EU-DSGVO: Umsetzung ist Compliance- und kein IT-Thema - Unternehmen sollten ihre Datenprozesse umgehend auf Konformität prüfen und anpassen / In drei Schritten zur Compliance

Die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) setzt Unternehmen europaweit unter Zugzwang, ihren Umgang mit personenbezogenen Daten grundlegend zu überarbeiten. Jüngste Datenskandale, wie der um „Cambridge Analytica“ und die darauffolgende Anhörung des Facebook-Chefs Mark Zuckerberg im US-Kongress, verschaffen dem Thema zudem eine breite Aufmerksamkeit.

Um Verstöße gegen die Verordnung zu vermeiden, sollten alle relevanten Verfahren auch unter Risikoaspekten beurteilt werden. Eine Analyse der Managementberatung Horváth & Partners zeigt: Das lässt sich nicht im Vorbeigehen erledigen. Empfehlenswert ist ein Vorgehen in drei Schritten.

Vor zwei Jahren wurde die neue EU-DSGVO vom Europäischen Parlament und dem Europäischen Rat beschlossen. Jetzt läuft die Übergangsfrist am 25. Mai 2018 endgültig ab. Ziel der EU-DSGVO ist es, die Rechte der von Datenverarbeitungen betroffenen Personen besser als bislang und europaweit einheitlich zu schützen. Dazu zählen unter anderem Kunden, Lieferanten, Geschäftspartner, aber auch Mitarbeiter. Betroffen sind alle in der Europäischen Union niedergelassenen und/oder geschäftstätigen Unternehmen. Sie alle stehen vor der Herausforderung, die betroffenen datenverarbeitenden Prozesse zu dokumentieren, anzupassen sowie effiziente technische und organisatorische Maßnahmen zu definieren und zu implementieren, um die neuen Anforderungen der EU-DSGVO erfüllen zu können, zum Beispiel jederzeit Transparenz über sämtliche von einer Person gespeicherten Daten herzustellen – und das möglichst auf Knopfdruck.

„Verstöße gegen die EU-DSGVO können nicht nur mit hohen Bußgeldern belegt werden, sondern auch der Reputation schaden“, sagt Andreas Hopfener, Experte im Beratungssegment Risikomanagement & Compliance von Horváth & Partners. „Unternehmen sollten daher Compliance-Lücken schnellstmöglich identifizieren und schließen.“

In drei Phasen zur Herstellung von Compliance

Mit einem stringenten Projektmanagement können Unternehmen in drei Phasen sicherstellen, dass ihre Personendaten verarbeitenden Prozesse alle Anforderungen der EU-DSGVO erfüllen. Phase eins dient der Identifikation von Compliance-Lücken. Unternehmen sollten die Risiken analysieren, die individuell für sie bestehen. Hat eine Verletzung der EU-DSGVO arbeitsrechtliche Konsequenzen? Welche Bußgelder drohen? Führen Verstöße zu einer Rufschädigung? „Risikorelevante Fragen stellen sich nach unserer Beobachtung noch zu wenige Unternehmen“, sagt Hopfener. Zudem sollten bereits vorhandene Datenschutzprozesse mit den Vorschriften abgeglichen werden, um möglichen Handlungsbedarf zu identifizieren.

In Phase zwei werden die relevanten Handlungsfelder definiert und die nötigen Maßnahmen geplant, um die von der EU-DSGVO geforderten Standards einhalten zu können. Dabei geht es um die Anpassung von Prozessen, die Aktualisierung des Verarbeitungsverzeichnisses, die Überprüfung der technischen und organisatorischen Maßnahmen für die Datensicherheit sowie die Erarbeitung von Löschkonzepten. Auch sollten Betriebsvereinbarungen geprüft und gegebenenfalls neu verhandelt werden. „Es ist absolut ratsam, in Phase eins und zwei juristische Expertise hinzuzuziehen und natürlich den Datenschutzbeauftragten sehr eng einzubinden“, so Hopfener.

Die Umsetzung aller definierten Maßnahmen erfolgt in Phase drei. Einer der Kernpunkte ist, ein stringentes Einwilligungsmanagement zu implementieren. Dieses hat die Aufgabe, strukturiert abzufragen und zu dokumentieren, welche Personen wann zugestimmt haben, dass und zu welchem Zweck ihre Daten im Unternehmen erhoben, gespeichert und verarbeitet werden dürfen. Zudem ist die Einrichtung eines risikorelevanten Beschwerdemanagements empfehlenswert.

Datenschutz bekommt höheren Stellenwert

„Grundsätzlich erhöht die EU-DSGVO den Stellenwert des Datenschutzes in Unternehmen, denn Verstöße werden nun deutlich Compliance-relevanter“, so Hopfener. Bei einer Missachtung der Verordnung können Bußgelder in Höhe von bis zu vier Prozent des gesamten Konzernumsatzes anfallen. Klare Richtlinien können Unternehmen dabei unterstützen, Mitarbeiter für die Bedeutung des Datenschutzes zu sensibilisieren. Zusätzlich sind Schulungen sinnvoll, um die Notwendigkeit der getroffenen Maßnahmen im Rahmen der EU-DSGVO aufzuzeigen. Gleichzeitig ist jetzt eine gute Gelegenheit für strategische Überlegungen darüber, was die höheren Datenschutzanforderungen grundsätzlich für die Modernisierung des eigenen Geschäftsmodells bedeuten. „Unternehmen müssen sich die Gretchenfrage stellen, wie sie es mit den Daten halten wollen: Ob sie führend im Datenmanagement und in der Ableitung entsprechender Wettbewerbsvorteile sein wollen, oder grundsätzlich bewusst sparsam bei der Speicherung von Daten. Beides ist möglich und kann sinnvoll sein“, schließt Hopfener ab.

KONTAKT
Raphaela Reber
Marketing & Communications
Horváth AG
Phoenixbau | Königstraße 5
70173 Stuttgart, Germany
Phone: +49 711 66919 3305
RReber@horvath-partners.com