Wie unsere Kunden von der Umsetzung der DSGVO durch Blackboard profitieren

Die EU-Datenschutzgrundverordnung (DSGVO) ist ein Meilenstein, den Blackboard begrüßt. Datenschutz ist uns wichtig und nach unserem Verständnis ein Menschenrecht. Die DSGVO stärkt die Rechte des Einzelnen und wird in der Konsequenz zu besseren Datenschutzpraktiken führen. Dies kommt natürlichen und juristischen Personen zugute, da es das gegenseitige Vertrauen stärkt.

Wir veröffentlichen dieses Dokument, um unseren Kunden einen Überblick über die Veränderungen und die Mythen rund um die DSGVO zu geben, unser Konzept zur Umsetzung zu erklären sowie zu erläutern, wie unsere Bemühungen Ihrer Einrichtung zugutekommt. Wir haben uns dabei auf Informationen konzentriert, von denen wir glauben, dass Sie Ihnen am meisten nützen. Dieses White Paper ist daher keinesfalls ein umfassender Leitfaden zur DSGVO. [1]

Diese Unterlagen wurden nur zu Informationszwecken erstellt und ersetzen keine Rechtsberatung. Zur Umsetzung der DSGVO in Ihrer Einrichtung und damit verbundenen rechtlichen Fragen lassen Sie sich bitte von Ihren internen oder externen Anwälten beraten.

DSGVO bringt wesentliche Veränderungen mit sich, aber wir bei Blackboard können auf unsere bereits existierenden soliden Datenschutzpraktiken bauen (z. B. Zertifizierung nach dem EU-US Privacy Shield). Wir sehen die DSGVO als eine Chance, unsere bestehenden Praktiken weiter zu stärken. Und wir werden auch weiterhin kundenorientiert arbeiten und Sie bei der Einhaltung der Datenschutzbestimmungen unterstützen.

INHALTSVERZEICHNIS

Blackboard ist nach dem Privacy Shield zertifiziert, stolzer Unterzeichner des Student Privacy Pledge und Mitglied des Future of Privacy Forum.

DSGVO – WAS SIE WISSEN MÜSSEN

Die DSGVO ist die neue EU-Datenschutzgesetzgebung, die die derzeitige EU-Datenschutzrichtlinie 96/46 (Richtlinie) und die Ausführungsgesetze in den EU-Mitgliedsstaaten ersetzt (z. B. den UK Data Protection Act von 1998).

Die DSGVO wurde im Mai 2016 erlassen; das Datum des Inkrafttretens ist der 25.
Mai 2018.

In den nachstehenden Abschnitten haben wir eine sehr kurze (und keinesfalls umfassende) Übersicht über die DSGVO-Anforderungen zusammengestellt. Im Abschnitt „Nützliche Quellen zur DSGVO“ finden Sie Links mit ausführlicheren Leitfäden.

Warum ein neues Gesetz?

Gesetzgeber und Regulierungsbehörden in der EU gelangten zu der Überzeugung, dass die Richtlinie aktualisiert werden musste, um der mangelhaften Harmonisierung und den sozialen und technologischen Entwicklungen in den 20 Jahren seit Inkrafttreten der Richtlinie gerecht zu werden. Ganz oben auf der Liste standen mehr Durchsetzungsbefugnisse, größere räumliche Reichweite und erweiterte Rechte für die Betroffenen.

Viele der neuen Bestimmungen (z. B. zur extraterritorialen Wirkung) zielen hauptsächlich auf soziale Medien und Internetunternehmen außerhalb der EU ab. Die EU-Gesetzgeber und Regulierungsbehörden hatten den Eindruck, dass die bestehende Richtlinie die Datenschutzrechte von EU-Bürgern, die soziale Medien und Internetdienste nutzen, nicht ausreichend schützt.

Blackboard arbeitet anders als diese sozialen Medien und anderen Internetunternehmen, deren Konzept darauf basiert Nutzerdaten „zu Geld zu machen“. Wir erfassen und nutzen die personenbezogenen Informationen[2] unserer Kunden auf deren Anweisung hin, um ihnen unsere Produkte und Dienstleistungen zur Verfügung stellen zu können. Wir erfassen oder nutzen personenbezogene Informationen nicht, um sie zu verkaufen oder um Werbung zu verkaufen. Wir wissen, dass uns personenbezogene Informationen anvertraut werden und daraus gewisse Verpflichtungen entstehen. Daher haben wir mit unseren Kunden ein gemeinsames Interesse und eine gemeinsame Verantwortung, diese Daten zu schützen.

Was ist neu?

S'il repose sur les principes et concepts de Wenngleich die DSGVO auf den bereits existierenden EU-Datenschutzgrundsätzen und -konzepten beruht, bringt sie doch erhebliche Veränderungen am Datenschutzsystem der EU mit sich, u. a.:

- Erweiterte Befugnis bei der Festsetzung von Bußgeldern (bis zu 4 % des Gesamtumsatzes oder EUR 20 Mio., wobei der jeweils höhere Betrag maßgeblich ist).
- Erweiterter räumlicher Anwendungsbereich unter Einbeziehung von für Organisationen außerhalb der EU, die EU-Ansässigen Produkte und Dienstleistungen zur Verfügung stellen oder EU-Ansässige überprüfen
- Verpflichtung der Datenverantwortlichen zur Meldung von Datenschutzverstößen an Aufsichtsbehörden[3] innerhalb von 72 Stunden
- Strengere Anforderungen in Bezug auf die Einwilligung
- Erweiterte Rechte der Betroffenen (u. a. das Recht auf Löschung und Datenübertragbarkeit)

Toutefois, Aber zu den wichtigsten Änderungen gehören die neuen Grundsätze der Verantwortlichkeit und Datenschutz durch Technikgestaltung. Diese Grundsätze erfordern effektive Datenschutzkontrollen und verfahren sowie genauere und aussagefähigere Dokumentation dessen, wie Organisationen bzw. Unternehmen die DSGVO-Anforderungen erfüllen.

Was bleibt gleich?

Viele der Begriffe und Definitionen aus der DSGVO bleiben gleich oder sind denen der Richtlinie ähnlich:

- La Die Definition von „personenbezogene Daten“ (oder personenbezogene Informationen) bleibt weitestgehend gleich, schließt jetzt aber ausdrücklich IP- Adressen, Cookies und Gerätekennungen mit ein
- Die Begriffe „Datenverantwortlicher“ und „Datenverarbeiter“ bleiben gleich (die DSGVO erlegt den Datenverarbeitern jedoch mehr direkte Verantwortlichkeiten auf)[4]
- Die etablierten Verarbeitungsgrundsätze in der Richtlinie (z. B. Verarbeitung nach Treu und Glauben, Zweckbindung, Aufbewahrung personenbezogener Daten nur so lange, wie erforderlich) bleiben erhalten
- Datenübermittlungsanforderungen bleiben auch weitestgehend gleich: Datenübermittlungen außerhalb der EU/des EWR sind zulässig, wenn bewährte Datenübertragungsmechanismen verwendet werden (z. B. EU-US Privacy Shield oder „Musterklauseln“)[5]

Die höheren Bußgelder in der DSGVO zeigen, dass die Nichteinhaltung bestehender Grundsätze und Anforderungen, wie z. B. die Aufbewahrung personenbezogener Daten nur so lange wie nötig oder geeignete Sicherheitsmaßnahmen, ein erhöhtes Risiko mit sich bringen können.

Wie wirkt sich der Brexit aus?

Die DSGVO gilt im Vereinigten Königreich ab dem 25. Mai 2018 bis zum „Brexit“ Ende März 2019. Aber auch nach dem Brexit wird die DSGVO der Maßstab für das Vereinigte Königreich sein:

- Die britische Regierung hat die UK Data Protection Bill 2017 (derzeit im Gesetzgebungsverfahren) veröffentlicht, die die DSGVO vor und nach dem Brexit[6]
- Nach dem Brexit gilt die DSGVO direkt für britische Organisationen, die EU-Ansässigen Waren und Dienstleistungen zur Verfügung stellen oder diese überprüfen (z. B. britische Universitäten, die aktiv Studierende aus der EU anwerben)

Auswirkungen auf Datenübermittlungen vom und in das Vereinigte/n Königreich:

- Die EU hat deutlich gemacht, dass das Vereinigte Königreich nach dem Brexit als „Drittland“ anzusehen ist und somit in Bezug auf Datenübermittlungen nicht mehr als „angemessenes“ (auf der weißen Liste geführtes) Land gelten wird.
- Sofern und solange das Vereinigte Königreich nicht von der EU-Kommission für angemessen erklärt wird (z. B. im Rahmen eines Übergangsabkommens), müssen Datenübertragungsvereinbarungen oder andere Datenübertragungsmechanismen für die Übermittlung personenbezogener Informationen aus der EU in das Vereinigte Königreich getroffen werden.
- Im Gegenzug muss das Vereinigte Königreich festlegen, welche Länder es für angemessen hält (was wahrscheinlich auf die EU-Länder und die Länder zutrifft, die sich auf der weißen Liste der EU befinden). Für jene Länder, die nicht als angemessen gelten, werden vom Vereinigten Königreich anerkannte Datenübertragungsmechanismen (wahrscheinlich ähnlich den EU-Mechanismen) für die Übermittlung personenbezogener Informationen aus dem Vereinigten Königreich eingesetzt werden müssen.

