# News und Produkte

## Wenige Wettbewerbsvorteile durch DSGVO

Einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitkom unter 503 Unternehmen ab 20 Beschäftigten in Deutschland zufolge loben 67 Prozent der Befragten, dass die Datenschutzgrundverordnung (DSGVO) weltweit Maßstäbe für den Umgang mit personenbezogenen Daten setzt. Jedes zweite Unternehmen (50 Prozent) glaube, dass die DSGVO zu einheitlichen Wettbewerbsbedingungen innerhalb der EU führe. Allerdings sehen 70 Prozent aufgrund der unterschiedlichen Auslegung der DSGVO in den Mitgliedstaaten noch keinen EU-weiten einheitlichen Datenschutz. Und auch die Bewertung mit Blick auf das eigene Unternehmen falle überwiegend kritisch aus: So können laut Studie 40 Prozent keinen Wettbewerbsvorteil durch die DSGVO auf dem internationalen Markt für das eigene Unternehmen erkennen – und 30 Prozent sehen sogar Wettbewerbsnachteile. Dem stehen 16 beziehungsweise 13 Prozent gegenüber, die die DSGVO als geringen oder großen Wettbewerbsvorteil bezeichnen.

Die große Mehrheit haben die DSGVO inzwischen umgesetzt, entweder vollständig (22 Prozent) oder größtenteils (40 Prozent). Ein Drittel (33 Prozent) sieht sich erst teilweise am Ziel, nur 2 Prozent haben erst mit der Umsetzung begonnen – und kein Unternehmen hat laut Studie bisher nichts getan. Praktisch alle Unternehmen haben seit Einführung der DSGVO ihren Aufwand für Datenschutz hochgefahren: 16 Prozent stellen fest, dass dieser langsam wieder abnimmt, aber 47 Prozent gehen von einem gleichbleibend höheren Aufwand aus, 30 Prozent erwarten sogar, dass der bereits gestiegene Aufwand noch weiter zunimmt. Nur 6 Prozent sehen keinen Mehraufwand, für kein Unternehmen ist der Aufwand gesunken.

Dass die Umsetzung der DSGVO noch nicht weiter ist, liege nach Ansicht der Unternehmen überwiegend an Gründen, die sie nicht selbst zu verantworten haben. So sehen sie sich vor allem mit Rechtsunsicherheit und einer widersprüchlichen Auslegung der Datenschutzvorgaben innerhalb Europas und zwischen den Bundesländern konfrontiert. 88 Prozent gaben an, die Umsetzung der DSGVO sei nie vollständig abgeschlossen, etwa weil es neue Guidelines gibt; 78 Prozent sehen bestehende Rechtsunsicherheiten zu den Vorgaben der DSGVO als Hemmnis. 77 Prozent haben festgestellt, dass durch das Ausrollen neuer Tools immer wieder eine neue Prüfung in Gang gesetzt werde. 57 Prozent sehen in der uneinheitlichen Auslegung der DSGVO innerhalb der EU ein Hemmnis, 40 Prozent in der uneinheitlichen Auslegung in Deutschland. Und 52 Prozent beklagen eine mangelnde Beratung durch Aufsichtsbehörden. Aber auch unternehmensinterne Gründe bremsen die DSGVO-Umsetzung: 45 Prozent sagen, die erforderliche IT- und Systemumstellungen kosten viel Zeit, 32 Prozent fehlt es an finanziellen Mitteln, 24 Prozent an qualifizierten Beschäftigten. Rund jedes vierte Unternehmen (23 Prozent) binde die Datenschutzbeauftragten nur mangelhaft ein, 15 Prozent sehen ganz allgemein eine mangelnde Unterstützung im Unternehmen.

