GDPR-Grundlagen und wie PwC helfen kann

Datenschutz-grundverordnung – kurz und bündig

Strengere EU-Datenschutzbestimmungen angenommen

Die Datenschutzgrundverordnung (General Data Protection Regulation = GDPR) trat am 24. Mai 2016 in Kraft. Sie schafft einen neuen Rechtsrahmen, der die Datenschutzgesetze in den 28 Mitgliedstaaten der Europäischen Union (EU) vereinheitlicht und die bisherige EU-Datenschutzrichtlinie ersetzt. Mit der GDPR wird Europa und der übrigen Welt ein tiefgreifender regulatorischer Rahmen in Bezug auf Datenschutz und Privatsphäre bei der Verarbeitung personenbezogener Daten von EU-Bürgern auferlegt. Obwohl eine Umsetzungsfrist von zwei Jahren für Länder und Unternehmen festgelegt ist, gibt es viele neue und deutlich erhöht Anforderungen, die Organisationen vor Ablauf der Frist im Mai 2018 umsetzen sollten.

Sind Schweizer Unternehmen betroffen?

Im Vergleich zur bisherigen EU-Datenschutzrichtlinie ist die GDPR inhaltlich umfangreicher und findet bei deutlich mehr Organisationen Anwendung. Alle Organisationen, die in Europa aktiv sind, müssen der GDPR entsprechen. Dies umfasst auch jene Organisationen ohne Niederlassung in der EU, die aber Güter und Dienstleistungen an Personen in der EU anbieten oder dort Personen überwachen. So muss beispielsweise ein Schweizer Einzelhändler ohne Niederlassung in der EU, der aber seine Produkte an Kunden mit Sitz in der EU verkauft, der GDPR entsprechen.

Auf dem Weg zur Compliance

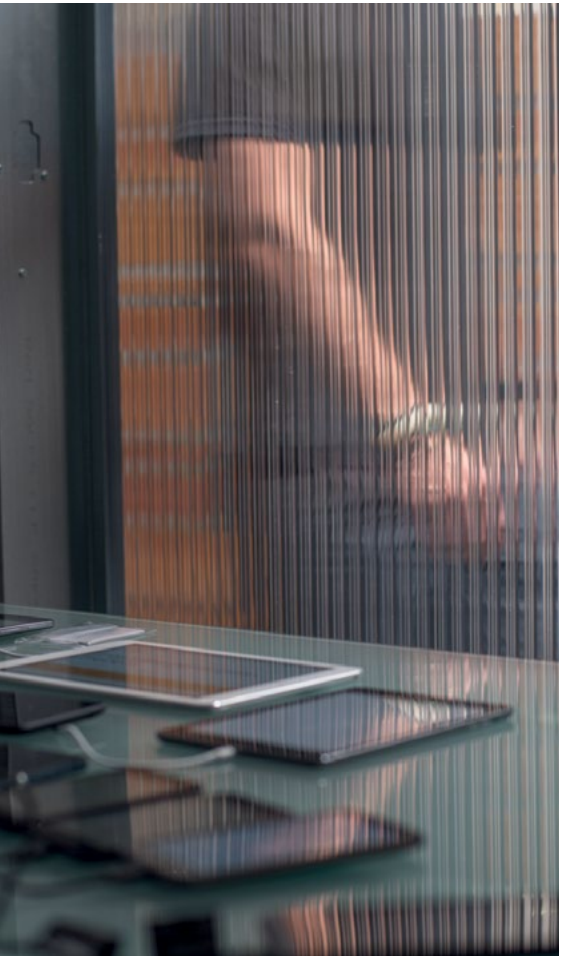
Die GDPR enthält eine Reihe neuer Regeln, die von Unternehmen fordern, ihre Systeme und Prozesse für den Datenschutz erneut zu überprüfen und zu aktualisieren. Gemeinsam legen diese neuen Regeln einen neuen «Weg zur Compliance» fest, den die Unternehmen befolgen müssen, um rechtlich weiterhin auf der sicheren Seite zu sein.

Es bestehen kaum Zweifel, dass die GDPR ein grosses Problem für viele Unternehmen darstellt. Dies gilt vor allem für jene, welche über grosse Datensammlungen mit Personendaten verfügen oder deren

pwc

Geschäftsmodell auf der kommerziellen Verwertung von personenbezogener Daten beruht. Der «Weg zur Compliance» beinhaltet viele komplexe Herausforderungen und zwingt Unternehmen schwierige Entscheidungen bezüglich ihrer Prioritäten zu treffen. Die Sicherstellung der Einhaltung der GDPR erfordert erhebliche Ressourceninvestitionen und viel Planung. Die harten Regulierungs- und Prozessrisiken sind beträchtlich, insbesondere für Unternehmen, die sensible personenbezogene Daten verarbeiten.

In einer Zeit mit vielen Rechtstreitigeiten müssen Unternehmen sicherstellen, dass ihre globalen Datenaustausch- und Übertragungsmodelle in der Lage sind, den hohen regulatorischen Anforderungen (der GDPR) zu genügen.



