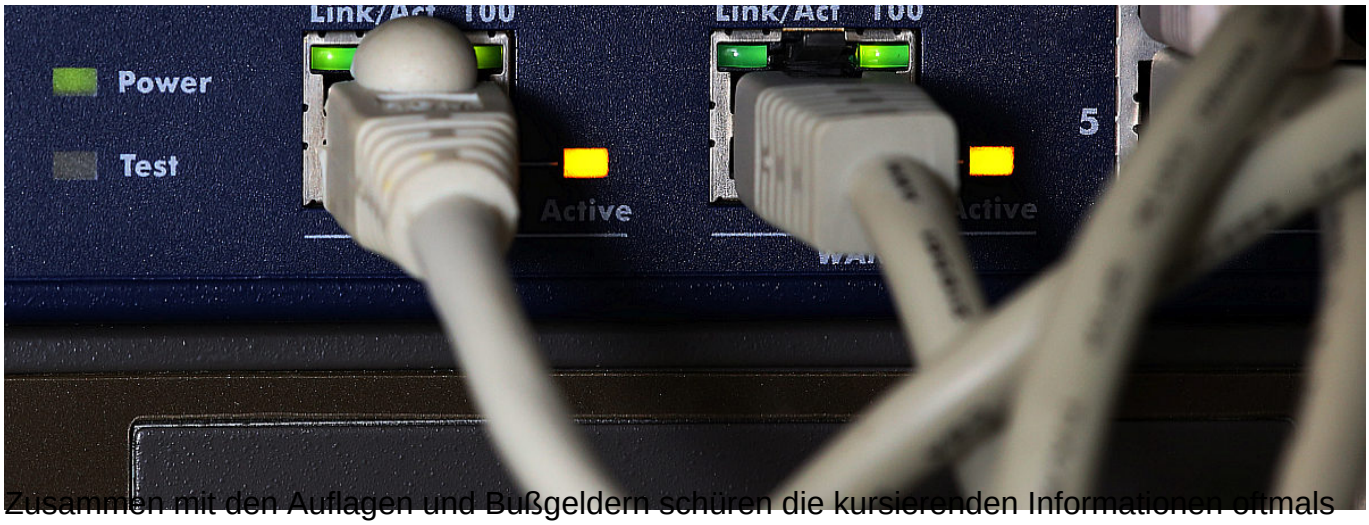
Richtig auf die DSGVO vorbereiten



Zusammen mit den Auflagen und Bußgeldern schüren die kursierenden Informationen oftmals Angst vor den bevorstehenden Änderungen. Dabei birgt die DSGVO große Chancen: Die Verordnung ist eine Modernisierung für wirksamen und konkreten Schutz personenbezogener Daten in Europa. Organisationen haben die Chance, ihr Vertrauensverhältnis gegenüber Kunden, Partnern und Mitarbeitern zu untermauern, wenn sie die Richtlinie umsetzen. Im Zeitalter der Digitalisierung und einer datengetriebenen Wirtschaft ist ein gewissenhafter und integrer Umgang mit Informationen unabdingbar – Geschäfte und Prozesse im Einklang mit der DSGVO belegen eine solche Handhabung.

DSGVO verlangt Datenschutzmanagementsystem

Helko Kögel

Um nachweisen zu können, dass eine Organisation datenschutzrechtliche Vorgaben einhält, muss es ein Datenschutzmanagementsystem einführen. Diese notwendige Bedingung der Verordnung stellt einen hohen Nutzen für die Organisation dar. Der Datenschutzbeauftragte erhält über ein risikobasiertes Managementsystem schnell eine Übersicht über die laufende Verarbeitung von personenbezogenen Daten und kann darauf seine datenschutzrechtliche Prüfung aufbauen. Zudem ist im Falle einer Prüfung durch die zuständige Aufsichtsbehörde für Datenschutz die Vorlage des Verfahrensverzeichnisses jederzeit möglich. Darüber hinaus gewährleistet ein solches Verzeichnis Transparenz und Qualität – auch gegenüber Dritten.

Hinzu kommt: Die DSGVO schließt sogenannte Backdoor-Lösungen, also Zugriffe über eine „Hintertür“ rigoros aus. Damit verschafft sie europäischen Unternehmen einen Vorteil gegenüber dem globalen Wettbewerb.

