datenschutz-berater.de

46. Jahrgang DSB 09/2022

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Dr. Markus Lang

Zeit für ein Datenschutz-Audit? – Notwendigkeit, Verantwortlichkeit und Umfang

Anlässe für ein Datenschutz-Audit kann es viele geben: Datenschutzvorfälle im Unternehmen, Verlautbarungen von Aufsichtsbehörden, Gerichtsentscheidungen oder der „Geburtstag der DSGVO" im Mai eines jeden Jahres. In der Praxis besteht jedoch oft Unklarheit darüber, ob es eine allgemeine Pflicht zur Vornahme von Datenschutz-Audits gibt und wenn ja, wer diese Pflicht zu erfüllen hat und in welchem Umfang solche Audits durchzuführen sind. Diese Fragen werden im vorliegenden Beitrag beantwortet.

Pflicht oder Kür?

„Audit" in der DSGVO

Die DSGVO enthält weder eine Vorschrift mit dem Begriff „Audit" noch eine explizite Verpflichtung im Sinne einer systematischen Untersuchung und Bewertung der Verarbeitung personenbezogener Daten sowie der Maßnahmen, die zur Gewährleistung des Datenschutzes getroffen wurden. Allerdings müssen die nach der DSGVO zu ergreifenden technischen und organisatorischen Maßnahmen (TOM) überprüft und aktualisiert werden. Diese Regelung in Art. 24 Abs. 1 Satz 2 DSGVO hat zwar genau genommen lediglich eine fest- und klarstellende Wirkung. Die zwingende Notwendigkeit, einmal getroffene Maßnahmen bei Bedarf anzupassen oder zu ergänzen, folgt bereits aus Art. 24 Abs. 1 Satz 1 DSGVO. Die Überprüfung und Aktualisierung sind untrennbar mit der fortlaufenden Umsetzungspflicht gem. Art. 24 Abs. 1 Satz 1 DSGVO verbunden. Nach dieser Vorschrift haben Verantwortliche – risikobasiert – geeignete TOM umzusetzen, um eine datenschutzrechtskonforme Verarbeitung sicherzustellen und hierfür den Nachweis erbringen zu können. Die Nachweispflicht konkretisiert die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO, wonach der Verantwortliche die Einhaltung der Datenschutzgrundsätze gem. Art. 5 Abs. 1 DSGVO nachweisen können muss.

Die übergreifende Verpflichtung gem. Art. 24 DSGVO, die ergriffenen TOM zu überprüfen und ggf. zu aktualisieren, wird in Art. 32 Abs. 1 lit. d DSGVO als Einzelpflicht in Bezug auf die Sicherheit der Verarbeitung konkretisiert: Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung geben. Diese konkretisierte Pflicht gilt gem. Art. 32 Abs. 1 DSGVO auch für Auftragsverarbeiter und ist als solche nach Art. 28 Abs. 3 Satz 2 lit. c DSGVO zwischen Verantwortlichen und Auftragsverarbeitern zwingend zu vereinbaren. Im Kontext der Regelungen zur Auftragsverarbeitung sieht Art. 28 Abs. 3 Satz 2 lit. h DSGVO außerdem vor, dass Auftragsverarbeiter Überprüfungen ermöglichen müssen, damit der Verantwortliche sich fortlaufend von der Ordnungsmäßigkeit der Auftragsverarbeitung überzeugen kann.

Schließlich sind regelmäßige Kontrollen der technischen und organisatorischen Maßnahmen als Pflicht des Datenimporteurs verankert in den Modulen I bis III der Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, die geeignete Garantien gem. Art. 46 Abs. 2 lit. c DSGVO sein können. Das geht einher mit der Verpflichtung, dem Datenexporteur Kontrollmöglichkeiten in Bezug auf die Einhaltung der in den Klauseln vereinbarten Pflichten einzuräumen, soweit es sich um eine Übermittlung von Verantwortlichen an Auftragsverarbeiter (Modul II) und eine Übermittlung zwischen Auftragsverarbeitern (Modul III) handelt. Eine entsprechende Verpflichtung – allerdings für den Datenexporteur – enthält auch Modul IV für die Übermittlung von Auftragsverarbeitern an Verantwortliche.

