BlackBerry

Warum die EU-Datenschutz-Grundverordnung (GDPR) wichtig ist und was Sie tun müssen, um sie in den Griff zu bekommen

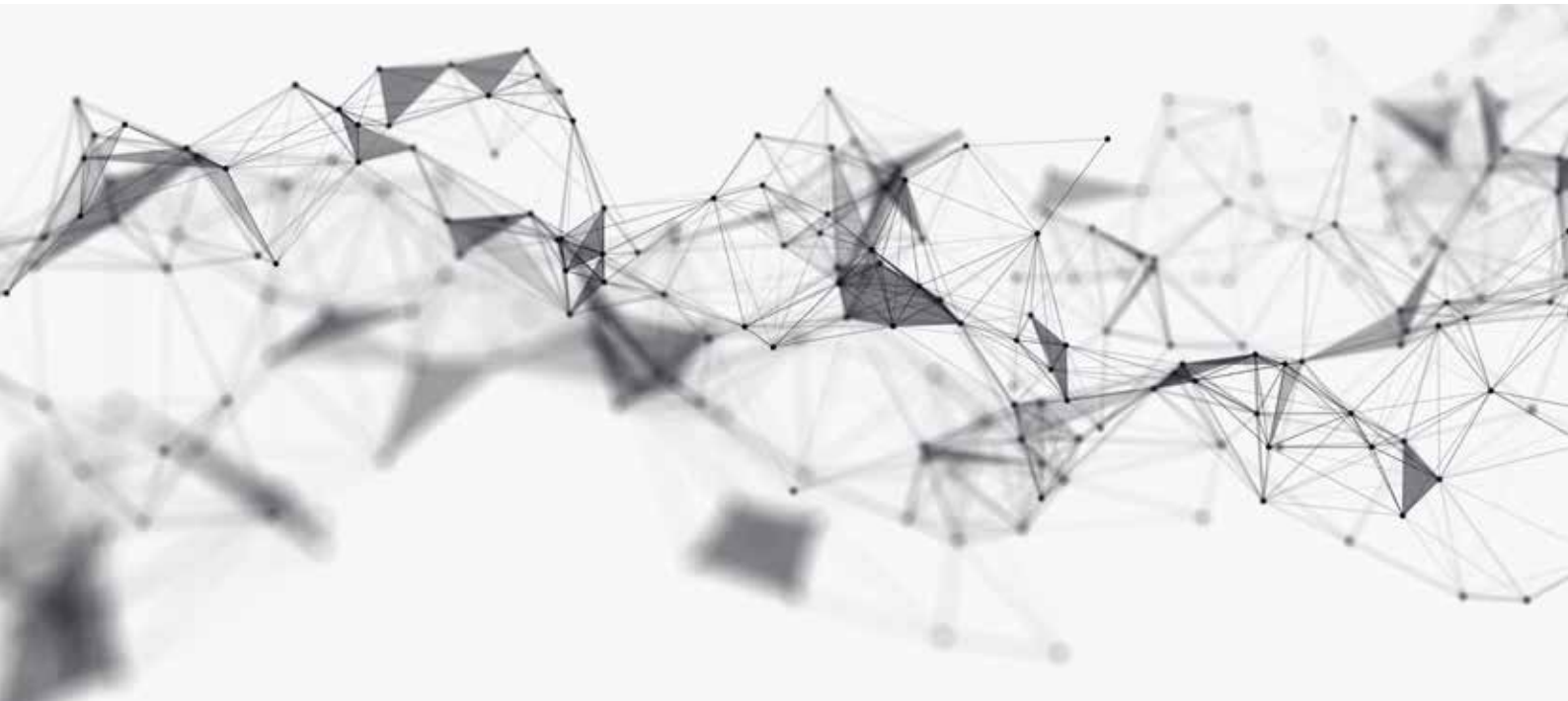
CIO
Strategic Marketing Services

Warum die EU-Datenschutz-Grundverordnung (GDPR) wichtig ist und was Sie tun müssen, um sie in den Griff zu bekommen

