Formularhandbuch Datenschutzrecht

Bearbeitet von
Herausgegeben von Dr. Ansgar Koreng, Rechtsanwalt, und Dr. Matthias Lachenmann, Rechtsanwalt, Bearbeitet von den Herausgebern und von Bilal Abedin, Dr. Holger Achtermann, Matthias Bergt, Nikolaus Bertermann, Dr. Martin Braun, Dr. Stefan Brink, Christian Diekmann, LL.M., Michael Huth, Jörg Jaenichen, Dr. Olaf Koglin, Sascha Kremer, Dr. Joachim Müller, Malaika Nolde, LL.M., Dr. Carlo Piltz, Dr. Frederike Rehker, Stefan Sander, LL.M., B.Sc., Stephan Schmidt, Sebastian Schwiering, Steffen Weiß, LL.M., und Bernhard C. Witt

2. Auflage 2018. Buch inkl. Online-Nutzung. XXVIII, 1042 S. Mit Zugang zur Online-Version in beck-online DIE DATENBANK für einen Nutzer. In Leinen

ISBN 978 3 406 69542 1

Format (B x L): 16,0 x 24,0 cm

fürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben; beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung); Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen; Anforderungen an die Eignung als Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren; den geprüften Sachbereich so zu umschreiben, dass Bürger, Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können; Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

Die Fachverbände „Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V." und „Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V." haben im Jahr 2013 eine Datenschutzzertifizierung mit der anschließenden Ausgabe eines Siegels für die **Auditierung der Auftragsdatenverarbeitung** entwickelt. Grundlage der Auditierung ist der öffentlich zugängliche Datenschutzstandard „DS-BvD-GDD-01". Der Standard gilt für alle Branchen und Dienstleistungen. Er beschreibt insbesondere, welche Anforderungen ein Auftragnehmer erfüllen muss. Die Zertifizierung geht in diesem Fall mit einer Auditierung des Datenschutzverfahrens und Datenschutzmanagements einher (es handelt sich also nicht um eine IT-produktbezogene Auditierung). Vor dem Hintergrund der Anwendbarkeit der DS-GVO ist die Überarbeitung des Datenschutzstandards „DS-BvD-GDD-01" durch den GDD für das Jahr 2017 geplant. Die im Rahmen einer Prüfung auf Grundlage dieses Standards untersuchten Bereiche umfassen unter anderem das Input-Management, das Auftragsmanagement, das Datenschutzkonzept, das IT-Sicherheitskonzept und das Datenschutz-Managementsystem. Die Überprüfung selbst wird durch unabhängige akkreditierte Auditoren durchgeführt. Diese erstellen einen Prüfbericht, der von einer unabhängigen Zertifizierungsstelle geprüft und veröffentlicht wird. Dieses Auditverfahren wurde aufgrund des offenen Standards und der Unabhängigkeit der Auditoren und damit auch der Prüfung von dem Landesdatenschutzbeauftragten in Nordrhein-Westfalen befürwortet.

Das Konzept des Datenschutzaudits findet sowohl Fürsprecher als auch Kritiker. So wird etwa darauf verwiesen, dass Prüfungen durch unabhängige Gutachter gerade für kleinere Unternehmen mit erheblichen Kosten und Aufwendungen verbunden sein können (zuletzt *Gola/Schomerus,* BDSG, § 9a Rn. 5). Hervorgehoben wird dagegen etwa der positive Effekt eines freiwilligen Datenschutzaudits, der eine öffentlichkeitswirksame Imagepflege und die Eigenwerbung für Unternehmen zur Folge haben kann (Plath/*Plath,* 1. Aufl., § 9a BDSG Rn. 2). Auch eine stärkere marktwirtschaftliche Effektivierung des Datenschutzes könnte die Folge sein (*Bäumler,* CR 2001, 795 (796)).

Wie schon die DSRL sieht auch die DS-GVO ein Datenschutzaudit nicht ausdrücklich vor. Allerdings enthält die DS-GVO weitreichende Selbstregulierungs- und Zertifizierungsmöglichkeiten, sodass sich jedenfalls die **Zertifizierungskomponente** des bisherigen Audits nach § 9a BDSG in der DS-GVO wiederfindet und darüberhinausgehend ausgebaut wird.

