DS-GVO: Fragen und Antworten

THE AUDIT COMPANY

Fragen	Antwort
Welche Verfahren/Prozesse sind innerhalb des Unternehmens zu implementieren, um dem Gesetz zu entsprechen?	Die DS-GVO sieht eine Reihe von Abläufen vor, die ab Mai 2018 umgesetzt werden müssen. Dabei ist es sowohl von der Organisation, dem Zweck und der Art der Verarbeitung personenbezogener Daten als auch von den Risiken für Rechte und Freiheiten natürlicher Personen abhängig, welche Prozesse in welcher Ausprägung etabliert werden müssen. Dies können u. a. Prozesse zum Risikomanagement (Datenschutz-Folgenabschätzung), zum Umgang mit Auskunftsersuchen von Personen oder Prozesse zu Reaktionsmechanismen bei Datenschutzverletzungen sein.
Gibt es Personen, die nicht interner Datenschutzbeauftragter werden können?	Prinzipiell kann jeder Beschäftigte – sowohl intern als auch extern – Datenschutzbeauftragter werden. Grundlage für eine Benennung ist eine geeignete berufliche Qualifikation. Umfassendes Fachwissen ist insbesondere auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis erforderlich. Wichtig ist auch die Fähigkeit, die in der DS-GVO genannten Aufgaben zu erfüllen. Da der Datenschutzbeauftragte für die Überwachung der Einhaltung der geltenden Datenschutzvorschriften zuständig ist, sollte es keine Person sein, welche im Interessenkonflikt mit der eigenen Hauptaufgabe stehen könnte, z. B. denkbar bei einem IT-Leiter oder Geschäftsführer. Der Datenschutzbeauftragte sollte seine Aufgaben unabhängig ausüben können. *Vgl. Artikel 37 und 39 DS-GVO*
Welche Informationen müssen der betroffenen Person mitgegeben werden?	Nach Artikel 12 DS-GVO lautet die Anforderung wie folgt: **Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person** (1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen …
Wie sieht die inhaltliche Gestaltung eines Vertrages mit einem Unternehmen aus, das Zugriff auf personenbezogene Daten erhält (Auftragsverarbeiter)?	Folgende Aspekte sind gem. Artikel 28 Absatz 2 und 3 DS-GVO im Vertrag zu regeln: Artikel 28 Absatz 2 ▪ Regeln sind festzulegen, z. B. zu Unterauftragsvergabe Artikel 28 Absatz 3 Satz 1 ▪ Gegenstand und Dauer der Verarbeitung ▪ Art und Zweck der Verarbeitung ▪ Art der personenbezogenen Daten ▪ Kategorien betroffener Personen ▪ Pflichten und Rechte des Verantwortlichen Artikel 28 Absatz 3 Buchstabe a)-h) ▪ Umfang der Weisungsbefugnisse ▪ Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit ▪ Sicherstellung von technischen und organisatorischen Maßnahmen ▪ Hinzuziehung von Subunternehmern ▪ Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener ▪ Unterstützung des Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen und der Datenschutz-Folgenabschätzung ▪ Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung ▪ Regelung, wie der Nachweis der Einhaltung der in Artikel 28 niedergelegten Pflichten erfolgt. Dies kann auch durch Überprüfungen und Inspektionen auch durch einen beauftragten Prüfer vereinbart werden. Artikel 28 Absatz 3 letzter Satz ▪ Pflicht des Auftragsverarbeiters, den Verantwortlichen unverzüglich zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt *Hinweis: Es ist zu überlegen, ob in dem Vertrag zur Auftragsverarbeitung auch das Thema Haftung aufgenommen werden soll (Artikel 28 Absatz 10).*

DQS GmbH
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen
August-Schanz-Straße 21
60433 Frankfurt am Main
Tel. +49 69 95427-0
informationssicherheit@dqs.de
www.dqs.de