Erforderlichkeit

Die Pflicht zur Überprüfung und etwaigen Aktualisierung der TOM steht gem. Art. 24 Abs. 1 Satz 2 DSGVO unter dem Vorbehalt der Erforderlichkeit („erforderlichenfalls"). Eine Überprüfung der Maßnahmen ist erforderlich, wenn sich die tatsächlichen oder rechtlichen Rahmenbedingungen ändern oder geändert haben. Relevant sein können Änderungen der Rechtslage durch

- neue oder geänderte Vorschriften,
- Rechtsprechung,
- aufsichtsbehördliche Entscheidungen zur Rechtmäßigkeit einer Verarbeitung und
- die Ausübung der Befugnisse durch die Aufsichtsbehörden, z. B. Abhilfe- und Genehmigungsbefugnisse gem. Art. 58 Abs. 2 und 3 DSGVO.

In tatsächlicher Hinsicht können insbesondere Änderungen bei der konkreten Verarbeitung – z. B. in Bezug auf die Art der Daten, den Umfang der Verarbeitung, die Einschaltung oder den Wechsel eines Auftragsverarbeiters – sowie (sicherheits-)technische Entwicklungen einen Überprüfungsbedarf auslösen.

Wer? (Verpflichtete)

Es obliegt dem Verantwortlichen, im Rahmen des Art. 32 Abs. 1 lit. d DSGVO auch dem Auftragsverarbeiter und bei

Datenübermittlungen in Drittländer auf der Grundlage von Standardvertragsklauseln – je nach Konstellationen – den Datenimporteuren und den Datenexporteuren, erstens die Umstände festzustellen, die einen Überprüfungsbedarf auslösen, und zweitens zu entscheiden, ob eine Anpassung oder Ergänzung bestehender Maßnahmen angezeigt ist.

Die Pflichten des Verantwortlichen und des Auftragsverarbeiters zur Überprüfung dürfen nicht verwechselt werden mit der eigenständigen Überwachungspflicht betrieblicher Datenschutzbeauftragter, die diesen in Art. 39 Abs. 1 lit. b DSGVO als originäre Aufgabe zugewiesen ist. Es ist allerdings zulässig, betriebliche Datenschutzbeauftragte bei Audits zur Beratung im Rahmen ihres gesetzlichen Mandats heranzuziehen. Damit gehen jedoch weder die rechtliche Pflicht noch die Verantwortlichkeit für deren Durchführung auf die Datenschutzbeauftragten über.

Was? (Gegenstand)

Die Überprüfungs- und Aktualisierungspflicht nach Art. 24 Abs. 1 Satz 2 DSGVO umfasst die nach der DSGVO zu ergreifenden Maßnahmen, die technischer und organisatorischer Art sein sollen. Im Rahmen der konkretisierten Einzelpflicht nach Art. 32 Abs. 1 lit. b DSGVO handelt es sich speziell um Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Der Begriff der „technischen und organisatorischen Maßnahmen" wird in der DSGVO nicht definiert, obwohl er auch an anderen Stellen mehrfach verwendet wird, z. B. in Art. 5 Abs. 1 lit. e und Art. 28 Abs. 1. Es gibt lediglich eine punktuelle Erläuterung anhand von Beispielen in ErwGr. 78 Satz 2 und 3 zur DSGVO. Der Begriff der technischen und organisatorischen Maßnahmen ist ein Ober- und Sammelbegriff, der weit auszulegen ist. Eine eindeutige Zuordnung und Unterscheidung zwischen technischen Maßnahmen einerseits und organisatorischen Maßnahmen andererseits ist nicht in jedem Fall möglich und mit Blick auf den Regelungszweck auch nicht nötig, da die gesetzlichen Vorgaben in Bezug auf die Art der Maßnahmen keinen Unterschied machen.

Was konkret als Gegenstand des Audits bestimmt werden sollte, hängt zunächst davon ab, ob es ein anlassbezogenes oder anlassunabhängiges Audit ist. Der Gegenstand eines anlassbezogenen Audits ergibt sich zwangsläufig aus dem Aspekt, der sich geändert hat. Gibt es bspw. neue oder geänderte Positionen der Datenschutzaufsicht oder Gerichtsentscheidungen – z. B. zu Anforderungen an bestimmte Verarbeitungen, Maßnahmen oder Prozesse wie die Erteilung einer Auskunft nach Art. 15 DSGVO – sollte sich das Audit aus Gründen der Zweckmäßigkeit auf diesen Punkt beschränken. Im Übrigen kann der Gegenstand eines Audits frei bestimmt werden.