Wichtig ist die Unterscheidung zwischen der Zertifizierung und dem Audit: Die Zertifizierung stellt die Folge eines zuvor durchgeführten Audits dar. Ein Audit (wie hier beschrieben) kann aber auch ohne anschließende Zertifizierung erfolgen. Zertifizierungen werden unter der DS-GVO eine wichtige Rolle für die Praxis spielen. Eine besondere Nähe besteht zwischen dem Datenschutzaudit und den Vorgaben

zur Zertifizierung in Art. 42 DS-GVO. Nach Art. 42 Abs. 1 S. 1 DS-GVO sind die nationalen Gesetzgeber, die Aufsichtsbehörden, der Europäischen Datenschutzausschuss sowie die Europäische Kommission verpflichtet, die Einführung von Zertifizierungsverfahren und Datenschutzsiegeln sowie -prüfzeichen zu fördern. Die unter der DS-GVO für eine Zertifizierung in Betracht kommenden Gegenstände umfassen, wie auch bisher, Produkte und Dienstleistungen (Gola/*Lepperhoff,* DS-GVO, Art. 43 Rn. 9).

Hauptzweck der Zertifizierung in der DS-GVO ist, den Nachweis gegenüber Aufsichtsbehörden und Verantwortlichen über die Einhaltung der Vorschriften der DS-GVO bei Verarbeitungsvorgängen führen zu können (vgl. Art. 42 Abs. 1 S. 1 DS-GVO). Audits können also eine Erleichterung bei der Erfüllung der **Nachweispflicht** des Art. 5 Abs. 2 DS-GVO sein (dazu → A.I.) Insbesondere für die Praxis im internationalen Datentransfer dürften die Vorgaben des Art. 42 Abs. 2 DS-GVO von Relevanz sein, wonach Zertifizierungen zum Nachweis geeigneter Garantien im Rahmen der Übermittlung personenbezogener Daten an **Drittländer** dienen können. Darüber hinaus können einige durch die DS-GVO etablierte Nachweispflichten, etwa der Nachweis über die Einhaltung geeigneter technischer und organisatorischer Maßnahmen gem. Art. 24 Abs. 3 und Art. 32 Abs. 3 DS-GVO oder der Nachweis der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 3 DS-GVO, mittels Zertifizierung erfüllt werden. Dabei soll gem. Art. 42 Abs. 1 S. 2 DS-GVO den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung getragen werden. Die Zertifizierungen sollen sich, zumindest dem Grundgedanken nach, also nicht nur an Konzerne und große Unternehmen richten (*Laue/Nink/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, S. 263 f.). Ob Zertifizierungsverfahren in der Praxis unter der DS-GVO tatsächlich auf die Bedürfnisse kleinerer Unternehmen zugeschnitten sein werden, muss sich jedoch zeigen. Potential für die Akzeptanz neuer, leicht umsetzbarer Zertifizierungsverfahren besteht in der Praxis sicherlich.

Nach richtiger Ansicht des Bayerischen Landesamtes für Datenschutzaufsicht, dient die Zertifizierung nach der DS-GVO zudem Kunden und Geschäftspartner eines Unternehmens, sich über die **Einhaltung datenschutzrechtlicher Vorgaben** vergewissern zu können (Arbeitspapier des BayLDA zur Zertifizierung – Art. 42 DS-GVO, https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf). Die in Art. 42 f. DS-GVO vorgesehenen Zertifizierungen helfen Verantwortlichen und Auftragsverarbeitern insbesondere, ihren Nachweispflichten nachzukommen (Gola/*Lepperhoff,* DS-GVO, Art. 43 Rn. 1). Ein durchgeführtes Audit, welches in der Erteilung eines Zertifikats mündet, bietet damit verschiedenen Stellen die Möglichkeit, schnell und effektiv eine rechtskonforme Verarbeitung bei einer Stelle prüfen zu lassen, ohne selbst zeit- und kostenintensive Prüfungen vornehmen zu müssen. Daneben muss auch auf die außenwirksame Bedeutung eines durchgeführten Audits und einer positiven Zertifizierung für datenverarbeitende Stellen hingewiesen werden. Gerade im B2C-Bereich kann der Nachweis eines Zertifikats Vertrauen bei Kunden schaffen.

Die Art. 42 f. DS-GVO regeln die Anforderungen an das Verfahren für Datenschutzsiegel und -prüfzeichen sowie an die Akkreditierung von Zertifizierungsstellen. Konkrete inhaltliche Anforderungen an das Audit im Rahmen der Zertifizierung oder einen Prüfkatalog fehlen jedoch.

