Hoe de implementatie van GDPR door Blackboard onze klanten ondersteunt

De Europese General Data Protection Regulation (GDPR, Algemene Verordening Gegevensbescherming) betekent een ommekeer. Blackboard ontvangt deze verandering met open armen. We geven om gegevensprivacy en begrijpen dat dit een mensenrecht is. De GDPR versterkt de rechten van individuen en zal leiden tot betere praktijken inzake gegevensprivacy. Dit is goed voor individuen en organisaties aangezien het vertrouwen tussen hen zal verhogen.

We publiceren dit document om onze klanten een overzicht te geven van de veranderingen en mythes rond de GDPR, om onze implementatieaanpak uit te leggen en te beschrijven hoe onze inspanningen uw organisatie zullen ondersteunen. We hebben ons hierbij gefocust op informatie waarvan wij van mening zijn dat deze het nuttigst is voor u. Dit witboek is daarom in geen geval een uitgebreide handleiding met betrekking tot de GDPR[1].

De GDPR brengt significante veranderingen met zich mee, maar bij Blackboard kunnen we verder bouwen op onze bestaande robuuste praktijken inzake gegevensprivacy (bijv. Onze EU-VS Privacyschild-certificering). We zien de GDPR als een opportuniteit om onze praktijken verder te versterken. En we zullen ons verder focussen op onze klanten en u ondersteunen om de gegevensprivacy te respecteren.

Dit materiaal is louter informatief en vormt geen juridisch advies. Vraag raad aan uw interne of externe advocaten voor de implementatie van de GDPR in uw organisatie en gerelateerde juridische vragen.

INHOUDSOPGAVE

Blackboard heeft het certificaat van het Privacy Shield (Privacyschild), is een trotse ondertekenaar van de Student Privacy Pledge en is lid van het Future of Privacy Forum.

GDPR – WAT U MOET WETEN

De GDPR is de nieuwe Europese wetgeving inzake gegevensbescherming die de huidige EU-richtlijn voor gegevensbescherming 96/46 (Richtlijn), en de implementerende wetten inzake de bescherming van persoonsgegevens in de EU-lidstaten (bijv. de Data Protection Act 1998 in het VK) zal vervangen.

De GDPR werd in een wet vastgelegd in mei 2016 en trad in werking op 25 mei 2018.

Hieronder hebben we een kort (en helemaal geen volledig) overzicht gegeven van de GDPR-vereisten. U vindt links naar meer gedetailleerde richtlijnen in de rubriek “Nuttige GDPR-bronnen”.

Waarom een nieuwe wet?

Wetgevers en regelgevende instanties in de EU waren ervan overtuigd dat de Richtlijn herzien moest worden om het gebrek aan harmonisering en de ontwikkelingen op maatschappelijk en technologisch vlak in de 20 jaar sinds de Richtlijn van kracht ging, aan te passen. Bovenaan de lijst stonden sterkere uitvoerende overheidsorganen, breder territoriaal bereik en versterkte rechten voor individuen.

Veel van de nieuwe bepalingen (bijv. extraterritoriaal effect) zijn hoofdzakelijk gericht op sociale media en internetbedrijven buiten de EU. De Europese wetgevers en regelgevende instanties waren van mening dat de bestaande Richtlijn onvoldoende bescherming bood inzake de gegevensprivacyrechten van Europese individuen die dergelijke sociale media en internetdiensten gebruiken.

Blackboard werkt anders dan deze sociale media en andere internetbedrijven wiens model is gebaseerd op het ‘monetiseren’ van gebruikersgegevens. Wij verzamelen en gebruiken persoonlijke informatie[2] van onze klanten in opdracht van hen en om onze producten en diensten aan hen en hun gebruikers te leveren. We verzamelen of gebruiken geen persoonlijke informatie om deze informatie te verkopen of om advertenties te verkopen. We begrijpen dat persoonlijke informatie aan ons wordt toevertrouwd en dat dit verplichtingen met zich meebrengt. Daarom hebben we een gedeeld belang en een gedeelde verantwoordelijkheid met onze klanten bij het beschermen van deze informatie.

Wat is nieuw?

Hoewel de GDPR is gebaseerd op de bestaande Europese principes en concepten inzake gegevensprivacy, brengt het significante veranderingen met zich mee voor de regelgeving inzake gegevensprivacy in de EU waaronder:

- Hogere boetes tot 4% van de jaaromzet of tot 20 miljoen euro (afhankelijk van wat het hoogst is)
- Uitbreiding van het territoriale toepassingsgebied tot organisaties buiten de EU die producten en diensten leveren aan inwoners van de EU of die inwoners van de EU monitoren
- Verplichte melding van datalekken aan de toezichthoudende instanties binnen de 72 uur voor gegevensverantwoordelijken[3]
- Striktere vereisten inzake toestemming
- Versterkte rechten van de individuen (waaronder het recht op verwijdering en overdracht van gegevens)

Sommige van de belangrijkste veranderingen zijn echter de nieuwe principes inzake verklaarbaarheid en privacy door ontwerp. Deze principes vereisen een doeltreffend beheer en doeltreffende processen inzake gegevensprivacy evenals gedetailleerdere en robuuste documentatie over hoe een organisatie voldoet aan de GDPR-vereisten.

Wat blijft hetzelfde?

Veel van de concepten en definities in de GDPR blijven dezelfde of zijn gelijkaardig vergeleken met de Richtlijn:

- De definitie van “persoonsgegevens” (of persoonlijke informatie) blijft grofweg dezelfde, maar omvat nu expliciet IP-adressen, cookies en identificeerders van toestellen
- De concepten van “gegevensverantwoordelijke” en “gegevensverwerker” blijven dezelfde (maar de GDPR legt meer rechtstreekse verantwoordelijkheden bij de gegevensverwerkers)[4]
- De vastgelegde principes voor verwerking in de Richtlijn (bijv. rechtmatige & behoorlijke verwerking, doelbinding, persoonsgegevens niet langer dan nodig bewaren) worden behouden
- De vereisten inzake gegevensoverdracht blijven grofweg dezelfde: gegevensoverdracht buiten de EU/EER is toegelaten zolang een goedgekeurd mechanisme voor gegevensoverdracht is gebruikt (bijv. EU-VS Privacyschild of “modelclausules”)[5]

De hogere boetes krachtens de GDPR betekenen dat het niet-naleven van de bestaande principes en vereisten zoals persoonsgegevens niet langer dan nodig bewaren of gepaste beveiligingsmaatregelen invoeren een verhoogd risico met zich meebrengt.

Wat is de impact van de Brexit?

De GDPR zal rechtstreeks van toepassing zijn in het VK vanaf 25 mei 2018 tot de 'Brexit' eind maart 2019. Zelfs na de Brexit zal de GDPR nog altijd de standaard bepalen voor het VK:

- De Britse regering heeft de UK Data Protection Bill 2017 gepubliceerd (momenteel in het wetgevende proces) dat de GDPR implementeert voor en na de Brexit[6]

- Na de Brexit is de GDPR rechtstreeks van toepassing op Britse bedrijven die goederen en diensten bieden aan inwoners van de EU of die hen monitoren (bijv. Britse universiteiten die actief Europese studenten rekruteren)

Impact op gegevensoverdrachten van en naar het VK:

- De EU heeft bepaald dat het VK na de Brexit zal worden beschouwd als een "derde land", hetgeen betekent dat het niet langer zal worden beschouwd als een "geschikt" (witte lijst) land voor gegevensoverdracht.

- Tenzij en tot het VK geschikt wordt verklaard door de Europese Commissie (bijv. als deel van een overgangsovereenkomst), moeten gegevensoverdrachtovereenkomsten of andere gegevensoverdrachtmechanismen worden ingevoerd voor de overdracht van persoonsgegevens van de EU naar het VK.

- Omgekeerd moet het VK bepalen welke landen als geschikt worden beschouwd (dit omvat waarschijnlijk de Europese Landen en de landen die door de EU op de witte lijst geplaatst zijn). Voor de landen die als niet geschikt beschouwd worden, zullen door het VK erkende gegevensoverdrachtmechanismen (waarschijnlijk gelijkaardig aan de Europese mechanismen) moeten worden gebruikt voor de overdracht van persoonsinformatie vanuit het VK.

