkomnar denna ändring. Vi bryr oss om dataintegritet och förstår att det är en mänsklig rättighet. GDPR förstärker personers rätt och kommer att leda till bättre dataintegritetspraxis. Detta kommer att gynna individer och organisationer, eftersom det kommer att öka förtroendet mellan dem.

Vi publicerar detta dokument för att ge våra kunder en översikt av ändringarna och myterna rörande GDPR, för att förklara vårt angreppssätt för implementering och för att i detalj förklara hur vårt arbete kommer att stöda din organisation. Vi fokuserade på information som vi tror kommer att vara till störst hjälp för dig. Denna vitbok är därför ingalunda en helomfattande guide till GDPR.[1]

GDPR medför väsentliga ändringar, men hos Blackboard kan vi bygga på vår existerande robusta dataintegritetspraxis (t.ex. vår EU-US certifiering för Integritetsskköld). Vi ser GDPR som en möjlighet att ytterligare förstärka vår praxis. Och vi kommer att fortsätta att vara kundfokuserade och stödja dig med din efterlevnad av dataintegritet.

Dessa material har producerats bara i informationssyfte och är inte juridisk rådgivning. Vänligen anlita råd från era interna eller externa advokater för implementering av GDPR i er organisation och för relaterade juridiska frågor.

INNEHÅLL

GDPR - VAD DU BEHÖVER VETA

Vi är certifierade för Integritetssköld, en stolt undertecknare av Integritetsutlovandet för studenter och en medlem av Future of Privacy Forum.

GDPR är den nya dataskyddslagstiftningen från EU, som kommer att ersätta det nuvarande EU Data Protection Directive . 96/46/EC (Direktiv), och de implementerande dataskyddslagarna i EU:s medlemsstater (t.ex. UK Data Protection Act 1998).

GDPR stadfästes i maj 2016 och trädde i kraft 2018-05-25.

I sektionerna nedan har vi tillhandahållit en mycket kort (och långt från heltäckande) översikt av GDPR-kraven. Du kan finna länkar till mer detaljerad vägledning i sektionen "Hjälpsamma källor för GDPR".

Varför en ny lag?

Lagstiftare och tillsynsmyndigheter inom EU var övertygade om att direktivet behövde uppdateras för att ta itu med bristen på samordning och den sociala och tekniska utvecklingen under de 20 åren sedan direktivet utfärdades. På toppen av listan fanns mer kraftfulla verkställighetsåtgärder, större territoriell räckvidd och förbättrade rättigheter för individer.

Många av de nya reglerna (t.ex. extraterritoriell effekt) är huvudsakligen riktade mot sociala medier och internetföretag utanför EU. EU-lagstiftare och tillsynsmyndigheter har tyckt att det existerande Direktivet inte tillräckligt skyddade dataintegritetsrättigheter för EU-individer som använder sådana sociala medier och internettjänster.

Blackboard drivs annorlunda än dessa sociala medier och andra internetföretag vars affärsmodell är byggd på att tjäna pengar på användardata. Vi samlar in och använder personinformation[2] från våra kunder enligt deras direktiv och för att tillhandahålla våra Produkter och tjänster till dem och deras användare. Vi samlar inte in och använder inte personinformation för att sälja denna information eller för att sälja annonsering. Vi förstår att personinformation är anförtrodd till oss och kommer med skyldigheter. Vi har därför ett gemensamt intresse och ett gemensamt ansvar med våra kunder att skydda denna information.

Vad är nytt?

Medan den är baserad på existerande EU-principer och begrepp för dataintegritet, så medför GDPR väsentliga ändringar för dataintegritet inom EU, inklusive:

- Ökade kraft att utdöma böter på upp till 4 % av global omsättning eller 20 miljoner EUR (den större summan används)
- Ökad territoriell omfattning till organisationer utanför EU, som tillhandahåller produkter och tjänster till EU-boende eller övervakning av EU-boende.
- Obligatorisk meddelandeplikt om läckor, till övervakande myndigheter inom 72 timmar för personuppgiftsansvarig[3]
- Skärpta krav rörande samtycke
- Förbättrade rättigheter för individer (inklusive rättighet att radera och dataportabilitet)

Men några av de viktigaste ändringarna är de nya principerna rörande redovisningsskyldighet och inbyggt integritetsskydd. Dessa principer kräver effektiv styrning och processer för dataintegritet, liksom en mer detaljerad och robust dokumentation rörande hur en organisation efterlever GDPR:s krav.

Vad förblir som förut

Många av begreppen och definitionerna i GDPR förblir desamma eller är liknande de som finns i Direktivet:

- Definitionen av "persondata" (eller personinformation) förblir i stora drag densamma men inkluderar nu explicit IP-adresser, cookies och apparatidentifierare
- Begreppen "personuppgiftsansvarig" och "personuppgiftsbehandlare" förblir desamma (men GDPR kräver mer direkt ansvar för personuppgiftsbehandlare)[4]
- De etablerade principerna för behandling i Direktivet (t.ex. laglig och rimlig behandling, begränsning av syfte, att bevara persondata bara så länge det är möjligt) upprätthålls.
- Kraven på dataöverföring är i stora drag desamma: dataöverföring utanför EU/EES är tillåten bara så länge en godkänd dataöverföringsmekanism används (t.ex. EU-US Integritetssköld eller "typklausuler")[5]

Den högre nivån på böter enligt GDPR betyder att uraktlåtenhet att efterleva existerande principer och krav såsom att behålla persondata bara så länge det är nödvändigt, eller att ha lämpliga säkerhetsåtgärder på plats, sannolikt innebär en ökad risk.

Vilka effekter får Brexit?

GDPR kommer att vara direkt tillämpbart i United Kingdom från 2018-05-25 fram till 'Brexit' vid slutet av mars 2019. Men även efter Brexit så kommer GDPR att sätta standarden för United Kingdom.

- Den brittiska regeringen har publicerat UK Data Protection Bill 2017 (för närvarande i lagstiftningsprocessen) som implementerar GDPR före och efter Brexit[6]
- Efter Brexit gäller GDPR direkt för organisationer som erbjuder varor och tjänster till _EU-invånare eller övervakar dem (t.ex. brittiska universitet som aktivt rekryterar studenter från EU)

Effekter på dataöverföringar till och från UK:

- EU har klargjort att efter Brexit kommer UK att betraktas som ett "tredje land" vilket betyder att det inte längre betraktas som ett "lämpligt" (på vita listan) land för dataöverföring.
- Såvida inte och inte förrän UK förklaras vara lämpligt av EU-kommissionen (t.ex. som en del av en övergångsöverenskommelse), så behöver överenskommelser om mekanismer för dataöverföring införas för överföringar av personinformation från EU till UK.
- Å andra sidan behöver UK fastställa vilka länder man bedömer som lämpliga (vilket sannolikt kommer att inkludera EU-länderna och de länder som är vitlistade av EU). För de länder som inte bedöms som lämpliga kommer UK-godkända mekanismer för dataöverföring (sannolikt liknande EU-mekanismerna) att behöva användas för överföringar av persondata ut ur UK.