Entmystifizierung der DSGVO

Eines der Ziele der DSGVO war es, mehr Klarheit durch genauere Vorschriften zu schaffen. Es gibt jedoch immer noch viele Aspekte der DSGVO, die Interpretationsspielraum bieten. Außerdem hat die Komplexität der DSGVO zu mangelndem Verständnis sowie übertriebenen Aussagen geführt. Daraus entstanden viele Mythen, von denen wir einige im Folgenden aufgedeckt haben:[7]

Mythos 1: Für die Verarbeitung personenbezogener Informationen ist grundsätzlich eine Einwilligung erforderlich

Fakt: Die „Einwilligung" ist nur eine der Rechtsgrundlagen, die die Verarbeitung von personenbezogenen Informationen ermöglicht (z. B. erforderliche Verarbeitung für die Erfüllung eines Vertrags oder für das „berechtigte Interesse" einer Organisation). Die Latte für diese Einwilligungen wurde sehr hoch gelegt. Beispielsweise gilt eine Einwilligung nicht als gültig, wenn die Betroffene keine echte freie Wahl haben und sie ihre Einwilligung nicht jederzeit unbeschadet widerrufen können. In vielen Datenverarbeitungsszenarien ist eine andere Rechtsgrundlage besser geeignet.[8]

Mythos 2 : Die Meldefrist von 72 Stunden bei Datenschutzverstößen gilt für die gesamte Lieferkette (d. h. ab dem Zeitpunkt, zu dem ein (Unter)auftragsverarbeiter Kenntnis darüber erlangt)

Fakt: Die DSGVO verlangt von Datenverarbeitern, dass sie im Falle einer Verletzung des Schutzes personenbezogener Daten ihren Datenverantwortlichen „ohne ungebührliche Verzögerung" benachrichtigen. Erst wenn der Datenverarbeiter den Verantwortlichen informiert hat, beginnt für den Datenverantwortlichen die Meldefrist von 72 Stunden. Die Artikel-29-Datenschutzgruppe (WP29), die Gruppe der EU-Datenschutzbehörden, hat in ihren letzten Leitlinien[9] klargestellt, dass „ohne ungebührliche Verzögerung" eine „zeitnahe" Benachrichtigung bedeutet (keine „unverzügliche" Benachrichtigung, wie ein vorangegangener Entwurf noch nahegelegt hat).

Mythos 3 : Datenübermittlungen außerhalb der EU/des EWR sind nicht zulässig bzw. nur mit Einwilligung des Kunden für jede einzelne Datenübermittlung

Fakt: Die DSGVO behält die bestehenden Datenübermittlungsanforderungen weitestgehend bei. Dementsprechend sind Datenübermittlungen zulässig, wenn von der EU anerkannte Datenübertragungsmechanismen wie der EU-US Privacy Shield oder Musterklauseln (Datenübertragungsvereinbarungen) bestehen. Blackboard verfügt über beides, um personenbezogene Informationen[10] ihrer Kunden gesetzeskonform zu übermitteln. Da Blackboard als Datenverarbeiter fungiert, ist eine allgemeine Anweisung des Kunden für Datenübermittlungen erforderlich (diese ist in unserer Standarddatenverarbeitungsvereinbarung enthalten); eine Einwilligung des Kunden in jede einzelne Datenübermittlung ist nicht erforderlich

Mythos 4 : Das Recht auf Löschung verlangt von Organisationen, alle Daten über eine Person zu löschen

Fakt: Das neue Recht auf Löschung ist kein absolutes „Recht darauf, vergessen zu werden." Es ist vielmehr ein Recht darauf, Daten löschen zu lassen, wenn sie nicht länger benötigt werden oder in Fällen, in denen die Organisation die DSGVO-Anforderungen nicht erfüllt. Wenn eine Organisation die Daten kraft Gesetzes dennoch aufbewahren muss (z. B. aufgrund von Aufbewahrungspflichten), müssen diese personenbezogenen Daten nicht gelöscht werden.

Mythos 5 : Die DSGVO gilt für alle Universitäten mit Studierenden aus der EU

Fakt: Dass Studierende aus EU-Ländern eingeschrieben sind, reicht noch nicht aus für die Anwendbarkeit der DSGVO. Die DSGVO gilt im Allgemeinen für Einrichtungen, die in der EU ansässig sind. Sie gilt auch für Universitäten außerhalb der EU, aber nur, wenn sie Personen Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Personen in der EU überprüfen. Um in die Kategorie „Dienstleistungen anbieten" zu fallen, ist eine gewisse Ausrichtung erforderlich. Die bloße Tatsache, dass Studierende aus EU-Ländern eingeschrieben sind, reicht nicht aus. Die DSGVO kann jedoch gelten, wenn Universitäten auf EU-Ansässige abzielen (z. B. für Online-Kurse) oder aktiv Studierende aus EU-Ländern anwerben. Diese Kriterien bieten Interpretationsspielraum. Wir empfehlen Kunden, sich selbst rechtlich beraten zu lassen.

UMSETZUNG DER DSGVO

Warum es so wichtig ist, den Datenschutz und die DSGVO zu verstehen

Das Risiko von Bußgeldern in Höhe von 4 % des Gesamtumsatzes ist sicherlich ein Grund dafür, warum viele Organisationen angefangen haben, den Datenschutz ernster zu nehmen. Aber wir sind der Meinung, dass die positiven Argumente für gute Datenschutzpraktiken mindestens ebenso überzeugend sind, weil der Datenschutz ein Menschenrecht ist und solide Datenschutzpraktiken Vertrauen schaffen.

In der heutigen Gesellschaft findet man überall personenbezogene Informationen. Personenbezogene Informationen werden oft als das neue Öl der Wirtschaft bezeichnet. Wir alle nutzen Onlinedienste und geben unsere personenbezogenen Informationen heraus. Aber eine Studie nach der anderen belegt, dass Organisationen in Bezug auf personenbezogene Informationen kein Vertrauen entgegengebracht wird. Es herrscht das Gefühl, dass wir als Einzelne die Kontrolle über unsere Daten verloren haben. Gesetzgeber und Regulierungsbehörden reagieren darauf. Die DSGVO ist hier wohl das bekannteste Beispiel. Organisationen müssen das Vertrauen des Einzelnen (wieder)erlangen. Gute Datenschutzpraktiken sind unerlässlich, um Vertrauen aufzubauen. Sie stellen auch einen Wettbewerbsvorteil dar. Und schlussendlich unterstützen sie Organisationen auch bei Innovationen. Wenn Studierende (und Personal) Ihrer Einrichtung vertrauen, werden sie ihre Daten eher weitergeben und neue Tools verwenden.

Falsch verstandener Datenschutz kann verhängnisvoll sein. Datenschutzverletzungen sind regelmäßig in den Nachrichten. Darauf folgen Rufschädigung, Verlust von Vertrauen des Einzelnen und das Risiko von Klagen jener, deren Daten falsch gehandhabt wurden. Die Datenschutzbehörden verhängen vielleicht nicht gleich zu Anfang Geldbußen in Höhe von 4 % des Gesamtumsatzes, aber sie verfügen über viele weitere Durchsetzungsinstrumente und können Einrichtungen zwingen, Ihre Datenschutzpraktiken zu ändern und Datenschutzprogramme mit regelmäßigen externen Audits einzuführen.

Unsere Rolle und die Rolle Ihrer Organisation gemäß der DSGVO

Die DSGVO behält die Begriffe „Datenverantwortlicher“ und „Datenverarbeiter“ bei. Dieses Konzept ist wesentlich, weil es die Verantwortlichkeiten und Verpflichtungen von Organisationen und ihrer Dienstleistungsanbieter festlegt.

Eine Organisation gilt als Datenverantwortliche, wenn sie die „Mittel und Zwecke“ der Verarbeitung personenbezogener Informationen festlegt, d. h. warum und wie personenbezogene Informationen verwendet werden. Der Datenverarbeiter dagegen ist die Organisation, die im Namen des Datenverantwortlichen und nach seinen Anweisungen handelt.

Für die meisten Produkte und Dienstleistungen von Blackboard (z. B. Learn, Collaborate, Open LMS) gilt/gelten Blackboard als Datenverarbeiter und unsere Kunden als Datenverantwortliche.

Die DSGVO stellt an Datenverarbeiter wie Blackboard mehr direkte Anforderungen. Der Großteil der DSGVO-Anforderungen gilt jedoch auch weiterhin für Datenverantwortliche (z. B. die Pflicht, die betroffenen Personen darüber zu informieren, wie ihre Daten verwendet werden, dem Auskunftsersuchen der Betroffenen in Bezug auf ihre Daten zu entsprechen, Meldepflicht gegenüber den Datenschutzbehörden und den Betroffenen bei Datenschutzverstößen).

Wie können Sie sich aufdie DSGVO vorbereiten??

Alle Organisationen im Anwendungsbereich der DSGVO müssen am 25. Mai 2018 startklar sein. Nachstehend finden Sie eine Liste wichtiger Punkte, die Kunden beachten sollten, um gerüstet zu sein. Diese Liste basiert auf unseren eigenen Erfahrungen und erhebt keinerlei Anspruch auf Vollständigkeit. Versäumen Sie bitte nicht, einen Datenschutzexperten an Bord zu holen, der Ihnen bei Ihrer Umsetzung helfen kann. Viele Datenschutzbehörden haben auch ihre eigenen Leitfäden zur Umsetzung der DSGVO[11] erstellt.