Erfahren Sie alles Wissenswerte zur neuen EU-Datenschutz-Grundverordnung (GDPR), den zentralen Regelungen, Geldbußen und sinnvollen Verfahren für den Arbeitsalltag

Die europäische Datenschutz-Grundverordnung (GDPR – General Data Protection Regulation) ist ein Meilenstein in der Geschichte des Datenschutzes. Sie tritt im Mai 2018 in Kraft und wird den Umgang mit personenbezogenen Daten drastisch verändern. Ob Unternehmen, Regierungen oder der öffentliche Sektor – jeder, der Daten von Bürgern der EU verarbeitet, ist von der Neuregelung betroffen. Dies gilt auch für Unternehmen mit Sitz in der EU, unabhängig vom Verbraucher und Standort. Spätestens jetzt heißt es, die eigene Datenverwaltung zu überdenken und sinnvoll vorzusorgen.

Viele der datenschutzrechtlichen Konzepte und Prinzipien von GDPR sind im Großen und Ganzen nicht viel anders als auch bisher unter der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), deren Vorschriften in Deutschland mit dem deutschen Bundesdatenschutzgesetz (BDSG) umgesetzt wurden. Wer sich im Unternehmen schon bisher um den Datenschutz gekümmert hat, sollte auch in Zukunft trotz der höheren Sanktionen nicht viel zu befürchten haben.



Einführung

Die GDPR muss im Gesamtkontext der bisherigen Datenschutzverordnungen gesehen werden. Europa hat seit über vier Jahrzehnten Gesetze zum Datenschutz erlassen. Die Datenschutzrichtlinie von 1995 hat dazu beigetragen, Regeln für das Informationsmanagement zu definieren. Diese Regeln wurden allerdings außerhalb von Deutschland kaum eingehalten, waren nicht nachhaltig und passen nicht in unser digitales Zeitalter, in dem die meisten Geschäftsvorgänge und Prozesse elektronisch ablaufen.

Dennoch ist es auch für deutsche Unternehmen unumgänglich, ihre Datenschutzpraxis zu überprüfen und das Datenschutzmanagement bis zum 25. Mai 2018 nach den Vorgaben der DS-GVO anzupassen und weiterzuentwickeln. Dabei gibt es keine Musterlösung, da jedes Unternehmen durch sein eigenes Geschäftsmodell auch unterschiedliche Datenverarbeitungsvorgänge durchführt.

Eines der wichtigsten Ziele der GDPR ist die EU-weite Harmonisierung der Regelungen. Die bisherigen Gesetze waren in ihrem Umfang begrenzt und die Geldbußen lächerlich gering. Außerdem gingen einzelne EU-Mitgliedsstaaten eigene Wege bei der Auslegung der Richtlinie. Die GDPR verhindert zukünftig diese Sonderwege. Hier noch ein wichtiger Hinweis: Auch Großbritannien ist von der Neuregelung betroffen. Denn die GDPR tritt in Kraft, bevor das Land die EU verlässt.

Eine zentrale Regelung ist, dass es für die Datenverwendung einer ausdrücklichen Einwilligung bedarf: Daten von Personen dürfen nur für den vereinbarten Zweck verwendet werden. Die Datendefinition ist sehr breit angelegt und umfasst nicht nur Namen, Adressen, E-Mails und Telefonnummern, sondern auch Social Media Updates, Bilder und IP-Adressen.

Unternehmen müssen das „Recht auf Löschung“ garantieren können und Informationen über Einzelpersonen auf Anfrage löschen.

Außerdem drohen bei einem Verstoß gegen die GDPR zukünftig viel höhere Bußgelder. Bis zu 20 Millionen Euro oder – falls höher – vier Prozent des jährlichen weltweiten Umsatzes. In der Summe können das sehr schnell mehrere Hundertmillionen sein. In der Spitze sogar Strafen in Milliardenhöhe. Geldbußen in dieser Größenordnung sind in Europa bisher unbekannt.