Avmystifiering av GDPR

Ett mål för GDPR var att ge mer klarhet genom en mer detaljerad beskrivning. Emellertid finns det fortfarande många aspekter hos GDPR som är föremål för tolkning. Dessutom har GDPR:s komplexitet lett till en brist på förståelse såväl som överdrivna påståenden. Detta har skapat många myter, några av vilka vi har avslöjat nedan:[7]

Myt 1: Samtycke krävs för all behandling av personinformation

Faktum: Samtycke är bara ett av de legala skälen som medger att personinformation behandlas (t.ex. behandling som krävs för att genomföra ett kontrakt eller för organisationens 'legitima intresse'). Ribban för samtycke ligger väldigt högt. Till exempel, om individerna inte har ett genuint fritt val och kan återta sitt samtycke när som helst, utan någon nackdel, så kommer det inte att betraktas som samtycke. I många databehandlingsscenarion så kommer andra lagliga skäl att vara mer passande.[8]

Myt 2: Tidsgränsen 72 timmar för notifiering om incidenter gäller hela leveranskedjan (dvs. från den tid som någon personuppgiftsbehandlare blir medvetet om incidenten)

Faktum: GDPR kräver att personuppgiftsbehanlsaren meddelar sin personuppgiftsansvarige "utan onödigt dröjsmål" vid en incident rörande persondata. Först när personuppgiftsbehandlare har meddelat personuppgiftsansvarig så börjar den 72-timmars meddelandeperioden för personuppgiftsansvarig. Artikel 29-arbetsgruppen (WP29), gruppen av EU:s dataskyddsmyndigheter, har klargjort i sina slutliga vägledningar[9] att "utan onödigt dröjsmål" betyder "skyndsamt" meddelande (inte "omedelbart" meddelande som förslogs i en tidigare arbetsversion).

Myt 3: Dataöverföringar ut ur EU/EES är inte tillåtna eller bara med kundens samtycke för varje dataöverföring

Faktum: GDPR bibehåller i stora drag existerande dataöverföringskrav. Som sådana är dataöverföringar tillåtna om en EU-godkänd mekanism för dataöverföring finns på plats, såsom EU-US-Integritetsköld eller de EU-godkända typklausulerna (överenskommelser om dataöverföring). Blackboard har båda dessa mekanismer på plats för att med efterlevnad av kraven kunna överföra personinformation.[10] Eftersom Blackboard agerar som en personuppgiftsbehandlare, så krävs en allmän instruktion för dataöverföringar från kunden (vilken finns i innehållet i vår standardöverenskommelse för databehandling), men kundens samtycke för varje dataöverföring är inte nödvändig.

Myt 4: Rätten att radera kräver att organisationer raderar alla data om en individ

Faktum: Den nya rätten till radering inkluderar inte en absolut "rätt att bli glömd": Snarare är det en rätt att få data raderad om dessa data inte längre krävs, och under andra omständigheter där organisationen inte uppfyller GDPR-kraven. Om en organisation fortfarande legitimt behöver behålla data (till exempel på grund av krav att behålla handlingar) behöver dessa persondata inte raderas.

Myt 5: GDPR gäller för alla universitet som har studenter från EU

Faktum: Enbart att ha studenter från EU registrerade räcker inte för att GDPR skall vara tillämplig. I allmänhet gäller GDPR för institutioner som är etablerade inom EU. Den gäller även för universitet utanför EU, men bara om de erbjuder varor och tjänster till individer inom EU eller övervakar beteenden hos individer inom EU. För att anses som att man "erbjuder tjänster" krävs någon grad av målinriktning. Det blotta faktum att EU-studenter finns registrerade räcker inte. GDPR kan dock vara tillämplig när universitet aktivt riktar sig till EU-studenter (t.ex. för kurser online) eller aktivt rekryterar studenter i EU-länder. Dessa kriterier är öppna för tolkning. Vi rekommenderar att kunder tar hjälp av sina egna juridiska rådgivare.

IMPLEMENTERING AV GDPR

Varför är det viktigt att få till dataintegritet och GDPR korrekt

Risken för böter på 4 % av global omsättning är förvisso ett skäl som fått många organisationer har börjat ta dataintegritet på allvar. Men vi tror att det positiva argumentet för bra dataintegritetspraxis är minst lika tvingande därför att dataintegritet är en mänsklig rättighet och därför att ha robust dataintegritetspraxis skapar förtroende.

I dagens samhälle finns personinformation överallt. Personinformation kallas ofta för den nya oljan i ekonomin. Vi använder alla online-tjänster och lämnar ut personinformation. Men den ena studien efter den andra visar att man inte litar på organisationer när det gäller personinformation. Det finns en känsla av att individer har förlorat kontrollen över sina data. Lagstiftare och tillsynsmyndigheter reagerar på detta. GDPR är troligen det mest prominenta exemplet. Organisationer behöver (åter)få individers förtroende. En bra dataintegritetspraxis är nyckeln till att bygga upp detta förtroende. Den är även en konkurrensfördel. Slutligen hjälper den även organisationen med innovation. Om studenter (och personal) har förtroende för er institution, så kommer de att med högre sannolikhet dela sin information och använda nya verktyg.

Fel i dataintegriteten kan vara katastrofala. Dataläckor finns ofta i nyheterna. Det som följer är ett skadat rykte, förlust av förtroende hos individer och risken för ersättningskrav från dem vars data har hanterats fel. Myndigheterna för dataskydd kanske inte använder böter på 4 % av omsättningen direkt från början, men de har många andra tillgängliga verktyg för att upprätthålla lagen och de kan tvinga institutioner att ändra sin datapraxis och implementera program för dataintegritet med regelbundna externa revisioner.

Vår och din organisations roller enligt GDPR

GDPR bibehåller begreppen "personuppgiftsansvarig" och "personuppgiftsbehandlare". Dessa begrepp är centrala eftersom de fastställer ansvar och ersättningsskyldighet för organisationer och deras tjänsteleverantörer.

En organisation betraktas som personuppgiftsansvarig om den fastställer "medel och ändamål" för behandling av personinformation, dvs. varför och hur persondata används. Å andra sidan är personuppgiftsbehandlaren den organisation som agerar på denpersonuppgiftsansvariges vägnar och enligt dess instruktioner.

För de flesta av Blackboards produkter och tjänster (dvs. Learn, Collaborate, Open LMS), betraktas Blackboard som personuppgiftsbehandlre och våra kunder som personuppgiftsansvariga.

GDPR påtvingar mer direkta krav på personuppgiftsbeandlre som Blackboard. Dock gäller huvuddelen av GDPR:s krav fortfarande för personuppgiftsansvarig (t.ex. ansvaret att informera individerna hur deras data används, för att uppfylla individernas krav på tillgång till sina data, absolut krav på meddelande om läcka till myndigheter för dataskydd och till individer).

Vad kan du göra för att förbereda GDPR?

Alla organisationer som omfattas av GDPR kommer att behöva vara färdiga2018-05-25. Här är några nyckelaktiviteter som kunder kan utföra för att göra sig redo. Denna stegvisa lista är baserad på vår egen erfarenhet och är på intet sätt avsedd att vara heltäckande. Vänligen säkerställ att experter på dataintegritet för att hjälpa dig med din egen implementering. Många dataskyddsmyndigheter har också skapat egna vägledningar rörande implementering av GDPR.[11]

Förhoppningsvis har du redan tagit stegen 1-6 och är mitt i aktiviteten att implementera dina handlingsplaner. Men det är aldrig för sent att starta. Även om du just har startat, så kan du implementera de mest kritiska ändringarna. Det betyder också att du kommer att kunna visa din dataskyddsmyndighet att du arbetar enligt en plan. Att ignorera GDPR är inte ett alternativ.

