KPMG

Der Weg zum effektiven Datenschutz

Der richtige Umgang mit der neuen Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union.

kpmg.ch/cyber

Das Europaparlament hat die neue EU Datenschutz-Grundverordnung (DS-GVO) am 14. April 2016 verabschiedet, welche die umfangreichste Revision in den Bereichen Privatsphären- und Datenschutz der letzten Jahrzehnte darstellt. Da die DS-GVO grosse Auswirkungen auf Organisationen und Unternehmen weltweit hat, sind fundamentale Änderungen in der Art und Weise notwendig, wie diese mit dem Thema Datenschutz zukünftig umgehen.

Die beschlossene DS-GVO ist in zwei Jahren anwendbar. Dies bedeutet, dass auch Ihr Unternehmen ab Anfang 2018 die Regeln der neuen Datenschutz-Grundverordnung vollumfänglich erfüllen muss. Einige der neuen Bestimmungen erfordern substanzielle Veränderungen in ihrem Unternehmen – daher ist nun der richtige Zeitpunkt, um in dieser Hinsicht aktiv zu werden.

Mit welchen Auswirkungen muss Ihr Unternehmen rechnen?

Bis vor Kurzem wurde dem Thema Datenschutz in der EU nur wenig Aufmerksamkeit gewidmet. Die möglichen Bussen für Regelverstösse waren beschränkt und Massnahmen zur Durchsetzung sah man nur sporadisch. Dies ändert sich mit der neuen DS-GVO jedoch grundlegend, dies insbesondere aus drei Gründen:

Hohe Reputationsrisiken

Durchsetzungsmassnahmen von Datenschutzbehörden werden zunehmen. Dadurch werden Datenschutzverletzungen schneller an die Öffentlichkeit gelangen. Das Reputationsrisiko von Unternehmen wird damit umso höher und realer.

Weiter Anwendungsbereich

Mit dem Inkrafttreten der DS-GVO erweitert sich die geographische Reichweite auf «alle Unternehmen und Organisationen, die in der EU ansässigen Personen Güter oder Dienstleistungen anbieten» und «Unternehmen und Organisationen, die das (Online-)Verhalten von diesen Personen überwachen». Dies bedeutet, dass auch Ihr Unternehmen künftig unter die EU-Datenschutzregulierung fallen könnte, auch wenn dies bislang nicht der Fall war.

Hohe Bussen

Wer es versäumt Datenschutz-Bestimmungen angemessen umzusetzen, kann mit hohen Bussen geahndet werden. Die DS-GVO sieht Bussen von bis zu 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes vor, je nachdem welche Summe höher ist. Dies stellt im Vergleich mit den eingeschränkten Sanktionsmöglichkeiten des bisherigen Systems eine weitreichende Änderung dar. Es ist deshalb wichtiger als je zuvor, dass die Datenschutzbestimmungen in Ihrem Unternehmen adäquat umgesetzt werden.

Welche fundamentalen Veränderungen sind zu erwarten?

Mit der Datenschutz-Grundverordnung treten zahlreiche neue Bestimmungen in Kraft, die wichtigsten werden nachfolgend kurz umrissen:

Datenschutz beim Design und als Standard

- Bereits unter den bisherigen Datenschutzregeln waren Unternehmen verpflichtet, «angemessene technische und organisatorische Massnahmen» zum Schutz persönlicher Daten zu treffen. Die Datenschutz-Grundverordnung verpflichtet Unternehmen künftig neu auch dazu, den Nachweis zu erbringen, dass die getroffenen Massnahmen konstant überprüft und aktualisiert werden.
- Zusätzlich müssen Unternehmen nachweisen, dass Datenverarbeitungsvorgänge schon durch das Design angemessene Schutzmassnahmen aufweisen und dass grundsätzlich nur dort persönliche Daten verarbeitet werden, wo dies tatsächlich notwendig ist.

Datenschutz-Folgenabschätzung

- Die Datenschutz-Grundverordnung verpflichtet Unternehmen zur Durchführung einer Datenschutz-Folgenabschätzung hinsichtlich der geplanten Verarbeitungsvorgänge, falls es wahrscheinlich erscheint, dass die Verarbeitung hohe Risiken für die Privatsphäre zur Folge hat.
- Falls das Resultat der Datenschutz-Folgenabschätzung ein hohes Risiko ergibt, muss vor Beginn der Verarbeitung die zuständige Datenschutzbehörde konsultiert werden.

