

24. Mai 2018

## **58% der Unternehmen haben keinen definierten Prozess, um auf Datenzugriffs-Anfragen gemäß DSGVO zu reagieren**

Eine neue Studie von BSI, dem British Standard Institution, hat ergeben, dass mehr als die Hälfte der europäischen Organisationen keinen festen Prozess zur Beantwortung von Datensubjekt-Zugriffsanordnungen (Data Subject Access Requests = DSAR) haben.

Ein DSAR ist der rechtliche Mechanismus, der es europäischen Bürgern ermöglicht, eine vollständige Übersicht über ihre gespeicherten persönlichen Daten zu erhalten, die eine Organisation über sie besitzt. Es ist eine Art Datenverwaltungsbericht, wie Informationen gespeichert werden, den jeder Bürger in der EU verlangen kann.

## **DSAR und die DSGVO**

Die am Freitag, den 25. Mai, in Kraft getretene DSGVO hat den Bürgerinnen und Bürger das Bewusstsein für ihre Datenrechte als betroffene Personen geschaffen.

Alle Unternehmen müssen im Rahmen der DSGVO strengere Vorschriften zum Datenschutz und zur Privatsphäre der betroffenen Personen (Bürger) in der EU einhalten. Die Nichteinhaltung könnte zu Geldstrafen von bis zu 20 Millionen Euro oder 4% des jährlichen globalen Umsatzes einer Organisation führen.

## **DSAR und Auswirkungen auf Ressourcen**

Während die Einreichung von Datenanfragen von Privatpersonen kein neues Phänomen ist, wird der Prozess mit der DSGVO deutlich einfacher. Die Art und Weise wie Organisationen einen Datenbericht erstellen hat sich außerhalb der traditionellen Postoption oder E-Mail-Kanäle erweitert und kann mündlich, über Live-Chat, per Telefon oder sogar über soziale Medien erfolgen.

Die Studie befragte die Organisationen auch, welche Kosten sie nach dem 25. Mai für den Umgang mit DSARs intern aufwenden würden. Jede fünfte Organisation veranschlagte hierbei Kosten von bis zu 28.000 €.

Gemäß der DSGVO wird erwartet, dass Organisationen die Datenberichte innerhalb eines Monats abschließen - anstatt wie bisher innerhalb von 40 Tagen. Datenquellen innerhalb einer Organisation können CCTV-Daten, Telefonanrufdaten, Web-Chat-Protokolldaten, CRM-Datensätze und Bestellhistorie enthalten. Wenn sich ein DSAR auf einen Mitarbeiter bezieht, kann er auch alle E-Mails, Besprechungsprotokolle, Dokumente und Korrespondenzen in Bezug auf ihre Arbeit enthalten. Es müssen alle Möglichkeiten offen gelegt werden, in denen der Name des Mitarbeiters erwähnt wird.

Stephen O'Boyle, Leiter der Abteilung Professional Services bei BSI, kommentierte die Studie folgendermaßen: "Die Implikationen von DSARs könnten sich als belastend erweisen: Die für die Durchführung eines DSAR erforderlichen Ressourcen können beträchtlich sein und sollten nicht unterschätzt werden. Von den Organisationen wird erwartet, dass sie innerhalb des durch die Datenschutz-Grundverordnung festgelegten Zeitraums von einem Monat riesige Datenmengen durchsuchen."

Es besteht auch die Befürchtung, dass Organisationen disruptive DSARs von verärgerten Kunden oder ehemaligen Mitarbeitern, Personen mit einem persönlichen Groll oder jemandem mit ausreichenden Kenntnissen, der eine Organisation mit einem umfassenden DSAR lähmen könnte, ausgesetzt sind. Stephen wandte sich direkt an britische Organisationen: "Das Motiv hinter DSARs ist nicht immer klar, aber das Endergebnis kann erhebliche Kosten in Bezug auf Ressourcen und das Risiko einer Beschwerde an das Büro des Informationskommissars beinhalten. Eine intensive Vorbereitung ist der Schlüssel:

Organisationen, die über einen strukturierten Plan verfügen und zusätzliche Ressourcen in Erwägung ziehen, wie z. B. zusätzliche Technologie und Schulung des Personals, werden das Risiko der Nichteinhaltung bei der Beantwortung eines DSAR reduzieren."

Die Cybersecurity- und Information Resilience-Abteilung von BSI bietet eine Reihe von Lösungen, die Organisationen dabei unterstützen, die Anforderungen der DSGVO zu erfüllen, darunter Beratung, Schulung, Forschung, technische Lösungen und ausgelagerte Datenschutzbeauftragte (DSB). Weitere Informationen finden Sie unter <https://www.bsigroup.com/de-DE/Unsere-Dienstleistungen/Cybersecurity/>.

**ENDE**

### Presseanfragen:

Maxi Kallina

BSI Group Deutschland GmbH

Tel: +49 69 2222 89 218

Email: [pr.de@bsigroup.com](mailto:pr.de@bsigroup.com)

### **Über BSI**

BSI Group (British Standard Institution) ist ein global agierendes Dienstleistungsunternehmen für Training, Auditierung und Zertifizierung. BSI prüft und bewertet weltweit Produkte und Managementsysteme nach international gültigen Normen in Unternehmen verschiedenster Branchen, zum Beispiel in der Luft- und Raumfahrt, der Automotive- und Lebensmittelindustrie sowie in den Bereichen Bau, Energie, Gesundheitswesen, IT und Handel.

Darüber hinaus gehören innovative Softwarelösungen, Cyber Security, Datenschutz, die Entwicklung von Standards und Normen sowie Weiterbildung zum Leistungsportfolio. Mit dem ganzheitlichen Modell zum Thema Organisatorische Widerstandsfähigkeit hilft BSI Unternehmen dabei, die eigene Organisation nachhaltig zukunftsfähig auszurichten. Als weltweit erste nationale Normungsorganisation und mit mehr als 100 Jahren Erfahrung ist BSI ein globaler Partner für 86.000 Unternehmen und Organisationen in über 193 Ländern.

Um mehr zu erfahren, besuchen Sie bitte: [www.bsigroup.com/de-DE/](http://www.bsigroup.com/de-DE/)

### **Über BSI Cybersecurity und Information Resilience Division**

Das Kompetenzzentrum für Cybersicherheit und Information Resilience der BSI Group hat seinen Sitz in Sandyford, Dublin. Es verwaltet und sichert die Unternehmensinformationen für globale Kunden. Das Unternehmen bietet seinen Kunden Fachwissen über die Identifizierung, den Schutz, die Einhaltung und die Verwaltung ihrer Informationsressourcen durch eine Kombination aus Beratung, Technologie, Forschung und Training. Die Mission ist es, Kunden dabei zu helfen, Informationen zu schützen und eine Umgebung zu schaffen, in der die Infrastruktur geschützt ist, in der regulatorische Compliance-Verpflichtungen erfüllt werden und die Menschen sicher sind.

Die Organisationen werden durch die Einhaltung international anerkannter Akkreditierungen und Zertifizierungen optimiert (CREST / Cyber-Essentials / Payment Card Industry Datensicherheitsstandard Qualified Security Assessor). BSI ist der Urheber der ISO 27000-Reihe für Informationssicherheitsstandards und der weltweit führende Anbieter von Schulungen und Zertifizierungen nach ISO 27001, der bewährten Methode für Informationssicherheits-Managementsysteme (ISMS).