1. **Kontrollera om din organisation omfattas av GDPR**

   Om din organisation är etablerad inom EU omfattas den av GDPR. Men GDPR kan även omfatta organisationer utanför EU.[12]

2. **Etablera ett GDPR-projekt.**

   Utforma och implementera ett dedikerat GDPR**-**projekt. Helst ska projektledare och anvisade kontakter, i varje avdelning, som kan stödja dig. Projektet kommer att sträcka sig över alla avdelningar inom organisationen och du kommer att behöva hjälp.

3. **Utse en erfaren GDPR-ledare för att leda projektet**

   Ledaren ska inte enbart vara en erfaren ledare inom dataintegritet, men även ha tillräcklig tid och tillräckliga resurser såväl som tillgång till externt stöd (t.ex. en advokatfirma). Om din organisation är en myndighet etablerad i EU, så behöver även ett dataskyddsombud utses.

4. **Säkerställ högsta ledningens acceptans och uppsikt**

   Genomförande av ett GDPR-projekt utan stöd, överinseende och uppsikt från högsta ledningen är svårt.

5. **Gå igenom användningen av personinformation och genomför en gap-analys.**

   Att förstå var och hur personinformation används och var GDPR-förbättringar krävs är den första nyckelfasen i GDPR-projektet.

6. **Utarbeta handlingsplaner för att stänga gapen.**

   Detta är troligtvis den svåraste delen av GDPR-arbetet då den kräver att översätta krav från GDPR på ofta hög nivå måste översättas till specifika och genomförbara aktiviteter för alla de olika processerna och systemen.

7. **Implementera handlingsplaner**

   Tillit är bra, men styrning är bättre i detta fall. Denna fas kräver uppföljning av andras handlingsplaner för att säkerställa att de uppfyller sina leveranstider.

8. **Gå igenom dina leverantörer**

   Enligt GDPR är du ansvarig för dina leverantörer. Att ha de rätta avtalsbestämmelserna på plats är viktigt, men inte tillräckligt. Du måste kunna lita på att dina leverantörer uppfyller GDPR:s krav och kan stödja din efterlevnad av kraven. Fråga hur de implementerar GDPR.

9. **Håll dig uppdaterad med gällande utveckling av lagstiftning/reglering (Art. 29-arbetsgrupps riktlinjer, medlemsstater som inför lagar)**

   Att känna till GDPR är tillräckligt, eller hur? Fel! Medan GDPR gäller direkt, så inför alla EU:s medlemsstater nationella kompletterande dataskyddslagar. Dessa är utformade för att reglera områden där medlemsstater har lagstiftande rätt (t.ex. anställdas dataintegritet) och där GDPR låter dem ytterligare lagstifta (t.ex. kriterier för dataskyddsombud och konsekvensbedömningar avseende dataskydd). Dessutom publicerar artikel 29-arbetsgruppen viktiga riktlinjer. Att hålla sig uppdaterad är en utmaning, men det är viktigt.[13].

BLACKBOARDS PLAN OCH ANGREPPSSÄTT

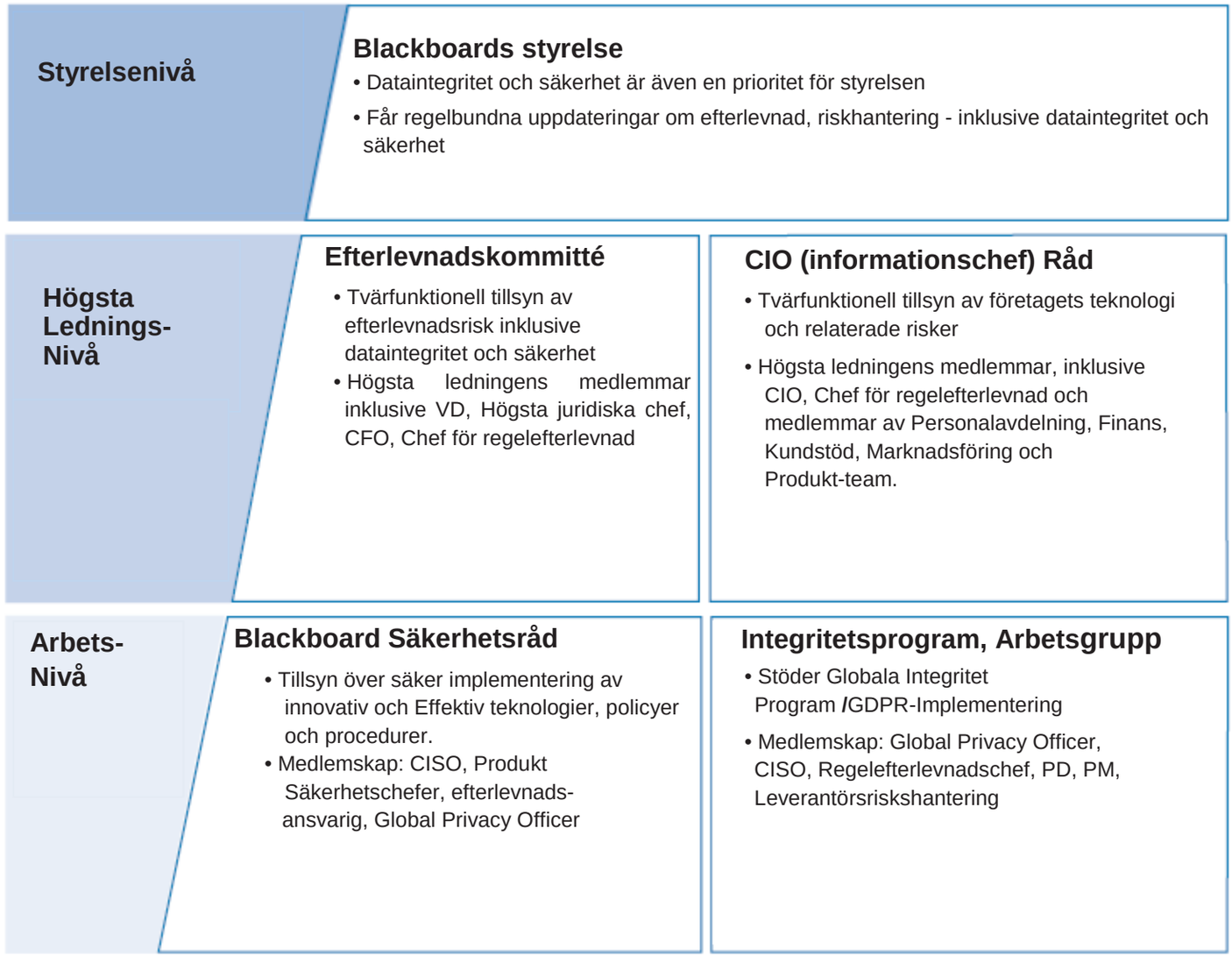
Dataintegritet och säkerhet hos Blackboard

Dataintegritet och säkerhet har en varit en nyckelprioritet sedan länge hos Blackboard . För oss är GDPR ett tillfälle att ytterligare stärka vår existerade praxis för dataintegritet.

Vår angreppsmetod för dataintegritet har alltid varit fokuserad på kunden. Vi förstår de utmaningar som våra klienter möter och vill hjälpa dig med dem.