Unterschätzen Sie auch nicht den Imageschaden, der mit einem Verstoß gegen den Datenschutz einhergeht. Reputationsschäden übersteigen oftmals sogar die Geldbußen. Unternehmen wie TalkTalk, Target, Sony und Yahoo mussten diese bittere Erfahrungen schon machen. Sie standen allesamt wegen ihres Umgangs mit dem Datenschutz wochenlang in den Medien. Die finanziellen Auswirkungen waren mitunter erheblich: Der Hackerangriff auf die E-Mail-Konten von Yahoo war der Grund dafür, warum Verizon bei der Übernahme von Yahoo 350 Millionen Dollar weniger zahlen musste.

Mit der GDPR müssen Unternehmen auch einen Datenschutzbeauftragten bestellen, der auf die Einhaltung der Richtlinien achtet, Prozesse überprüft und Aktionspläne erstellt. Dabei kann der Datenschutzbeauftragte sowohl ein interner Mitarbeiter als auch ein externer Dienstleister sein.

Aber es gibt auch eine gute Nachricht: Wenn Sie jetzt überlegt handeln, können Sie mit den richtigen Tools Ihre Prozesse datenschutzkonform gestalten. So werden Sie auch für die Zukunft nicht nur der neuen Verordnung gerecht, sondern erhalten auch wertvolle Einblicke in Ihre Unternehmensdaten. Nutzen Sie die Chance, sich als verantwortliches Unternehmen zu profilieren, das Wert auf Datenschutz legt und sichern Sie sich damit einen echten Wettbewerbsvorteil.

Zusammenfassung:

- Alle Mitgliedsstaaten der EU müssen die GDPR bis Mai 2018 in nationales Recht umsetzen.
- Die GDPR definiert eindeutig, wie mit den Daten von EU-Bürgern umzugehen ist. Unabhängig davon, ob der Firmensitz innerhalb oder außerhalb der Europäischen Union liegt.
- Vor der Verwendung der personenbezogenen Daten muss eine ausdrückliche Einwilligung vorliegen, die den Verwendungszweck spezifiziert.
- In der GDPR gehören auch Social Media Daten, Fotos, E-Mail-Adressen und sogar Computer-IP-Adressen zu den personenbezogenen Daten.
- Die Daten müssen über offene und gängige Dateiformate übertragbar sein.
- Das „Recht auf Löschung“, bei dem persönliche Daten gelöscht werden, muss garantiert sein.
- Unternehmen müssen für die Datenschutzbehörden einen Datenschutzbeauftragten benennen.
- Prozesse und Workflows müssen für einen „integrierten Datenschutz“ überarbeitet werden.
- Die GDPR fordert die Mitteilung von Datenverlusten innerhalb von 72 Stunden nach der ersten Erkennung von Vorfällen ein.
- Betroffene einer Datenschutzverletzung müssen informiert werden.
- Die GDPR ermöglicht drastische Strafen von bis zu 20 Millionen Euro oder – falls höher – vier Prozent des jährlichen weltweiten Umsatzes.

Die Bedeutung des Datenschutzes

Noch nie wurde so viel über die Bedeutung von Daten gesprochen. Kein Wunder. Fast jedes Unternehmen besitzt in irgendeiner Form personenbezogene Daten: Kundendaten, Mitarbeiterdaten oder Daten von Interessenten. Für Web-Giganten wie Google und Facebook bilden sie sogar das Fundament für den Geschäftserfolg.

Sensible Daten finden sich mittlerweile überall. Unternehmen speichern Informationen nicht nur auf mobilen Geräten, Desktop-Computern und Servern in Rechenzentren, sondern auch auf webbasierten Services von Dritten und in der Cloud. Die personenbezogenen Daten sichtbar zu machen und alle Vorschriften der GDPR einzuhalten, kann zur Herausforderung werden. Vor allem für globale Unternehmen, die meist mehrere Datenbanken, CRM-Systeme, Tabellenkalkulationen und andere Software über verschiedene Versionen, Betriebssysteme und Hardwareplattformen hinweg betreiben.