Opheldering van mythes rond de GDPR

Één doel van de GDPR was het bieden van meer duidelijkheid door een meer gedetailleerde regelgeving. Er zijn echter nog steeds veel aspecten van de GDPR die open staan voor interpretatie. Daarnaast heeft de complexiteit van de GDPR geleid tot een gebrek aan begrip evenals overdreven uitspraken. Hierdoor zijn veel mythes ontstaan, waarvan we er hieronder enkele willen ophelderen.[7]

Mythe 1: Voor alle verwerking van persoonlijke informatie is toestemming vereist

Feit: Toestemming is slechts één van de verscheidene wettelijke bases die de verwerking van persoonlijke informatie toelaten (bijv. verwerking vereist voor de uitvoering van een contract of voor het 'wettelijk belang' van een organisatie). De drempel voor toestemming is erg hoog geworden. Bijvoorbeeld, tenzij individuen een echte vrije keuze hebben en hun toestemming op elk ogenblik kunnen intrekken zonder enig nadeel, zal dit niet beschouwd worden als een geldige toestemming. In veel scenario's voor gegevensverwerking zullen andere wettelijke bases geschikter zijn.[8]

Mythe 2: De verplichte melding van een schending binnen de 72 uur is van toepassing op de volledige toeleveringsketen (d.w.z. vanaf het ogenblik dat een (sub)verwerker op de hoogte is van de schending)

Feit: De GDPR stelt dat gegevensverwerkers hun gegevensverantwoordelijken "zonder onnodige vertraging" op de hoogte moeten brengen in het geval van een schending van persoonsgegevens. Het is pas op het ogenblik dat de gegevensverwerker de gegevensverantwoordelijke op de hoogte heeft gebracht dat de 72-uur durende meldingstermijn voor de gegevensverantwoordelijke ingaat. De Artikel 29-werkgroep (WP29), een groep Europese instanties voor gegevensbescherming, heeft in haar laatste richtlijnen[9] uitgelegd dat deze "zonder onnodige vertraging" een "snelle" melding betekent (niet "onmiddellijke" melding zoals in een vorige versie werd voorgesteld).

Mythe 3: Gegevensoverdrachten buiten de EU/EER zijn niet toegelaten of enkel met de toestemming van de klant voor elke gegevensoverdracht

Feit: De GDPR behoudt in grote lijnen de bestaande vereisten inzake gegevensoverdracht. Bijgevolg zijn gegevensoverdrachten toegelaten als een door de EU goedgekeurd mechanisme voor gegevensoverdracht zoals het EU-VS Privacyschild of door de EU goedgekeurd modelclausules (gegevensoverdrachtovereenkomsten) gebruikt worden. Blackboard heeft deze beide mechanismen ingevoerd om op een correcte manier persoonlijke informatie van klanten over te dragen.[10] Aangezien Blackboard optreedt als een gegevensverwerker, is een algemene instructie door gegevensoverdrachten van de klant vereist (die is opgenomen in onze standaard gegevensverwerkingsovereenkomst), maar toestemming van de klant voor elke gegevensoverdracht is niet noodzakelijk.

Mythe 4: Het recht op verwijdering van gegevens betekent dat organisaties alle gegevens van een individu moeten verwijderen

Feit: Het nieuwe recht op verwijdering van gegevens is geen absoluut "recht om te worden vergeten". Het is eerder een recht om gegevens te laten wissen, als de gegevens niet langer noodzakelijk zijn en in andere omstandigheden waar de organisatie niet voldoet aan de GDPR-vereisten. Als het voor een organisatie nog steeds wettelijk noodzakelijk is om de gegevens te bewaren (bijvoorbeeld omwille van vereisten voor het bewaren van dossiers), dan moet deze persoonlijke informatie niet worden verwijderd.

Mythe 5: De GDPR is van toepassing op alle universiteiten met Europese studenten

Feit: Louter studenten uit de EU ingeschreven hebben is niet voldoende opdat de GDPR van toepassing zou zijn. De GDPR geldt in het algemeen voor instellingen die in de EU zijn gevestigd. Ze is ook van toepassing op universiteiten buiten de EU, maar enkel als ze goederen en diensten aanbieden aan individuen in de EU of het gedrag van individuen in de EU monitoren. "Diensten aanbieden" veronderstelt een bepaalde graad van targeting. Het loutere feit dat er Europese studenten ingeschreven zijn, is niet voldoende. De GDPR kan echter van toepassing zijn wanneer universiteiten zich actief richten tot inwoners van de EU (bijv. voor online cursussen) of actief studenten rekruteren in Europese landen. Deze criteria zijn onderhevig aan interpretatie. We raden klanten aan hun eigen juridisch advies in te winnen.

IMPLEMENTATIE VAN DE GDPR

Waarom het belangrijk is het recht op gegevensprivacy en de GDPR goed te begrijpen

Het risico van een boete ter waarde van 4% van de jaarlijkse omzet is zeker een reden waarom organisaties gegevensprivacy nu ernstiger nemen. Maar we denken dat het pleidooi voor goede praktijken inzake gegevensprivacy ten minste even noodzakelijk is omdat gegevensprivacy een mensenrecht is en het hebben van robuuste praktijken inzake gegevensprivacy vertrouwen creëert.

In de huidige maatschappij is persoonlijke informatie overal aanwezig. Persoonlijke informatie wordt vaak de nieuwe olie van de economie genoemd. We maken allemaal gebruik van online diensten en overhandigen onze persoonlijke informatie. Alle studies tonen echter aan dat we organisaties niet vertrouwen als het over persoonlijke informatie gaat. Individuen hebben het gevoel dat ze de controle over hun gegevens verloren hebben. Wetgevers en regelgevende instanties reageren hierop. De GDPR is waarschijnlijk het meest opmerkelijke voorbeeld. Organisaties moeten het vertrouwen van individuen (her)winnen. Goede praktijken inzake gegevensprivacy zijn belangrijk om deze vertrouwensband op te bouwen. Ze zijn ook een competitief voordeel. Tot slot helpen ze organisaties ook met innovatie. Als studenten (en personeel) een instelling vertrouwen, is de kans groter dat ze hun informatie delen en nieuwe tools gebruiken.

Een gebrek aan inzicht in gegevensprivacy kan catastrofaal zijn. Gegevensschendingen komen regelmatig in het nieuws. Het gevolg is reputatieschade, verlies van vertrouwen van individuen en het risico op claims van diegene van wie de gegevens verkeerd beheerd zijn. De autoriteiten inzake gegevensbescherming zullen de boetes van 4% van de jaarlijkse omzet misschien niet vanaf het begin opleggen, maar ze hebben veel andere middelen ter beschikking en kunnen instellingen verplichten hun gegevenspraktijken te veranderen en gegevensprivacyprogramma's te implementeren met regelmatige externe audits.

De rol van onze en uw organisatie krachtens de GDPR

De GDPR behoudt het concept van "gegevensverantwoordelijke" en "gegevensverwerker". Dit concept is cruciaal aangezien het de verantwoordelijkheden en verplichtingen van organisaties en hun dienstverleners bepaalt.

Een organisatie wordt beschouwd als een gegevensverantwoordelijke als het de "middelen en doelen" van de verwerking van persoonlijke informatie bepaalt, d.w.z. waarom en hoe persoonlijke informatie wordt gebruikt. De gegevensverwerker anderzijds is de organisatie die optreedt in naam van de gegevensverantwoordelijke en op diens instructie.

Voor de meeste producten en diensten van Blackboard (bijv. Learn, Collaborate, Open LMS wordt Blackboard beschouwd als een gegevensverwerker en onze klanten als de gegevensverantwoordelijke.

