DSGVO-Arbeitshilfe: Sieben essentielle Datenschutz-Maßnahmen für Start-Ups und Unternehmen

München – 16. Juni 2020: Die Digitalisierung der Wirtschaft hat Cyberkriminellen zahlreiche neue Einfallstore geöffnet. Um sich und die Daten ihrer Angestellten, Kunden und Partner zu schützen, müssen Unternehmen geeignete Maßnahmen ergreifen. Aber was müssen sie dabei beachten?

Die meisten Vorgaben des Bundesdatenschutzgesetzes (BDSG) und der Datenschutz-Grundverordnung (DSGVO) laufen auf eine einfache Forderung hinaus: Die Verantwortlichen haben die Sicherheit sensibler Daten zu gewährleisten. Zuwiderhandlungen können schnell teuer werden: Bei besonders schwerwiegenden Datenschutz-Verstößen sieht die DSGVO Bußgelder in Höhe von bis zu 20 Millionen Euro bzw. von bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes vor (vgl. DSGVO Art. 83). Wir stellen sieben essentielle Datenschutz-Maßnahmen für Unternehmen vor.

1. Compliance-Evaluierung

Compliance – also die Einhaltung von Gesetzen und regulatorischen Vorgaben – betrifft alle Unternehmen, jedoch in unterschiedlichem Ausmaß. Je nach Branche können neben DSGVO und BDSG zusätzliche Richtlinien gelten, etwa aus dem Wettbewerbs- oder Finanzrecht.

2. Risikobewertung

Als nächsten Schritt sollten Unternehmen eine Risikobewertung durchführen. Denn je schutzbedürftiger die Daten sind, die erhoben und/oder verarbeitet werden sollen, desto aufwändiger müssen die Maßnahmen zu ihrem Schutz ausfallen. Bewertungen dieser Art erfordern häufig die Unterstützung eines Datenschutzbeauftragten.

3. Verschlüsselung

Es sollte eigentlich selbstverständlich sein: Sensible Daten gehören verschlüsselt, und zwar sowohl bei der Übertragung als auch bei der Speicherung[1]. Ausreichend verschlüsselte Daten gelten per se als sicher; selbst im Falle eines Datenverlusts sind die Daten für Angreifer ohne den passenden Schlüssel nicht lesbar oder wiederherstellbar.

4. Pseudonymisierung

Bei der Pseudonymisierung von personenbezogenen Daten werden gezielt identifizierende Informationen aus Datenschnipseln entfernt. Beispielsweise ersetzt man die Namen von Personen durch zufällig generierte Zeichenketten. So bleiben zwar noch nützliche Daten übrig, diese enthalten allerdings keine sensiblen Informationen mehr.

5. Zugangskontrollen

Die Einführung von Zugriffskontrollen in den Arbeitsablauf Ihres Unternehmens ist ebenfalls eine effiziente Methode zur Risikominimierung. Je weniger Personen Zugriff auf die Daten haben, desto geringer ist das Risiko einer versehentlichen oder vorsätzlichen Verletzung oder eines Datenverlusts.

---

[1] *Bei der Verarbeitung müssen die Daten zwar unverschlüsselt vorliegen, können aber durch entsprechende Infrastrukturen so geschützt werden, als wären sie weiterhin verschlüsselt. Beim Confidential Computing oder Sealed Computing erfolgt die Verarbeitung etwa in speziell versiegelten Hardware-Umgebungen, die einen unbefugten Zugriff auf unverschlüsselte Daten zuverlässig ausschließen. (Siehe: https://de.wikipedia.org/wiki/Sealed_Cloud)*

6. Backups

Backups können helfen, Datenverluste zu verhindern, die durch Benutzerfehler oder technische Störungen auftreten können. Sie sollten regelmäßig erstellt und aktualisiert werden. Regelmäßige Backups verursachen zwar zusätzliche Kosten für Ihr Unternehmen, aber potenzielle Unterbrechungen des Geschäftsbetriebs sind meist weitaus kostspieliger.

7. Löschung

Laut DSGVO sind Unternehmen dazu verpflichtet, die Daten zu löschen, die Sie nicht benötigen (vgl. Art. 5 („Datenminimierung“) und Art. 17 („Recht auf Vergessenwerden“)). Unternehmen sollten daher ein entsprechendes Löschkonzept aufstellen. Darin sind abhängig von der Datenart beispielsweise auch Löschfristen und Laufzeiten festzulegen.

„Letztlich stehen Unternehmen vor der Wahl, entweder selbst geeignete Maßnahmen zu treffen oder Dienste von Drittanbietern in Anspruch zu nehmen, die sich auf Datenschutz und Datensicherheit spezialisiert haben“, sagt Ulrich Ganz, Director Software Engineering bei der TÜV SÜD-Tochter uniscon. „Je nach Branche, Unternehmensgröße und Art der erhobenen bzw. verarbeiteten Daten lassen sich dadurch Kosten sparen und Prozesse vereinfachen. Nutzen Unternehmen etwa entsprechend zertifizierte Dienste, erfüllen Sie damit bereits nachweisbar ihre vom Gesetzgeber geforderten Kontroll- und Sorgfaltspflichten.“ So können sich die Unternehmen auf ihr Kerngeschäft konzentrieren – und überlassen den Datenschutz den Experten.

Weiterführende Informationen erhalten Sie auf Anfrage bei presse@uniscon.de.

Diese privacyblog-Beiträge könnten Sie interessieren:
CIO: Quickcheck für Cloud-Dienste
Checkliste für sicheres Homeoffice

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.uniscon.com

Pressekontakt

uniscon GmbH, Wilhelm Würmseer (Corporate Communications)
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20