Auf den ersten Blick unscheinbare Daten wie Surfverhalten, Suchhistorie, Transaktionen, Präferenzen und Interessen werden in den Händen von Marketingprofis zu einem unschlagbaren Wettbewerbsvorteil. Auch bei Sicherheitsfragen setzen Unternehmen auf Datenanalysen. So lassen sich verdächtige Verhaltensweisen, die auf Betrug oder kriminelles Verhalten hindeuten, eindeutig identifizieren.

Im Zeitalter der Digitalisierung sind Daten so wertvoll wie nie. Doch nur für den, der sie zu nutzen weiß. Das reine Sammeln und Speichern von Informationen bringt keinen Mehrwert. Erst durch die Analyse und Weiterverarbeitung, durch das Entdecken von Mustern und Trends eröffnen sich große Chancen. Und große Risiken. In dem Maße, wie der Wert der Daten steigt, steigt auch das Risiko von Angriffen und Bedrohungen.

Die EU und der Datenschutz

Im Januar 2016 wurde berechnet, dass über 510 Millionen Menschen in Ländern leben, die von der Europäischen Union regiert werden – mehr als das Eineinhalbfache der Bevölkerung der Vereinigten Staaten. Bedenkt man, dass die GDPR nicht nur für EU-Mitglieder gelten wird, sondern für alle Unternehmen, die Daten unter ihrer Gerichtsbarkeit sammeln, kann man durchaus von einem erweiterten Geltungsbereich sprechen.

In der Vergangenheit wurden die europäischen Datenschutzregelungen von nationalen Datenschutzbehörden oft unterschiedlich ausgelegt. Ob vom britischen Information Commissioner's Office (ICO), der französischen Commission Nationale de l'Information et des Libertés (CNIL) oder dem deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) bzw. den einzelnen Länderorganisationen. Trotz aller Unterschiede gab es eine Gemeinsamkeit: Die Geldbußen waren im Vergleich zur Gewinnmarge zu gering. Nur selten betrugen die Strafen mehr als hunderttausend Euro.

Die CNIL verhängte beispielsweise eine Geldbuße von 100.000 Euro gegen Google für die unbefugte Erhebung von Daten, die für den Street View Service gesammelt wurden. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit brummte dem Suchriesen dafür eine Strafe von 145.000 Euro auf.

Wie die Anwälte von Pinsent Masons bemerkten: „Keiner von CNIL, der Hamburger Kommissar, der für Google in Deutschland zuständig ist, oder der ICO haben alle Befugnisse voll und ganz gegen die Unternehmen genutzt."

Selbst bei „prominenten" Fällen wie beispielsweise Talk Talk (2015) oder Sony PlayStation Network (2011) gab es kaum höhere Bußgelder. Angesichts jährlicher Einnahmen von Milliarden Dollar nur Peanuts.

Das wird sich mit der GDPR ändern. Eine kleine Rückstellung für den Fall einer Datenschutzverletzung reicht dann längst nicht mehr aus. Denn zukünftig können Geldbußen im Milliardenbereich angesiedelt sein. Rechnet man mögliche Imageschäden mit ein, kann eine Verletzung des Datenschutzes zu einer Frage der Existenz werden. Deshalb ist es wenig verwunderlich, dass die Drohung mit Strafen in dieser Größenordnung bei manchem globalen Unternehmen Besorgnis verursacht.

Ausdrückliche Einwilligung

Der Anwendungsbereich der Verordnung wird auf alle Verarbeitungen ausgeweitet, die sich an EU-Bürger richten und personenbezogene Daten von EU-Bürgern verarbeiten. Personenbezogene Daten – egal aus welchen Quellen – dürfen nicht länger ohne ausdrückliche Einwilligung genutzt werden. Und das auch nur für den benannten Zweck.

Das ist ein wichtiger Aspekt. Persönliche Daten sind schließlich „die“ Währung des Internets. Mit „kostenlosen“ Services wie Websuche, Cloud E-Mail oder sozialen Netzwerken bezahlen die Nutzer für scheinbar kostenfreie Dienstleistungen. Die GDPR schränkt den freien Fluss der persönlichen Daten ein und legt genau fest, wie Daten gesammelt, verwendet und geteilt werden dürfen.