Hoffentlich haben Sie die Schritte 1-6 schon hinter sich und befinden sich mitten in der Umsetzung Ihrer Aktionspläne. Aber für einen Anfang ist es nie zu spät. Selbst wenn Sie gerade erst begonnen haben, können Sie die wichtigsten Änderungen noch umsetzen. So können Sie Ihrer zuständigen Datenschutzbehörde auch zeigen, dass Sie an einem Plan arbeiten. Die DSGVO zu ignorieren ist keine Option.

1. **Prüfen Sie, ob die DSGVO auf Ihre Organisation Anwendung findet**

   Ist Ihre Organisation in der EU ansässig, dann gilt auch die DSGVO. Die DSGVO kann aber auch für Organisationen außerhalb der EU [12] gelten.

2. **Richten Sie ein DSGVO-Projekt ein**

   Konzipieren und implementieren Sie ein spezielles DSGVO-Projekt. Im Idealfall verfügen Sie über Projektmanagementsupport und ausgewählte Kontaktpersonen, die Sie in jeder Abteilung unterstützen können. Dieses Projekt erstreckt sich über alle Abteilungen Ihrer Einrichtung und Sie werden Hilfe benötigen.

3. **Ernennen Sie einen erfahrenen DSGVO-Verantwortlichen zum Projektleiter**

   Der Verantwortliche sollte nicht nur auf dem Gebiet des Datenschutzes Erfahrung haben, sondern auch über ausreichend Zeit und Mittel verfügen sowie Zugang zu externem Support haben (z. B. zu einer Anwaltskanzlei). Wenn Ihre Organisation eine in der EU ansässige öffentliche Behörde ist, müssen Sie auch einen Datenschutzbeauftragten benennen.

4. **Vergewissern Sie sich der Zustimmung und Kontrolle der Geschäftsführung**

   Die Umsetzung eines DSGVO-Projektes ohne Unterstützung, Weisung und Kontrolle der Geschäftsführung gestaltet sich schwierig.

5. **Überprüfen Sie Ihre Verwendung personenbezogener Informationen und führen Sie eine Lückenanalyse durch**

   Das Verständnis dafür, wo und wie personenbezogene Informationen verwendet werden und wo Optimierungsbedarf in Bezug auf die DSGVO besteht, ist Teil der ersten entscheidenden Phase des DSGVO-Projektes.

6. **Entwickeln Sie Aktionspläne, um Lücken zu schließen**

   Das ist vermutlich der schwierigste Teil der DSGVO, weil hier die oftmals hohen Anforderungen der DSGVO in spezifische und realisierbare Aktionen für alle unterschiedlichen Verfahren und Systeme umgewandelt werden müssen.

7. **Setzen Sie Aktionsplänen um**

   Vertrauen ist gut, aber in diesem Fall ist Kontrolle besser. In dieser Phase müssen die Aktionspläne der anderen verfolgt werden, um sicherzustellen, dass sie ihre Fristen einhalten.

8. **Überprüfen Sie Ihre Dienstleister**

   Nach der DSGVO sind Sie für Ihre Dienstanbieter verantwortlich. Die richtigen vertraglichen Regelungen sind wichtig, reichen aber nicht aus. Sie müssen sich sicher sein, dass Ihre Dienstleister die DSGVO-Anforderungen erfüllen und Sie bei der Einhaltung der Vorschriften unterstützen können. Fragen Sie nach, wie sie die DSGVO umsetzen.

9. **Tragen Sie den gesetzlichen/behördlichen Entwicklungen Rechnung (Leitlinien der Artikel-29-Datenschutzgruppe, Ausführungsgesetze der Mitgliedsstaaten)**

   Es reicht aus die DSGVO zu kennen, richtig? Falsch! Die DSGVO findet zwar direkt Anwendung, aber alle EU-Mitgliedsstaaten haben ergänzende nationale Datenschutzgesetze.

   Diese sind erforderlich, um Bereiche zu regeln, in denen die Mitgliedsstaaten Gesetzgebungsbefugnisse haben (z. B. Arbeitnehmerdatenschutz) oder in denen die DSGVO es ihnen gestattet, weitere Rechtsvorschriften zu erlassen (z. B. Kriterien für DSB (*Datenschutzbeauftragte*) und DPIA (*Datenschutz-Folgenabschätzungen*)). Darüber hinaus veröffentlicht die WP29 wichtige Orientierungshilfen. Auf dem Laufenden zu bleiben ist eine anspruchsvolle, aber wichtige Aufgabe[13].

UNSER PLAN UND KONZEPT

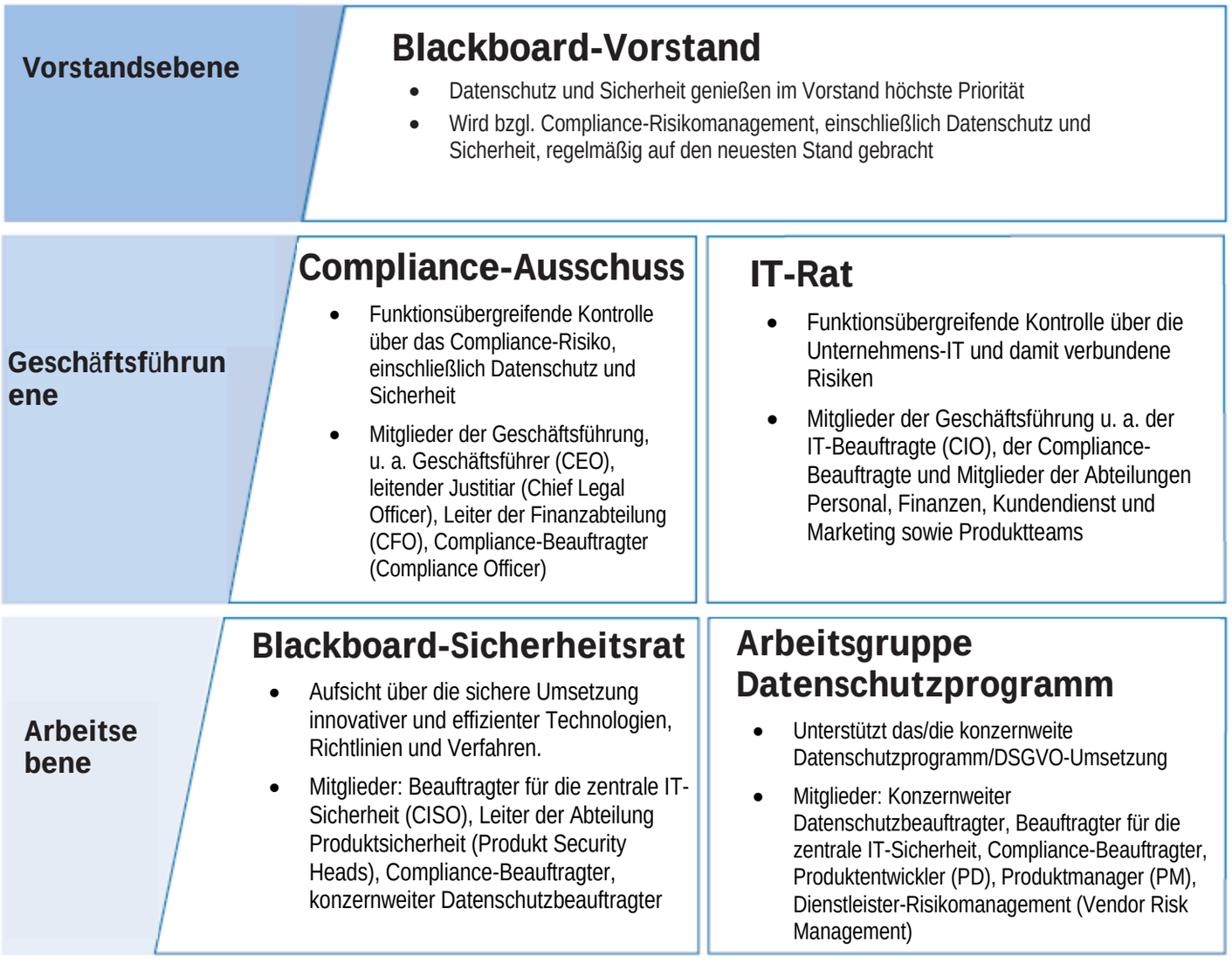
Datenschutz und Sicherheit bei Blackboard

Datenschutz und Sicherheit haben bei Blackboard seit Langem höchste Priorität. Für uns ist die DSGVO eine Chance, unsere bestehenden Datenschutzpraktiken weiter zu stärken.

Unser Datenschutzkonzept war schon immer kundenorientiert. Wir verstehen die Herausforderungen, denen sich unsere Kunden stellen müssen, und wollen Ihnen dabei helfen.