Die bisher wirkungslose Regelung des § 9a BDSG a.F. wird nach dem 25.5.2018 keinen Bestand haben (*Kühling/Martini et al.,* Die DS-GVO und das nationale Recht, 2016, S. 362 f.). Allerdings ist mit Einführung der Art. 42 f. DS-GVO zumindest eine Zertifizierung vorgesehen, die der Selbstregulierung von Unternehmen dienen soll (vgl. oben). In § 39 BDSG n. F. ist eine Regelung zur Erteilung der Befugnis, als Zertifizierungsstelle nach der DS-GVO tätig zu werden, vorgesehen. Die Befugnis wird durch die Deutsche Akkreditierungsstelle erteilt, muss aber in Einvernahme mit der zuständigen Aufsichtsbehörde erfolgen. Dies zeigt, dass der deutsche Gesetzgeber ein Interesse daran hat, die Regeln der DS-GVO zu Zertifizierungen national mit Leben zu füllen. In Zukunft werden die Zertifizierung und damit die ihr vorgelagerte Auditierung eine deutlich größere Rolle spielen als derzeit. Je nach konkreter Ausformung in der Praxis bieten die Regelungen der DS-GVO zudem das Potential, Zertifizierungen und Prüfzeichen zu attraktiven Alternativen (etwa im Fall von Datentransfers in Drittstaaten) für Unternehmen zu entwickeln und damit auch Datenschutzaudits weiter zu etablieren.

Der nachfolgende Fragenkatalog ermöglicht eine Basisauditierung von Unternehmen zur Feststellung des im Unternehmen bestehenden Datenschutzstandards. In den Anmerkungen werden jeweils Hinweise auf weitere vertiefende Prüfformulare in diesem Buch gegeben, die mit dem Basisaudit kombiniert werden können.

Nr.	*Frage*	*Anm. Auditor*
1	**Unternehmen**	
1.1	**Bitte legen Sie ein aktuelles Organigramm des Unternehmens oder der Unternehmensgruppe vor.[1]**	
1.2	**Benennen Sie sämtliche Standorte Ihres Unternehmens jeweils mit Angabe der wesentlichen am Standort stattfindenden Datenverarbeitungen (Stichworte).[2]**	
1.3	**Befinden sich Standorte des Unternehmens außerhalb der EU oder des Europäischen Wirtschaftsraumes („EWR")?**	
1.4	**Sofern es Standorte außerhalb der EU oder des EWR gibt, erfolgt mit diesen Standorten ein Austausch von Daten oder eine gemeinsame Nutzung von IT-Ressourcen?[3]**	
1.5	**Geben Sie die Anzahl der Mitarbeiter Ihres Unternehmens an, bei mehreren Standorten bitte auch pro Standort. Differenzieren Sie nach fest angestellten Mitarbeitern, Auszubildenden, Aushilfen, Praktikanten, Studenten etc.[4]**	
1.6	**Benennen Sie Produkte und Dienstleistungen Ihres Unternehmens und erläutern Sie diese stichwortartig.[5]**	
1.7	**Werden im Unternehmen – außerhalb der Personalabteilung – besondere Arten personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) verarbeitet?[6]**	

Nr.	*Frage*	*Anm. Auditor*
1.8	Werden im Unternehmen automatisierte Einzelfallentscheidungen mit unmittelbarer Wirkung für den Betroffenen getroffen? [7]	
1.9	Verarbeitet das Unternehmen (auch) personenbezogene Daten von Kindern? Falls ja, auf welcher Rechtsgrundlage erfolgt die Verarbeitung? [8]	
1.10	Besteht in Ihrem Unternehmen oder der Unternehmensgruppe ein Betriebsrat?[9]	
2	Datenschutzdokumentation	
2.1	Bitte legen Sie das aktuelle Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO) vor.[10]	
2.2	Falls das Verzeichnis von Verarbeitungstätigkeiten unvollständig ist oder nicht existiert, benennen Sie bitte die Abteilungen und Prozesse im Unternehmen, die mit personenbezogenen Daten umgehen.[11]	
2.3	Sofern konzernverbundene Unternehmen mit personenbezogenen Daten des Unternehmens umgehen, legen Sie bitte die entsprechenden Vereinbarungen nach Art. 28 DS-GVO vor oder benennen Sie die Rechtsgrundlage für die Übermittlung. [12]	
2.4	Legen Sie bitte eine Liste aller Dienstleister vor, die für Sie im Rahmen einer Auftragsverarbeitung tätig sind und fügen Sie die abgeschlossenen Verträge zur Auftragsverarbeitung bei. Vermerken Sie bitte – soweit bekannt – jeweils, wenn der Vertrag ganz oder teilweise auf Standardvertragsklauseln (Art. 28 Abs. 7, 8 DS-GVO) beruht, ob sich der Auftragsverarbeiter zur Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) verpflichtet hat und/oder gem. Art. 42 DS-GVO zertifiziert ist.[13]	
2.5	Bitte legen Sie von den Auftragsverarbeitern bereitgestellte Unterlagen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DS-GVO vor.[14]	
2.6	Falls die Liste der Auftragsverarbeiter unvollständig ist oder nicht existiert, übergeben Sie dem Auditor bitte eine Liste der Unternehmen und Dienstleister, die für Sie Datenverarbeitungen vornehmen (inkl. Wartung von Datenverarbeitungsanlagen).	
2.7	Wie wird im Unternehmen sichergestellt, dass die Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur nach Weisung des Verantwortlichen verarbeiten?[15]	