Das Recht auf Vergessen

Das „Recht auf Vergessen“ ist elementar in einer Zeit, in der fast alle unsere Daten digital verfügbar sind. Ob mit oder ohne unsere Hilfe. Ob wir das wollen oder nicht. Und unabhängig davon, ob wir eine Breitbandverbindung benutzen, einen Computer oder das Telefon.

Konkreter als das „Recht auf Vergessen“ ist das „Recht auf Löschung“. Einzelpersonen können nach Artikel 17 der GDPR verlangen, dass ihre personenbezogenen Daten gelöscht und für die Weiterverarbeitung gesperrt werden.

Das Recht auf Löschung kann nur in Ausnahmefällen verweigert werden. Meistens im Zusammenhang mit der Freiheit der Meinungsäußerung, von Rechtsverfahren und der Forschung im öffentlichen Interesse. Die GDPR verpflichtet Datenverantwortliche dazu, dem Recht auf Löschung nachzukommen. Sie müssen sich zukünftig nachweislich bemühen, die Löschung relevanten Dritten mitzuteilen.

Das Recht auf Löschung ist zentraler Bestandteil der GDPR und in seiner Strenge ein wichtiges und sehr sichtbares Zeichen für die gesamte Gesetzgebung.

Und zwar immer dann, wenn

- die Daten nicht mehr nur für den ursprünglichen Zweck verwendet werden.
- die Zustimmung zurückgezogen wurde und kein berechtigter Anspruch für die Bearbeitung besteht.
- die betroffene Person noch minderjährig ist.
- die Daten rechtswidrig verarbeitet wurden.
- keine gesetzliche Verpflichtung für eine Aufbewahrung besteht.

Benachrichtigung bei Datenverlust

Ein weiterer, sehr wichtiger Aspekt der GDPR ist die sogenannte Benachrichtigung bei Datenverlust. Nach der neuen Regelung müssen die Datenverantwortlichen innerhalb von 72 Stunden die Datenschutzbehörde über einen Datenverlust informieren. Die Behörde berät dann darüber, welche Informationen veröffentlicht werden und was dem Kunden offengelegt werden muss.

Einige US-Bundesstaaten haben die Benachrichtigungspflicht schon eingeführt. Die Wirksamkeit zeigt sich dort sehr deutlich. Die mediale Aufmerksamkeit sorgt zwar für einen mehr oder weniger großen Imageverlust beim betroffenen Unternehmen, sie bietet aber die Möglichkeit, Transparenz in die Vorgänge zu bringen und Trends zu erkennen. So können ähnliche Angriffe auf Unternehmen verhindert werden.

Eine Benachrichtigung an die Datenschutzbehörde muss mindestens die personenbezogene Datenverletzung, den Umfang des Datenverlustes, die Kontaktdaten des Datenschutzbeauftragten, die wahrscheinlichen Konsequenzen des Verstoßes und die Art und Weise, wie dies behandelt wird, beschreiben.

Unternehmen müssen also ihre Prozesse und ihren Umgang mit Daten so gestalten, dass sie im Bedarfsfall Sicherheitsverletzungen schnell identifizieren und einen sinnvollen Aktionsplan starten können.

Das Ausmaß der Herausforderung ist enorm. Mehr als die Hälfte der befragten Unternehmen glaubten, dass sie innerhalb eines Jahres von erfolgreichen Cyberangriffen getroffen werden, so ein Bericht. Die durchschnittliche Anzahl von Tagen, die Angreifer vor der Erkennung in Netzwerken verbringen, beträgt nach einem anderen Bericht etwa 200. Obwohl die Verlustmitteilung auf die Entdeckung des Verlusts datiert ist, erhöhen Anzeichen für einen zu laxen Umgang bei der Erkennung dieser Verstöße wahrscheinlich die Strafen.