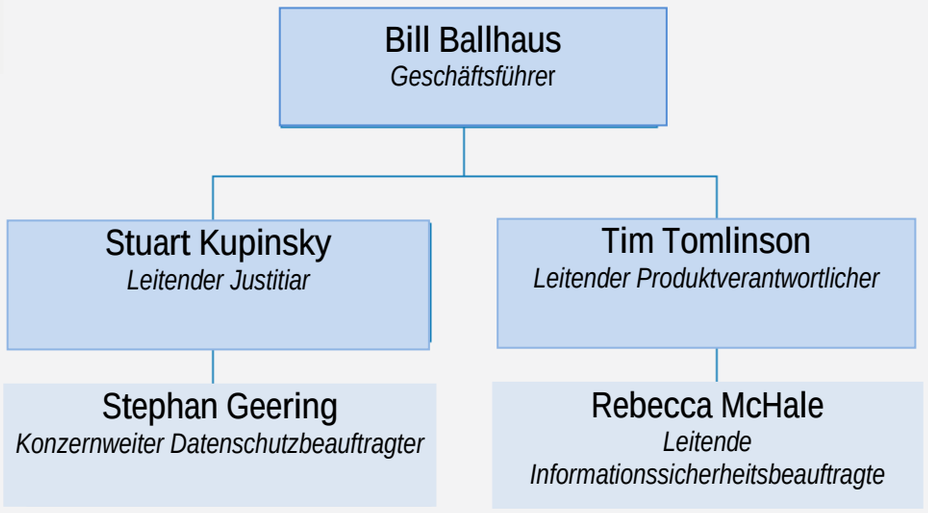
Gute Datenschutzpraktiken erfordern eine solide Führungsstruktur. Bei Blackboard sind Datenschutz und Sicherheit Prioritäten des Vorstands und unser Governance-Modell (siehe unten) gewährleistet, dass die Geschäftsführung unsere Datenschutz- und Sicherheitsbemühungen in leitender Funktion unterstützt.

Die Bedeutung, die Blackboard dem Datenschutz und der Sicherheit beimisst, zeigt sich auch daran, dass unser konzernweiter Datenschutzbeauftragter (Global Privacy Officer) und unsere leitende Informationssicherheitsbeauftragte (Chief Information Security Officer[14]) dem Führungsteam (CEO Leadership Team) unterstellt sind (siehe Organigramm unten).



Datenschutz und Sicherheit

Die Bedeutung, die Blackboard dem Datenschutz beimisst, zeigt sich auch daran, dass unser konzernweiter Datenschutzbeauftragter und unsere leitende Informationssicherheitsbeauftragte dem Führungsteam unterstellt sind.



Unser DSGVO-Konzept

Wir haben ein umfassendes Projekt zur Umsetzung der Anforderungen der DSGVO mit folgendem Konzept erstellt:

- Die Umsetzung der DSGVO baut auf den bestehenden Datenschutzerfahrungen und Compliance-Mechanismen von Blackboard auf
- Die DSGVO-Umsetzung wird federführend von unserem konzernweiten Datenschutzbeauftragten betrieben und von einem fest zugeordneten Projektmanager und „DSGVO-Verantwortlichen“ für jeden Funktionsbereich unterstützt
- Die renommierte Anwaltskanzlei Bristows LLP (u. a) wurde zur Unterstützung bei der Umsetzung der DSGVO herangezogen
- Die DSGVO-Umsetzung wird von Blackboards Compliance-Ausschuss überwacht. Diesem Ausschuss gehören auch der Geschäftsführer und der leitende Justitiar sowie weitere Führungskräfte an

Die DSGVO als Chance

Die Umsetzung der DSGVO bedeutet für uns nicht nur das bloße Bestreben, die neuen EU-Datenschutzanforderungen zu erfüllen, sondern auch eine Chance. Dementsprechend wollen wir die DSGVO-Umsetzung nutzen, um Folgendes zu erreichen:

- Stärkung unserer globalen Datenschutzpraktiken – wir nutzen das DSGVO-Projekt, um unser globales Datenschutzprogramm in der EU und darüber hinaus zu verbessern
- Entwicklung von „Datenschutz durch Technikgestaltung“-Prozessen, welche die Datenschutz-Compliance tiefer in unseren alltäglichen Abläufen verankern
- Unterstützung unserer Kunden in ihren Bemühungen um DSGVO-Compliance
- Positionierung von Blackboard als der anerkannte Vorreiter in puncto Datenschutz bei Bildungstechnologien

Unser Umsetzungsplan

Für die Umsetzung unseres globalen Datenschutz-/DSGVO-Programms wenden wir die von Bristow LLP entwickelte 3-Phasen-Methode an. Diese Methode wird auch in zahlreichen anderen Unternehmen angewandt, u. a. in führenden Technologiekonzernen. Die drei zentralen Phasen sehen folgendermaßen aus:

- **PHASE 1 - Beschaffung von Informationen**
- **PHASE 2 - Entwicklung von Lösungen**
- **PHASE 3 - Aufteilung in Arbeitsbereiche zur Umsetzung**

Wir haben diese 3-Phasen-Methode angewandt, um unser Programm mit den folgenden vier Hauptstufen zu entwickeln:

Projektinitialisierung

Diese Stufe umfasste die folgenden Maßnahmen:

- Unterrichtung und Einholung der Zustimmung der Geschäftsleitung
- Beauftragung eines konzernweiten Datenschutzbeauftragten mit der Verantwortung für die Leitung des DSGVO-Projekts
- Erarbeitung eines Projektplans und Projektsteuerungskonzeptes
- Erstbeschaffung von Informationen und Prüfung der aktuellen Compliance-Maßnahmen für die Bereiche, in denen auf Grund der DSGVO Verbesserungsbedarf besteht

PHASE 1 - Beschaffung von Informationen (Workshops)

In dieser Anfangsphase fanden strukturierte Gespräche/Workshops mit Personen in Schlüsselpositionen aus den einzelnen Funktionsbereichen und Produktgruppen von Blackboard statt, um genaue Informationen über die Datenverarbeitungspraktiken innerhalb dieser Bereiche zu erhalten.

Die Ergebnisse dieser Workshops wurden zur Durchführung der Lückenanalyse und zur Entwicklung von Lösungen und Umsetzungsplänen für Phase 2 herangezogen.

PHASE 2 - Entwicklung von Lösungen

Auf Grundlage der Informationen aus den Workshops haben wir die folgenden Lösungen und Dokumentationen erarbeitet:

- Verbesserte interne Datenschutzdokumentation (Richtlinie und detaillierte Betriebsnormen), die den DSGVO-Anforderungen entsprechen und erläutern, wie diese Anforderungen für die unterschiedlichen Datenverarbeitungsvorgänge erfüllt werden müssen (z. B. Anforderungen für die Verarbeitung von Kundendaten, „Datenschutz durch Technikgestaltung“-Verfahren)
- Produktanforderungen
- Umsetzungsplan für die Funktionsbereiche und für zentral erforderliche Maßnahmen

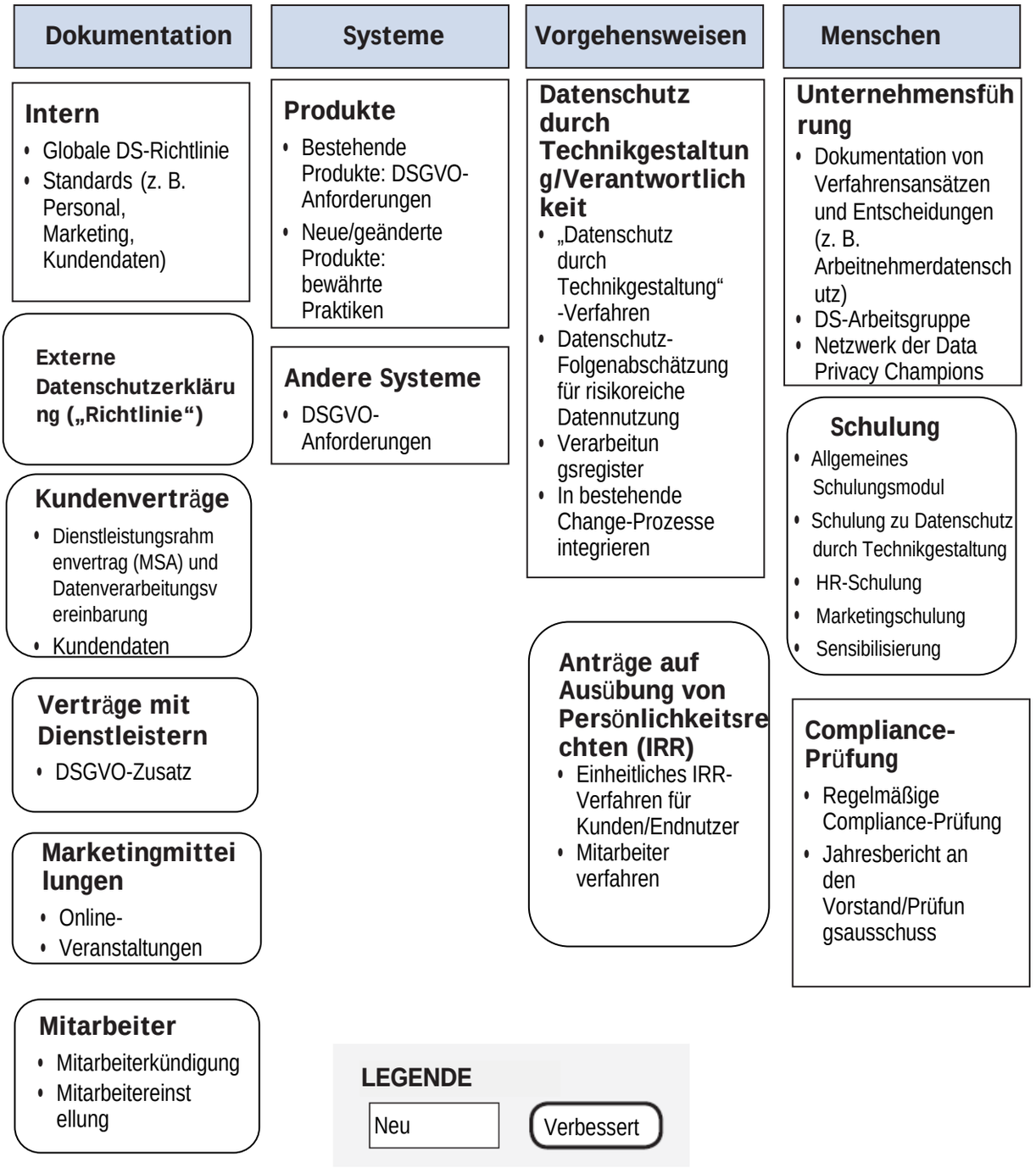
PHASE 3 - Aufteilung in Arbeitsbereiche zur Umsetzung