De GDPR legt meer rechtstreekse vereisten op aan gegevensverwerkers zoals Blackboard. Het merendeel van de GDPR-vereisten zijn echter nog steeds van toepassing op gegevensverantwoordelijken (bijv. de verantwoordelijkheid om de individuen te informeren over hoe hun gegevens worden gebruikt, om te voldoen aan de verzoeken van individuen voor toegang tot hun gegevens, verplichte melding van schendingen aan instanties voor gegevensbescherming en individuen.)

Wat kunt u doen om u voor te bereiden op de GDPR?

Alle organisaties die vallen onder de GDPR zullen klaar moeten zijn tegen 25 mei 2018. Hieronder vindt u enkele belangrijke zaken die klanten kunnen doen om zich voor te bereiden. De lijst van stappen is gebaseerd op onze eigen ervaring en is in geen geval bedoeld om volledig te zijn. Laat u zeker bijstaan door experts inzake gegevensprivacy om u te helpen bij uw implementatie. Veel instanties voor gegevensbescherming hebben ook hun eigen gids gemaakt over hoe de GDPR moet worden geïmplementeerd.[11]

Hopelijk hebt u stappen 1-6 al uitgevoerd en bent u nu bezig met de implementatie van uw actieplannen. Het is echter nooit te laat om te starten. En zelfs als u nog maar net gestart bent, kunt u de belangrijkste veranderingen al implementeren. Het betekent ook dat u aan uw instantie voor gegevensbescherming zult kunnen aantonen dat u momenteel aan een plan werkt. De GDPR negeren is geen optie.

1. **Controleer of de GDPR van toepassing is op uw organisatie**
   Als uw organisatie in de EU gevestigd is, dan is de GDPR van toepassing. De GDPR kan echter ook van toepassing zijn op organisaties buiten de EU.[12]

2. **Start een GDPR-project**
   Ontwerp en implementeer een speciaal GDPR-project. Idealiter hebt u ondersteuning van het projectmanagement en contactpersonen die u in elke afdeling kunnen ondersteunen. Dit project strekt zich uit over alle afdelingen van uw instelling en u zult daarbij hulp kunnen gebruiken.

3. **Stel een ervaren GDPR-verantwoordelijke aan om het project te leiden**
   De verantwoordelijke moet niet enkel ervaring in gegevensprivacy hebben, maar ook voldoende tijd en middelen evenals toegang tot externe ondersteuning (bijv. advocatenkantoor). Als uw organisatie een openbare instelling gevestigd in de EU is, zult u een Data Protection Officer (functionaris voor gegevensbescherming) moet aanstellen.

4. **Zorg voor betrokkenheid en toezicht van het senior management**
   Een GDPR-project implementeren zonder steun, leiding en toezicht van het senior management is moeilijk.

5. **Herzie uw gebruik van persoonlijke informatie en voer een verschillenanalyse uit**
   Begrijpen waar en hoe persoonlijke informatie wordt gebruikt en waar verbeteringen van de GDPR vereist zijn, is de eerste belangrijke fase van het GDPR-project.

6. **Ontwikkel actieplannen om de verschillen weg te werken**
   Dit is waarschijnlijk het moeilijkste deel van GDPR aangezien de vaak hoge vereisten van de GDPR hierbij moeten worden vertaald naar specifieke en uitvoerbare acties voor alle verschillende processen en systemen.

7. **Implementeer actieplannen**
   Vertrouwen is goed, maar controle is in dit geval beter. Deze fase vereist opvolging van de actieplannen van anderen om ervoor te zorgen dat ze hun deadlines halen.

8. **Controleer uw verkopers**
   Krachtens de GDPR bent u verantwoordelijk voor uw verkopers. Het is belangrijk over de juiste contractuele bepalingen te beschikken, maar dat is niet voldoende. U moet zeker zijn dat uw verkopers de GDPR-vereisten ook respecteren en u kunnen ondersteunen door hun naleving ervan. Vraag na hoe ze de GDPR implementeren.

9. **Blijf op de hoogte van wettelijke / regelgevende ontwikkelingen (Art. 29 Werkgroep Richtlijnen, Lidstaten die wetten implementeren)**
   De GDPR kennen is toch voldoende? Niet dus! Hoewel de GDPR rechtstreeks van toepassing is, implementeren alle Europese lidstaten aanvullende nationale wetten inzake gegevensbescherming. Deze zijn noodzakelijk om gebieden te regelen waar lidstaten wetgevende macht hebben (bijv. gegevensprivacy van werknemers) of waar de GDPR hen toelaat verder wetten uit te vaardigen (bijv. criteria voor DPO's – Data Protection Officers - en DPIA's – Data Protecion Impact Assessments). Daarnaast publiceert WP29 belangrijk advies. Up-to-date blijven is dus een belangrijke uitdaging.[13]

PLAN EN BENADERING VAN BLACKBOARD

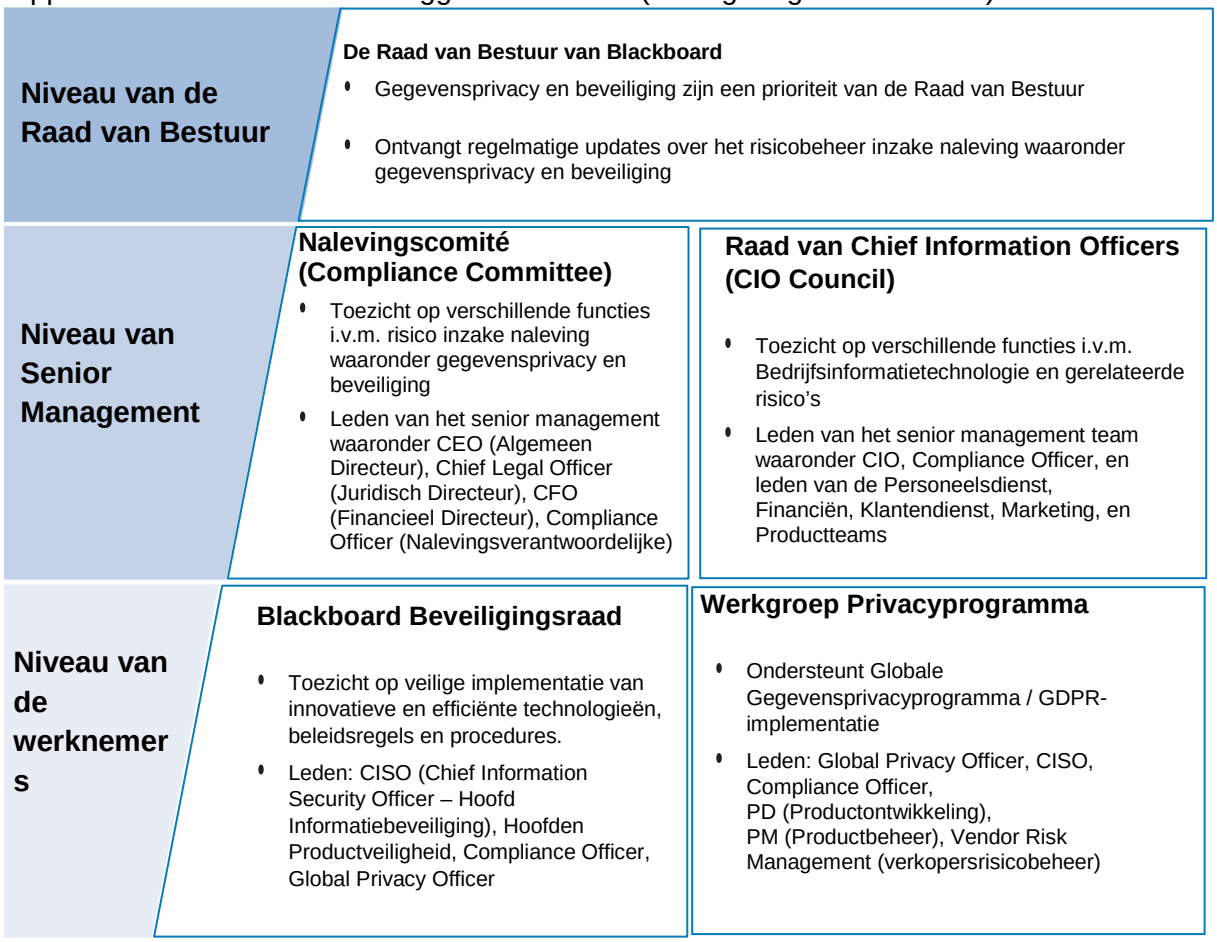
Gegevensprivacy en beveiliging bij Blackboard

Gegevensprivacy en beveiliging zijn reeds lang een belangrijke prioriteit van Blackboard. Voor ons is de GDPR een opportuniteit om onze bestaande privacypraktijken te versterken.