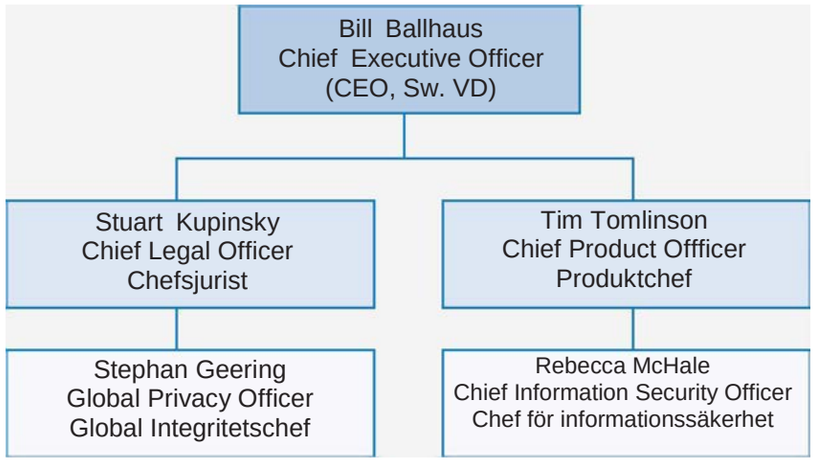
En bra praxis för dataintegritet kräver en solid ledningsmodell. Hos Blackboard är dataintegritet och säkerhet en prioritet för styrelsen och vår ledningsmodell (se nedan) säkerställer att högsta ledningen har uppsikt över och stöder vårt arbete med dataintegritet och säkerhet.

Den vikt som Blackboard placerar på dataintegritet och säkerhet belyses även av det faktum att vår Global Privacy Officer och Chief Information Security Officer[14] rapporterar till VD:s ledningsgrupp (se organisationskarta nedan)



Integritet och Säkerhet

Den vikt som Blackboard lägger på dataintegritet och säkerhet belyses även av det faktum att vår Global Privacy Officer och Chief Information Security Officer rapporterar till VD:s ledningsgrupp.



Blackboards angreppssätt för GDPR

Vi har etablerat ett övergripande projekt för att implementera kraven från GDPR med användning av följande angreppssätt:

- GDPR-implementeringen bygger på Blackboards existerande dataskyddserfarenhet och efterlevnadsmekanismer
- GDPR-implementeringen leds av Global Privacy Officer och stöds av en dedikerad projektledare och "GDPR-ledare" inom varje funktionellt område
- Den namnkunniga advokatfirman Bristows LLP har bland många andra anlitats för att stödja GDPR-implementeringen
- GDPR-implementeringen övervakas av Blackboards Efterlevnadskommitté, vilken inkluderar företagets VD, dess juridiska chef, och andra högt uppsatta chefer.

GDPR som en möjlighet

Vi ser inte enbart GDPR-implementeringen som en ansträngning för att efterleva EU:s krav på dataintegritet, utan även som en möjlighet. Som sådan siktar vi på att använda GDPR-implementeringen för att uppnå följande:

- Stärka den globala dataintegritetspraxisen - vi kommer att använda GDPR-projektet för att förbättra vårt globala dataintegritetsprogram inom EU och utanför EU
- Utveckla integritet genom utformningsprocesser för inbyggt integritetsskydd som ytterligare bygger på efterlevnaden av dataintegritet i våra dagliga processer.
- Stödja våra kunder med ansträngningar för GDPR-efterlevnad
- Placera Blackboard som den erkända dataintegritetsledaren i undervisningsteknologi

Vår implementeringsplan

Vi följer Bristow LLP:s etablerade 3-fas metodik för att implementera vårt globala Dataintegritets- / GDPR-program. Denna metodik används av ett stort antal företag, inklusive ledande högteknologi-företag. De tre faserna är följande:

- **FAS 1 - Informationsinsamling**
- **FAS 2 - Utveckling av lösningar**
- **FAS 3 - Implementeringsarbetsströmmar**

Vi har använt denna 3-fas metodik för att utveckla våra program med följande fyra nyckelsteg:

Projektinitiering

Projektets startfas inkluderar följande aktiviteter

- Presentation för högsta ledningen, och dess accepterande
- Anställning av en Global Privacy Officer med ansvaret för att leda GDPR-projektet
- Utveckling av projektplan och projektstyrning
- Inledande insamling av information och bedömning av aktuella efterlevnadsaktiviteter inom områden som kräver förbättringar enligt GDPR

FAS 1 - Informationsinsamling (workshops)

Under denna inledande fas utförde vi strukturerade konversationer/workshops med nyckelintressenter från Blackboards funktionella områden och produktgrupper för att få information om databehandlingspraxis inom dessa områden.

Resultatet från dessa workshops användes för att genomföra gap-analysen och utveckla lösningar och implementeringsplaner i fas 2.

FAS 2 - Utveckling av lösningar

Baserat på informationen från workshops utvecklade vi följande lösningar och dokumentation.

- Förbättrad intern dataintegritetsdokumentation (policy och detaljerade driftstandarder) som återspeglar GDPR:s krav och förklarar hur GDPR-krav kommer att behöva uppfyllas för de olika databehandlande aktiviteterna (t.ex. krav för behandling av kunddata, process för inbyggt integritetsskydd)
- Produktkrav
- Implementeringsplaner för de funktionella områdena och för centrala aktiviteter som krävs