Obligatorischer Datenschutzbeauftragter

- Die Datenschutz-Grundverordnung macht in vielen Situationen die Ernennung eines Datenschutzbeauftragten obligatorisch.
- Der Datenschutzbeauftragte muss über Fachwissen bezüglich Datenschutzgesetzgebung und -praxis verfügen sowie seine Rolle genügend unabhängig ausüben können.
- Die Rolle des Datenschutzbeauftragten darf von einem externen Dienstleistungsunternehmen ausgeübt werden.

Verpflichtung zur Meldung von Datenschutzverletzungen

- Im Rahmen der Datenschutz-Grundverordnung sind neu alle Unternehmen dazu verpflichtet, Datenschutzverletzungen zu melden.
- Unternehmen müssen der zuständigen Datenschutzbehörde im Falle einer meldepflichtigen Datenschutzverletzung innerhalb von 72 Stunden Meldung erstatten.
- Verletzungen personenbezogener Daten müssen nicht gemeldet werden, wenn es unwahrscheinlich ist, dass die betreffende Datenschutzverletzung Risiken für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.
- Im Falle einer Datenschutzverletzung mit hohen Risiken für die Privatsphäre müssen auch die betroffenen Personen informiert werden.

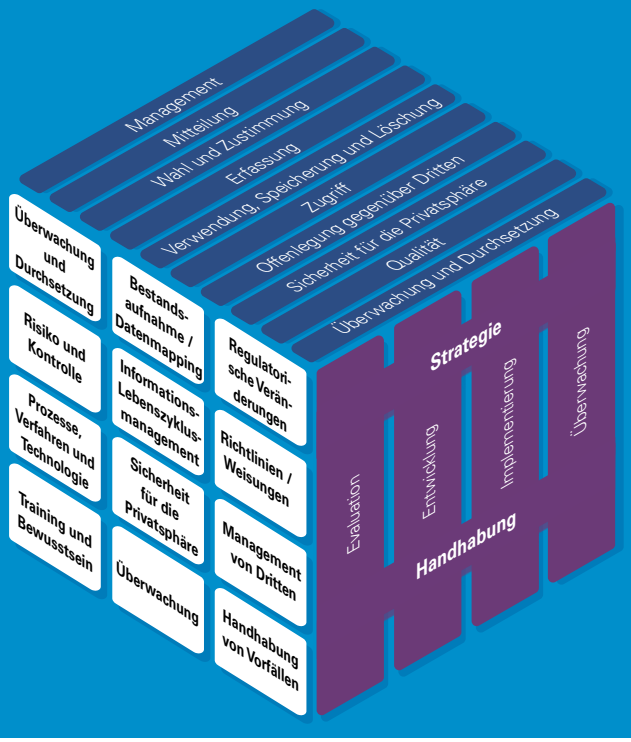
Zusätzlich zu den hier umrissenen neuen Bestimmungen, bleiben zahlreiche der bereits unter dem alten Regelsystem geltenden Datenschutzbestimmungen in ähnlicher oder ergänzter Form bestehen (z.B. Einschränkungen des grenzüberschreitenden Datenverkehrs, Zustimmungserfordernisse, Bestimmungen über die Zugangsrechte betroffener Personen etc.). Die Datenschutz-Grundverordnung verpflichtet Unternehmen zur Implementierung von angemessenen und massgeschneiderten Rahmenwerken zur Sicherstellung des Datenschutzes sowie zu einem entsprechenden Risikomanagement. Eine blosse Aktualisierung bestehender, unternehmensinterner Datenschutz-Weisungen genügt somit nicht. Vielmehr sind Prozesse und Kontrollmassnahmen zur Gewährleistung des Datenschutzes erforderlich. Die Datenschutz-Grundverordnung verlangt die Implementierung und die Pflege revisionsgerechter Datenschutz-Massnahmen. Wir unterstützen Sie bei der Implementierung der notwendigen Massnahmen und bei der Sicherstellung der adäquaten Umsetzung.

Was ist der nächste Schritt?

Um zu bestimmen, welche Auswirkungen die Datenschutz-Grundverordnung auf Ihr Unternehmen hat, sollte zunächst die allgemeine Situation Ihres Unternehmens in Sachen Datenschutz evaluiert werden. Diese Evaluation nehmen wir mittels unserem bewährten Datenschutz Governance Rahmenwerk vor.