Datenschutz-Audits können eine bestimmte oder mehrere Verarbeitungen, Anwendungen, Systeme, Unternehmensbereiche oder das ganze Unternehmen umfassen. Allerdings ist auch für die Planung und Durchführung anlassunabhängiger Audits eine Schwerpunktsetzung im Hinblick auf Prozesse, Produkte/Services oder Organisationseinheiten zu empfehlen. Das erfordert keine strikte Trennung dieser Bereiche. Eine isolierte Herangehensweise ist aufgrund der inhaltlichen Überschneidungen häufig auch gar nicht möglich und nicht sinnvoll, was auch die folgenden Beispiele für eine Schwerpunktsetzung erkennen lassen:

- Prozesse zum Löschen von Daten, ggf. differenziert nach Kategorien der betroffenen Personen (Kunden, Beschäftigte etc.);
- Prozess für Datenschutzverletzungen;
- Datenverarbeitung im Online-Bereich, ggf. differenziert nach Website, Social-Media-Anwendungen etc.;
- Auftragsverarbeitung, ggf. Auswahl bestimmter Verarbeitungen oder Auftragsverarbeiter oder Differenzierung nach Art und Umfang der Verarbeitung;
- Datenverarbeitung durch bestimmte Organisationseinheiten wie Vertrieb, Personal etc.;
- Sicherheitstechnische Aspekte im Rahmen von cloudbasierten Verarbeitungen;
- Datenschutzmanagement des Unternehmens.

Wie? (Vorgehen)

Regelmäßige Überprüfung

Die Pflicht, die ergriffenen TOM zu überprüfen und ggf. zu aktualisieren, lässt sich nicht durch einmaliges Handeln erfüllen, sondern ist eine dauerhafte Verpflichtung. Das bedeutet: Bei sich ändernden Rahmenbedingungen, aufgrund derer eine Anpassung oder Ergänzung der TOM angezeigt ist, muss eine entsprechende Aktualisierung der Maßnahmen erfolgen. Daher ist unter Risikogesichtspunkten, eine regelmäßige Überprüfung der ergriffenen TOM zu empfehlen.

Während Art. 32 Abs. 1 lit. d DSGVO als konkretisierte Einzelpflicht in Bezug auf die Sicherheit der Verarbeitung sowohl für Verantwortliche als auch Auftragsverarbeiter eine regelmäßige Überprüfung vorsieht, enthält die übergreifende Verpflichtung des Verantwortlichen gem. Art. 24 Abs. 1 DSGVO keine entsprechende Vorgabe. Art. 24 Abs. 1 DSGVO schreibt auch keinen bestimmten oder regelmäßigen Prüfrhythmus vor. Das ändert allerdings nicht daran, dass es Sache des Verantwortlichen und mit Blick auf die eigene Pflicht gem. Art. 32 Abs. 1 lit. d DSGVO auch Sache des Auftragsverarbeiters ist, relevante Änderungen der rechtlichen und tatsächlichen Rahmenbedingungen, also etwaige Umstände festzustellen, die einen Überprüfungs- und Änderungsbedarf hinsichtlich der TOM auslösen können. Das wird ohne eine gewisse Regelmäßigkeit und Dauerhaftigkeit kaum möglich sein. Für Verantwortliche ist eine regelmäßige Überprüfung schließlich auch mit Blick auf die Rechenschaftspflicht („Accountability") gem. Art. 5 Abs. 2 DSGVO angezeigt.

Daher sollte die Durchführung regelmäßiger Audits ein Element des Datenschutzmanagements sein. Dabei sind die Zeiträume für Datenschutz-Audits risikoorientiert zu bestimmen und hierzu insbesondere die Art der personenbezogenen Daten, die Kategorien und Anzahl der betroffenen Personen sowie der Umfang der Verarbeitung zu berücksichtigen. Allgemeingütige Empfehlungen wie „alle ein bis zwei Jahre" stehen diesem risikobasierten Ansatz entgegen. Die festgelegten Zeiträume müssen im Ergebnis zu keinem starren Prüfrhythmus führen, z. B. wenn zwischenzeitlich andere Umstände eine Überprüfung vor dem geplanten Zeitpunkt ausgelöst haben.