Onze aanpak van gegevensprivacy is altijd klantgericht geweest. We begrijpen de uitdagingen waarvoor onze klanten staan en we willen hen daarbij helpen.

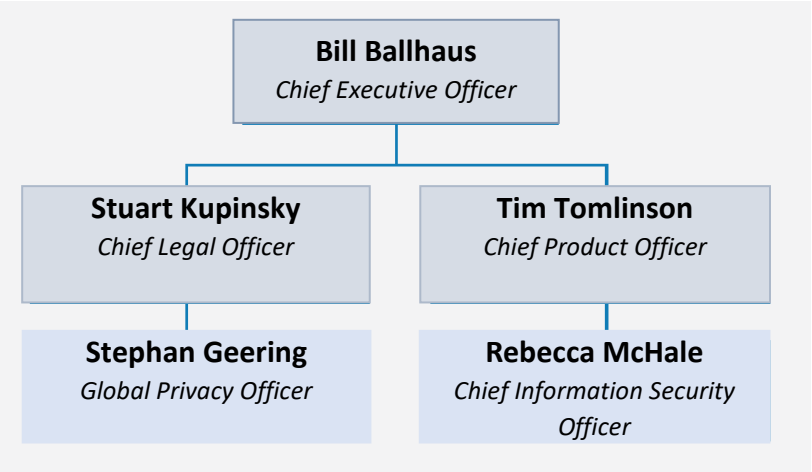
Goede praktijken inzake gegevensprivacy vereisen een goed onderbouwd bestuursmodel. Bij Blackboard zijn gegevensprivacy en beveiliging een prioriteit van de Raad van Bestuur en ons bestuursmodel (zie hieronder) garandeert dat het senior management toezicht houdt over en ondersteuning biedt aan onze inspanningen inzake gegevensprivacy en beveiliging.

Het belang dat Blackboard hecht aan gegevensprivacy en beveiliging wordt ook onderstreept door het feit dat onze Global Privacy Officer en Chief Information Security Officer[14] rapporteren aan het CEO Leidinggevende Team (zie organogram hieronder).



Privacy en beveiliging

Het belang dat Blackboard hecht aan gegevensprivacy en beveiliging wordt ook onderstreept door het feit dat onze Global Privacy Officer en Chief Information Security Officer rapporteren aan het CEO Leidinggevende Team.



De GDPR-aanpak van Blackboard

We hebben een uitgebreid project opgestart om aan de vereisten van de GDPR te voldoen met behulp van de volgende aanpak:

- De GDPR-implementatie bouwt verder op de bestaande ervaring inzake gegevensprivacy en nalevingsmechanismen van Blackboard
- De GDPR-implementatie wordt geleid door de Global Privacy Officer en ondersteund door een speciale project manager en “GDPR-verantwoordelijke” in elk functioneel gebied
- Het bekende advocatenkantoor Bristows LLP is, onder andere, aangesteld om de GDPR-implementatie te ondersteunen
- De GDPR-implementatie wordt gecontroleerd door het Compliance Committee van Blackboard, waarvan de CEO, Chief Legal Officer, en andere leidinggevenden van het bedrijf lid zijn

GDPR als een opportuniteit

We zien de GDPR-implementatie niet louter als een inspanning om te voldoen aan de nieuwe Europese vereisten inzake gegevensprivacy, maar als een opportuniteit. Bijgevolg streven we ernaar de GDPR-implementatie te gebruiken om het volgende te bereiken:

- Globale gegevensprivacypraktijken versterken – we zullen het GDPR-project gebruiken om ons globaal gegevensprivacyprogramma in de EU en daarbuiten te versterken
- Privacy-door-ontwerpprocessen ontwikkelen die de naleving van gegevensprivacy verder integreren in onze dagelijkse processen
- Onze klanten ondersteunen in hun inspanningen om te voldoen aan de GDPR
- Blackboard positioneren als erkende leider inzake gegevensprivacy in Onderwijstechnologie

Ons implementatieplan

We volgende de gevestigde methodologie in 3 fases van Bristow LLP om ons Globaal Gegevensprivacy-/GDPR-programma te implementeren. Deze methodologie wordt gebruikt voor veel andere bedrijven, waaronder toonaangevende technologiebedrijven. De drie belangrijkste fases zijn als volgt:

- **FASE 1 – Informatie verzamelen**
- **FASE 2 – Ontwikkeling van oplossingen**
- **FASE 3 – Implementatie van werkstromen**

We hebben deze methodologie in 3 fases gebruikt om ons programma met de volgende vier belangrijke fases te ontwikkelen:

Start van het project

De beginfase van het project omvatte de volgende activiteiten:

- Briefing en betrokkenheid van het senior management
- Aanwerving van een Global Privacy Officer met de verantwoordelijkheid om het GDPR-project te leiden
- Ontwikkeling van projectplan en projectleiding
- Initiële verzameling van informatie en beoordeling van de huidige nalevingsactiviteiten voor gebieden die verbetering vereisen krachtens de GDPR

FASE 1 – Verzameling van informatie (Workshops)

Tijdens deze beginfase hebben we gestructureerde gesprekken/workshops gevoerd met de voornaamste belanghebbenden uit functionele gebieden en productgroepen van Blackboard om gedetailleerde informatie te krijgen over de praktijken inzake gegevensbescherming binnen deze gebieden.

Het resultaat van de workshops werd gebruikt om de verschillenanalyse uit te voeren en de oplossingen en implementatieplannen in fase 2 te ontwikkelen.

FASE 2 – Ontwikkeling van oplossingen

Op basis van de informatie van de workshops hebben we de volgende oplossingen en documentatie ontwikkeld:

- Verbeterde interne documentatie inzake gegevensbescherming (beleid en gedetailleerde werkingsstandaarden) die de GDPR-vereisten weerspiegelen en uitleggen hoe aan de GDPR-vereisten zal moeten worden voldaan voor de verschillende gegevensverwerkings-activiteiten (bijv. vereisten voor verwerking van klantengegevens, privacy-door-ontwerp-proces)

- Productvereisten

- Implementatieplannen voor de functionele gebieden en voor centraal vereiste inspanningen