In der letzten Phase führen wir die entwickelte Datenschutzdokumentation ein und die Umsetzungspläne durch. Dafür werden wir sechs Arbeitsbereiche definieren:

1. Ausführung der Umsetzungspläne für die Funktionsbereiche und Produktgruppen
2. Prüfung und Aktualisierung öffentlicher Richtlinien, Mitteilungen und Einwilligungen
3. Optimierung der Führungsstruktur (Funktionen und Verantwortungsbereiche, Schulungen, Datenschutz durch Technikgestaltung)
4. Prüfung und Aktualisierung von Verträgen mit Dienstleistern (sofern erforderlich)[15]
5. Änderungen an den IT-Systemen (sofern erforderlich)
6. Einrichtung eines Datenverarbeitungsregisters

Überblick über die Veränderungen

Das Schaubild unten zeigt, wie wir uns das Endstadium unseres DSGVO-/Datenschutzprogramms nach vollzogenen Umsetzungsmaßnahmen vorstellen. Nach der Umsetzung der DSGVO werden wir unsere Datenschutzpraktiken weiterentwickeln und anpassen.



WIE KÖNNEN SIE VON UNSEREM DSGVO-PROGRAMM PROFITIEREN?

Das globale Datenschutz-/DSGVO-Umsetzungsprogramm zielt darauf ab, Ihre Organisation bei der Umsetzung der DSGVO zu unterstützen. Die folgenden Abschnitte enthalten weitere Informationen, die sich zusammenfassend auf diese7 Hauptpunkte reduzieren lassen:

1. DSGVO-konforme Produkte: Wir führen Produktanforderungen ein, um Kunden bei der Einhaltung von Transparenzanforderungen, bei Anträgen auf Ausübung von Persönlichkeitsrechten usw. zu unterstützen.
2. Datenschutz durch Technikgestaltung: Wir führen ein Verfahren zum Datenschutz durch Technikgestaltung und zur Datenschutz-Folgenabschätzung (DPIA) ein, um die Dokumentation der Einhaltung der Verordnung zu erleichtern.
3. Data transfers: Wir verfolgen weiterhin unseren vielschichtigen Ansatz: Regionalisierung, EU-US Privacy Shield und von der EU anerkannte Musterklauseln
4. Verträge mit Kunden: Wir haben einen DSGVO-konformen Datenverarbeitungszusatz zu unserer Standardrahmenvereinbarung entwickelt.
5. Unsere Dienstleister: Wir verfügen über hieb- und stichfeste Verträge und ein Risikomanagementgerüst für Dienstanbieter
6. Sicherheit: Wir haben Richtlinien, Verfahren und Führungsstrukturen eingerichtet, die ständig verbessert werden, um die Sicherheit der Kundendaten zu wahren
7. Meldepflicht bei Datenschutzverstößen: Wir verfügen über ein dokumentiertes und geprüftes Verfahren für die Reaktion auf Sicherheitsvorfälle

1. DSGVO-konforme Produkte:

Einer der Hauptaspekte in unseren Arbeitsbereichen zur Umsetzung ist es, unsere Kunden zu unterstützen, indem wir unsere Produkte DSGVO-konform machen. Dazu, machen wir für unsere Produkte Mindestanforderungen in Bezug auf die DSGVO/den Datenschutz geltend. Im Einklang mit unserer Absicht, unsere Datenschutzpraktiken weltweit zu stärken, gelten die meisten dieser Anforderungen für alle unsere Produkte und nicht nur für die Produkte, die wir in der EU anbieten. Davon profitieren auch unsere Kunden außerhalb der EU, die eventuell in den Anwendungsbereich der DSGVO fallen.
Wir haben unsere DSGVO-/Datenschutz-Produktanforderungen in einem soliden und intensiven Verfahren entwickelt. Wir haben mit einem externen Berater einen ersten Entwurf erarbeitet. In zahlreichen Arbeitssitzungen und Überarbeitungen mit Personen in Schlüsselpositionen in unseren Produktentwicklungs- und Produktmanagementteams haben wir die Fassung weiterentwickelt zu spezifizierten und tragfähigen allgemeinen Produktanforderungen mit detailliertem Leitfaden. Die DSGVO-/Datenschutz-Produktanforderungen wurden anschließend als produktspezifische Maßnahmen in die Produktumsetzungspläne für die jeweilige Produktgruppe aufgenommen.

Unsere Produktanforderungen[16] lassen sich folgendermaßen kategorisieren:

Transparenz

- Möglichkeit für Kunden, auf ihre Datenschutzrichtlinien/-erklärungen zu verlinken
- Bereitstellung von Informationen darüber, wie personenbezogene Informationen im Allgemeinen in einem Produkt verwendet werden

Datenminimierung/-löschung

- Überprüfung der Produkte auf unnötige/optionale Felder
- Überprüfung der Produkte auf Möglichkeiten, pseudonyme oder anonyme Daten statt personenbezogenen Informationen zu verwenden.
- Möglichkeit, personenbezogene Informationen auf Wunsch der Kunden zu löschen (wenn Kunden/Benutzer die Daten nicht selbst löschen können)

Droits généraux des personnes concernées

- Capacité à permettre l'accès à et à la rectification des informations personnelles sur demande de la personne concernée
- Capacité à effacer les informations personnelles sur demande de la personne concernée

Allgemeine Rechte betroffener Personen

- Möglichkeit, auf Wunsch Zugriff auf und Berichtigung von personenbezogene(n) Informationen anzubieten
- Möglichkeit, auf Wunsch personenbezogene Informationen zu löschen

Rechte betroffener Personen in der EU

- Möglichkeit, Datenübertragbarkeitsanfragen zu bearbeiten (Recht der Betroffenen, unter bestimmten Umständen Daten in maschinenlesbarer Form zu erhalten)Respect des données dès la conception
- Möglichkeit, die Verwendung personenbezogener Informationen einzustellen (Recht auf Widerspruch/Beschränkung unter bestimmten Umständen)

Blackboard verfügt bereits über klar definierte Programme für unsere Produktsicherheit, die die DSGVO berücksichtigen. Daher haben wir keine zusätzlichen DSGVO-spezifischen Sicherheitsanforderungen definiert[17]

2. Datenschutz durch Technikgestaltung:

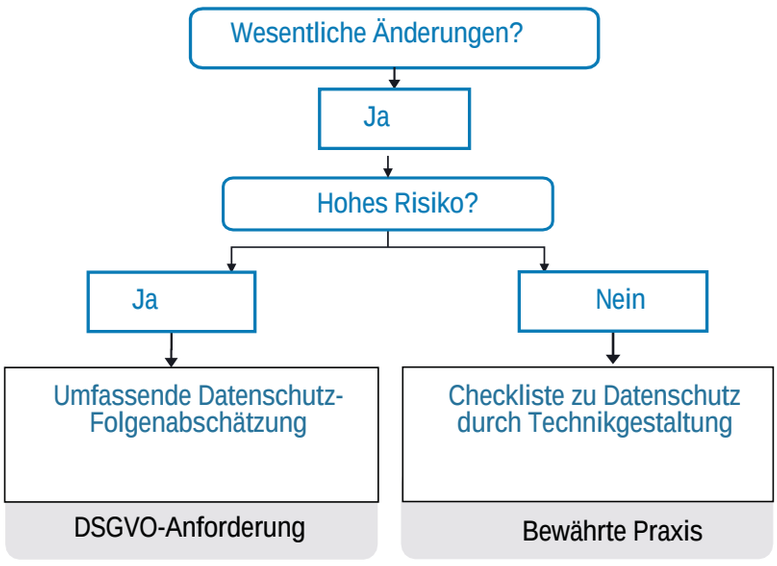
Da es in der heutigen Welt für Privatpersonen immer schwieriger wird, die Kontrolle über ihre Daten zu behalten (siehe dazu unseren Blog-Beitrag zum Datenschutztag), gewinnen Datenschutz durch Technikgestaltung und Verantwortlichkeit zunehmend an Bedeutung, um das Vertrauen der betroffenen Personen, von Kunden und Regulierungsstellen zu bewahren und um zu dokumentieren, wie eine Organisation die DSGVO erfüllt. Daher stellen wir unseren Ansatz „Datenschutz durch Technikgestaltung“ in den Mittelpunkt unseres globalen Datenschutz-/DSGVO-Programms.

