axians

AUF EINEN BLICK

Die EU-Datenschutz-Grundverordnung (EU-DSGVO)

VINCI ENERGIES

AUF EINEN BLICK

Die EU-Datenschutz-Grundverordnung (EU-DSGVO)

In diesem Factsheet erhalten Sie einen ersten Überblick über die neue EU-Datenschutz-Grundverordnung mit einer Übersicht der Grundprinzipien, wesentlichen Änderungen und der zu erwartenden Bußgelder.

Grundsätze des Datenschutzrechts bleiben erhalten:

Die wesentlichen datenschutzrechtlichen Grundprinzipien werden beibehalten und weiterentwickelt:

- Verarbeitung personenbezogener Daten: Verbot mit Erlaubnisvorbehalt
- Datenvermeidung und Datensparsamkeit als zentrale Prinzipien des Datenschutzes
- Enge Zweckbindung der Datenerhebung
- Transparenz und Datensicherheit

Was ist neu und was bringt die EU-DSGVO?

- EU-DSGVO wurde im April 2016 verabschiedet und wird im Mai 2018 in Kraft treten
- Marktortprinzip – ein Datenschutzgesetz für alle 28 EU Mitgliedsstaaten, gilt auch für Unternehmen außerhalb der EU, die Waren und Dienstleistungen in der EU anbieten
- Beschwerden können nun bei der deutschen Datenschutzbehörde eingereicht werden, auch wenn Unternehmen in einem anderen EU-Land sitzen
- Datenübertragbarkeit – das Recht, Daten zu einem neuen Anbieter „mitzunehmen“
- Mehr Transparenz – Recht auf Informationsansprüche über Zwecke der Datenverarbeitung, Speicherdauer, Empfänger der Daten etc.
- Recht auf Vergessenwerden/Löschung – bei rechtswidriger Datenverarbeitung besteht Löschanspruch der Daten sowie Verweise und Links auf diese Daten (physikalische Löschung, nicht nur Markierung „nicht mehr nutzen“)
- Stärkung des Datenschutzniveaus für Betroffene in der EU
- Keine Richtlinie mehr, sondern eine Verordnung, die ab 25.05.2018 rechtsverbindlich ist, EU-weit
- Bußgelder für Non-Compliance und Verletzung des Datenschutzes wurden deutlich erhöht
- Umgang mit personenbezogen Daten wird schärfer reguliert
- Umfangreiche Informations- und Dokumentationspflichten (z. B. Verarbeitungsverzeichnis, Auskunftspflichten, etc.)

UMGANG MIT DATENPANNEN:

Stand heute (BDSG)

- Nur manche Vorfälle sind meldepflichtig
- Zwei Voraussetzungen sind zu erfüllen:
  - Es müssen sehr sensible Daten betroffen sein (bspw. Bank- oder Gesundheitsdaten)
  - Hohes Risiko für die Betroffenen
- Folge: Nur wenige Meldungen an Aufsichtsbehörden und Betroffene – selbst bei festgestellten Mängeln wurden sehr geringe Strafen verhängt (max. 25.000 € in Deutschland)

Stand morgen (DSGVO)

- Alle Vorfälle sind meldepflichtig, es sei denn, dass nicht von einem Risiko für die Betroffenen ausgegangen werden kann
- Keine Informationspflicht der Betroffenen bei Verschlüsselung/Pseudonymisierung
- Konkrete Fristen (72 Stunden)
- Gestaffelte Höhe für verschiedene Verstöße von 2%/10 Mio. EUR, bzw. 4%/20 Mio. EUR (bezogen auf weltweit erzielten Jahresumsatzes „des Unternehmens“)
- Wesentlich konkretere Beschreibung der „technischen und organisatorischen Maßnahmen“ als im BDSG

AUF EINEN BLICK

Die EU-Datenschutz-Grundverordnung (EU-DSGVO)

Technischer und organisatorischer Datenschutz:

- Privacy by Design – Privacy by Default: Die Einführung des „Datenschutzes durch Technik und datenfreundliche Voreinstellungen“ (Art. 25 DSGVO) stellt ausdrücklich Anforderungen an die Produktentwicklung und -implementierung. Es gilt weiterhin das Prinzip von Datenvermeidung und -sparsamkeit, z.B. Pseudonymisierung. Es dürfen nur personenbezogene Daten verarbeitet werden, die für den Zweck erforderlich sind. Das betrifft den Umgang der erhobenen Daten, den Umfang Ihrer Verarbeitung, Speicherfrist und Zugänglichkeit.
- Auftragsdatenverarbeitung: Die Einhaltung der Verpflichtungen des Auftragnehmers kann durch Einhaltung genehmigter Verhaltensregeln oder Zertifizierung nach Art. 42 DSGVO nachgewiesen werden.
- Meldung von Datenschutzverletzungen: Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich (innerhalb von 72 Stunden) an die Aufsichtsbehörden gemeldet werden. Es besteht keine Informationspflicht der Betroffenen bei Verschlüsselung/ Pseudonymisierung, d.h. wenn kein hohes Risiko von Rechten und Freiheit besteht.
- Datenschutz-Folgenabschätzung: Der Verantwortliche muss bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen, wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten besteht.
- Pflicht zur Bestellung eines Datenschutzbeauftragten: Pflicht für öffentliche Stellen; Pflicht für Nicht-öffentliche Stellen bei „Kerntätigkeit“ in Durchführung von Verarbeitungsvorgängen mit Personendaten.
- Stärkung der Selbstregulierung durch Zertifizierung und Verhaltensregeln.

IHR ANSPRECHPARTNER

Erwin Ritter (Datenschutzbeauftragter/
Leiter Organisation und Prozesse)
Telefon: +49 731 1551-0
E-Mail: erwin.ritter@axians-infoma.de

AUF EINEN BLICK

Die EU-Datenschutz-Grundverordnung (EU-DSGVO)

Sanktionen unter DSGVO

- Deutlich breitere Sanktionspalette: Für bestimmte Rechtsverstöße sind Bußgelder bis zu 4 % des Jahresumsatzes eines Unternehmens, beziehungsweise 20 Mio. Euro, zulässig, wobei der jeweils höhere Wert gilt. Die Sanktionen sollen abschreckend sein.
- Fast alle Pflichten der Verantwortlichen und Auftragsverarbeiter sehen bei Verstößen Bußgelder vor, Verantwortliche Stelle und Auftragsverarbeiter haften gemeinsam.
- Neu in DSGVO: Bußgelder auch bei Verstoß gegen Pflichten zur Ergreifung technischer und organisatorischer Maßnahme. Dies bedeutet dass nun auch Management und IT-Verantwortliche in der Haftung stehen, nicht nur der Datenschutzbeauftragte.
- Öffnungsklauseln: Gesetzgeber in Bund und Ländern werden bis 2018 die wichtigsten nationalen Regelungen zur Anpassung an das neue Europäische Datenschutzrecht schaffen.
- Zusätzliche Regelungsspielräume für Mitgliedstaaten insbesondere für die Verarbeitung personenbezogener Daten zur Erfüllung öffentlicher Aufgaben.

AUF EINEN BLICK

Die EU-Datenschutz-Grundverordnung (EU-DSGVO)

Fragen, die sich Unternehmen jetzt stellen sollten:

- Speichern wir nur die notwendigen Daten und werden diese auch nicht länger als notwendig gespeichert?
- Können wir sicherstellen, dass die Daten nur für einen spezifischen Zweck gespeichert und nicht anderweitig genutzt werden?
- Haben wir einen Prozess, um Personen Auskunft über ihre personengebundenen Daten zu geben?
- Sind die gespeicherten personenbezogenen Daten ausreichend gegen Missbrauch geschützt?
- Gibt es einen Prozess, wie wir personenbezogene Daten auf Anforderung löschen?
- Haben wir die notwendigen Prozesse, um im Falle eines Datenschutzverstoßes die betroffenen Personen und die Aufsichtsbehörden innerhalb von 72 Stunden zu informieren?
- Ist unser Budget ausreichend, um die neuen Regelungen umzusetzen zu können?
- Haben wir einen Datenschutzbeauftragten mit der erforderlichen Fachkenntnis um die Neuerungen der EU-DSGVO umzusetzen?

IT-Workshop zur DSGVO

Für eine schnellere und gezieltere Umsetzung der neuen Richtlinien, bieten wir unseren Kunden einen fokussierten Workshop an. Dieser richtet sich in erster Linie an IT-Leiter und beinhaltet unter anderem die Identifizierung und Priorisierung der notwendigen Maßnahmen für ihre Unternehmen. Mehr Informationen finden Sie auf www.axians.de/dsgvo-workshop

axians

Axians IT Solutions GmbH · Hörvelsinger Weg 17 · 89081 Ulm
Tel.: +49 731 1551-0 · Fax: +49 731 1551-555
E-Mail: info@axians.de · www.axians.de

Deutschland Berlin · Düsseldorf · Frankfurt · Hamburg · Hannover · Karlsruhe · Leipzig · Mannheim · München · Münster · Nürnberg · Stuttgart

07/2017