Fragen	Antwort
Welche Aufzeichnungen / Dokumente sind vorzuhalten?	Der sogenannte Verantwortliche ist für die Einhaltung der DS-GVO „Grundsätze der Verarbeitung von personenbezogenen Daten“ verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht). Diese Rechenschaftspflicht kann zu erheblichen zusätzlichen Dokumentations- und Nachweispflichten führen, da Unternehmen nicht nur sicherstellen müssen, dass die einzelnen Anforderungen der DS-GVO erfüllt werden, sondern dies auch nachgewiesen werden kann. Dazu gehören u. a. das Verzeichnis aller Verarbeitungstätigkeiten, die Dokumentation der Datenschutz-Folgenabschätzung und der datenschutzrelevanten Prozesse und Anweisungen sowie die Ergebnisse der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen. *Vgl. Artikel 5 und 24 DS-GVO*
Wer hat das Recht auf Einsicht in diese Dokumente und in welcher Tiefe?	Jede Aufsichtsbehörde verfügt über die Untersuchungsbefugnis, die es ihr u. a. gestattet anzuweisen, alle zur Erfüllung ihrer Aufgaben – wie die Überwachung und Durchsetzung der DS-GVO – erforderlichen Informationen bereitzustellen. Es ist gut möglich, dass Aufsichtsbehörden künftig bei Beschwerden von betroffenen Personen oder bei Kontrollmaßnahmen grundsätzlich das Verarbeitungsverzeichnis einfordern werden. Auch der Auftragsverarbeiter hat gegenüber dem Verantwortlichen, der ihn beauftragt hat, bestimmte Informationspflichten.
Welche Fristen sind bei Anfragen auf Einsicht einzuhalten?	Die DS-GVO macht keine konkreten Angaben dazu. Sie regelt nicht, binnen welcher Frist z. B. die Auskunft bei einem Ersuchen durch eine Person über seine Daten zu erteilen ist. Empfehlung: Die Information sollte jedoch im zeitlichen Zusammenhang mit der Anfrage erteilt werden bzw. den Aufwand und die im Geschäftsverkehr üblichen Fristen berücksichtigen.
Wie sehen die konkreten aufeinanderfolgenden Schritte zum Aufbau eines Datenschutzsystems aus?	Es gibt aktuell einige behördliche Aktivitäten, die als Orientierungshilfe dienen können: z. B. das Kurzpapier Nr. 8 „Maßnahmenplan DS-GVO für Unternehmen“ der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) oder das Standard-Datenschutzmodell (SDM-Methodik).
Mit welchem zeitlichen Aufwand ist zu rechnen?	Der zeitliche Aufwand hängt im Wesentlichen von der Komplexität und dem Umfang der Verarbeitung personenbezogener Daten ab sowie vom Kenntnisstand des Auftragverarbeiters bzw. der Organisation. Siehe auch DS-GVO ▪ Artikel 2 „Sachlicher Anwendungsbereich“ Absatz 1 ▪ Artikel 3 „Räumlicher Anwendungsbereich“ Absatz 1-3
Welche Punkte des neuen Datenschutzgesetzes sind unbedingt umzusetzen, welche Punkte sind optional?	Ein Gesetz ist nie „optional“. Allerdings gibt es unter Umständen Anforderungen, die nicht zutreffend sind. Dies ist abhängig vom Unternehmen, der Art und dem Zweck der Verarbeitung personenbezogener Daten. Die DS-GVO sieht Öffnungsklauseln vor, die aber nur Konkretisierungen und Präzisierungen und keine grundsätzlichen Änderungen der Architektur erlauben (zukünftig im BDSGneu geregelt). Zusätzlich ist Folgendes vorgesehen: 1) Leitlinien der Artikel-29-Gruppe zur Umsetzung der DS-GVO. Nach Konstituierung des Europäischen Datenschutzausschusses (EDSA) sollen diese vom EDSA übernommen werden. *Hinweis: Der Europäische Datenschutzausschuss ist eine Einrichtung der Europäischen Union. Er soll sicherstellen, dass die DS-GVO in den EU-Mitgliedstaaten einheitlich angewandt wird. Dazu soll er zusätzlich zu den nationalen Datenschutzbehörden die ordnungsgemäße Anwendung der DS-GVO überwachen und sicherstellen, die Europäische Kommission in Datenschutzfragen beraten, Leitlinien und Empfehlungen bereitstellen.* 2) Auslegungshilfen zum neuen Datenschutzrecht Die deutsche Datenschutzkonferenz (DSK) veröffentlicht Kurzpapiere. „Diese Kurzpapiere dienen als erste Orientierung, wie nach Auffassung der Datenschutzkonferenz die DS-GVO im praktischen Vollzug angewendet werden sollte.“ Dabei ist zu beachten, dass diese Auffassung unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss steht. *Hinweis: DS-GVO Artikel 63: Kohärenzverfahren* *Um zur einheitlichen Anwendung dieser Verordnung in der gesamten Union beizutragen, arbeiten die Aufsichtsbehörden im Rahmen des in diesem Abschnitt beschriebenen Kohärenzverfahrens untereinander und ggf. mit der Kommission zusammen.*

Fragen	Antwort
Wie kann man aus der europaweit gültigen DS-GVO ersehen, welche Regeln für alle Länder gleich gelten oder wo es länderspezifisch unterschiedliche Regeln gibt?	Länderspezifische Regelungen sind in der DS-GVO nicht zu finden. Die sogenannten Öffnungsklauseln sollen den Mitgliedstaaten aber die Möglichkeit geben, nationale Regelungen zu treffen. Allgemeine Öffnungsklauseln finden sich beispielsweise in Artikel 6 Absatz 2, 3 und 4 DS-GVO.
Gibt es eine Übersicht, wie mögliche Vertragsgestaltungen für die Angebote externer Datenschutzbeauftragter an Unternehmen ausschließlich nach den Pflichten aus der neuen DS-GVO und auch die Ausgestaltung von allgemeinen Beratungsangeboten an Unternehmen ausschließlich nach den neuen EU-Regelungen aussehen könnten?	Die DQS kann und darf hierzu nicht beratend tätig sein oder gar solche Empfehlungen aussprechen. Als akkreditiertes Unternehmen müssen wir neutral und unabhängig sein.

Stand: August 2017

Die umfangreichen Vorschriften der DS-GVO bereiten Unternehmen oftmals Schwierigkeiten: „Wo fängt man mit der Umsetzung an, was ist neu?“, „Welche Prozesse müssen datenschutzgerecht gestaltet werden, um Compliance sicherzustellen?“ und „Wie ist die Konformität zum Schutz und zum Umgang mit personenbezogenen Daten zu dokumentieren?“

Die Nichterfüllung der gesetzlichen Anforderungen birgt ein hohes Risikopotenzial. Es wird also nicht ausbleiben, die eigene Datenschutzpraxis zu überprüfen und das Datenschutzmanagement bis zum 25. Mai 2018 nach den Vorgaben der DS-GVO anzupassen und weiterzuentwickeln. Vor diesem Hintergrund haben die Mitglieder des Arbeitskreises Datenschutz der Bitkom eine Reihe praktischer Leitfäden erarbeitet, die im Internet kostenfrei zur Verfügung stehen – www.bitkom.org/Bitkom/Publikationen. Die DQS GmbH ist Mitglied im Bitkom und im Arbeitskreis Datenschutz. Wir freuen uns auf das Gespräch mit Ihnen: informationssicherheit@dqs.de.