Für Blackboard bedeutet das eher eine Evolution als eine Revolution. Wir haben schon immer rechtliche Prüfungen für neue Produkte und Verfahren durchgeführt. Mit unserem Ansatz „Datenschutz durch Technikgestaltung“ formalisieren wir diese Prüfungen und verbessern ihre Dokumentation.

Ansatz

- Wir haben ein dokumentiertes „Datenschutz durch Technikgestaltung“-Verfahren mit Checkliste entworfen.
- Einzelne Funktionsbereiche und Produktgruppen integrieren diese Checkliste in ihre Change-Prozesse.
- Jede wesentliche Veränderung an der Art und Weise, wie personenbezogene Informationen verwendet werden, erfordert das Ausfüllen dieser Checkliste. Dies wird zwar in der DSGVO nicht ausdrücklich gefordert, gehört aber zur bewährten Praxis.
- Die Checkliste bedingt dann die ausführlichere Datenschutz-Folgenabschätzung (DPIAA) für eine risikoreiche Nutzung personenbezogener Informationen (DSGVO-Anforderung).

Das Flussdiagramm unten veranschaulicht diesen Ansatz:



3. Datenübermittlungen

Die DSGVO bringt keine wesentlichen Veränderungen an der Art und Weise, wie personenbezogene Informationen außerhalb der EU/des EWR übermittelt werden dürfen, mit sich.Nous maintiendrons donc notre approche redondante et à plusieurs niveaux de la conformité des transferts de données. Cela signifie que nous appliquerons les exigences en matière de transfert de données de différentes façons pour garantir l'existence de mesures adéquates de protection de vos données : Die derzeitigen Beschränkungen und Datenübertragungsmechanismen bleiben erhalten. Dementsprechend sind Datenübermittlungen zulässig, wenn von der EU genehmigte Datenübertragungsmechanismen wie der EU-US Privacy Shield oder Musterklauseln (Datenübertragungsvereinbarungen) vorliegen. Diese Mechanismen stellen sicher, dass personenbezogene Informationen auch dann noch angemessen geschützt sind, wenn sie die EU/den EWR verlassen.

Wir verfolgen weiterhin unseren vielschichtigen und redundanten Compliance-Ansatz bzgl. Datenübermittlung. Das bedeutet, dass wir die Anforderungen an Datenübermittlungen auf vielerlei Weise erfüllen, um sicherzustellen, dass angemessene Sicherheitsvorkehrungen für Ihre Daten getroffen werden:

- Regionales Hosting: Wir verfolgen eine regionale Hosting-Strategie, bei der fast alle Produkte in der EU gehostet werden und die Verlagerung weiterer Produkte auf regionale Hosting-Lösungen geplant ist. Die DSGVO schreibt zwar keine regionale Speicherung vor und wir sind auch nicht der Ansicht, dass eine Datenlokalisierung einen besseren Datenschutz oder eine bessere Datensicherheit,[18] bietet, aber wir verstehen, dass viele Kunden aus der EU ihre Daten lieber in der EU gespeichert wissen.
- Privacy Shield : Blackboard ist nach dem EU-US Privacy Shield zertifiziert und wir dürfen daher rechtmäßig personenbezogene Daten in die USA. Übermitteln.
- **Musterklauseln:** Wir verwenden auch von der EU anerkannte „Musterklausel"-Vereinbarungen, durch die wir innerhalb unserer Unternehmensgruppe gesetzeskonform personenbezogene Daten außerhalb des EWR übermitteln können („Kundendatenübertragungsvereinbarung").
- **Dienstleister:** Wir verfügen über unanfechtbare Verträge mit Dienstleistern und Partnern (z. B. IBM, Amazon Web Services), um sicherzustellen, dass Datenübertragungsanforderungen (und andere Datenschutzverpflichtungen) an unsere Dienstleister und Partner weitergegeben werden.

Wir unterhalten derzeit[19] mehrere regionale Rechenzentren, um für unsere in der EU ansässigen Kunden den Umgang mit Daten in der EU zu erleichtern:Hébergement géré (centres de données de Blackboard) : centres de données à Amsterdam (Pays-Bas) et Francfort (Allemagne).

- Managed Hosting (Blackboard-Rechenzentren): Rechenzentren in Amsterdam (Niederlande) und Frankfurt (Deutschland).
- Cloud-Hosting (AWS-Rechenzentren): AWS, Region Frankfurt, Deutschland (eu-central-1).

AWS-Rechenzentren erfüllen eine Vielzahl an Zertifizierungen und Anforderungen von ISO 27001 und ISO 27018 bis SOC2 und DSGVO-Compliance sowie Compliance mit lokalen Anforderungen wie dem deutschen C5 und IT-Grundschutz[20].

Es ist wichtig zu verstehen, dass personenbezogene Informationen von Kunden aus der EU für die meisten Produkte (u. a. Learn 9.1, Learn SaaS, Open LMS und Collaborate) zwar in diesen Rechenzentren gespeichert werden, aber für die Bereitstellung mancher Produkte und Dienstleistungen (z. B. 24/7-Support) ein Zugriff auf diese Daten von außerhalb der EU/des EWR erforderlich sein kann. Derartige Datenübermittlungen sind dank der bereits erwähnten Zertifizierung nach dem EU-US Privacy Shield und den Musterklauseln zulässig.

4. Verträge mit Kunden

Die aktuelle Richtlinie sieht vor, dass ein Datenverantwortlicher einen Vertrag mit dem Dienstleister (Datenverarbeiter) hat, schreibt aber keinen expliziten Vertragsinhalt vor. Die DSGVO ist hier sehr viel strenger und beinhaltet eine Liste mit erforderlichen Inhalten.[21]

Notre Unser aktueller Standard-Datenverarbeitungszusatz berücksichtigt all die erforderlichen Punkte unten. Für Kunden, die sich im Anwendungsbereich der DSGVO befinden, ist der Zusatz automatisch in der Standardrahmenvereinbarung enthalten.

- ✓ Verwendung personenbezogener Daten nur gemäß Anweisung
- ✓ Personal muss Vertraulichkeitsvereinbarungen unterzeichnen
- ✓ Angemessene Sicherheitsvorkehrungen müssen getroffen sein
- ✓ Es dürfen nur Dienstleister (Unterauftragsverarbeiter) beauftragt werden .....
  - gemäß der Autorisierung des Datenverantwortlichen (dabei kann es sich um eine allgemeine Autorisierung handeln)
  - die vertraglich an dieselben Datenschutzverpflichtungen gebunden sind
- ✓ Unterstützung des Datenverantwortlichen bei der Bearbeitung von Anträgen zur Ausübung der Rechte betroffener Personen
- ✓ Unterstützung des Datenverantwortlichen bzgl. Sicherheitsmaßnahmen, Meldepflicht bei Datenschutzverstößen und Datenschutz-Folgenabschätzungen
- ✓ Rückgabe oder Löschung der Daten bei Vertragsende
- ✓ Bereitstellung von Informationen, die erforderlich sind, damit der Datenverantwortliche Konformität mit den Vorschriften nachweisen kann
- ✓ Unverzügliche Benachrichtigung des Datenverantwortlichen, wenn dessen Anweisungen gegen die DSGVO verstoßen

5. Verwaltung unserer Dienstleister

Blackboard bedient sich Dienstleistern (z. B. IBM, Amazon Web Services), damit wir unseren Kunden unsere Produkte und Dienstleistungen zur Verfügung stellen können. Insoweit dies den Zugriff auf personenbezogene Kundendaten erforderlich macht, ist Blackboard für die Datenschutzpraktiken der Dienstleister verantwortlich.

Teil unserer DSGVO-Programmes ist es, den Ansatz „Datenschutz durch Technikgestaltung“ eng mit unseren bestehenden Verfahren bzgl. Risikomanagement für Dienstleister und Beschaffung zu verknüpfen. Dies führt zu den folgenden wichtigen Kontrollelementen:

- Unanfechtbare Verträge mit Dritten mit einem Datenschutz- und DSGVO-Zusatz, die im Wesentlichen die gleichen Bestimmungen vorsehen, die in unserem Verhältnis zu den Kunden gelten
- „Musterklausel“-Vereinbarungen und/oder DSGVO- und Privacy-Shield-Zusätze, die rechtmäßige Datenübermittlungen an unsere Dienstleister ermöglichen
- Dokumentierte Risikomanagementrichtlinie und -rahmenvereinbarung mit Dienstleistern
- Neue Dienstleister mit Zugriff auf personenbezogene Informationen müssen einen Fragenbogen zur Sicherheitsbewertung von Dienstleistern mit Fragen zur Datenschutz-Compliance ausfüllen
- Dienstleister mit Zugriff auf von Blackboard verwaltete Systeme müssen die folgenden internen Zugriffskontroll- und Identitäts- sowie Autorisierungsrichtlinien befolgen. Hierzu gehören ggf. auch Kontoprüfungen
- Dienstleister müssen über genehmigte Mechanismen (z. B. VPN) auf die Ressourcen von Blackboard zugreifen
- Dienstleister haben Zugangsbeschränkungskontrollen für Datenverkehr, Benutzer und Vermögenswerte eingerichtet

6. Sicherheit

Die DSGVO ändert nichts Wesentliches an den technischen und organisatorischen Maßnahmen („TOMs“) für die Sicherheit personenbezogener Daten. Diese Maßnahmen müssen, wie auch in der aktuellen Richtlinie vorgesehen, dem damit verbundenen Risiko „angemessen“ sein. Daher vertrauen wir weiterhin auf unsere etablierten Informationssicherheitsprogramme.