Das Datenschutz Governance Rahmenwerk von KPMG basiert auf der folgenden Vorgehensweise: (1) Evaluation, (2) Entwicklung, (3) Implementierung und (4) Überwachung. Auf Basis bekannter Business- und IT-Governance-Bausteine bieten die 12 Komponenten des Rahmenwerks eine pragmatische Struktur für den Umgang mit dem Thema Datenschutz in Ihrem Unternehmen.

Das Datenschutz Governance Rahmenwerk



Damit können wir Ihnen auf jedem Schritt Ihres Weges hin zu einem verbesserten Datenschutz Unterstützung bieten. Nachfolgend präsentieren wir Ihnen einige unserer Dienstleistungen:

	Dienstleistung	Dienstleistungsbeschrieb
Evaluation	**Quick Scan DS-GVO**	Evaluation auf Basis der wichtigsten neuen Bestimmungen der Datenschutz-Grundverordnung im Vergleich zur bisherigen EU-Datenschutzrichtlinie. Die Evaluation zeigt die Bereitschaft bezüglich der neuen Bestimmungn der Datenschutz-Grundverordnung auf, einschliesslich entsprechender Empfehlungen. Diese Evaluation ist vor allem dann ideal, wenn in Ihrem Unternehmen bereits vor kurzem eine Datenschutz-Evaluation auf Basis der bisherigen Bestimmungen der EU-Datenschutzrichtlinie durchgeführt wurde.
Entwicklung	**Evaluation des Reifegrads bezüglich Datenschutz**	Diese Evaluation verschafft Ihnen einen Gesamtüberblick über den Reifegrad Ihres Unternehmens bezüglich Datenschutz. Die Resultate werden gemäss den 12 Komponenten des Rahmenwerks gruppiert. Diese Evaluation bietet eine perfekte Basis für die Einführung und die individuelle Anpassung des Datenschutz Governance Rahmenwerks ihres Unternehmens an die Datenschutz-Grundverordnung und andere internationale Datenschutzbestimmungen.
	Strategieentwicklung zur DS-GVO	Die Strategie für den Umgang mit den Anforderungen der Datenschutz-Grundverordnung umfasst einen Projektplan und eine Roadmap, die aufzeigen, welche Massnahmen getroffen werden müssen um in Ihrem Unternehmen den Datenschutz zu optimieren. Zusätzlich beschreibt die Roadmap ausführlich, welche Aktivitäten notwendig sind sowie den entsprechenden Zeitrahmen dafür. Eine Strategie für den Umgang mit den Anforderungen der Datenschutz-Grundverordnung ist eine wichtige Grundlage für eine strukturelle Optimierung des Datenschutzes in Ihrem Unternehmen. Diese Strategie stellt die Grundlage dafür dar, um den Anfoderungen der DS-GVO entsprechen zu können.
Implementierung	**Umsetzung von DS-GVO Massnahmen**	Bei der Umsetzung von Massnahmen bezüglich Datenschutz-Grundverordnung empfiehlt sich eine strukturierte Herangehensweise. Nutzen Sie dazu unsere branchenweit anerkannten Best-Practice-Vorgehensweisen und unsere bewährten Projektmanagementmethoden.
Überwachung	**Datenschutzzertifizierung/-bescheinigung**	Politische Entscheidungsträger, Geschäftspartner und Kunden verlangen zunehmend, dass Unternehmen einen Nachweis ihrer Anstrengungen im Bereich Datenschutz und Schutz der Privatsphäre erbringen. Eine Datenschutzzertifizierung empfiehlt sich besonders dann, wenn Ihr Unternehmen bereits heute adäquate Massnahmen zum Schutz der Privatsphäre umgesetzt hat. Die Erlangung eines entsprechenden Zertifikates stellt den Reifegrad und die Verantwortung Ihres Unternehmens in Sachen Privatsphäre und Datenschutz unter Beweis.

Was sind Ihre Vorteile?