Warum sollten sich die CISO Sorgen machen?

Die Einführung der GDPR stellt die CISO vieler Organisationen auf der ganzen Welt vor zahlreiche neue Herausforderungen. Zu den zentralen Problemen gehören:

- Erweiterung der Definition der «personenbezogenen Daten»
  Gemäss der GDPR gehören zu den personenbezogenen Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person («Datensubjekt») beziehen.

  Diese Definition von personenbezogenen Daten ist wichtig, weil sie Daten beinhaltet, die auf den ersten Blick vielleicht nicht als persönlich einzustufen sind. IP-Adressen, Nutzer-IDs oder User-IDs, GPS-Daten (Global Positioning System), Cookies, Media Access Control(MAC)-Adressen, eindeutige Mobilgerätekennungen (Unique mobile device identifiers = UDID) und International Mobile Equipment IDs (IMEI) sind nur einige Beispiele.

- Festlegung von Datenschutzstandards
  Die GDPR verpflichtet Organisationen, technische und organisatorische Massnahmen zu ergreifen, um ein angemessenes Mass an Sicherheit für ihre persönlichen Daten zu gewährleisten.

  In der Verordnung wird ausdrücklich erläutert, dass solche Massnahmen Folgendes umfassen:

  – Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  – die Fähigkeit, die laufende Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit von Verarbeitungssystemen und -diensten zu gewährleisten;
  – die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen, und
  – ein Verfahren zur regelmässigen Prüfung, Messung und Bewertung der Wirksamkeit von technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Neue Anforderungen an die Anzeigepflicht bei Vorfällen hinsichtlich Datenschutzverletzungen

  Kommt es bei einem Unternehmen zu einem Sicherheitsvorfall bei welchem die gespeicherten personenbezogenen Daten betroffen sind, so müssen sie diesen Vorfall der zuständigen Datenschutzbehörden melden.

  Die Mitteilung ist unverzüglich und soweit möglich spätestens 72 Stunden nach Kenntnisnahme vorzulegen. Wenn die Benachrichtigung nicht innerhalb von 72 Stunden erfolgt, müssen die Unternehmen eine stichhaltige Begründung für die Verzögerung vorlegen. Wenn der Vorfall zu Diskriminierung, Identitätsdiebstahl oder Betrug, finanziellem Verlust, Reputationsschäden oder anderen erheblich wirtschaftlichen oder sozialen Benachteiligungen für die betroffenen Personen führen kann, müssen die Organisationen diese Personen darüber in Kentnis setzen. Wichtig ist, dass keine Mitteilung an die entsprechenden Personen erforderlich ist, wenn Unternehmen geeignete technische und organisatorische Sicherheitsmassnahmen, beispielsweise durch Verschlüsselung, umgesetzt haben.

- Die hohen Kosten von Sicherheitsfehlern

  Die EU will, dass die neuen Datenschutzbestimmungen zu einer Angelegenheit auf Vorstandsebene werden, und hat daher beschlossen, die Regeln mit hohen Geldstrafen zu versehen:

  – Wenn ein Unternehmen den GDPR Datenschutzbestimmungen nicht nachkommt, kann es eine Geldstrafe von bis zu 10 000 000 € oder 2 % seines gesamten weltweiten Jahresumsatzes erhalten, je nachdem, welcher Wert höher ist.
  – wenn einer Organisation bei einem Vorfall nachgewiesen werden kann, dass sie gegen bestimmte Verpflichtungen der GDPR verstossen hat, kann die Geldstrafe auf bis zu 4 % des gesamten weltweiten Jahresumsatzes steigen.

Wie PwC helfen kann

Dank unserer branchenübergreifenden Erfahrungen sind wir sehr gut aufgestellt, um unseren Kunden bei der Anpassung an das neue Umfeld zu unterstützen. Unser Datenschutzteam umfasst Anwälte, Berater, Spezialisten für Cybersicherheit, Wirtschaftsprüfer, Spezialisten für technische Risiken, forensische Experten und Strategen. Unser Team ist global, schlägt innovative Lösungen vor und verfügt über fundierte Kenntnisse in allen wichtigen Volkswirtschaften der EU. Unser Leistungsspektrum umfasst:

- Bereitschaftsbewertung

  Wir haben einen interaktiven, risikogewichteten Fragekatalog entwickelt, um die GDPR-Bereitschaft unserer Kunden kostengünstig zu beurteilen. Die Befragung besteht aus rund 60 Schlüsselfragen mit vorformulierten Antworten, die mit einer Reifegradmatrix verknüpft sind. Die Befragten wählen dabei für die verschiedene Dimensionen den Reifegrad aufgrund der Konformität der eigenen Compliance-Regelwerke mit der GDPR.