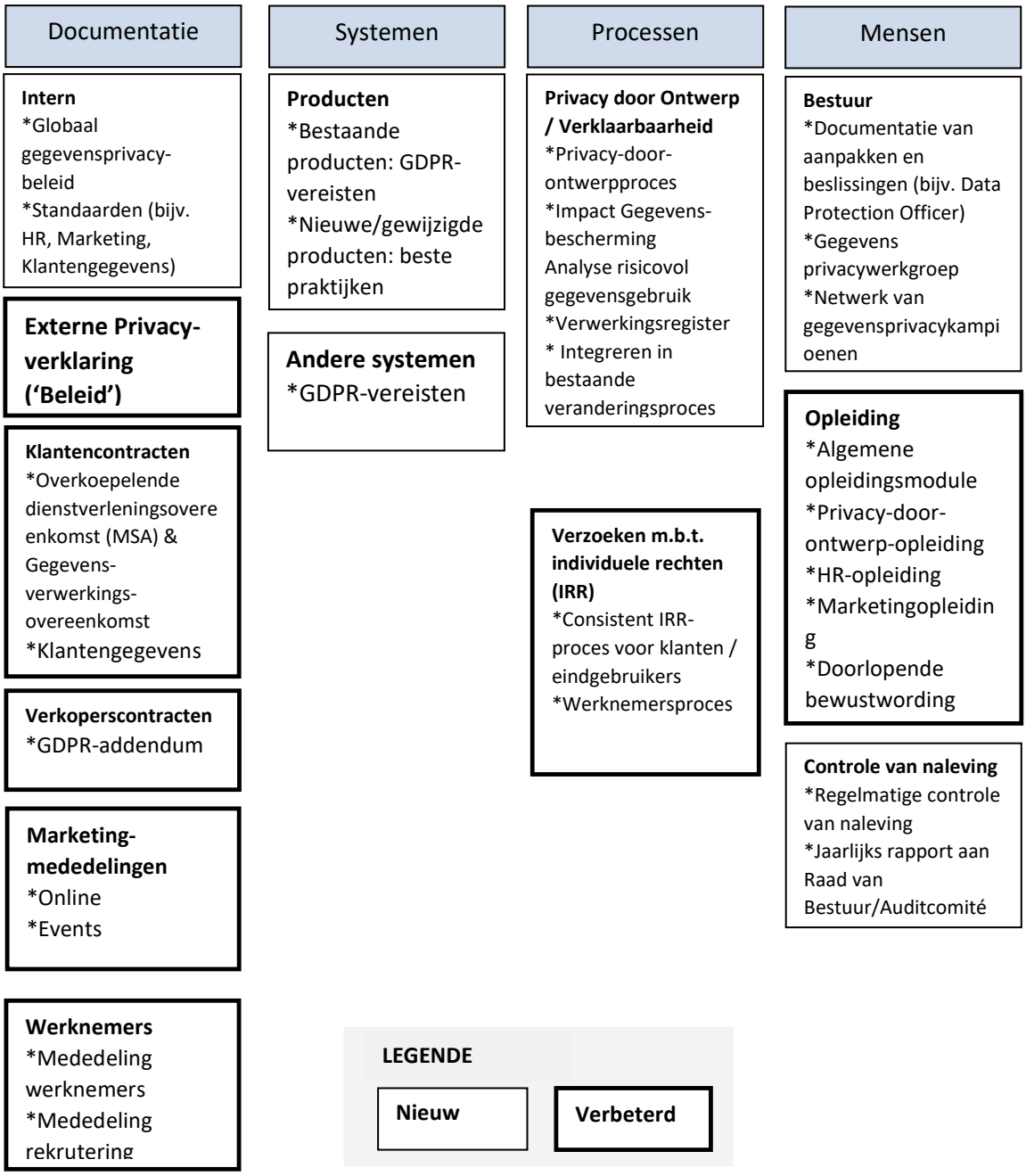
FASE 3 – Implementatie van werkstromen

Tijdens de laatste fase implementeren we de ontwikkelde documentatie inzake gegevensprivacy en voeren de we implementatieplannen uit. Er zullen zes hoofdwerkstromen worden gebruikt om de implementatie uit te voeren:

1. De implementatieplannen voor de functionele gebieden en productgroepen uitvoeren
2. Beleidsregels, mededelingen en toestemmingen voor het publiek controleren en bijwerken
3. Bestuur (rollen & verantwoordelijkheden, opleiding, privacy door ontwerp, enz.) verbeteren
4. Verkoperscontracten herzien en bijwerken (indien nodig)[15]
5. Veranderingen aan IT-systemen (indien nodig)
6. Gegevensverwerkingsregister opstellen

Overzicht van de veranderingen

Het onderstaande schema toont de eindstatus van ons GDPR-/gegevensprivacyprogramma die we voor ogen hebben na de implementatieactiviteiten. Na de GDPR-implementatie zullen we verder innoveren en ons aanpassen om onze gegevensprivacypraktijken verder uit te werken.



HOE ZAL ONS GDPR-PROGRAMMA U HELPEN?

Blackboard's Globaal Gegevensprivacy-/GDPR-implementatieprogramma is gericht op de ondersteuning van uw organisatie met uw implementatie van de GDPR. De volgende segmenten geven meer details, maar samengevat vindt u hieronder de 7 belangrijkste punten:

1. **GDPR-conforme producten:** We implementeren productvereisten om klanten te ondersteunen met transparantievereisten, verzoeken m.b.t. individuele rechten, enz.

2. **Privacy door ontwerp:** We implementeren privacy door ontwerp een proces van Data Protection Impact Assessment (DPIA, Beoordeling van de impact van gegevensbescherming) om de documentatie van de naleving te vergemakkelijken

3. **Gegevensoverdrachten:** We gaan verder met onze meerlagige aanpak: Regionalisering, EU-VS Privacyschild en door de EU goedgekeurde modelclausules

4. **Contract met klanten:** We hebben een GDPR-conform gegevensverwerkings-addendum bij onze standaard hoofdovereenkomst

5. **Onze verkopers:** We hebben robuuste contracten en een kader voor risicobeheer van verkopers ingevoerd

6. **Beveiliging:** We hebben een beleid, procedures en bestuur ingevoerd die constant worden verbeterd om de beveiliging van klantengegevens te garanderen

7. **Melding van schendingen:** We hebben een gedocumenteerd en getest proces om te reageren op beveiligingsincidenten

1. GDPR-conforme producten

Onze klanten ondersteunen door onze producten GDPR-conform te maken is één van de belangrijke aspecten van onze implementatiewerkstromen. Daartoe hebben we minimale GDPR-/gegevensprivacyvereisten voor onze producten ontworpen. In lijn met onze aanpak om onze praktijken inzake gegevensprivacy wereldwijd te versterken, zijn de meeste van deze vereisten van toepassing op al onze producten, niet enkel de producten die wij in de EU op de markt brengen. Dit ondersteunt ook onze klanten buiten de EU die onder de GDPR zouden kunnen vallen.

We hebben onze GDPR-/gegevensprivacyproductvereisten ontwikkeld door middel van een robuust en intensief proces. We hebben een initiële versie opgesteld met externe adviseurs. Tijdens verschillende werksessies en herzieningen met belangrijke betrokkenen uit onze productontwikkeling- en productmanagementteams hebben we de versie verfijnd tot specifieke en werkbare algemene productvereisten met gedetailleerd advies. De GDPR-/gegevensprivacyproductvereisten werden vervolgens vertaald in productspecifieke acties in de productimplementatieplannen voor elke productgroep.

Onze productvereisten[16] kunnen als volgt ingedeeld worden:

Transparantie

- Het vermogen voor klanten om een verband te leggen met hun privacybeleid/mededelingen
- Informatie geven over hoe persoonlijke informatie in het algemeen in een product wordt gebruikt

Minimaliseren/wissen van gegevens

- Controle van producten voor niet-noodzakelijke/optionele velden
- Controle van producten voor opportuniteiten om pseudonieme of anonieme gegevens te gebruiken in plaats van persoonlijke gegevens
- Vermogen om persoonlijke informatie te wissen wanneer dit wordt gevraagd door klanten (wanneer klanten/gebruikers zelf geen gegevens kunnen wissen)

Algemene individuele rechten

- Vermogen om toegang te bieden tot persoonlijke gegevens en deze te corrigeren wanneer dit wordt gevraagd door het individu
- Vermogen om persoonlijke informatie te wissen wanneer dit wordt gevraagd door het individu

EU individuele rechten

- Vermogen om verzoeken voor overdraagbaarheid van gegevens te verwerken (recht van individuen om gegevens te ontvangen in een door een machine leesbaar formaat in bepaalde omstandigheden)
- Vermogen om het gebruik van persoonlijke informatie stop te zetten (recht om bezwaar aan te tekenen/recht op beperking in bepaalde omstandigheden)

Blackboard heeft reeds gedefinieerde programma's voor onze productbeveiliging die rekening houden met GDPR. Daarom hebben we geen aanvullende GDPR-specifieke beveiligingsvereisten gedefinieerd.[17]