Umfang

Der Umfang eines Datenschutz-Audits muss ebenfalls dem Risiko der Verarbeitung angemessen sein. Die Detailtiefe von Audits ist wie deren Häufigkeit auf der Grundlage des in Art. 24 Abs. 1 Satz 1 DSGVO verankerten risikobasierten Ansatzes zu bestimmen, der auch bei der Festlegung der TOM zum Tragen kommt. Der gesetzlich notwendige Umfang einer Überprüfung der Maßnahmen hängt also von den Risiken ab, die von der Verarbeitung ausgehen. Die bei der Risikoabwägung zu berücksichtigenden Aspekte werden in Art. 24 Abs. 1 Satz 1 DSGVO genannt: Art, Umfang, Umstände und Zweck der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen. Für die konkretisierte Einzelpflicht in Bezug auf Sicherheit werden in Art. 32 Abs. 1 DSGVO außerdem noch der Stand der Technik und die Implementierungskosten aufgeführt. Darüber hinaus sollten bei der Konzeption von Datenschutz-Audits auch Art, Umfang, Ergebnis und Zeitpunkt bereits erfolgter Maßnahmen zur Umsetzung und Überprüfung der DSGVO-Vorgaben bedacht werden.

Methodik

Das Vorgehen bei einem Datenschutz-Audit unterscheidet sich grundsätzlich nicht davon, wie andere Audits durchgeführt werden. Regelmäßig bietet sich ein Mix aus Dokumentensichtung, Vor-Ort-Prüfung und Befragung an. Dabei können standardisierte Fragebogen und Checklisten eine gute Arbeitshilfe sein. Ihr Einsatz stellt sicher, dass alle relevanten Aspekte berücksichtigt werden, die erhobenen Informationen sich relativ einfach analysieren lassen und gewisse inhaltliche Audit-Standards im Unternehmen etabliert und genutzt werden können. Bei der Frage nach dem Inhalt und Aufbau solcher Fragebogen und Checklisten können u. a. die von einigen Datenschutzaufsichtsbehörden veröffentlichten Fragebogen hilfreich sein, z. B. vom Bayerischem Landesamt für Datenschutz (www.lda.bayern.de/media/pruefungen/201810_rechenschaftspflicht_fragebogen.pdf). Das Beispiel der bayerischen Aufsicht deckt die wesentlichen Vorgaben der DSGVO ab, z. B. Datenschutzorganisation, rechtskonforme Verarbeitung, Rechte der betroffenen Personen und Datenschutzverletzungen. Der Fragenkatalog kann daher für eine übergreifende Überprüfung der Datenschutzkonformität im Unternehmen als eine Art „Basis-Audit" genutzt werden. Es lassen sich aber auch einzelne Fragen herausgreifen und Teil-Audits für die entsprechenden Themenkomplexe durchführen.

Für Datenschutz-Audits wird zuweilen auch eine an die ISO-Management-Methodik und den entsprechenden Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018) angelehnte Vorgehensweise in Betracht gezogen. Das kann von Vorteil sein, wenn ein Datenschutz-Managementsystem nach ISO/IEC 27701 installiert wurde. Abgesehen davon sollte in Abhängigkeit von den konkreten Gegebenheiten – wie z. B. der Etablierung von ISO-Standards im Unternehmen und insbesondere auch dem konkreten Gegenstand des Datenschutz-Audits – im Einzelfall entschieden werden, ob ein solches Vorgehen tatsächlich geeignet ist. Hierbei ist zu beachten, dass der Gegenstand einer Auditierung nach ISO 19011:2018 die Managementsysteme sind, also – lediglich – die Prozesse, mit denen sichergestellt wird, dass die jeweiligen Anforderungen wirksam umgesetzt werden.