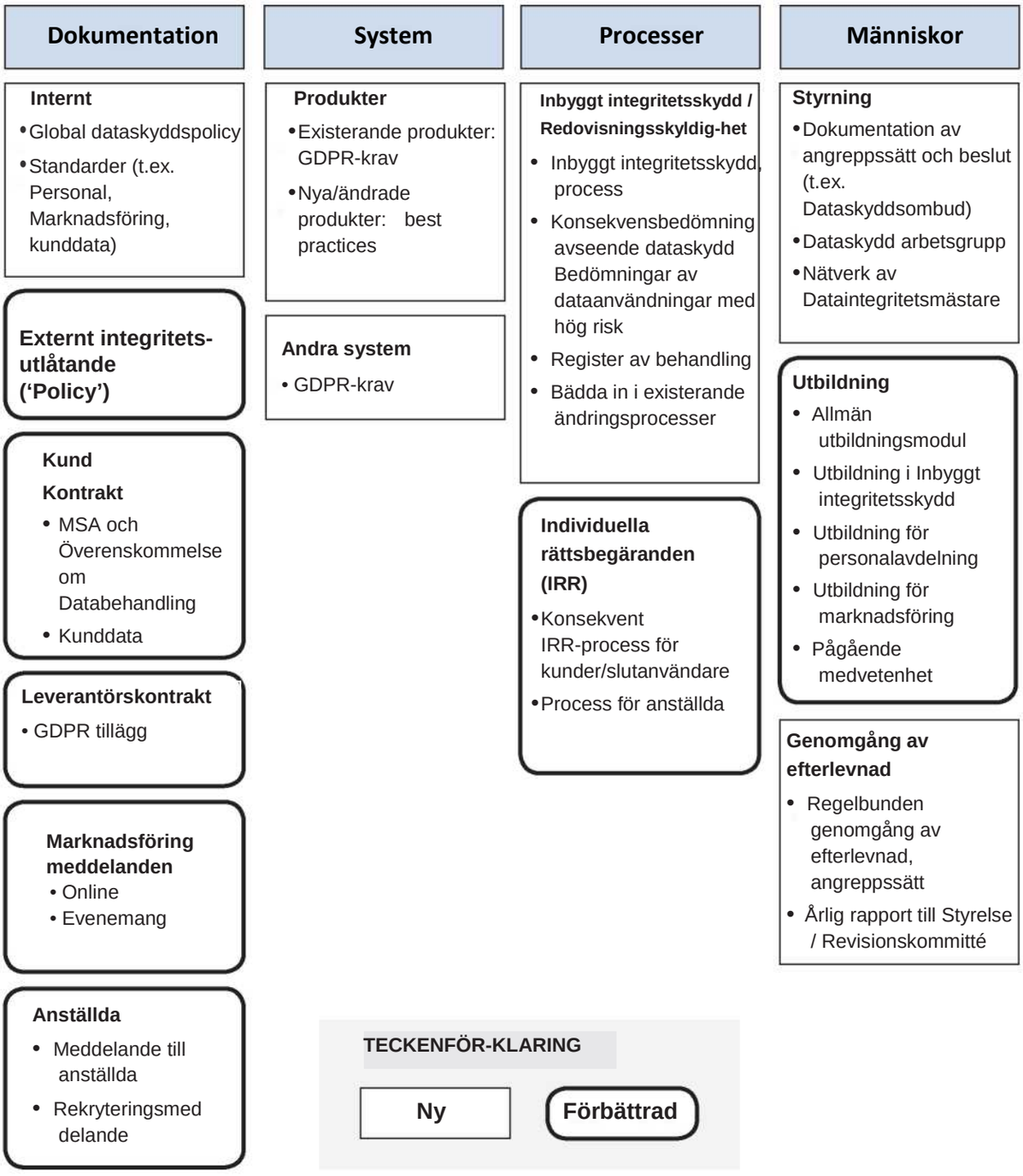
FAS 3 - Implementeringsarbetsströmmar

Under den slutliga fasen, så implementerar vi den utvecklade dataintegritetsdokumentationen och genomför implementeringsplanerna. Sex huvud-arbetsströmmar kommer att användas för att genomföra implementeringen:

1. Utför implementeringsplanerna för de funktionella områdena och produktgrupperna
2. Gå igenom och uppdatera policyer, meddelanden och samtycken som är vända mot allmänheten,
3. Förbättra styrning (roller och ansvar, utbildning, inbyggt integritetsskydd, etc.)
4. Gå igenom och uppdatera leverantörskontrakt (där så är nödvändigt)[15]
5. IT-system, ändringar (där så är nödvändigt)
6. Etablera ett databehandlingsregister

Översikt av ändringar

Diagrammet nedan visar hur vi föreställer oss slutstadiet av vårt GDPR/ dataintegritetsprogram efter implementeringsaktiviteterna. Efter GDPR-implementeringen kommer vi att fortsätta att innovera och anpassa oss för att ytterligare befästa våra policyer för dataintegritet.



HUR KOMMER VÅRT GDPR-PROGRAM ATT HJÄLPA DIG

Blackboards globala dataintegritets- /GDPR-implementeringsprogram är fokuserat på att stödja din organisation med din implementering av GDPR. De följande avsnitten ger dig fler detaljer, men sammanfattningsvis så är de 7 nyckelpunkterna:

1. **Produkter färdiga för GDPR** Vi håller på att implementera produktkraven för att stödja kunder med krav på genomsynlighet, begäran om individuella rättigheter etc.
2. **Inbyggt integritetsskydd** Vi implementerar inbyggt integritetsskydd och en process för konsekvensbedömning av dataskydds genomslag (Assessment) för att underlätta dokumentationen av efterlevnad
3. **Dataöverföringar:** Vi kommer att fortsätta med vårt angreppssätt i flera skikt: Regionalisering, EU-US Integritetssköld och EU-godkända typklausuler
4. **Avtal med kunder** Vi har ett GDPR-färdigt tillägg för databehandling till vårt standardramavtal
5. **Våra leverantörer:** Vi har robusta kontrakt och ett ramverk på plats för hantering av leverantörsrisk
6. **Säkerhet:** Vi har en etablerad policy, procedurer och styrning som kontinuerligt förbättras för att skydda säkerheten hos kunddata
7. **Meddelande om läcka:** Vi har dokumenterat och testat en åtgärdsprocess för säkerhetsincidenter

1. Produkter färdiga för GDPR

Att stödja våra kunder genom att göra våra produkter färdiga för GDPR är en av nyckelaspekterna hos våra implementeringsteam. För detta syfte har vi utvecklat minimikrav för GDPR/Dataintegritet för våra produkter. I linje med vårt angreppssätt att stärka vår praxis för dataintegritet globalt, så gäller de flesta av dessa krav för alla våra produkter, inte bara de produkter vi gör tillgängliga inom EU. Detta stöder också våra klienter utanför EU som kan omfattas av GDPR.

Vi utvecklade våra GDPR/dataintegritsproduktkrav genom en robust och intensiv process. Vi gjorde en initial version tillsammans med externa rådgivare. Under ett flertal arbetssessioner och revisioner med nyckelintressenter från våra produktutvecklings- och produkthanteringsteam förfinade vi versionen till specifika och genomförbara allmänna produktkrav med detaljerade riktlinjer. Produktkraven för GDPR/dataintegritet översattes därefter till produktspecifika aktiviteter i produktimplementeringsplanerna för varje produktgrupp.

Våra produktkrav[16] kan kategoriseras enligt följande:

öppenhet

- Möjlighet för kunder att länka till sina integritetspolicyer/meddelanden.
- Tillhandahålla information om hur personinformation i allmänhet används i en produkt.

Dataminimering/radering

- Genomgång av produkter avseende onödiga/valfria fält
- Genomgång av produkter avseende möjligheter att använde pseudonymdata eller anonyma data i stället för personinformation.
- Möjlighet att radera personinformation när detta begärs av kunder (när kunder/ användare inte kan radera data själva)

Allmänna individuella rättigheter

- Möjlighet att ge tillgång till och rätta personinformation när en person begär detta
- Möjlighet att radera personinformation när en person begär detta

EU Individuella rättigheter

- Möjlighet att hantera begäran om dataportabilitet (rätt för individer att få data i maskinläsbart format under vissa omständigheter)
- Möjlighet att sluta använda personinformation (rätt att invända/rätt till begränsning under vissa omständigheter)

Blackboard har redan definierat program för vår produktsäkerhet, som beaktar GDPR. Vi har därför inte definierat ytterligare GDPR-specifika säkerhetskrav[17]

2. Inbyggt integritetsskydd

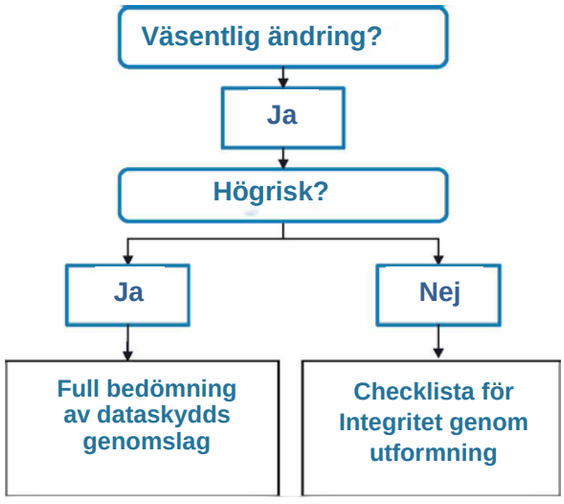
Eftersom det blir alltmer av en utmaning i dagens värld att upprätthålla kontroll över sin information för individer (se vår dagliga bloggpost om integritet rörande detta ämne) får inbyggt integritetsskydd och redovisningsskyldighet allt större vikt för att upprätthålla individers, kunders och reglerande myndigheters förtroende, och att dokumentera hur en organisation efterlever GDPR. Vi sätter därför vårt angreppssätt med inbyggt integritetsskydd i centrum för vårt Globala Integritets- /GDPR-program.

