

PERSONENDATEN RICHTIG SCHÜTZEN

Dass durch die zunehmende Vernetzung zu viele Unternehmen Einsicht in ihre persönlichen Daten gewinnen, ist eine der größten Ängste von Internet-Nutzern: Mit gutem Datenschutz und Transparenz können Online-Händler und Dienstleister bei ihren Kunden punkten.

DATENSCHUTZ /// DSGVO /// EUROPÄISCHE UNION

VON TILMAN DRALLE UND THOMAS WERNER

Das europäische Datenschutzrecht harmonisieren und damit Rechtssicherheit, Wettbewerbsgleichheit und ein einheitliches, hohes Datenschutzniveau herstellen: Das war das Ziel, das der europäische Gesetzgeber mit der Datenschutz-Grundverordnung (DSGVO) verfolgte. Doch die erwünschte EU-weite Vereinheitlichung des Datenschutzrechts wurde damit nicht in allen Punkten konsequent umgesetzt. Die Grundverordnung beinhaltet rund 60 sogenannte Öffnungsklauseln, die es den Mitgliedstaaten erlauben, vom europäischen Standard abzuweichen. Um Probleme und Komplexität zu vermeiden, sollten Unternehmen, die in mehreren EU-Mitgliedstaaten aktiv sind, sicherheitshalber die neue DSGVO vollständig

heute den Umgang mit Daten regeln und für das Thema Verantwortliche bestimmen. Diese sollten den Datenschutz und auch die Rechtslage nicht nur durch die juristische Brille betrachten, sondern außerdem Erfahrungen mit elektronischen Managementsystemen sowie über Informationstechniken und deren Sicherungen mitbringen.

ACHTUNG: STRAFE

Datenschutzregeln im Unternehmen zu implementieren und vor allem so zu etablieren, dass alle Mitarbeitenden die Relevanz rechtlicher Bestimmungen, aber auch die Kundenwünsche kennen, braucht Zeit. In wenigen Wochen sind daher die neuen Bestimmungen nicht umzusetzen. Unternehmen, die bis Masi 2018 den neuen Datenschutz nicht umsetzen, müssen mit Sanktionen rechnen. Was die DSGVO neu regelt und wie sich Firmen vorbereiten:

ACCOUNTABILITY-ANSATZ: Jede Stelle im Unternehmen, die mit personenbezogenen Kundendaten hantiert, muss künftig beweisen können, dass sie diese rechtskonform und nach den Vorgaben der DSGVO verarbeitet. Sonst drohen Bußgelder und Schadensersatzpflichten gegenüber Betroffenen.

DATENSCHUTZ-FOLGEN: Gibt es bei der Verarbeitung von Personendaten ein Risiko für die Rechte und Freiheiten der betroffenen Kunden, aber auch An-



Rund **60**

Öffnungsklauseln konterkarieren den Datenschutz in der DSGVO

umsetzen. Dann bleiben sie rechtlich überall auf der sicheren Seite.

Zwar sind noch elf Monate Zeit, die DSGVO umzusetzen. Doch Kunden erwarten heute schon den Schutz ihrer persönlichen und vor allem wirtschaftlichen Daten. Daher sollten Unternehmen schon



gestellten, muss das Unternehmen diese Folgen zuvor abschätzen und dokumentieren. Die DSGVO fordert eine Datenschutz-Folgenabschätzung (DSFA) für den Umgang mit Daten.

LÖSCHPFLICHTEN: Unternehmen können sich nicht mehr auf die allgemeine Verpflichtung zurückziehen, Daten unter bestimmten Voraussetzungen auf den eigenen Systemen zu löschen. In Zukunft müssen sie mehr tun, wenn Kunden oder Angestellte die Löschung verlangen: Zur Umsetzung des Rechts auf Vergessenwerden müssen sie Dritte, die ebenfalls ihre Daten verarbeiten und sogar veröffentlichen, identifizieren, über die Löschung informieren und diese dort durchsetzen.

SCHWACHSTELLEN BESEITIGEN: Technische und organisatorische Schwachstellen beim Datenschutz sind nach der neuen Verordnung Gründe für Bußgelder. Als Strafe drohen Zahlungen bis zu

zwei Prozent des Vorjahresumsatzes. Das zwingt Unternehmen, technische und organisatorische Maßnahmen – TOM – zu planen, die den Schutz von Personendaten sicherstellen. Diese müssen zwingend dem neuesten „Stand der Technik“ entsprechen, damit trägt das Gesetz auch dem Fortschritt Rechnung.

DATENPORTABILITÄT: Unternehmen müssen personenbezogene Daten auf Antrag in einem gängigen und maschinenlesbaren Format übergeben und auf Wunsch direkt an ein anderes Unternehmen übermitteln können.

DATENSCHUTZBEAUFTRAGTER: In Zukunft brauchen alle Unternehmen, die mindestens zehn Personen mit automatisierter Verarbeitung beschäftigen, einen Datenschutzbeauftragten. Von dieser Pflicht sind künftig auch jene Unternehmen betroffen, zu deren Kerngeschäft die umfangreiche Verarbeitung besonderer personenbezogener Daten gehört, etwa Daten zum Kundenverhalten, zu Gesundheit oder Bankverbindungen.

ZERTIFIZIERUNG: Die DSGVO erlaubt durchaus den Unternehmen und ihren Datenschutz-Verantwortlichen, die Schutzmaßnahmen von einem gesetzlich festgelegten Zertifizierungsverfahren überprüfen zu lassen. Dieses sollte aber besonders die Regeln der DSGVO kontrollieren.

Es drohen Bußgelder bis zu

20 MILLIONEN €

STRAFEN: Noch ist Datenschutz kein Thema, um das sich Unternehmen Sorgen machen – offensichtlich konnten die geltenden Strafen nicht abschrecken. Höchstens 300.000 Euro wurden fällig, wenn Unternehmen gegen das Gesetz verstießen. Das ändert sich jetzt: Die neue DSGVO gibt nicht nur Pflichten zum Umgang mit personenbezogenen Daten vor, sie arbeitet auch mit hohen Strafen und Bußgeldern: Bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten Vorjahresumsatzes eines Unternehmens können Richter nun bei Nichtbeachtung von Gesetzen verlagern.

Datenschutz lohnt sich nicht nur, weil damit hohe Bußgelder vermieden werden. Praktischer und nachvollziehbarer Datenschutz ist ein Merkmal, mit dem insbesondere Online-Händler und Dienstleister bereits heute positiv auffallen und erfolgreich werben können. Nichts verunsichert Kunden mehr als die Nutzung ihrer Daten von unbekanntem Stellen und Unternehmen. ❖

✎ **DIE AUTOREN:** Tilman Dralle und Thomas Werner sind Juristen des TÜV Rheinland und haben sich auf Fragen rund um den Datenschutz spezialisiert.



DATENSCHUTZ

Der TÜV Rheinland veranstaltet am 7. und 8. November in Frankfurt am Main einen IT-Sicherheitskongress. Hier können Unternehmer, Datenschutz- und Sicherheitsverantwortliche in Workshops neue Gesetze und Sicherheitsverfahren diskutieren und in der begleitenden Fachausstellung neue Sicherheitstechnologien kennenlernen.

➔ Mehr Infos:

www.tuv.com/it-sicherheits-kongress