Kontrolle des Datensicherheitsrisikos

Wir haben Anforderungen in Bezug auf Unternehmensstrategie, Verfahren, Unternehmensführung und Technik festgelegt, um IT-Sicherheitsrisiken unternehmensweit zu kontrollieren.

Vom ersten Tag an muss sich das Personal bei Blackboard seiner Verantwortung für den Schutz personenbezogener Kundendaten bewusst sein:

- Bestätigung der Unternehmensstrategie bzgl. des Schutzes sensibler Daten
- Jährliche Nutzersicherheits- und Datenschutzschulung
- Übung von Phishing-Szenarien
- Sensibilisierungsmerkblätter

Die folgenden Anforderungen gelten für den Datenschutz durch unser Personal:

- Es werden Datenklassifizierungen mit Anforderungen bzgl. des Schutzes des jeweiligen Datentyps vorgenommen: Kundendaten (Daten der Einrichtungen und ihrer Lernenden) gehören der Kategorie mit der höchsten Sensibilität an.
- Es liegen technische Kontrollen zum Schutz der Daten vor, z. B.:
  - Verwendung von Verschlüsselungstechniken
  - zeitnahe Sicherheitsupdates
  - verbesserte Authentifizierungskontrollen
  - Schutz vor schädlichen E-Mails und des Internetverkehrs
  - Endpunktschutztechnologien
  - bedarfsorientierter beschränkter Zugriff

Es geht nicht nur um die DSGVO ...

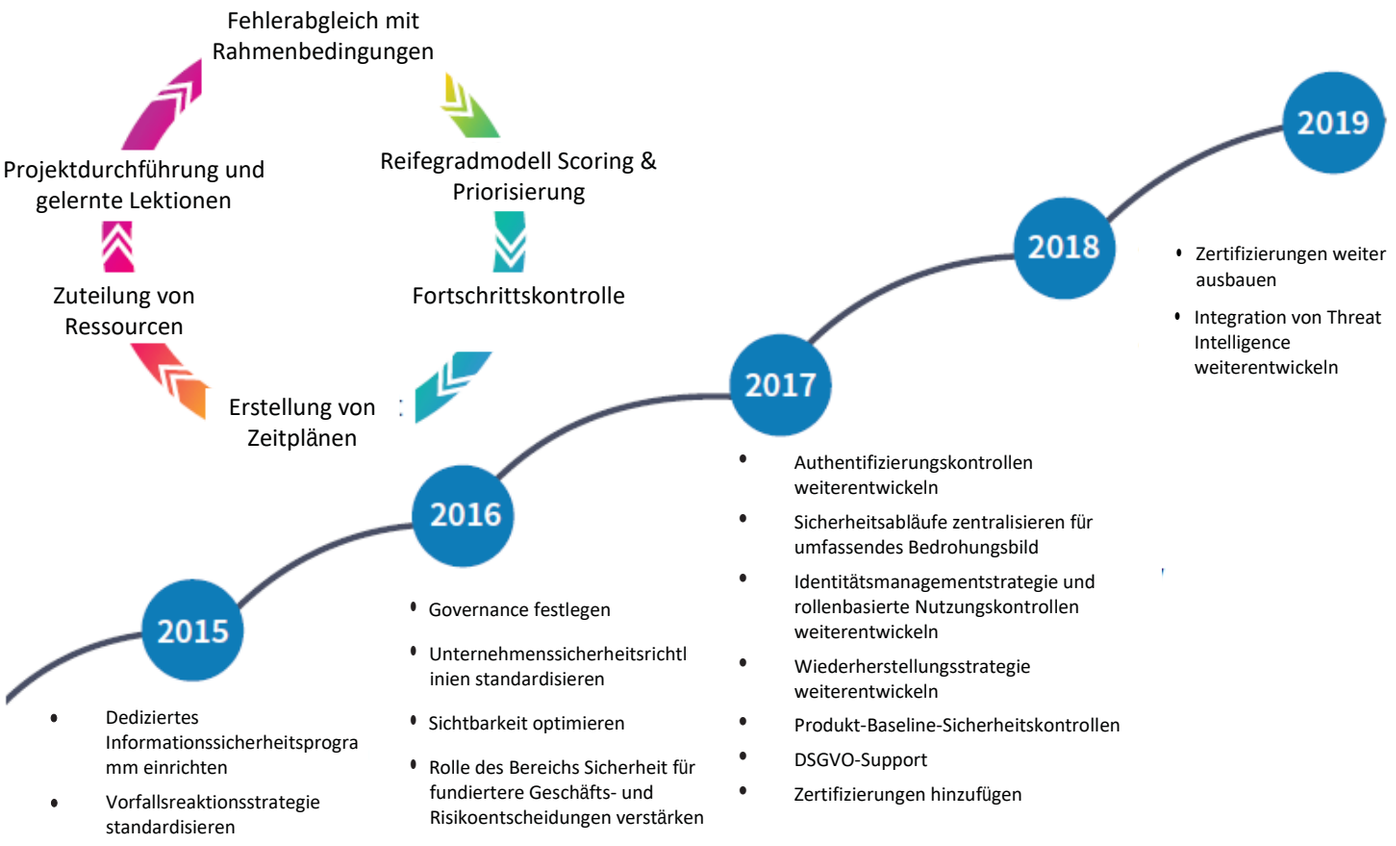
Als globaler Akteur im Dienste der Bildung verfolgen wir relevante geographische und bildungssektorspezifische Datenschutz- und Sicherheitsgesetze und -bestimmungen.
Die folgende Liste enthält nur einige Beispiele für Sicherheits- und Datenschutzvorschriften, Normen und Rahmenverträge, die Blackboard bei der Ausarbeitung seiner Sicherheitsrichtlinien, Verfahren und technischen Kontrollen zusätzlich zur DSGVO berücksichtigt.

- US Family Education Right and Privacy Act; Family Educational Rights and Privacy Act (US-amerikanisches Gesetz zum Schutz von Ausbildungsunterlagen; FERPA) und Protection of Pupil Rights Amendment (Zusatz über den Schutz der Rechte von Lernenden; PPRA)
- US Children’s Online Privacy Protection Act (US-amerikanisches Gesetz zum Schutz der Privatsphäre von Kindern im Internet; COPPA)
- US-amerikanische einzelstaatliche Gesetze (bestehendes und neues 50-State-Patchwork)
- US-Regierungsnormen – FedRAMP
- PCI-Datensicherheitsstandards, soweit anwendbar
- ISO/IEC, OWASP, NIST
- Internationale Normen (MTCS, IRAP)

Reifegradbestimmung und Roadmaps

Wir arbeiten hart daran, unsere technischen und operativen Sicherheitsmaßnahmen stetig zu verbessern.
Das Diagramm auf der nächsten Seite veranschaulicht unsere fortlaufenden Reifegradbestimmungen und unsere Roadmaps.

Rahmenbedingungen festlegen: Reifegradbestimmung und Roadmaps



7. Meldepflicht bei Datenschutzverstößen

Eine der wesentlichen Änderungen der DSGVO ist die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Datenschutzbehörde und (in einigen Fällen) an die betroffenen Personen.[22]

Für die meisten unserer Produkte und Dienstleistungen ist Blackboard nach der DSGVO Datenverarbeiter[23] Die Meldepflicht gegenüber Datenschutzbehörden und betroffenen Personen im Falle eines Datenschutzverstoßes, an dem Blackboard beteiligt ist, läge daher bei unseren Kunden. Die DSGVO verlangt jedoch von Datenverarbeitern wie Blackboard in so einem Fall, ihre Kunden (Datenverantwortliche) ohne ungebührliche Verzögerung (d. h. „zeitnah“)[24] zu benachrichtigen.

Wir haben die folgenden Vorkehrungen getroffen, um unsere Kunden bei der Erfüllung ihrer Verpflichtungen im Falle einer Verletzung des Schutzes personenbezogener Daten bei Blackboard in Bezug auf einen Kunden zu unterstützen:

- Sicherheitsvorfallsreaktionsverfahren (SIR) von Blackboard
  - Regelmäßig dokumentiert und geprüft
  - Erleichtert die rasche Identifizierung, Untersuchung und Behebung bei einem Vorfall
  - Ermöglicht schnelle Benachrichtigung der Kunden
  - Stützt sich auf das etablierte Sicherheitsvorfallsreaktionsteam, dem der leitende Informationssicherheitsbeauftragte und der konzernweite Datenschutzbeauftragte angehören
- Unsere Verpflichtung, Kunden zeitnah zu benachrichtigen, ist in unserer aktuellen Standardrahmenvereinbarung und dem Datenschutzzusatz[25] festgehalten.