För Blackboard är detta en utveckling snarare än en revolution. Vi har alltid utfört juridiska genomgångar av nya produkter och praxis. Med vårt angreppssätt med inbyggt integritetsskydd formaliserar vi och dokumenterar dessa genomgångar bättre.

Angreppssätt

- Vi skapade en dokumenterad process för inbyggt integritetsskydd och en checklista.
- Funktionella områden och produktgrupper inkluderar checklistan för inbyggt integritetsskydds i sina ändringsprocesser.
- Varje väsentlig ändring av hur personinformation används kräver att checklistan för inbyggt integritetsskydds fullbordas. Medan detta inte specifikt krävs av GDPR, så är det best practice.
- Checklistan kommer att starta den mer detaljerade processen för konsekvensbedömning av dataskydd) för högriskanvändning av personinformation (GDPR-krav)

Flödesschemat nedan visualiserar angreppssättet:



3. Dataöverföringar

GDPR medför inga väsentliga skillnader för hur personinformation kan överföras ut från EU/EES. De nuvarande restriktionerna och dataöverföringsmekanismerna förblir. Detta betyder att dataöverföringar är tillåtna om en EU-godkänd mekanism för dataöverföring finns på plats, såsom EU-US -Integritetssköld eller de EU-godkända typklausulerna (överenskommelser om dataöverföring). Dessa mekanismer säkerställer att personinformation är tillräckligt skyddad även när den lämnar EU/EES.

Vi kommer att fortsätta med vår flerskikts- och redundanta angreppsmetod för efterlevnad av dataöverföring. Detta betyder att vi betraktar dataöverföringskrav via ett flertal vägar för att säkerställa att korrekta skydd för din information är på plats.

- **Regional hosting:** Vi har en strategi med regional hosting där nästan alla produkter har en host inom EU och andra produkter är planerade att flytta till regionala hosting-lösningar. Medan regional lagring inte krävs av GDPR och vi heller inte tror att datalokalisering leder till bättre dataintegritet eller säkerhet,[18] så förstår vi att många kunder inom EU föredrar att deras data lagras inom EU.
- **Integritetssköld:** Blackboard är EU-U.S. Integritetsköldcertifierat vilket medger att vi lagligt kan överföra persondata till USA.
- **Typklausuler:** Vi använder också EU-godkända typklausulavtal som medger att vi med bibehållen efterlevnad kan överföra persondata ut ur EES inom Blackboards företagsgrupp ("Kunddataöverföringsavtal").
- **Leverantörer:** Robusta kontrakt finns på plats med leverantörer och partners (t.ex. IBM, Amazon Web Services) för att säkerställa att dataöverföringskrav (och andra skyldigheter rörande dataskydd) överförs på våra leverantörer och partners.

Vi har för närvarande[19] ett flertal regionala datacentra för att stödja datahantering inom EU för våra EU-kunder:

- Managed hosting (Blackboard datacentra): Datacentra i Amsterdam (Nederländerna) och Frankfurt (Tyskland).
- Molnlagring (AWS datacentrum): AWS region Frankfurt, Tyskland (eu-central-1).

AWS datacentra uppfyller en mängd certifieringar och krav från ISO 27001 och ISO 27018, till SOC2 och till efterlevnad av GDPR såväl som efterlevnad av lokala krav, såsom den tyska C5 och IT-Grundschutz.[20]

Det är viktigt att förstå att medan personinformation för kunder lagras i dessa datacentra för de flesta av produkterna (inklusive Learn 9.1, Learn SaaS, Open LMS och Collaborate) för EU-kunder, kan tillgång till dessa data från länder utanför EU/EES krävas för att tillhandahålla produkterna eller tjänsterna t.ex. för stöd 7/24. Sådana dataöverföringar är tillåtna genom den nämnda EU-US-Dataköldscertifieringen och typklausuler.

4. Avtal med kunder

Det nuvarande Direktivet kräver att en personuppgiftsansvarig ska ha ett kontrakt på plats med leverantören (personuppgiftsbehandlare), men föreskriver inte i detalj innehållet i detta kontrakt. GDPR är mer beskrivande och inkluderar en lista med innehåll som krävs.[21]

Vårt nuvarande standardtillägg för databehandling inkluderar alla de punkter som krävs nedan. Det är automatiskt inkluderat för de av våra kunder med vårt standardramavtal som omfattas av GDPR.

✓ Användning av persondata enbart såsom instruerat

✓ Personal måste skriva på överenskommelser om konfidentialitet

✓ Lämpliga säkerhetsåtgärder måste vara på plats

✓ Anlita bara leverantörer (underpersonuppgiftsbehandlare)...

- Som är auktoriserade av personuppgiftsansvarig (kan vare en allmän auktorisering)
- Som enligt kontrakt är avkrävda att följa samma åligganden för dataskydd

✓ Assistera ansvarig med svar på krav rörande individuella rättigheter

✓ Assistera ansvarig med säkerhetsåtgärder, meddelande om incidenter och konsekvensbedömningar av dataskydd

✓ Returnera eller radera data vid kontraktets utgång

✓ Tillhandahålla information som är nödvändig för att personuppgiftsansvarig skall kunna demonstrera efterlevnad

✓ Omedelbart informera personuppgiftsansvarig om några instruktioner från personuppgiftsansvarig byter mot GDPR

5. Hantering av våra leverantörer

Blackboard använder leverantörer (t.ex. IBM, Amazon Web Services) för att hjälpa oss tillhandahålla våra produkter och tjänster till våra kunder. När detta kräver tillgång till vår kunds personinformation, så är Blackboard ansvariga för dataintegritetspraxis hos leverantörerna.

Som en del av vårt GDPR-program så kopplar vi nära samman angreppssättet för inbyggt integritetsskydd med existerande processer för leverantörsriskhantering och inköp. Detta resulterar i följande nyckelkontroller:

- Robusta kontrakt med integritets- och GDPR-tillägg på plats med tredje part, och krav på väsentligen ekvivalenta bestämmelser som vi har på plats med våra kunder.
- Typklausulöverenskommelse och/eller tillägg för GDPR och Integritetssköld, för att möjliggöra lagliga dataöverföringar till våra leverantörer
- Dokumenterad policy för riskhantering av leverantörer och ramverk.
- Nya leverantörer med tillgång till personinformation måste fylla i en leverantörssäkerhetsutvärdering med frågor rörande efterlevnad av dataintegritet.
- Leverantörer med tillgång till system hanterade av Blackboard avkrävs att följa Blackboards interna policy för tillgångskontroll och identitet och auktorisering, och att inkludera kontogenomgångar såsom lämpligt
- Leverantörer behöver ansluta till Blackboards resurser via godkända mekanismer (t.ex. VPN)
- Leverantörer har begränsad tillgång till styrning av trafik, användare och tillgångar.