Datenschutzbeauftragte

Die GDPR verlangt, dass Datenschutzbeauftragte bestellt und der zuständigen Aufsichtsbehörde gemeldet werden müssen. In größeren Unternehmen ist mit dieser Funktion oft eine besondere Position mit einem unterstützenden Team verbunden. In kleineren Unternehmen fällt der Datenschutz oftmals in den Aufgabenbereich eines Einzelnen: Mitarbeiter aus der Rechtsabteilung bieten sich hier an, aber auch Mitarbeiter aus der IT-Abteilung. Denn technisches Wissen ist von großem Vorteil, wenn es darum geht, Daten zu schützen und zu überwachen.

In deutschen Unternehmen gibt es schon seit vielen Jahren die Position des Datenschutzbeauftragen. Andere Länder werden an dieser Stelle mit der Neuregelung größere Probleme haben.

Wenn allerdings die Kernaktivitäten auf der Datenverarbeitung liegen (zum Beispiel Wertpapierhändler oder Kreditinstitute) oder wenn es sich um sensible Daten handelt (zum Beispiel Patientenakten, Sozialhilfedaten oder das Strafregister), dann sind absolute Spezialisten gefragt.

Der Datenschutzbeauftragte kann eine externe Person sein, die im Auftrag des Datenverantwortlichen tätig wird. Allerdings muss sie auf die IT-Systeme zugreifen können und über fundiertes Wissen bezüglich der Datengesetze verfügen.

Zumindest in Deutschland bleibt der **betriebliche Datenschutzbeauftragte** für die meisten Unternehmen voraussichtlich unabdinglich.

Grenzüberschreitende Datentransfers

Deshalb gilt die GDPR auch bei Datenübermittlung an Drittländer. Eine Datenübermittlung über die EU-Grenzen hinaus ist daher nur erlaubt, wenn die strikten Regelungen und Bedingungen der GDPR eingehalten werden. Die Übermittlung der Daten an ein Drittland, welches kein angemessenes Datenschutzniveau bietet, muss verboten werden, es sei denn, bestimmte Ausnahmen liegen vor. Die Europäische Kommission stellt hierfür fest, ob ein Drittland oder ein Gebiet eines Drittlandes ein angemessenes Datenschutzniveau (mehr) bietet.

Von der strengen Regelung zum Wettbewerbsvorteil

Bringt die GDPR auch Vorteile? Tatsächlich ja. Die GDPR wird die unverantwortliche und rücksichtslose Nutzung von personenbezogenen Daten stark reduzieren und unser Bewusstsein für die Verwendung von Daten (und für den Missbrauch) wachsen lassen.

Die GDPR kann auch ein Motor für die Transformation von Unternehmen sein. Denn die Umsetzung der Regelung erfordert neue Datenverwaltungsstrukturen. Die Überarbeitung von Workflows sorgt für mehr Effizienz und eine zentrale Plattform für datengesteuerte Einblicke. Sie können die GDPR als ein lästiges Übel sehen und nur rein defensive Maßnahmen ergreifen. Oder aber die GDPR als Chance für eine breitere Veränderung sehen und Ihre Geschäftsprozesse zukunftsfähig machen.

Auch Marketingabteilungen profitieren vom Datenschutz. Dank der ausdrücklichen Einwilligung der Kunden und der rechtssicheren Verwendung der Daten, kann sich die Kundenbeziehung nachhaltig verbessern. Denn der Kunde weiß nun seine persönlichen Daten in sicheren Händen.

Der Umgang mit den neuen Datenschutzanforderungen ist sicherlich eine Herausforderung. Allerdings ist es möglich, mit angepassten Prozessen und einer robusten Datenplattform sensible Daten nachhaltig zu schützen.

Was nun?

Wenn Sie noch nicht damit begonnen haben, Ihre GDPR-Konformität zu planen, sollten Sie umgehend damit anfangen. Die GDPR tritt bereits im Mai 2018 in Kraft, sodass Service-Level-Vereinbarungen jetzt notwendig sind, um diese neuen Maßnahmen zu berücksichtigen.