  Das Tool erzeugt einen Bericht mit Aussagen, die mit den von den Befragten angegebenen Reifegraden verknüpft sind. Das Risiko wird unter Bezugnahme auf das regulatorische Risiko die Anwendungstrends, die Verbraucher- und Mitarbeiterzufriedenheit, das Prozessrisiko sowie das B2B-Risiko in Bezug auf Dritte und das Outsourcing beurteilen.

- Persönliche Datenbestände

  Neben einer umfassenderen globalen Regulierungs- und Konsumentenkontrolle fordert die GDPR von Unternehmen, Anstrengungen zu unternehmen, um operative Angemessenheit und Verantwortung zu demonstrieren, anstatt lediglich die Einhaltung zu gewährleisten. Die Fähigkeit, den Beweis für Compliance und operative Angemessenheit zu erbringen, setzt ein umfassendes Verständnis der globalen Datenverarbeitung voraus. Dies kann nur durch eine Inventarisierung der Datenbestände und Verarbeitungsprozesse sowie entsprechende Massnahmen zur Sicherung dieses Wissens erreicht werden.

  Wir haben individuell konfigurierbare Vorlagen und Werkzeuge entwickelt, um Datenbestände zu erfassen und entsprechende Verarbeitungprozesse zu dokumentieren.

- Entwicklung eines Massnahmeplans

  Wir verfügen über umfassende Erfahrungen in der Gestaltung von Datenschutzprogrammen. Wir können Ihnen dabei helfen, Ihre zukünftigen Datenschutzfunktionen zu entwerfen. Dazu entwickeln wir eine Reihe von pragmatischen Empfehlungen zusammen mit den zugehörigen Massnahmeplänen und einer Roadmap zur Implementierung, um identifizierte Lücken in Bezug auf die GDPR-Anforderungen mit unseren Kunden anzugehen. Auf diese Weise erhalten Sie ein klares Bild davon, wo Sie stehen, was Ihr Ziel sein muss und wie Sie bestehende Lücken füllen können.

- Unterstützung bei der Umsetzung von Compliance-Massnahmen

  Wir haben eine hohe Kompetenz in der Beratung unserer Kunden in Bezug auf Compliance-Strategien, Überprüfungen und Sicherheit entwickelt. Wir unterstützen Sie bei der Umsetzung einer breiten Palette an Massnahmen zum Erreichen der GDPR-Konformität, indem wir unser globales Netzwerk von Anwälten, IT-Beratern sowie Prüfungs- und Risikospezialisten mobilisieren. Eine der zentralen Herausforderungen, denen sich Unternehmen bei Veränderungen von Datenschutzrichtlinien gegenübersehen, ist die des Umgangs mit Komplexität, Interdependenzen und der Sequenzierung von Massnahmen. Wir verfügen nachweislich über Erfahrung in der Überwachung komplexer Programme und haben Werkzeuge und Vorlagen entwickelt, die speziell dazu beitragen, die damit verbundenen Herausforderungen zu bewältigen.

- Umfassende Lückenanalyse

  Wir haben auch eine umfassende Methodik entwickelt, um den Reifegrad der Massnahmen zum Datenschutz einer Organisation zu bewerten und Lücken in Hinblick auf die GDPR-Anforderungen zu ermitteln. Unsere bewährte und praxiserpropte Lückenanalyse umfasst 41 Kontrollen, die in den folgenden acht Bereichen gruppiert sind:

1. Strategie, Governance und Rechenschaftspflicht
2. Rechte betroffener Personen und Datenverarbeitung
3. Datenschutzerklärung und Policy Management
4. Risikomanagement und Compliance
5. Datenlebenszyklusmanagement
6. Incident Response und Incident Management
7. Drittrisikomanagement
8. Datenschutz

- Am Ende der Beurteilung geben wir einen Bericht mit folgenden Erkenntnissen ab:

  – eine Zusammenfassung Ihrer wichtigsten Fähigkeiten mit Hervorhebung Ihrer Stärken bezüglich Datenschutz;
  – eine Zusammenfassung Ihrer wichtigsten Einschränkungen und Beschreibung der Bereiche, die Verbesserungen bedürfen, um die Einhaltung der GDPR zu erreichen;
  – Ihren aktuellen Reifegrad, verglichen mit den risikogewichteten GDPR-Anforderungen und Best Practices der Branche;
  – unsere Empfehlungen zur Verbesserung Ihrer Datenschutzfähigkeit und zur Einhaltung der GDPR-Richtlinien und
  – unsere Bewertung des Aufwands, der zur Erfüllung der GDPR-Anforderungen erforderlich ist.

PwCs globale Cybersicherheit und Datenschutzpraxis

Kontakte

Reto Häni
Cybersecurity Partner and Leader
PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Andrea Gergen
Cybersecurity as a Service, Data Protection and Regulatory Compliance
PwC Digital Services
+41 79 419 25 07
andrea.gergen@ch.pwc.com

Susanne Hofmann-Hafner
Legal Compliance Leader
PwC Tax and Legal Services
+41 58 792 17 12
susanne.hofmann@ch.pwc.com