Entsprechend kritisch beurteilen die Unternehmen die Umsetzung des Datenschutzes in Deutschland. Zwei Drittel stellen fest, dass der strenge Datenschutz in Deutschland die Digitalisierung erschwert (68 Prozent), für fast ebenso viele hemmt der uneinheitliche Datenschutz die Digitalisierung (65 Prozent). Und 61 Prozent sagen, Deutschland übertreibe es mit dem Datenschutz – vor einem Jahr lag der Anteil noch bei 50 Prozent. (www.bitkom.org)

## Informationspaket „Risiko im Datenschutz"

Der Umgang mit Risiken ist nicht immer einfach – das sei auch im Datenschutzrecht so, stellt der Bayerische Landesbeauftragte für den Datenschutz (BayLDA) fest und hat bereits einige Hilfestellungen zum Thema veröffentlicht. Damit sich Risiken bei der Verarbeitung personenbezogener Daten noch leichter aufspüren und bewältigen lassen, habe man seine Erkenntnisse zu diesem Thema in einer Orientierungshilfe zusammengefasst. Das Papier „Risikoanalyse und Datenschutz-Folgenabschätzung" stelle Methode und Bausteine einer datenschutzrechtlichen Risikoanalyse vor, erläutere die Erarbeitung technisch-organisatorischer Maßnahmen und gebe Praxishinweise für die Durchführung von Risikoanalysen. Besonderen Wert lege das Papier auf den Gedanken der Skalierung: Risikoanalysen müssen nicht in jedem Fall aufwändig sein; je nach Anlass sind verschiedene „Ausbaustufen" möglich. Das werde anhand mehrerer konkreter Anwendungsfälle dargestellt.

Dabei ist die Orientierungshilfe nur das Kernstück eines umfangreicheren Informationspakets zum Thema „Risiko im Datenschutz". Zu diesem Paket gehört laut BayLDA insbesondere ein Set von Formularen, welche die Durchführung von Risikoanalysen anleiten und eine ordnungsgemäße Dokumentation unterstützen sollen. Der bereits vorhandene Werkzeugkasten werde auch in Zukunft weiter ergänzt.

„Mein Informationsangebot versetzt auch kleinere Staatsbehörden und Kommunen in die Lage,

mit Datenschutzrisiken adäquat umzugehen. Es enthält Werkzeuge, die zu einem strukturierten und systematischen Vorgehen anleiten. Der Einsatz dieser Werkzeuge ist an zahlreichen Beispielen erläutert. Wer sie ausprobiert, wird feststellen, dass eine Risikoanalyse kein theoretisches Glasperlenspiel ist, sondern einen ganz konkreten Nutzen hat," so der Bayerische Landesbeauftragte für den Datenschutz Prof. Dr. Thomas Petri.

Die Orientierungshilfe und die anderen Elemente des Informationspakets sind kostenfrei unter www.datenschutz-bayern.de/dsfa verfügbar. (www.datenschutz-bayern.de)

## Verhaltensregel „Trusted Data Processor" genehmigt

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat die nationale Verhaltensregel „Trusted Data Processor" genehmigt, mit der deutsche Unternehmen die Möglichkeit bekommen, Rechtssicherheit im Bereich Auftragsverarbeitung zu erhalten. „Trusted Data Processor" sorge durch Standardisierung für eine Vereinfachung sowohl für diejenigen, die sich der Verhaltensregel unterordnen, als auch für ihren Kundenkreis und die Unternehmenspartner. Verhaltensregeln sind ein mit der DSGVO eingeführtes Instrument, das der Konkretisierung von datenschutzrechtlichen Anforderungen dienen soll. An der Entwicklung von „Trusted Data Processor" wirkten Experten der Fachverbände Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. und Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V. mit.