FAZIT

Die DSGVO erfordert erhebliche Veränderungen, deren Auswirkungen weit über den Stichtag 25. Mai 2018 hinausreichen. Wir hoffen, dass dieses White Paper zu Ihrer erfolgreichen Umsetzung der DSGVO beitragen kann und dass es verdeutlicht hat, wie ernst Blackboard die Einhaltung der DSGVO und des Datenschutzes nimmt.

Die folgenden Abschnitte enthalten zusätzliche hilfreiche Informationen und eine Liste mit unseren Kontakt-E-Mail-Adressen, falls Sie Fragen oder Anmerkungen zu diesem White Paper haben.

NÜTZLICHE QUELLEN ZUR DSGVO

Die nachfolgend verlinkten Quellen stellen nur eine kleine Auswahl des hilfreichen Materials dar, das online verfügbar ist. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

Für eine genaue Analyse, inwieweit die DSGVO für Sie gilt, sollten Sie einen Fachmann zu Rate ziehen. Es ist wichtig, auf einen erfahrenen Datenschutzexperten zurückzugreifen (z. B. aus der Anwaltskanzlei Ihrer Wahl).

Offizielle EU-Quellen

- DSGVO-Text
- Leitlinien der Artikel-29-Datenschutzgruppe
- DSGVO-Website der EU-Kommission

Material der EU-Datenschutzbehörde

- Die britische Datenschutzbehörde (ICO) verfügt über eine hervorragende und laufend aktualisierte DSGVO-Website mit nützlichem Material in leicht verständlicher Sprache.
- Die irische Datenschutzbehörde (DPC) unterhält eine spezielle DSGVO-Seite für Organisationen
- Die französische Datenschutzbehörde CNIL stellt teilweise Material in Englisch zur Verfügung, u. a. eine kostenlose Datenschutzfolgenabschätzungssoftware (und umfangreiches Material in französischer Sprache)
- Die spanische Datenschutzbehörde AEPD hat einen Leitfaden für Bildungseinrichtungen erstellt (PDF, auf Spanisch)

Leitfäden von Anwaltskanzleien

- Leitfaden zur DSGVO von Bird & Bird
- Übersicht über die Gesetzgebung in den Mitgliedsstaaten von Bird & Bird (mit einem Überblick über nationale Abweichungen von der DSGVO)
- DSGVO-Survival-Ratgeber von Linklaters (PDF)
- DSGVO-Handbuch von White & Case

Andere Organisationen

- Das britische JISC bietet nützliche Quellen, Veranstaltungen und aktualisierte Blogs zur DSGVO
- Die UCISA hat ein Best-Practice-Dokument zur DSGVO mit praktischen Schritten und Fallstudien veröffentlicht
- Die International Association of Privacy Professionals (IAPP) betreibt einen guten (kostenlosen) wöchentlichen Newsletter über die Entwicklungen im europäischen Datenschutz
- Die IAPP stellt auch eine nützliche Übersicht der Anbieter von Datenschutz-Tools (PDF) zur Verfügung
- Amazon Web Services unterhält ein eigenes DSGVO-Zentrum

BIOGRAPHIEN

Stephan Geering

Konzernweiter Datenschutzbeauftragter

- Konzernweite Verantwortung für die Einhaltung der Datenschutz- und Sicherheitsgesetze
- Leiter konzernweiter Datenschutz/DSGVO-Umsetzungsprogramm
- Dem leitenden Justitiar unterstellt; Mitglied der Rechtsabteilung bei Blackboard
- In London ansässig

Stephans Hintergrund:

- Anwalt/stellvertretender Leiter einer Schweizerischen Kantonsdatenschutzbehörde (2002-2008)
- LLM-Studiengang am University College London (2008-2009)
- Stellvertretender Leiter der Group Privacy bei Barclays (2010-2012)
- EMEA-Regionalleiter Data Privacy Operations bei der Citigroup (2012-2014)
- Leitender Datenschutzbeauftragter für die Räume EMEA und APAC bei der Citigroup (2014-2017)
- CIPP/E-zertifiziert

Rebecca McHale

Leitende Informationssicherheitsbeauftragte

- Leitet den Bereich Sicherheitsstrategie für Produkte und Infrastruktur
- Überwacht die Cybersicherheitstrategie bei Blackboard
- Ist dem leitenden Produktverantwortlichen unterstellt
- In Washington, D.C., ansässig.

Rebeccas Hintergrund:

- Bei Blackboard seit 2016; jüngste Projekte: Zusammenlegung der Sicherheitsteams und Stärkung der Rolle der Sicherheitsorganisation innerhalb des Unternehmens
- Master in Diskreter Mathematik und Computeranwendungen am Royal Holloway der University of London
- Zuvor Leiterin der Abteilung Cyber Programs bei Novetta und CSRA für US-Behörden und gewerbliche Kunden – z. B. US-Außenministerium, Transportsicherheitsbehörde (TSA) und Federal Deposit Insurance Corporation (FDIC)

WEITERE INFORMATIONEN

Weitere Informationen finden Sie auf unserer speziellen Community-Seite Datenschutz und Sicherheit.

Wir betreiben auch einen Datenschutz-Newsletter. Wenn Sie unseren Newsletter erhalten möchten oder Fragen bzw. Anmerkungen zu diesem White Paper haben, kontaktieren Sie uns bitte über privacy@blackboard.com.

Quellen

1 Siehe Abschnitt „Nützliche Quellen zur DSGVO“ am Ende mit einer detaillierteren Orientierungshilfe zur DSGVO.

2 Wir bevorzugen den Begriff „personenbezogene Informationen“ anstelle von „personenbezogene Daten“, verwenden ihn aber im gleichen Sinn und Umfang wie „personenbezogene Daten.“

3 Der Datenverantwortliche ist die Organisation, die die Mittel und Zwecke der Verarbeitung personenbezogener Daten festlegt (wie und warum personenbezogene Informationen verwendet werden).

4 Siehe Abschnitt „Unsere Rolle und die Rolle Ihrer Organisation gemäß der DSGVO“.

5 Siehe Abschnitt „Entmystifizierung der DSGVO“ unten für weitere Informationen zu Datenübermittlungen.

6 Siehe „An introduction to the Data Protection Bill“ (Einführung in das Datenschutzgesetz)” der britischen Datenschutzbehörde für einen nützlichen Überblick über das Gesetz.

7 Siehe auch die Blogbeiträge der britischen Datenschutzbehörde zum Thema DSGVO-Mythen.

8 Siehe auch die WP29-Leitlinien (im Entwurf) bzgl. Einwilligungen gemäß Verordnung 2016/679 (WP259) und die Orientierungshilfe der britischen Datenschutzbehörde zum Thema Einwilligungen.

9 WP29-Leitlinien über Verletzung des Schutzes personenbezogener Daten gemäß Verordnung 2016/679 (WP250überarb.01).

10 Siehe auch Abschnitt „Datenübermittlungen“.

11 Siehe z. B. „Preparing for the GDPR – 12 steps to take now“ (Vorbereitung auf die DSGVO – 12 Schritte, die Sie jetzt unternehmen müssen“ der britischen Datenschutzbehörde (PDF).

12 Siehe auch Abschnitt „Entmystifizierung der DSGVO“.

13 Siehe Abschnitt „Nützliche Quellen zur DSGVO“.

14 Für weitere Informationen über den konzernweiten Datenschutzbeauftragten und die leitende Informationssicherheitsbeauftragte siehe Abschnitt „Biographie“.

15 Im Rahmen des EU-US-Privacy-Shield-Zertifizierungsprojekts haben wir bereits die erforderlichen DSGVO-Vertragsbestimmungen in viele unserer Verträge mit unseren Dienstleistern (Unterauftragsverarbeitern) aufgenommen, die Zugriff auf personenbezogene Informationen aus der EU haben.

16 Bitte beachten Sie, dass nicht alle Produktanforderungen für alle Produkte gelten. Einige Produkte haben beispielsweise keine Benutzeroberfläche, die den Kunden eine Verlinkung auf ihre Datenschutzrichtlinien/-erklärungen ermöglichen würde.

17 Siehe Abschnitt „Sicherheit“ für weitere Informationen.

18 Wenn ein Netzwerk oder System mit dem Internet verbunden ist, hat der physische Standort der Daten so gut wie keine Auswirkungen auf Sicherheitsbedrohungen. Siehe White Paper des Amazon Web Services (AWS)“Data Residency AWS Policy Perspective“ (Perspektive der AWS-Data-Residency-Richtline)”(insbesondere Seite 2 und 3) für überzeugende Argumente gegen die Datenlokalisierung.

19 Zum Zeitpunkt der Erstellung dieses Dokuments.

20 Siehe AWS-Compliance-Programme für die vollständige Liste der Zertifizierungen und Gesetzeskonformität.

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

22 Art. 33 und 34 DSGVO.

23 Für eine Erläuterung der Rolle des Datenverarbeiters siehe Abschnitt „Unsere Rolle und die Rolle Ihrer Organisation gemäß der DSGVO“.

24 Siehe Abschnitt „Entmystifizierung der DSGVO“ oben für weitere Informationen zum zeitlichen Ablauf und zur Meldepflicht bei Datenschutzverstößen.

25 Siehe auch Abschnitt „Verträge mit Kunden“.