2. Privacy door ontwerp

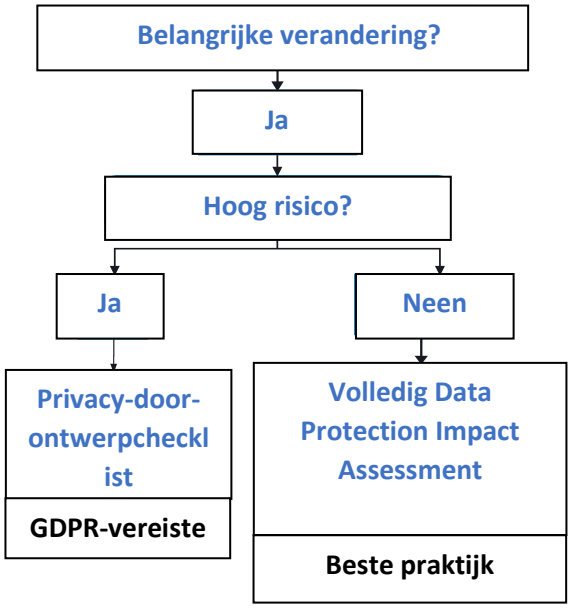
Aangezien het vandaag de dag een steeds grotere uitdaging wordt voor individuen om de controle over hun informatie te behouden (zie onze dagelijkse blogpost over privacy i.v.m. dit onderwerp), worden privacy door ontwerp en verklaarbaarheid steeds belangrijker om het vertrouwen van individuen, klanten en regelgevende instanties te behouden en te documenteren hoe een organisatie voldoet aan de GDPR. We hebben onze privacy-door-ontwerpaanpak daarom centraal geplaatst in ons Globaal-Gegevensprivacy-/GDPR-programma.

Voor Blackboard is dit eerder een evolutie dan een revolutie. We hebben altijd wettelijke controles van nieuwe producten en praktijken uitgevoerd. Met onze aanpak van privacy door ontwerp formaliseren en documenteren we deze analyses beter.

Aanpak

- We hebben een gedocumenteerd privacy-door-ontwerpproces en controlelijst opgesteld.
- Functionele gebieden en productgroepen nemen de privacy-door-ontwerpcontrolelijst op in hun veranderingsprocessen.
- Bij elke belangrijke verandering in hoe persoonlijke informatie wordt gebruikt, moet een privacy-door-ontwerpcontrolelijst worden ingevuld. Hoewel dit niet specifiek vereist wordt door de GDPR, is dit de beste praktijk.
- De controlelijst zal leiden tot de meer gedetailleerd Data Protection Impact Assessment (DPIA) voor risicovol gebruik van persoonlijke informatie (GDPR-vereiste)

Het onderstaande schema visualiseert de aanpak:



3. Gegevensoverdrachten

De GDPR brengt geen significante veranderingen met zich mee over hoe persoonlijke informatie kan worden overgedragen buiten de EU/EER. De huidige beperkingen en gegevens-overdrachtsmechanismen blijven dezelfde. Dit betekent dat gegevensoverdracht toegelaten is als een door de EU goedgekeurd gegevens-overdrachtsmechanisme zoals het EU-VS Privacyschild of door de EU goedgekeurde modelclausules (overeenkomsten inzake gegevensoverdracht) gebruikt worden. Deze mechanismen zorgen ervoor dat persoonlijke informatie op geschikte wijze beschermd wordt zelfs als ze de EU/EER verlaat.

We zullen onze meerlagige en overvloedige aanpak inzake naleving van gegevensoverdracht verderzetten. Dit betekent dat we de vereisten inzake gegevensoverdracht via verschillende kanalen respecteren om ervoor te zorgen dat uw informatie goed beschermd wordt:

● **Regionale hosting:** We hebben een regionale hostingstrategie met bijna alle producten die in de EU wordt gehost en andere producten die naar regionale hostingoplossingen zullen worden verplaatst. Hoewel regionale opslag niet vereist is door de GDPR en we niet denken dat gegevenslokalisatie leidt tot betere ondersteuning. Dergelijke gegevensoverdrachten zijn toegelaten dankzij de genoemde EU-VS Privacyschild-certificering en modelclausules.

gegevensprivacy of -beveiliging,[18] begrijpen we dat veel EU-klanten er de voorkeur aan geven dat hun gegevens in de EU bewaard worden.

● **Privacyschild:** Blackboard is gecertificeerd voor het EU-VS Privacyschild dat ons toelaat op een wettelijke manier gegevens over te dragen naar de VS.

● **Modelclausules:** We gebruiken ook door de EU goedgekeurde overeenkomsten met “modelclausules” die ons toelaten op correcte wijze persoonsgegevens buiten de EER over te dragen binnen de bedrijvengroep van Blackboard (“Customer Data Transfer Agreement”).

● **Verkopers:** Er zijn robuuste contracten ingevoerd met verkopers en partners (bijv. IBM, Amazon Web Services) om ervoor te zorgen dat vereisten inzake gegevensoverdracht (en andere verplichtingen inzake gegevensbescherming) worden doorgegeven aan onze verkopers en partners.

We hebben momenteel[19] verschillende regionale gegevenscentra om de verwerking van gegevens in de EU voor onze EU-klanten te ondersteunen:

- Managed hosting (gegevenscentra van Blackboard): gegevenscentra in Amsterdam (Nederland) en Frankfurt (Duitsland).
- Cloud hosting (AWS-gegevenscentrum): AWS-gebied Frankfurt, Duitsland (eu-central-1).

AWS-gegevenscentra voldoen aan een heleboel certificeringen en vereisten van ISO 27001 en ISO 27018, tot SOC2 en naleving van GDPR evenals naleving van lokale vereisten zoals het Duitse G5 en IT-Grundschutz.[20]

Het is belangrijk te begrijpen dat hoewel persoonlijke informatie van klanten wordt opgeslagen in deze gegevenscentra voor de meeste van de producten (waaronder Learn 9.1, Learn SaaS, Open LMS en Collaborate) voor EU-klanten, toegang tot deze gegevens van buiten de EU/EER vereist kan zijn om de producten en diensten te bieden, bijv. voor 24/7 even welke instructie van gegevensverantwoordelijken ingaat tegen de GDPR

4. Contracten met klanten

De huidige Richtlijn vereist dat een gegevensverantwoordelijke een contact heeft met de verkoper (gegevensverwerker), maar bepaalt de inhoud van het contract niet in detail. De GDPR is eerder normatief en omvat een lijst van vereiste inhoud.[21]

Ons huidige gegevensverwerkings-addendum omvat alle vereiste punten hieronder. Dit wordt automatisch opgenomen voor klanten die onder onze standaard hoofdovereenkomst en onder de GDPR vallen.

- ✓ Gebruik persoonlijke gegevens enkel zoals aangegeven
- ✓ Personeel moet vertrouwelijkheids-overeenkomsten ondertekenen
- ✓ Er moeten geschikte beveiligingsmaatregelen worden ingevoerd
- ✓ Werf enkel verkopers (subverwerkers) aan …
  - met de goedkeuring van de gegevensverantwoordelijke (dit kan een algemene toestemming zijn)
  - die contractueel dezelfde verplichtingen inzake gegevensbescherming moeten volgen
- ✓ Help de gegevensverantwoordelijke met het beantwoorden van verzoeken m.b.t. individuele rechten
- ✓ Help de gegevensverantwoordelijke met beveiligingsmaatregelen, meldingen van schendingen en beoordelingen van de gegevensbeschermingsimpact
- ✓ Stuur gegevens terug of wis ze aan het einde van het contract
- ✓ Geef informatie die noodzakelijk is voor de gegevensverantwoordelijke om naleving aan te tonen
- ✓ Breng de gegevensverantwoordelijke onmiddellijk op de hoogte indien om het

5. Onze verkopers beheren

Blackboard gebruikt verkopers (bijv. IBM, Amazon Web Services) om ons te helpen onze producten en diensten aan onze klanten aan te bieden. Wanneer dit toegang vereist tot de persoonlijke informatie van onze klanten, is Blackboard verantwoordelijk voor de gegevensprivacypraktijken van de verkopers.