Durch eine Selbstverpflichtung auf die Verhaltensregel können Auftragsverarbeiter nach außen sichtbar machen, dass sie sowohl den in der Verhaltensregel festgelegten Vorgaben folgen als auch sich deren Überwachung durch eine Überwachungsstelle unterwerfen. Die Überwachungsstelle ist Anlaufstelle für Beschwerden und kontrolliert regelmäßig die Einhaltung der Verhaltensregel. Mit der Genehmigung der Verhaltensregel wurde auch die DSZ Datenschutz Zertifizierungsgesellschaft mbH als Überwachungsstelle akkreditiert. Sie bearbeitet die Anträge auf Selbstverpflichtung und übernimmt die Kontrolle und Bearbeitung von Beschwerden.

Die aufsichtsbehördlich genehmigte Verhaltensregel „Trusted Data Processor" und weitere kostenlose Hilfsmittel für die tägliche Arbeit sind auf www.verhaltensregel.eu zu finden. (www.bvdnet.de)

## Über 90 Prozent der Gesundheitseinrichtungen haben Datenschutzvorfall erlitten

Laut einer aktuellen Studie des Unternehmens SOTI haben 91 Prozent der Gesundheitseinrichtungen in Deutschland (70 % weltweit) seit dem Jahr 2020 mindestens einen Datenschutzvorfall erlitten. Dennoch seien 83 Prozent der Befragten (76 % weltweit) der Meinung, eine vollständige Digitalisierung von Patientenakten könne die Datensicherheit verbessern und die Gefahr von Datenverlusten verringern. Doch die IT-Fachkräfte in Gesundheitseinrichtungen warnen auch vor Sicherheitslücken beim Umgang mit elektronisch geführten Patientendaten: So sind laut Studie fast zwei Drittel der in Deutschland Befragten (50 % weltweit) wegen mangelhafter Mitarbeiterschulung sowie gestohlenen beziehungsweise verloren gegangenen Geräten besorgt, die mitunter sensible Patientendaten beinhalten. 74 Prozent der befragten Fachkräfte aus dem Gesundheitsbereich (57 % weltweit) sehen hochsensible Patientendaten in Gesundheitseinrichtungen als gefährdeter denn je zuvor an. Ursachen für Sicherheitsvorfälle waren im Studienzeitraum besonders Datenverlust durch vorsätzliches oder fahrlässiges Fehlverhalten der Mitarbeiter (63 % in Deutschland; 49 % weltweit) und Datenschutzverletzungen aufgrund externer Ursachen, beispielsweise durch Distributed-Denial-of-Service-(DDoS)-Attacken (59 % in Deutschland; 48 % weltweit).

„Unter den von uns untersuchten Ländern ist Deutschland trauriger Spitzenreiter, wenn es um Sicherheitsvorfälle geht", sagt Stefan Mennecke, VP of Sales, Central, Eastern und Southern Europe bei SOTI. „Mangelnder Datenschutz zählt neben einer unvollständigen Integration verbundener Geräte und hohen Geräteausfallzeiten zu den Haupthindernissen einer erfolgreichen Digitalisierung im Gesundheitswesen."

Die befragten IT-Fachkräfte im Gesundheitswesen sehen an verschiedenen Stellen dann auch Nachholbedarf, allerdings werden mittlerweile immerhin bei 85 Prozent der in Deutschland befragten Gesundheitseinrichtungen (73 % weltweit) Datenschutztrainings für alle Mitarbeiter mit Zugriff auf Patientendaten durchgeführt. In 75 Prozent der Einrichtungen (68 % weltweit) sind laut Studie IT-Helpdesks oder entsprechende Apps für die schnelle Lösung von Problemen bei der Verwendung von IoT- und Telehealth-Geräten im Einsatz.

Die Studie „Eine entscheidende Investition: Am Puls der Technologie im Gesundheitswesen", für die im Juni 1300 IT-Entscheidungsträger in Einrichtungen, die Gesundheitsdienste für Patienten anbieten und in Unternehmen mit 50 oder mehr Mitarbeitern arbeiten, online befragt wurden, ist unter https://soti.de/branchen/gesundheitswesen kostenfrei als PDF verfügbar.(https://soti.de)