6. Säkerhet

GDPR förändrar inte väsentligen de tekniska och operativa åtgärderna (TOM:ar) för personinformationens säkerhet. Sådana åtgärder måste vara "lämpliga" jämförda med den risk som finns, liksom under det nuvarande Direktivet. Vi fortsätter därför att förlita oss på etablerade program för informationssäkerhet.

Hantering av informationssäkerhetsrisk

Vi har en etablerad policy, procedurer, styrning och tekniska krav för att hantera IT-säkerhetsrisker inom hela vår verksamhet.

Från dag ett måste Blackboards personal förstå sitt ansvar för att skydda kundens persondata:

- Vidkännas policy för att skydda känslig information
- Årlig utbildning i användarsäkerhet och dataskydd
- Övningar i nätfiske
- Bulletiner om medvetenhet

Följande krav är på plats för dataskydd från vår personal.

- Dataklassificeringar definieras med krav för att skydda varje datatyp. Våra kunders data är vår högsta känslighet - data från institutioner och deras studenter.
- Tekniska kontroller är på plats för att skydda data, t.ex.:
  - användning av kryptering
  - snabba säkerhetsuppdateringar
  - förbättrade kontroller för autentisering
  - skydd mot elakartad e-post och webbtrafik
  - teknologier för skydd vid terminalen
  - tillgång begränsad baserat på behovsenlig behörighet

Det är inte bara GDPR ...

Som ett globalt företag som tjänar undervisningssamhället övervakar vi noga relevanta geografiska- och undervisningssektor-specifika lagar och förordningar rörande dataintegritet och säkerhet.

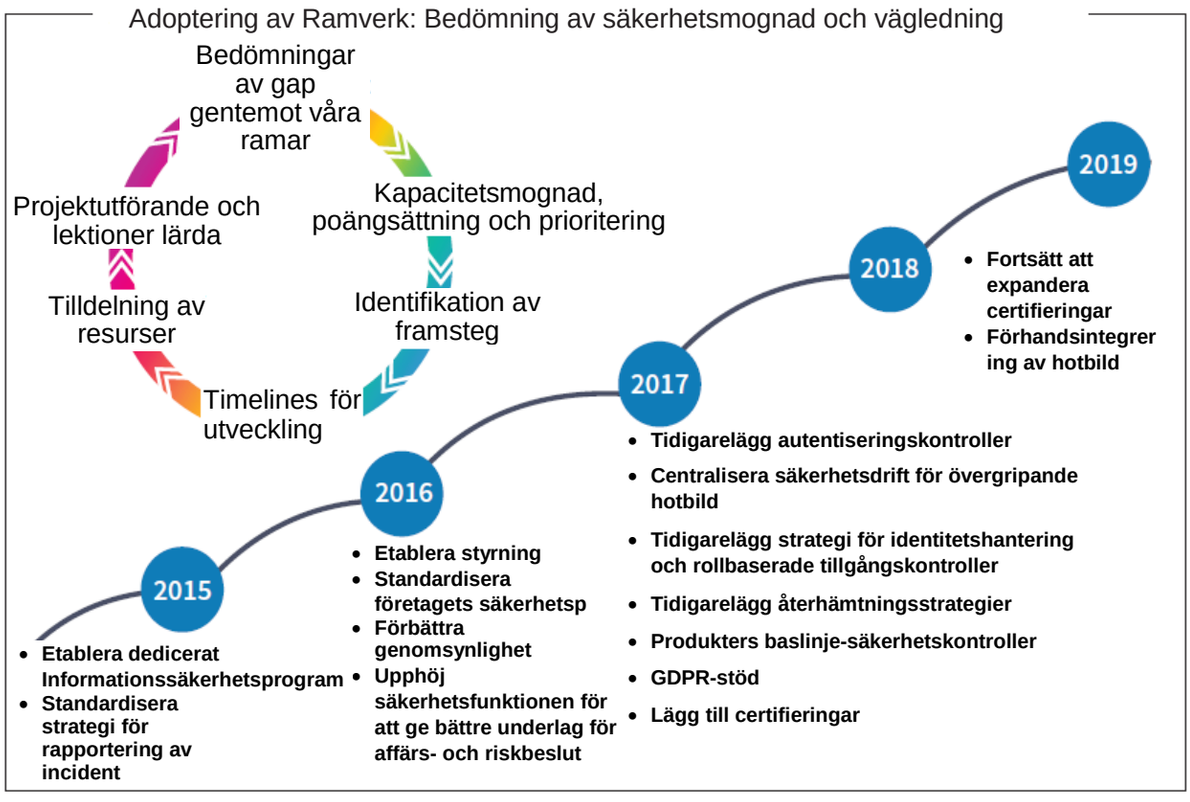
Listan nedan ger bara några exempel på förordningar, standarder och ramverk rörande säkerhet och dataintegritet, som Blackboard beaktar utöver GDPR när vi utvecklar våra policyer, processer och tekniska kontroller för säkerhet.

- US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
- US Children’s Online Privacy Protection Act (COPPA)
- Amerikanska delstatliga lagar (existerande och kommande, lappverk med 50 stater)
- Standarder från USA:s regering - FedRAMP
- PCI Data Security Standards, där de är tillämpliga

  ISO/I EC, OWASP, NIST
- Internationella standarder (MTCS, IRAP)

Bedömning av säkerhetsmognad och vägledning

Vi arbetar hårt för att kontinuerligt förbättra våra tekniska och driftsmässiga säkerhetsåtgärder. Diagrammet på nästa sida visualiserar våra kontinuerliga bedömningar av mogenhet och vår väg framåt .



7. Meddelande om läcka

En av nyckeländringarna hos GDPR är det nya obligatoriska meddelandet om läckor för persondata, till gällande myndighet för dataskydd och (i en del fall) till de påverkade individerna [22]

För de flesta av våra produkter och tjänster är Blackboard en databehandlare [23] under GDPR. Skyldigheten att meddela myndigheter för dataskydd och individer i fall av en läcka som involverar Blackboard skulle därför gälla våra kunder. Emellertid kräver GDPR att databehandlare såsom Blackboard meddelar sina kunder (datastyrare) utan onödigt dröjsmål (dvs. "genast")[24] i ett sådant fall.

Vi har följande åtgärder på plats, som stödjer våra kunder i uppfyllandet av sina skyldigheter vid en läcka rörande persondata hos Blackboard relaterad till en kund

• Blackboards säkerhetsincidentresponsprocess (SIR)

- Dokumenterad och regelbundet testad
- Underlättar snabb identifiering, undersökning och åtgärd vid en incident
- Medger snabb notifiering till kunder
- Förlitar sig på det etablerade säkerhetsincidentresponsteamet (som inkluderar Chief Information Security Officer och Global Privacy Officer)

• Vår skyldighet att meddela kunder snarast är uttryckligen uttalad i vårt nuvarande standardramavtal och dataskyddstillägg [25]

SAMMANFATTNING

GDPR kräver väsentliga skillnader med effekt bortom dess ikraftträdande den 2018-05-25. Vi hoppas att denna vitbok kan bidra till din framgångsrika implementering av GDPR och har demonstrerat hur allvarligt Blackboard ser på GDPR och efterlevnad av dataintegritet.