Die Zusammenarbeit mit KPMG bietet Ihnen folgende Vorteile:

- Eine Datenschutz-Evaluation gibt den (internen) Anspruchsgruppen Ihrer Organisation Auskunft über Ihren **Reifegrad in Sachen Datenschutz**, und Ihnen klare und umsetzbare **Empfehlungen für eine allfällige Optimierung** des Umgangs mit dem Datenschutz insgesamt.
- Sie profitieren von einer bewährten Vorgehensweise im Bereich Datenschutz-Management. Unser Ansatz ist **pragmatisch, flexibel und skalierbar**, was Ihnen erlaubt, sich auf die Herausforderungen und Chancen zu fokussieren, die das Thema Datenschutz für Ihr Unternehmen mit sich bringt.
- Sie erhalten eine Übersicht über die allgemeine Praxis in Sachen Datenschutz in Ihrer Branche, basierend auf einem **Echtzeit-Benchmarking**.
- Nutzen Sie für die Durchführung von Evaluationen und für die (kontinuierliche) Überwachung unsere bewährten Governance-, Risikomanagement- und Compliance-Instrumente **(GRC)**.
- Eine **Kombination** dieser Aktivitäten z.B. **mit anderen Zertifizierungs-Aktivitäten sorgt für Kosteneffizienz**.
- Sie profitieren von einem multidisziplinären Beratungsteam bestehend aus **hochqualifizierten Fachexperten** mit viel praktischer Erfahrung bei der Durchführung von Datenschutz-Evaluationen und -Transformationen.
- Unsere Berater sind auf alle Aspekte des Datenschutzes spezialisiert, darunter: Rechtliche Fragen, Information Governance, Geschäftsabläufe, Sicherheitstechnologie und GRC-Instrumente.
- Die **weltweite Präsenz** von KPMG ermöglicht eine kosteneffiziente **Dienstleistungserbringung vor Ort**. KPMG verfügt über ein globales Netzwerk von über 152'000 Spezialisten in 56 Ländern, mit einer starken Präsenz in der EU sowie viel Erfahrung mit dem Thema Datenschutz in der EU.
- Die Beratung von KPMG dreht sich nicht nur um die Einhaltung gesetzlicher Vorschriften, sondern legt den Fokus auch auf die Evaluation, Umsetzung und auf die Überwachung adäquater Datenschutz-Massnahmen und -Prozesse.

Referenzen

KPMG kann eine umfangreiche Erfahrung in Sachen Datenschutz ausweisen. Unsere Berater haben Kunden aus verschiedenen Branchen weltweit dabei unterstützt, Datenschutzkonformität zu erreichen und diese zu wahren. Nachfolgend eine Auswahl unserer Kunden:

International tätige Schweizer Grossbank	International tätiges Technologieunternehmen	Internationales Pharmaunternehmen	Öffentlich-rechtliche Körperschaften
KPMG betreut und begleitet die Umsetzung des Programmes zur Gewährleistung der Vertraulichkeit von Kundendaten sowie weitere Initiativen der Bank im Bereich Privatsphäre und Datenschutz.	KPMG evaluiert die Strategie und Vorgehensweise zum Schutz der Richtlinien hinsichtlich Privatsphäre und Meinungsäusserungsfreiheit.	KPMG berät und unterstützt das Unternehmen bei der Optimierung des Kontrollsystems für grenzüberschreitenden Datenverkehr in Folge von Regulierungsänderungen.	KPMG führt im Auftrag von Datenschutzbehörden lokale Datenschutz-Überprüfungen durch.
2013 – 2016	**laufend**	**2015 – 2016**	**laufend**

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
8036 Zürich

kpmg.ch/cyber

Matthias Bossardt
Partner, Consulting

+41 58 249 36 98
mbossardt@kpmg.com

Jeffrey Bholasing
Manager, Consulting,
Head of Data Protection & Governance

+41 58 249 42 88
jeffreybholasing@kpmg.com

Thomas Bolliger
Partner, Consulting

+41 58 249 28 13
tbolliger@kpmg.com

Die hierin enthaltenen Informationen sind allgemeiner Natur und beziehen sich daher nicht auf die Umstände einzelner Personen oder Rechtsträger. Obwohl wir uns bemühen, genaue und aktuelle Informationen zu liefern, besteht keine Gewähr dafür, dass diese die Situation zum Zeitpunkt der Herausgabe oder eine künftige Situation akkurat widerspiegeln. Die genannten Informationen sollten nicht ohne eingehende Abklärungen und professionelle Beratung als Entscheidungs- oder Handlungsgrundlage dienen. Bei Prüfkunden bestimmen regulatorische Vorgaben zur Unabhängigkeit des Prüfers den Umfang einer Zusammenarbeit.

©2016 KPMG AG ist eine Konzerngesellschaft der KPMG Holding AG und Mitglied des KPMG Netzwerks unabhängiger Mitgliedsfirmen, der KPMG International Cooperative ("KPMG International"), einer juristischen Person schweizerischen Rechts. Alle Rechte vorbehalten.