Als deel van ons GDPR-programma verbinden we de privacy-door-ontwerpaanpak nauw met de bestaande Verkopersrisicobeheer- en aankoopprocessen. Dit resulteert in de volgende belangrijke controles:

- Robuuste contracten met een Privacy- en GDPR-addendum afgesloten met derden dat belangrijke equivalente bepalingen oplegt die we overeengekomen zijn met onze klanten
- Overeenkomsten met “modelclausules” en/of GDPR- en Privacyschildaddendum om wettelijke gegevensoverdrachten naar onze verkopers toe te laten
- Gedocumenteerd Verkopersrisico-beheerbeleid en -kader
- Nieuwe verkopers met toegang tot persoonlijke informatie moeten een Vragenlijst ter Beoordeling van de Beveiliging van de Verkoper invullen met vragen over de nalevering van gegevensprivacy
- Verkopers met toegang tot door Blackboard beheerde systemen moeten interne toegangscontrole en identiteits- en toestemmingsregels volgen, om accountcontroles op geschikte wijze op te nemen
- Verkopers hebben toegang nodig tot Blackboardhulpmiddelen via goedgekeurde mechanismen (bijv. VPN)
- Verkopers hebben beperkte toegangscontroles op verkeer, gebruikers en activa

6. Beveiliging

De GDPR verandert de technische en operationele maatregelen (“TOM’s”) voor de beveiliging van persoonlijke informatie niet aanzienlijk. Dergelijke maatregelen moeten “aangepast” zijn aan het risico dat wordt gelopen krachtens de huidige Richtlijn. Daarom vertrouwen we verder op onze gevestigde informatiebeveiligingsprogramma’s.

Informatiebeveiligingsrisico beheren

We hebben gevestigde beleidsregels, procedures, leiding en technische vereisten om het IT-beveiligingsrisico binnen het bedrijf onder controle te houden.

Vanaf dag één moet het personeel van Blackboard zijn verantwoordelijkheid kennen om de persoonlijke gegevens van klanten te beschermen:

- Kennis van het beleid voor de bescherming van gevoelige informatie
- Jaarlijkse opleiding over gebruikersbeveiliging en gegevensprivacy
- Phishingoefeningen
- Bewustwordingsbulletins

De volgende vereisten zijn ingevoerd voor de beveiliging van gegevens door ons personeel:

- Gegevensclassificaties worden gedefinieerd met vereisten om elk gegevenstype te beschermen. Onze klantengegevens zijn erg gevoelig – de gegevens van de instellingen en hun leerlingen.
- Technische controles zijn ingevoerd om gegevens te beschermen, bijv.
  - gebruik van codering
  - snelle beveiligingsupdates
  - verbeterde authenticatiecontroles
  - bescherming tegen schadelijke e-mails en webverkeer
  - technologieën voor beveiliging van eindpunten
  - toegang beperkt tot wat niet meer dan noodzakelijk is

Het is niet enkel de GDPR…

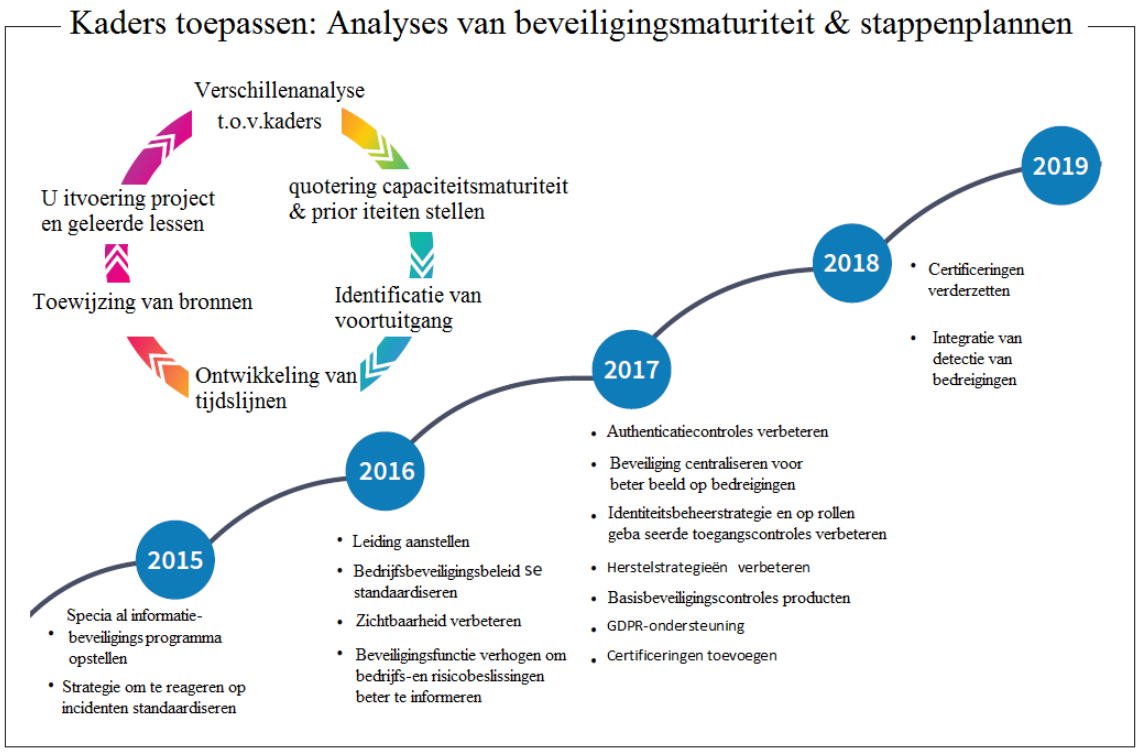
Als een wereldwijd bedrijf, dat actief is in de opleidingswereld, monitoren we nauwkeurig relevante geografische en voor de opleidingssector specifieke gegevensprivacy- en beveiligingswetten en regelgeving.

In de onderstaande lijst vindt u slechts enkele voorbeelden van regels, normen en modellen inzake beveiliging en gegevensprivacy die Blackboard in aanmerking neemt naast GDPR bij de ontwikkeling van ons beveiligingsbeleid, processen en technische controles.

- US Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA)
- US Children’s Online Privacy Protection Act (COPPA)
- Amerikaanse staatswetten (mengeling van bestaande en opkomende wetten in 50 staten)
- Amerikaanse overheidsnormen – FedRAMP
- PCI-gegevensbeveiligingsnormen, waar van toepassing
- ISO/IEC, OWASP, NIST
- Internationale normen (MTCS, IRAP)

Analyses van beveiligingsmaturiteit en stappenplannen

We werken hard om onze technische en operationele beveiligingsmaatregelen continu te verbeteren. Het schema op de volgende pagina illustreert onze continue maturiteitsbeoordelingen en onze stappenplannen.



7. Melding van schendingen

Een van de belangrijke veranderingen van de GDPR is de nieuwe verplichte melding van schendingen van persoonsgegevens aan de bevoegde instantie inzake gegevensbescherming en (in sommige gevallen) de getroffen individuen.[22]

Voor de meeste van onze producten en diensten is Blackboard een gegevensverwerker[23] krachtens de GDPR. De verplichting om gegevensbeschermingsinstanties en individuen op de hoogte te brengen in geval van een schending waarbij Blackboard betrokken is, ligt daarom bij onze klanten. De GDPR vraagt aan gegevensverwerkers als Blackboard echter om hun klanten (gegevensverantwoordelijken) in een dergelijk geval op de hoogte te brengen in geval van overmatige vertraging (d.w.z. “snel”)[24].

We hebben de volgende maatregelen ingevoerd die onze klanten ondersteunen om te voldoen aan hun verplichtingen in geval van een schending van persoonsgegevens bij Blackboard met betrekking tot een klant:

- Blackboard’s Security Incident Response (SIR)-proces
  - Gedocumenteerd en regelmatig getest
  - Vergemakkelijkt de snelle identificatie, onderzoek en oplossing in geval van een incident
  - Laat toe klanten snel op de hoogte te brengen
  - Berust bij het gevestigde security incident response-team (met daarin de Chief Information Security Officer en de Global Privacy Officer)
- Onze verplichting om klanten snel op de hoogte te brengen staat uitdrukkelijk vermeld in onze huidige standaard hoofdovereenkomst en gegevensbeschermingsaddendum[25]

CONCLUSIE

De GDPR vereist significante veranderingen met een impact na de datum van inwerkingtreding op 25 mei 2018. We hopen dat dit witboek zal bijdragen aan uw geslaagde implementatie van de GDPR en heeft aangetoond hoe ernstig Blackboard de GDPR en nalevering van de gegevensprivacy neemt.