> „Unternehmen bietet die EU-DSGVO viele Chancen: Das Vertrauen von Kunden und Partnern kann gestärkt und die nötige Transparenz gegenüber Dritten untermauert werden. Um sich den konkreten Herausforderungen der DSGVO erfolgreich zu stellen, empfiehlt sich ein Ansatz, der Datenschutz und Informationssicherheit gleichermaßen betrachtet. Ein auf allen Ebenen nahtlos zusammenarbeitendes Lösungsportfolio, bestehend aus sicheren Netzwerken, Monitoring, Endpoints, Applikationen und Clouds, ist dabei unabdingbar.“

© „Die Stiftung“ Media GmbH – Ein Unternehmen der F.A.Z.-Verlagsgruppe

Grundsätze zur Gewährleistung der Datenverordnung

Konkret wird die Modernisierung des Datenschutzes durch mehrere Grundsätze gewährleistet, die in Art. 5 der EU-DSGVO festgelegt sind. Die zentralen Prinzipien der neuen Verordnung lauten:

- Rechtmäßigkeit und Transparenz: Ohne eine Ermächtigungs- bzw. Rechtsgrundlage dürfen keine personenbezogenen Daten erhoben und benutzt werden.
- Zweckbindung: Die personenbezogenen Daten, für die eine Ermächtigungsgrundlage vorhanden ist, dürfen nur zu dem Zweck verwendet werden, für den ebendiese Ermächtigung erteilt wurde.
- Datenminimierung: Die Datenverarbeitung muss auf das notwendigste Maß beschränkt werden.
- Richtigkeit von Daten: Bei falschen und unsachlichen Daten hat das Datensubjekt sofortigen Anspruch auf Berichtigung bzw. Löschung.
- Speicherbegrenzung: Die neue Verordnung besagt, dass die Datenspeicherung auf den Zeitraum der Verarbeitung beschränkt ist und unbegrenzte Datenspeicherung vermieden werden muss.
- Integrität und Vertraulichkeit: Die personenbezogenen Daten müssen angemessen gesichert werden vor Manipulation oder Fälschung. Vor dem Hintergrund, dass die Zahl der Cyberangriffe auf Datenbanken und Zugangsberechtigungen stetig steigt, hat dieses Prinzip in der EU-Verordnung einen neuen Stellenwert.
- Rechenschaftspflicht: Die Einhaltung dieser Grundsätze muss nachgewiesen werden.

Zentrales Thema: Sicherheit der Datenverarbeitung

Ein wesentlicher Aspekt der DSGVO ist die Sicherheit der Datenverarbeitung. Um Integrität und Vertraulichkeit zu gewährleisten, müssen Organisationen bei der Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen ergreifen, die einen Schutz vor unbefugter oder unrechtmäßiger Verarbeitung der Daten, ihren Verlust sowie ihre unbeabsichtigte Zerstörung oder Schädigung sicherstellen. Die Wahl der konkreten Technologien und Maßnahmen soll dabei gemäß der Wahrscheinlichkeit und Schwere des Risikos für die Rechte der Betroffenen abgewogen werden.

Um sich den Herausforderungen der DSGVO zu stellen, empfiehlt sich die Einführung eines sogenannten Informationssicherheitsmanagementsystems (ISMS). Darin werden Verfahren und Regeln aufgestellt, die dafür sorgen, dass die benötigte Informationssicherheit in der Organisation zunächst definiert, dann umgesetzt und kontinuierlich verbessert wird. Um dem erhöhten Anspruch der DSGVO gerecht zu werden, müssen die IT-Sicherheitslösungen der Organisation auf allen Ebenen zusammenarbeiten und ineinandergreifen. Dazu gehört das Einrichten sicherer Netzwerke, des Monitorings, der Endpoints, Applikationen und Clouds. Verantwortlich für die Initiierung und Umsetzung der oben genannten Maßnahmen ist immer der Datenschutzbeauftragte und teilweise auch der IT-Sicherheitsbeauftragte.

Über den Autor:
Helko Kögel ist Director Consulting beim IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity.

© „Die Stiftung“ Media GmbH – Ein Unternehmen der F.A.Z.-Verlagsgruppe