Integration in das Datenschutz- und Informationssicherheitsmanagement

Ein regelmäßiges Datenschutz-Audit muss nicht zwingend als ganz neuer oder separater Prozess aufgesetzt und durchgeführt werden. Vielmehr kann und sollte das Audit mit vorhandenen oder geplanten Datenschutzmanagement-Prozessen verknüpft werden, um unnötigen Aufwand zu vermeiden und Synergien nutzen zu können. Das gilt nicht nur für die gesetzlich explizit vorgeschriebenen Überprüfungen, z. B. für Verarbeitungen, die Gegenstand einer Datenschutz-Folgenabschätzung sind (Art. 35 Abs. 11 DSGVO). Für diese Fälle hat der Gesetzgeber die in Art. 24 Abs. 1 DSGVO festgeschriebene Pflicht von Überprüfungen nochmals aufgegriffen und bereits konkretisiert. Vielmehr lässt sich die Durchführung von Datenschutz-Audits auch sehr gut mit Prozessen rund um das Verzeichnis von Verarbeitungstätigkeiten verknüpfen oder in diese integrieren. Besteht ein – zu empfehlender – Prozess für eine regelmäßige Überprüfung und Aktualisierung der im Verzeichnis enthaltenen Angaben, sollte er auch die Überprüfung der Geeignetheit der TOM umfassen oder zumindest damit verknüpft sein. Weitergehende Aspekte eines Datenschutz-Audits – wie z. B. die Überprüfung der Rechtsgrundlage – können sich daran anschließen.

Aufgrund der inhaltlichen Überschneidungen bietet sich grundsätzlich auch eine Verknüpfung mit den Prozessen des Informationssicherheitsmanagements an. Dabei sind die jeweils spezifischen Besonderheiten zu berücksichtigen, indem die hierfür erforderlichen gesonderten Betrachtungen und Teilprozessschritte vorgesehen werden. Diese besondere Herausforderung besteht allerdings nicht

nur in Bezug auf Audits, sondern bei der Verknüpfung von Datenschutz- und Informationssicherheitsmanagement insgesamt.

Folgemaßnahmen

Führt ein Audit zu dem Ergebnis, dass die getroffenen TOM nicht mehr i. S. d. Art. 24 Abs. 1 Satz 1 DSGVO bzw. Art. 32 Abs. 1 DSGVO geeignet sind, müssen die Maßnahmen aktualisiert werden. Diese Aktualisierung kann zu einer Änderung oder Anpassung bestehender oder zur Einführung neuer und zusätzlicher Maßnahmen führen. Auf diese Weise kann sichergestellt und der Nachweis erbracht werden, dass die Verarbeitung gem. den DSGVO-Vorgaben erfolgt.

Es ist auch möglich, dass bestehende Maßnahmen infolge einer Überprüfung eingeschränkt oder ganz zurückgenommen werden. Das kann bspw. der Fall sein, wenn aufgrund geänderter rechtlicher oder tatsächlicher Rahmenbedingen bestimmte Risiken in Bezug auf die konkrete Verarbeitung personenbezogener Daten entfallen oder geringer geworden sind. Es ist z. B. denkbar, dass die Notwendigkeit eines Transfer Impact Assessment (TIA) für Übermittlungen in ein bestimmtes Drittland aufgrund eines neuen Angemessenheitsbeschlusses entfällt. Maßstab und Grenze zugleich ist in jedem Fall die Feststellung, dass die Verarbeitung weiterhin gem. den Vorgaben der DSGVO erfolgt.

Sonderfall: Auftragsverarbeitung

Der Verantwortliche ist auch im Fall einer Auftragsverarbeitung alleiniger Adressat der Pflicht, geeignete TOM gem. Art. 24 Abs. 1 Satz 1 DSGVO zu ergreifen. Auftragsverarbeiter haben zwar eigene gesetzliche und vertragliche Pflichten gem. Art. 32 und Art. 28 Abs. 3 Satz 2 lit. c und h DSGVO einschließlich der Pflicht zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung. Ungeachtet dieser eigenen Pflichten sind Auftragsverarbeiter nicht Adressat der Vorgaben von Art. 24 DSGVO. Das korrespondiert zum einen mit der Pflicht des Verantwortlichen, nur mit Auftragsverarbeitern zusammenzuarbeiten, die hinreichende Garantien für geeignete technische und organisatorische Maßnahmen bieten (Art. 28 Abs. 1 DSGVO), und zum anderen mit den gesetzlichen Vorgaben für den Inhalt eines Vertrags über eine Auftragsverarbeitung. Dieser Vertrag muss u. a. verbindliche Vorgaben zu den TOM und deren Überprüfung enthalten (Art. 28 Abs. 3 Satz 2 lit. b, c und h DSGVO). Der Verantwortliche muss die Überprüfung durchführen oder von einem Beauftragten durchführen lassen und angezeigte Aktualisierungen der TOM herbeiführen, um seiner Pflicht aus Art. 24 Abs. 1 DSGVO zu genügen.