In onderstaande segmenten vindt u aanvullende nuttige informatie en een lijst van e-mailadressen van onze contactpersonen als u vragen of feedback hebt over dit document.

NUTTIGE GDPR-BRONNEN

Onderstaande bronnen zijn slechts een kleine selectie van nuttig materiaal dat online beschikbaar is. Het is niet bedoeld om volledig te zijn.

Voor een gedetailleerde analyse over hoe de GDPR van toepassing is op u, wint u best ook advies in van specialisten. Het is belangrijk een beroep te doen op een ervaren deskundige inzake gegevensbescherming (bijv. het advocatenkantoor van uw keuze).

Officiële EU-bronnen

- GDPR-tekst
- Richtlijnen Artikel-29-werkgroep
- GDPR-website van de Europese Commissie

Materiaal van de Europese instantie inzake gegevensbescherming

- Het Britse Information Commissioner's Office (ICO) heeft een uitstekende GDPR-website met nuttig materiaal in eenvoudige taal dat constant bijgewerkt wordt
- De Ierse Data Protection Commissioner (DPC) heeft een speciale GDPR-pagina voor organisaties
- De Franse CNIL biedt materiaal in het Engels waaronder gratis Privacy Impact Assessment-software (en veel meer materiaal in het Frans)
- De Spaanse AEPD heeft een gids voor onderwijsinstellingen gemaakt (PDF, in het Spaans)

Gids van advocatenkantoren

- Bird & Bird's gids voor de GDPR
- Bird & Bird's zoeker voor wetten van lidstaten (zoeken naar nationale GDPR-variaties)
- Linklater's GDPR-overlevingsgids (PDF)
- White & Case GDPR-handboek

Overige organisaties

- JISC UK heeft nuttige bronnen, evenementen en blogupdates over GDPR
- UCISA heeft een GDPR beste-praktijk-document met praktische stappen en gevalsstudies gepubliceerd
- De International Association of Privacy Professionals (IAPP) heeft een goede (gratis) wekelijkse nieuwsbrief over ontwikkelingen binnen de Europese gegevensprivacy
- De IAPP heeft ook een nuttig overzicht van leveranciers van tools voor gegevensprivacy (PDF)
- Amazon Web Services heeft een speciaal GDPR-centrum

BIOGRAFIEËN

Stephan Geering
Global Privacy Officer

- Wereldwijde verantwoordelijkheid voor naleving van gegevensprivacy- en beveiligingswetten
- Leidt het Global Data Privacy/GDPR-implementatieprogramma
- Rapporteert aan de Chief Legal Officer (Juridisch Directeur); lid van het juridisch team van Blackboard
- Gevestigd in Londen

Achtergrond van Stephan

- Jurist/Plaatsvervangend Gegevensbeschermingsverantwoordelijke (Deputy Data Protection Commissioner) bij een Zwitserse kantonnale instantie inzake gegevensbescherming (2002-2008)
- LLM aan University College London (2008-2009)
- Associate Director, Group Privacy bij Barclays (2010-2012)
- EMEA Regionaal verantwoordelijke Gegevensprivacy-activiteiten bij Citigroup (2012-2014)
- EMEA en APAC Directeur Privacy bij Citigroup (2014-2017)
- CIPP/E-gecertificeerd

Rebecca McHale
Chief Information Security Officer

- Leidt de beveiligingsstrategie voor producten en infrastructuur
- Controleert Blackboard's cyberbeveiliging
- Rapporteert aan Chief Product Officer (Productdirecteur)
- Gevestigd in Washington, D.C.

Achtergrond van Rebecca

- Ging aan de slag bij Blackboard in 2016; combineerde onlangs de beveiligingsteams en verhoogde de rol van de beveiligingsorganisatie binnen het bedrijf
- MS *Discrete Mathematics and Computing Applications* aan Royal Holloway, University of London
- Vroeger Senior Director for Cyber Programs bij Novetta en CSRA die de Amerikaanse overheid en commerciële klanten bedient – bijv. Department of State (ministerie van binnenlandse zaken), Transportation Security Administration (TSA), en Federal Deposit Insurance Corporation (FDIC)

MEER INFORMATIE

U vindt meer informatie op onze speciale Gegevensprivacy- en Beveiligingsgemeenschapspagina.

We hebben ook een Nieuwsbrief over Gegevensprivacy. Als u onze nieuwsbrief wilt ontvangen of als u vragen of feedback hebt met betrekking tot dit witboek, neem dan contact op met ons via privacy@blackboard.com.

Bronnen

1 Zie de rubriek “Nuttige GDPR-bronnen” aan het einde voor meer gedetailleerde informatie over de GDPR.

2 We verkiezen de term “persoonlijke informatie” boven “persoonsgegevens”, maar gebruik hem met dezelfde betekenis en hetzelfde bereik als ”persoonsgegevens”.

3 De gegevensverantwoordelijke is de organisatie die de betekenis en het doel van de gegevensverwerking bepaalt (hoe en waarom persoonlijke informatie wordt gebruikt).

4 Zie de rubriek “De rol van onze en uw organisatie krachtens de GDPR”.

5 Zie de rubriek “Opheldering van mythes rond de GDPR ” hieronder voor meer details over gegevensoverdrachten

6 Zie ICO’s “Inleiding tot de Data Protection Bill” voor een nuttig overzicht van het wetsvoorstel.

7 Zie ook UK ICO’s blogposts over GDPR-mythes.

8 Zie ook de WP29 (voorlopige) Richtlijnen over Toestemming ingevolge Regelgeving 2016/679 (WP259) en ICO’s richtlijnen over toestemming.

9 W29 Richtlijnen over melding van schending van persoonlijke gegevens ingevolge Regelgeving 2016/679 (WP250rev.01).

10 Zie ook de rubriek “Gegevensoverdrachten”.

11 Zie bijvoorbeeld UK ICO’s Voorbereiding op de GDPR – 12 stappen om nu te nemen (PDF).

12 Zie ook de rubriek “Opheldering van mythes rond de GDPR”.

13 Zie de rubriek “Nuttige GDPR-bronnen”.

14 Voor meer informatie over de Global Privacy Officer en Chief Information Security Officer, zie de rubriek Biografieën

15 Als deel van het EU-VS Privacyschild-certificeringproject hebben we reeds de noodzakelijke GDPR-contractbepalingen opgenomen in veel van de contracten met onze verkopers (subverwerkers) die toegang hebben tot EU persoonlijke informatie.

16 Let op, niet alle productvereisten zijn van toepassing op alle producten. Sommige producten hebben bijvoorbeeld geen gebruikersinterface die klanten toelaat een link te maken met hun privacybeleid/-vermeldingen.

17 Zie de rubriek “Beveiliging” voor meer informatie.

18 Zodra een netwerk of systeem aangesloten is op het internet, heeft de fysieke plaats van gegevens weinig tot geen impact op beveiligingsbedreigingen. Zie het Amazon Web Services (AWS) witboek “Data Residency AWS Policy Perspective” (in het bijzonder pagina’s 2 en 3) voor overtuigende argumenten tegen gegevenslokalisatie.

19 Vanaf de datum van dit document.

20 Zie de AWS Compliance Programs voor de volledige lijst van certificeringen en wettelijke naleving.

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

22 Art. 33 en 34 van de GDPR.

23 Voor uitleg over de rol van de gegevensverwerker, zie de rubriek “De rol van onze en uw organisatie krachtens de GDPR”.

24 Zie de rubriek “Opheldering van mythes rond de GDPR” hierboven voor meer details over de timing en het proces van de melding van schendingen van persoonlijke informatie.

25 Zie ook de rubriek “Contracten met klanten”.

Blackboard.com