Unternehmen sind verunsichert, weil sie – oft unwissentlich – ganze Deponien mit redundanten, veralteten und irrelevanten Daten angelegt haben. Da die Speicherung meist recht günstig ist, konnten Datenberge ins Unermessliche wachsen.

Führen Sie daher als erstes ein umfassendes Datenaudit durch. Mit Lückenanalyse und Überprüfung von Prozessen und Workflows unter einem sogenannten Data Protection Impact Assessment (DPIA).

Bringen Sie Ordnung in Ihre Daten mit Routinen zum Löschen oder zum Verschieben. Konzentrieren Sie sich auf Ihre Kernprozesse. So erfahren Sie schnell, welche Daten wichtig sind, wo sich Daten überschneiden und ob sie repliziert werden.

Führen Sie einen Vorher-Nachher-Vergleich durch. Betrachten Sie, wie Sie aktuell mit Daten umgehen, wo es Optimierungsbedarf gibt und wie der ideale Umgang aussieht.

Überprüfen Sie Ihre Sicherheitsprozesse regelmäßig und führen Sie sorgfältige Tests durch. Vergessen Sie auch bitte nicht, einen Notfallplan zu erarbeiten und Ihre Mitarbeiter für den Ernstfall zu schulen. Im Falle einer Verletzung ist schnelles Handeln gefragt. Vor allem die Kommunikation sollte eindeutig geregelt sein. Denn die Benachrichtigung von Mitarbeitern und Medien muss dann reibungslos funktionieren.

Wie kann BlackBerry Ihnen helfen?

Stellen Sie sich den Herausforderungen der GPDR. Es geht darum, Daten zu sichern, Bedrohungen zu minimieren, Datenbestände zu prüfen und Vorfälle zu bewerten.

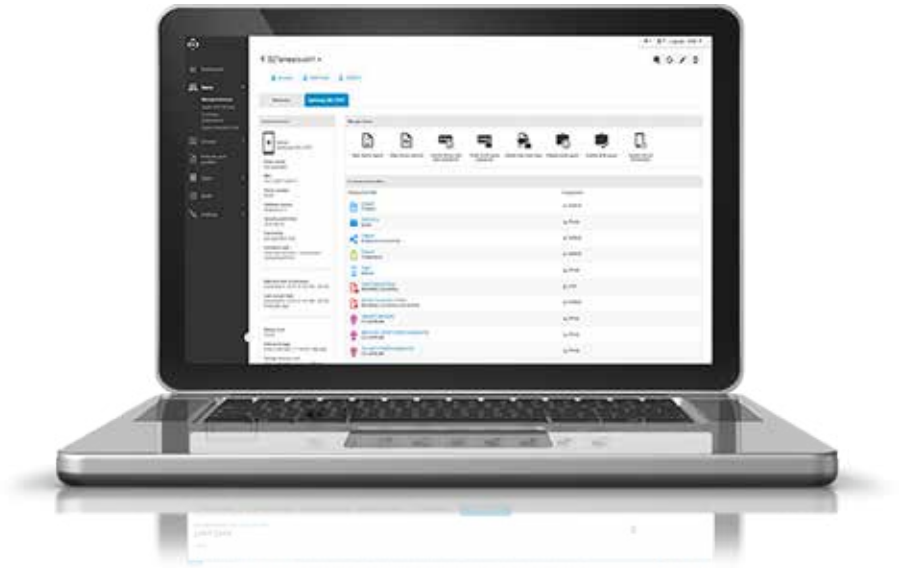
Ein Datenschutzbeauftragter mit viel Fachverständnis hilft dabei. Ebenso wie sichere Prozesse und moderne technische Lösungen. Mit seiner langjährigen Expertise und seinem umfassenden Sicherheitsportfolio steht Ihnen BlackBerry auch bei den komplexesten Sicherheitsfragen zuverlässig zur Seite.