Die Überprüfung muss nicht zwangsläufig als Vor-Ort-Kontrolle stattfinden. Sie kann bspw. auch remote und durch Vorlage von Dokumenten erfolgen. Hierzu eignen sich insbesondere Sicherheitskonzepte und Berichte von externen und internen Prüfern des Auftragsverarbeiters, z. B. der Revision. Die Entscheidung, wie im konkreten Fall vorzugehen ist, muss auf Basis des risikobasierten Ansatzes erfolgen. Dabei ist wieder auf die in Art. 24 Abs. 1 Satz 1 DSGVO genannten und bereits oben aufgegriffenen Faktoren abzustellen.

Nicht ausreichend ist es, sich ausschließlich auf mehr oder weniger allgemeine Aussagen des Auftragsverarbeiters zu verlassen, z. B. „regelmäßige Audits mit Zertifizierung; zuletzt 2021“. Es sollte zumindest die entsprechende Dokumentation angefordert und eingesehen werden. Bei dieser Vorgehensweise können bspw. konkret der Gegenstand und Umfang des Audits, die Person und Institution des Auditors sowie die Art eines etwaigen Zertifikats festgestellt werden. Im Extremfall – wie ihn der Autor dieses Beitrags in seiner Beratungspraxis erleben musste – kann bei der Kontrolle der Dokumentation sogar zum Vorschein kommen, dass ein Audit tatsächlich nur mittelbar oder gar keine Aspekte des Datenschutzes zum Gegenstand hatte, weil ein allgemeines Qualitätsaudit oder ein Umweltaudit durchgeführt wurde.

Zertifizierung

Art. 42 DSGVO sieht für Verantwortliche und Auftragsverarbeiter die Möglichkeit vor, die Einhaltung der DSGVO bei Verarbeitungsvorgängen in einem gesetzlich festgelegten Verfahren durch eine externe Stelle zertifizieren zu lassen. Das in diesem Rahmen letztlich zu durchlaufende Audit ist von dem in diesem Beitrag behandelten Datenschutz-Audit abzugrenzen. Die Zertifizierung nach Art. 42 DSGVO wird freiwillig sein (Abs. 3) und mindert nicht die Verantwortung des Verantwortlichen und des Auftragsverarbeiters für die Einhaltung der DSGVO (Abs. 4). Es bleibt also bei sämtlichen Pflichten nach der DSGVO einschließlich der Überprüfung und Aktualisierung der TOM gem. 24 Abs. 1 Satz 2 DSGVO und Art. 32 Abs. 1 lit. d DSGVO sowie des entsprechenden Nachweises durch Verantwortliche und Auftragsverarbeiter. Allerdings wird eine – bislang noch nicht verfügbare – Zertifizierung nach Art. 42 DSGVO u. a. als Nachweis für die Erfüllung dieser Pflichten herangezogen werden können.

Sanktionen

Ein Verstoß des Verantwortlichen gegen seine Überprüfungs- und Aktualisierungspflicht nach Art. 24 Abs. 1 Satz 2 DSGVO kann für sich genommen nicht nach Art. 83 Abs. 4 und 5 DSGVO sanktioniert werden. Art. 24 DSGVO ist anders als die weiter konkretisierenden Vorschriften Art. 25 ff. DSGVO nicht in den Bußgeldkatalogen aufgeführt. Es ist jedoch nicht ausgeschlossen, dass Aufsichtsbehörden im Rahmen ihrer Befugnisse gem. Art. 58 Abs. 2 lit. d DSGVO Anweisungen zur Einhaltung von Art. 24 DSGVO erteilen, z. B. die Überprüfung der TOM, und bei Nichtbefolgen gem. Art. 83 Abs. 5 lit. e oder Abs. 6 DSGVO eine Geldbuße verhängen.