De följande sektionerna ger ytterligare hjälpsam information och listar vår e-postadress för kontakt om du har frågor eller feedback rörande denna vitbok.

HJÄLPSAMMA KÄLLOR RÖRANDE GDPR

Resurserna som är länkade nedan är bara ett litet urval av hjälpsamt material som finns tillgängligt online. Det är inte avsett att vara en uttömmande lista.

För en detaljerad analys av hur GDPR påverkar dig bör du också söka råd från specialister. Det är viktigt att anlita erfarna dataskyddsexperter (t.ex. från en advokatfirma som du väljer)

Officiella resurser från EU

- GDPR text
- Artikel 29-arbetsgrupp riktlinjer
- EU-Kommissionens GDPR-webbplats

Material från EU:s Dataskyddsmyndighet

- UK Information Commissioner's Office (ICO) har en utmärkt GDPR-webbplats med hjälpsamt material på enkelt språk och som konstant uppdateras
- Irish Data Protection Commissioner (DPC) har en dedikerad GDPR-sida för organisationer
- Franska CNIL tillhandahåller en del material på engelska inklusive en gratis programvara för bedömning av integritetspåverkan (och mycket mer material på franska språket)
- Spanska AEPD producerade en guide för undervisande institutioner(PDF, på spanska)

Guider från advokatfirmor

- Bird & Birds guide till GDPR
- Bird & Birds Spårare för medlemsländers lagar

  (håller reda på nationella GDPR-variationer)
- Linklaters GDPR survival guide (PDF)
- White & Case GDPR handbook

Andra organisationer

- JISC UK har hjälpsamma resurser, evenemang och blogg-uppdateringar om GDPR
- UCISA har publicerat ett GDPR ”best practice”-dokument med praktiska steg och fallstudier
- International Association of Privacy Professionals (IAPP) har ett bra (gratis) veckovis nyhetsbrev om europeisk dataintegritetsutvecklingar
- IAPP har också en hjälpsam översikt över leverantörer av verktyg för dataintegritet (PDF)
- Amazon Web Services har ett dedikerat GDPR-Centrum

BIOGRAFIER

Stephan Geering
Global Privacy Officer

- Globalt ansvar för efterlevnad av dataintegritets- och säkerhetslagar
- Leder Globalt dataintegritet/GDPR-implementering sprogram
- Rapporterar till Chief Legal Officer; medlem av Blackboards juridiska team
- Baserad i London

Stephans bakgrund:

- Advokat/Vice dataskyddskommissionär hos en schweizisk kantonal dataskyddsmyndighet (2002-2008)
- LLM vid University College London (2008-2009)
- Associate Director, Group Privacy vid Barclays (2010-2012)
- Regionalt ansvarig för dataintegritetsverksamhet inom EMEA vid Citigroup (2012-2014)
- EMEA och APAC Chief Privacy Officer vid Citigroup (2014-2017)
- CIPP/E certifierad

Rebecca McHale
Chief Information Security Officer

- Leder säkerhetsstrategi för produkter och infrastruktur
- Övervakar Blackboards cybersäkerhetsstyrning
- Rapporterar till Chief Product Officer
- Baserad i Washington, D.C., USA

Rebeccas bakgrund:

- Kom till Blackboard 2016; kombinerade nyligen säkerhetsteam och upphöjde säkerhetsorganisationens roll inom bolaget
- MS Discrete Mathematics and Computing Applications vid Royal Holloway, University of London
- Tidigare Senior Director for Cybernetik Programs vid Novetta och CSRA, tjänade USA:s regering och kommersiella kunder - t.ex. USA:s utrikesdepartementet, Transportation Security Administration (TSA) och Federal Deposit Insurance Corporation (FDIC)

MER INFORMATION

Du kan finna mer information på vår dedikerade **Data Privacy and Security Community-sida.**

Vi har också ett nyhetsbrev rörande Dataintegritet Om du vill få vårt nyhetsbrev eller har några frågor eller feedback rörande denna vitbok, vänligen kontakta oss på **privacy@blackboard.com.**

Källor

1 Se "Hjälpsamma GDPR-resurser"-sektionen på slutet för mer detaljerad vägledning för GDPR.

2 Vi föredrar termen "personinformation" i stället för "persondata" men använder termen med samma mening och omfattning som "persondata".

3 Personuppgiftsansvarig är den organisation som bestämmer medlen och ändamålen för databehandling (hur och varför personinformation används).

4 Se sektionen "Vår och din organisations roll under GDPR".

5 Se sektionen "Avmystifiering av GDPR" nedan för mer detaljer om dataöverföringar.

6 Se ICO:s "En introduktion till dataskyddslagförslag" för en hjälpsam översikt av lagförslaget.

7 Se även UK ICO:s bloggposter om GDPR-myter.

8 Se också WP29 (draft) vägledningar för samtycke under förordnande 2016/679 (WP259) och ICO:s guidning om samtycke.

9 WP29 Vägledning om meddelande om persondataläckor under förordning 2016/679 (WP250rev.01).

10 Se även sektionen "Dataöverföringar"

11 Se till exempel UK ICO:s Preparing för GDPR - 12 steg att ta nu (PDF).

12 Se även sektionen "Avmystifiera GDPR"

13 Se sektionen "Hjälpsamma GDPR-resurser".

14 För mer information om Global Privacy Officer och Chief Information Security Officer se biografisektionen.

15 Som en del av EU-US projektet för certifiering av Integritetssköld, så har vi redan inkluderat de nödvändiga GDPR-kontraktreglerna i många av de kontrakt med våra leverantörer underpersonuppgiftsbehandlaren) som har tillgång till EU personinformation.

16 Vänligen notera att produktkraven gäller alla produkter. Till exempel, en del produkter har inget användargränssnitt som skulle medge för kunder att länka till sina integritetspolicyer/meddelanden.

17 Se sektion "Säkerhet" för fler detaljer.

18 Så snart ett nätverk eller system är kopplat till Internet, så har den fysiska platsen för data ringa eller ingen betydelse för säkerhetshot. Se Amazon Web Services (AWS) white paper "Data Residency AWS Policy Perspective" (särskilt sidorna 2 och 3) för tvingande argument mot datalokalisering.

19 Vid datumet för detta dokument.

20 Se AWS Compliance Programs för den fulla listan av certifieringar och juridisk efterlevnad.

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

22 Art. 33 och 34 GDPR.

23 För en förklaring av personuppgiftsbehandlarens roll, se sektionen "Vår och din organisations roll under GDPR".

24 Se sektionen "Avmystifiering av GDPR" ovan för fler detaljer rörande tidsfrister och behandling av meddelanden om läckor för persondata

25 Se även sektionen "Kontrakt med kunder".

Blackboard.com

Copyright© 2018. Blackboard Inc. All rights reserved. Blackboard, Blackboards logga, Blackboard Web Community Manager, Blackboard Mobile Communications App, Blackboard Mass Notifications, Blackboard Social Media Manager, Blackboard Collaborate är varumärken eller registrerade trademarks för Blackboard Inc. eller dess dotterföretag i USA och/eller andra länder. Blackboards produkter och tjänster kan vara täckta under en eller flera av följande U.S Patents: 8,265,968,7,493,396; 7,558,853; 6,816,878; 8,150,925