Diese Anforderungen sollten Sie mindestens erfüllen:

- Sichtbarkeit aller Endpunkte, die mit personenbezogenen Daten verbunden sind.
- Starke Analysefunktionen für ein besseres Verständnis der Datennutzung.
- Eine sichere Netzwerkumgebung.
- Verschlüsselung von Daten auf dem Gerät und während der Übertragung.
- Ein Identity Management System, das alle Nutzer des Netzwerks authentifiziert.
- Eine umfassende digitale Rechteverwaltung.
- Den umfassenden Schutz aller Endpunkte unabhängig von Gerätetyp und Betriebssystem.
- Schutz für Mitarbeiter und externe Dienstleister.
- Umfassender Support für ein Unternehmen mit praktischer Erfahrung in allen genannten Anforderungen.

BlackBerry verfügt über ein umfassendes Portfolio von Tools und Services, die Ihnen dabei helfen, den Anforderungen der GDPR gerecht zu werden.

Die **BlackBerry Enterprise Mobility Suite** bietet Ihnen flexible Optionen für mehr Sicherheit und Produktivität und sorgt damit gleichzeitig für die Einhaltung der GDPR. Je nach den individuellen Anforderungen Ihres Unternehmens können Sie nach Bedarf weitere Funktionen hinzufügen.



Folgende Werkzeuge sind in der Enterprise Mobility Suite enthalten:

Unified Endpoint Management (UEM) hilft Ihnen dabei, eine der größten Herausforderungen zu bewältigen: die massive Verbreitung von Gerätetypen, von Smartphones über Desktops und Laptops, Tablets oder E-Readern bis hin zu intelligenten Wearables und verbundenen Endpunkten. BlackBerry UEM unterstützt die neuesten Container-Technologien – Android Enterprise, Samsung Knox und BlackBerry Dynamics.

BlackBerry Software bietet Ihnen Verschlüsselung, die Datensicherung über Netzwerke, auf Geräten, rund um Apps und in Dateien. Besonders wichtig für die Einhaltung der GDPR ist die **Verschlüsselung auf dem Gerät und während der Übertragung**.

BlackBerry Work sorgt für sichere Kommunikation mit umfassendem Datenschutz sowohl für E-Mail als auch bei der Zusammenarbeit. Diese All-in-one Produktivitäts-App bietet Ihnen höchsten Bedienkomfort, um Multitasking zwischen geschäftlichen Apps möglich zu machen. Gleichzeitig verhindert ein sicherer Container unnötige Datenverluste.

BlackBerry Workspaces bietet eine sichere Dateisynchronisierung und gemeinsame Nutzung von Services mit Support für das Digital Rights Management (DRM) über jedes Gerät. Mit Workspaces können Sie verfolgen, wie Dateien geteilt werden – wichtig für die GDPR – und bestimmen, wer auf diese Dateien zugreifen kann, auch nachdem sie gesendet wurden.

BlackBerry Dynamics erweitert die Sicherheit, die in den eigenen Apps von BlackBerry verwendet wird. Dies schützt eigene und fremde Apps vor manipulierten Informationen und ermöglicht eine sichere gemeinsame Nutzung von Daten zwischen Apps und Anwendern.

BlackBerry Enterprise Identity ermöglicht Single Sign-on für Services von jedem Gerät und bietet Sicherheit mit schnellerem Zugriff auf gesicherte Apps.

Mit **BlackBerry 2FA** kann Ihre IT eine Zwei-Faktor-Authentifizierung für einen sicheren Zugriff bereitstellen sowie den Zugriff auf die VPN-Infrastruktur und damit die Schlüsseldaten schützen.

BlackBerry bietet Ihnen eine breite Palette an Beratungsdienstleistungen für Cybersicherheit und kann Ihnen bei der Planung, Bereitstellung und Verwaltung Ihres GDPR-Projekts helfen.

Weitere Informationen

Die Top 10 operational impacts of the GDPR sind eine hervorragende, leicht zu lesende Anleitung in englischer Sprache, die von der International Association of Privacy Professionals (IAPP) veröffentlicht wurde.

CIO
Strategic Marketing Services

Autor: Martin Veitch ist Editorial Director von IDG Connect.
Seit mehr als 25 Jahren schreibt er über Geschäfts- und Technologiethemen.

BlackBerry

Stand: 05/17