EU-GDPR: Wie gut sind Sie vorbereitet?

Unsere Antwort auf Ihre Fragen zur Europäischen Datenschutz-Grundverordnung (GDPR)

Strengere EU-Datenschutzbestimmungen beschlossen

- Am 14. April 2016 hat das Europäische Parlament die Datenschutz-Grundverordnung (GDPR) gebilligt. Sie bildet das neue regulatorische Rahmenwerk, das die Datenschutzgesetze von 28 EU-Mitgliedsstaaten vereinheitlicht und die bisherige EU-Datenschutzrichtlinie ersetzt.
- Auch wenn die neue Datenschutz-Grundverordnung nicht vor Mai 2018 in Kraft treten wird, sind bereits vor diesem Termin Massnahmen erforderlich, um die neuen und erheblich verschärften Anforderungen des Rahmenwerks erfüllen zu können.
- Dank unserer branchenübergreifenden Erfahrungen sind wir bestens positioniert, um unsere Kunden bei der Anpassung an das neue regulatorische Umfeld zu unterstützen. Unser Datenschutzteam umfasst Anwälte, Berater, Wirtschaftsprüfer, Spezialisten für technische Risiken, forensische Experten und Strategen. Unser globales Team verfügt über fundierte Kenntnisse betreffend alle wichtigen Volkswirtschaften der EU.

Sind Schweizer Unternehmen betroffen?

- Die GDPR ist deutlich umfangreicher als die bisherige EU-Datenschutzrichtlinie und gilt somit für mehr Unternehmen. Alle Unternehmen, die in Europa aktiv sind, müssen der GDPR entsprechen. Dies gilt auch für Unternehmen ohne Niederlassung in der EU, sofern sie Güter an Personen in der EU liefern bzw. Dienstleistungen für solche erbringen 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 vermarktet, der GDPR entsprechen.

Wie gut sind Sie vorbereitet? Finden Sie es heraus mit unserer GDPR-Bereitschaftsbewertung

- Durchlaufen Sie zusammen mit einem unserer Datenschutzexperten die GDPR-Bereitschaftsbewertung. Für die interaktive Befragung müssen Sie etwa einen halben Tag einplanen.
- Der Test enthält rund 60 Schlüsselfragen zum Thema Datenschutz mit vorformulierten Antworten, die mit einer Reifegradmatrix verknüpft sind. Die Befragten wählen die Reifegradratings aus einer Reihe von Antworten aus, die sich auf den in ihrer Organisation geltenden Compliance-Rahmen und die Einhaltung der in der GDPR enthaltenen Datenschutzgrundsätze beziehen.

pwc

- Das Tool erstellt einen Bericht mit Risikoaussagen, die sich aus den angegebenen Reifegraden ableiten. Das Risiko wird unter Bezugnahme auf das regulatorische Risiko und die Anwendungstrends, die Verbraucher- und Mitarbeiterzufriedenheit, das Prozessrisiko sowie das B2B-Risiko in Bezug auf Dritte und das Outsourcing beurteilt.

Unser Ansatz

1. GDPR-Anforderungen

Die GDPR verschärft die Compliance-Vorschriften der bisher geltenden EU-Datenschutzrichtlinie in mehreren Bereichen. Sie enthält wesentliche neue Vorschriften für die Verwendung, Nutzung, Erhebung, Speicherung und Weitergabe von Daten. Auch die bei Nichteinhaltung drohenden Sanktionen wurden verschärft.

Um sicherzugehen, dass Sie über die aktuellen Anforderungen in der EU vollständig im Bilde sind, betrachten wir zunächst in einer kurzen Einführung die wichtigsten Punkte der neuen Verordnung. Grundlage hierfür ist eine fundierte, von unserem globalen Expertennetzwerk durchgeführte Analyse.

2. Beurteilung

Die Beurteilung erfolgt über verschiedene Fragen. Zu jeder Frage gibt es vier mögliche Antworten, die verschiedenen Reifegraden entsprechen. Der Reifegrad kann mit einem Wert zwischen 1 (geringe Reife = mangelnde Compliance) und 4 (umfassende und optimierte Compliance) beurteilt werden

Die Fragen sollen Aufschluss über die Ausgereiftheit der Komponenten in folgenden beiden Schlüsselbereichen geben:

- Datenschutzarchitektur – Beurteilung der bestehenden Strukturen im Unternehmen zur Gewährleistung der Compliance
- Datenschutzgrundsätze – Beurteilung der operativen Bereitschaft zur Erfüllung der Datenschutzgrundsätze der GDPR.

Um den Reifegrad detailliert beurteilen zu können, werden die vorgenannten beiden Bereiche in eine Reihe von Unterkategorien aufgeschlüsselt. Der Reifegrad ist für alle Fragen innerhalb jeder Unterkategorie angegeben.