Zudem kann das Fehlen eines Verfahrens zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung sowohl bei Verantwortlichen als auch bei Auftragsverarbeitern nach Art. 83 Abs. 4 lit. a DSGVO mit Geldbußen von bis zu 10 Mio. EUR oder 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden. Aufgrund der abstrakten Vorgaben mit einer Vielzahl unbestimmter Rechtsbegriffe, mit denen die Pflichten gem. Art. 32 Abs. 1 DSGVO normiert sind, und aufgrund der Notwendigkeit einer Abwägung wird in der Praxis regelmäßig eine konkretisierende Anordnung der Aufsichtsbehörde gem. Art. 58 Abs. 2 DSGVO vorausgehen, deren Nichtbefolgung gem. Art. 83 Abs. 5 lit. e und Abs. 6 DSGVO bußgeldbewehrt ist.

Schließlich kann die Nichtdurchführung von Datenschutz-Audits mittelbar zu Sanktionen führen, wenn technische und organisatorische Maßnahmen aufgrund geänderter Rahmenbedingungen nicht mehr geeignet sind, weil sie im Laufe der Zeit – z. B. in Form von Audits – nicht überprüft und entsprechend angepasst wurden. Stellt die Aufsicht fest, dass die u. a. in Art. 25 DSGVO und Art. 32 DSGVO konkretisierten TOM nicht geeignet sind, ist dies ein bußgeldbewehrter Verstoß nach Art. 83 Abs. 4 lit. a DSGVO. Entsprechendes gilt für die Kontrollen der TOM, die für Vereinbarungen über eine Auftragsverarbeitung und in den Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer vorgeschrieben sind.

Fazit

Die DSGVO enthält keine explizite Verpflichtung zu einem „Audit“ im Sinne einer systematischen Untersuchung und Bewertung der Verarbeitung personenbezogener Daten sowie der Maßnahmen, die zur Gewährleistung des Datenschutzes getroffen wurden. Es gibt lediglich konkretisierte Einzelpflichten, regelmäßige Kontrollen bzw. ein entsprechendes Verfahren vorzusehen, die in Bezug auf die Sicherheit der Verarbeitung gesetzlich in Art. 32 Abs. 1 lit. d DSGVO und im Kontext der Auftragsverarbeitung sowie der Datenübermittlung in Drittländer auf der Grundlage von Standardvertragsklauseln als vertragliche Pflichten vorgesehen sind.

Eine systematische Untersuchung und Bewertung der Verarbeitungsprozesse einschließlich der Schutzmaßnahmen sind jedoch erforderlich, um die umfangreichen DSGVO-Pflichten erfüllen zu können. Das gilt im besonderen Maße für den Verantwortlichen, der nur auf diese Weise eine datenschutzrechtskonforme Verarbeitung sicherstellen und den Nachweis hierfür erbringen kann. Darüber hinaus können Datenschutz-Audits auch dabei helfen, die Datenschutzorganisation kontinuierlich zu verbessern.

Wann ein Datenschutz-Audit angezeigt ist und wie ein solches konkret aufzusetzen und durchzuführen ist, hängt von mehreren Faktoren ab. Dazu zählen u. a. der Umfang und die Art der Verarbeitung, aber auch Art, Umfang, Ergebnis und Zeitpunkt bereits erfolgter Maßnahmen zur Umsetzung der DSGVO-Vorgaben.

Datenschutz-Audits müssen nicht als separater Prozess aufgesetzt werden und sollten grundsätzlich als ein wesentliches Element im Datenschutzmanagement implementiert sein.

Autor: **Dr. Markus Lang ist selbständiger Rechtsanwalt in Düsseldorf mit den Tätigkeitsschwerpunkten Datenschutz- und IT-Recht (www.datenschutzrecht-praxis.de). Er ist zertifizierter Datenschutzbeauftragter und Datenschutzauditor sowie Lehrbeauftragter an der Hochschule Düsseldorf (Business Analytics).**