Die Unterkategorien sind nachstehend aufgelistet:

Datenschutz-architektur	• Territorialer Geltungsbereich • Vision und Strategie • Programmaufbau • Governance	• Datenschutz: Rollen und Aufgaben • Register • Richtlinien	• Aufbau • Kontrollen • Wissens-vermittlung und Sensibilisierung • Absicherung	• Drittparteien • Kritische Prüfung • Rechenschafts-pflicht • Korrektur
Datenschutz-grundsätze	• Rechtmässigkeit, Fairness und Transparenz	• Zweckbindung • Datenminimierung	• Genauigkeit • Speicherungs-begrenzung	• Integrität und Datenschutz • Rechte • Datentransfers

Die Aussagekraft unseres Berichts hängt von der Qualität der uns zur Verfügung gestellten Informationen ab. Um zu einem verlässlichen Ergebnis zu gelangen, sollten fachkundige Personen aus Ihrem Unternehmen an der Beurteilung teilnehmen. Das ist wichtig, weil die Befragten umfangreiches Wissen und Erfahrung in Zusammenhang mit dem Unternehmen benötigen, um den Reifegrad der Compliance-Position bei jeder Frage richtig einschätzen zu können. Idealerweise sollten Mitarbeiter aus folgenden Bereichen an der Beurteilung mitwirken:

- Legal/Compliance – eine Person, die die Compliance-Architektur in Ihrem Unternehmen genau kennt
- Datenverwaltung – eine Person, die mit dem Lebenszyklus von Daten in Ihrem Unternehmen vertraut ist, von der Erhebung bis zur Vernichtung
- Informationssicherheit – eine Person, die über umfassende Kenntnis der technischen und organisatorischen Massnahmen zur Datensicherheit einschliesslich Erkennung und Beseitigung von Datenschutzverstössen verfügt

Unser GDPR-Bewertungstool gewährleistet nicht die Richtigkeit der uns zur Verfügung gestellten Daten.

3. Analyse

Jede Unterkategorie bezieht sich auf ein Thema, zu dem verschiedene Fragen gestellt werden, um relevante Aspekte zu prüfen. Im GDPR-Bewertungstool ist jede Frage mit den entsprechenden Artikeln und Erwägungsgründen in der GDPR verknüpft. Auf diese Weise können wir Ihren Reifegrad – also Ihre operative Bereitschaft in Bezug auf die GDPR – ermitteln.

Im Verlauf der Beurteilung werden ausserdem zu jeder Frage weitere Informationen zusammengetragen. Diese werden verwendet, um die Analyseergebnisse Ihres Unternehmens in einen Kontext zu setzen.

4. Berichterstellung

Unser Bericht enthält eine zusammenfassende Beschreibung der Compliance-Position Ihres Unternehmens in den beiden Bereichen «Datenschutzarchitektur» und «Datenschutzgrundsätze». Diese wird nach den beurteilten Unterkategorien aufgeschlüsselt, und damit wird der Reifegrad in den einzelnen Kategorien ermittelt.

Im Bericht sind alle Fragen und die von Ihren Mitarbeitern abgegebene Einschätzung zum Reifegrad Ihres Unternehmens aufgelistet. Darüber hinaus verweist unser Bericht auf die jeweils relevanten Artikel und Erwägungsgründe in der GDPR.

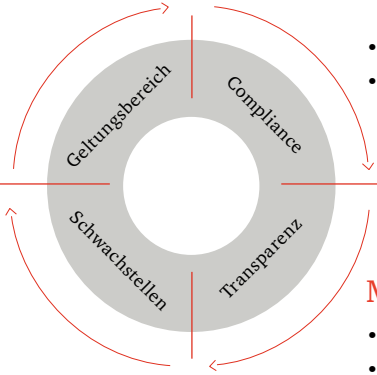
Weitere Informationen dazu, wie Sie dieses interessante neue Angebot nutzen können, erhalten Sie bei den unter «Kontakt» genannten Ansprechpartnern.

Erweiterter Geltungsbereich

- Mehr Unternehmen werden reguliert
- Datenverarbeiter werden stärker reguliert
- Datenverantwortliche und Datenverarbeiter ausserhalb der EU werden reguliert
- Ohne Umsetzungsrechtsakt einzelner Länder sofort für alle EU-Mitgliedsstaaten verbindlich
- Neue Datenschutzgrundsätze

Mehr Compliance-Pflichten

- Eingebauter Datenschutz («Privacy by Design»)
- Datenschutzfolgen-Abschätzungen («Privacy Impact Assessments»)
- Rechenschaftspflichten: schriftliche Compliance-Pläne, gesetzlich vorgeschriebene Audits und Inspektionen
- Nutzungskontrollen wie: Recht von Bürgern auf Löschung ihrer Daten, Datenportabilität, Datenminimierung
- Datenschutzbeauftragte
- Profilierung neuer Anforderungen von Kunden, z.B. Zustimmungsformalitäten



Sanktions- und Prozessrisiko

- Erweiterte Durchsetzungsbefugnisse
- Strafen bis zu 4 % des weltweiten Jahresumsatzes oder 20 Millionen Euro
- Regressansprüche und Sammelklagen mehrerer Parteien

Mehr Transparenz

- Ausdrückliche Zustimmung
- Jugendschutz
- Datenschutzrichtlinien
- Einbeziehung von Interessengruppen
- Offenlegung von Verstössen
- Neue Regeln für die Nutzung von Daten, z.B. Verbot von Datenbündelung und -aggregation

Contacts

Reto Haeni
Cyber Security Partner and Leader, PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Susanne Hofmann-Hafner
Legal Compliance Lead, PwC Tax and Legal Services
+41 79 286 83 67
susanne.hofmann@ch.pwc.com

Nicolas Vernaz
Data Protection and Regulatory Compliance Lead, PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com