Nr.	*Frage*	*Anm. Auditor*
2.8	Verfügt das Unternehmen über ein Datenschutzmanagementsystem und wird dieses aktiv genutzt?[16]	
2.9	Bestehen Zertifizierungen nach Art. 42 DS-GVO?[17]	
3	Datenschutzorganisation	
3.1	Ist im Unternehmen ein Datenschutzbeauftragter („DSB") bestellt? Falls ja, teilen Sie bitte die Kontaktdaten mit und machen Sie Angaben zur Qualifikation des DSB.[18]	
3.2	Falls kein DSB bestellt ist: Bitte legen Sie unter Berücksichtigung von Art. 37 DS-GVO und nationaler Regelungen zum Datenschutzbeauftragten dar, warum eine Bestellung nicht erforderlich ist.[19]	
3.3	Wenn ein DSB bestellt ist: Wie wird sichergestellt, dass er über neue Verfahren oder Änderungen bestehender Verfahren frühzeitig informiert wird?[20]	
3.4	Wie ist organisatorisch sichergestellt, dass vor jeder Verarbeitung von personenbezogenen Daten geprüft wird, ob die geplante Verarbeitung zulässig ist?	
3.5	Besteht ein Prozess für die Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen?[21]	
3.6	Wie ist im Unternehmen sichergestellt, dass die Informationspflichten gegenüber den Betroffenen vollständig und rechtzeitig erfüllt werden?[22]	
3.7	Wie werden im Unternehmen die Grundsätze des „Datenschutz durch Technikgestaltung" (Privacy-by-design) und der „datenschutzfreundlichen Voreinstellungen" (Privacy-by-default) umgesetzt?[23]	
3.8	Hat das Unternehmen ein Datenschutzkonzept?[24] Falls ja: Bitte vorlegen.	
3.9	Gibt es im Unternehmen ein aktuelles Rollen- und Rechtekonzept?[25]	
3.10	Wer legt im Unternehmen fest, welche (Zugriffs-)Rechte Mitarbeiter bei Einstellungen oder Versetzungen erhalten und welche ggf. entzogen werden müssen?	
3.11	Erfolgt die organisatorische Rechtebewilligung getrennt von der technischen Rechteeinräumung? Wie wird dokumentiert, welche Rechte ein User erhält?	
3.12	Besteht ein standardisierter Prozess beim Ausscheiden von Mitarbeitern?[26]	

Nr.	*Frage*	*Anm. Auditor*
3.13	Ist die private Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und ggf. weiteren dienstlichen Geräten klar geregelt? Bitte Regelung vorlegen.[27]	
3.14	Wie wird bei einem bestehenden Verbot der privaten Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und weiteren dienstlichen Geräten die Einhaltung des Verbots kontrolliert?[28]	
3.15	Besteht ein Prozess zur Beauftragung externer Dienstleister, die mit personenbezogenen Daten umgehen? Bitte legen Sie eine Prozessbeschreibung vor.	
3.16	Wer legt die Anforderungen an die technischen und organisatorischen Maßnahmen fest, die externe Dienstleister einzuhalten haben?	
3.17	Existiert ein dokumentierter Prozess zum Umgang mit Auskunftsverlangen nach Art. 15 DS-GVO? Bitte legen Sie die Prozessbeschreibung vor.[29]	
3.18	Wie wird das Recht auf Datenübertragbarkeit vom Unternehmen sichergestellt? Besteht ein entsprechender Prozess?[30]	
3.19	Wie ist sichergestellt, dass Forderungen Betroffener nach Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten geprüft und umgesetzt werden können?[31]	
3.20	Sofern personenbezogene Daten öffentlich gemacht wurden: Welche Prozesse sind implementiert, wenn Betroffene ihr Recht auf Vergessenwerden gelten machen?[32]	
3.21	Wie werden Widersprüche Betroffener gegen Datenverarbeitungen auf Grundlage einer Interessenabwägung vom Unternehmen geprüft und umgesetzt?[33]	
3.22	Wie ist die Einhaltung der gesetzlichen Archivierungs- und Löschungsfristen im Unternehmen sichergestellt?	
3.23	Besteht ein Maßnahmenplan für den Fall, dass der Schutz personenbezogener Daten verletzt wird (Art. 33, 34 DS-GVO)?[34]	
3.24	Wie erfolgt die regelmäßige Unterrichtung der Beschäftigten zu Datenschutzthemen? Besteht ein Schulungsplan?[35]	
4	IT-Systeme	
4.1	Bitte legen Sie eine Übersicht über die IT-Infrastruktur und alle Systeme vor, auf denen personenbezogene Daten verarbeitet werden.	

Nr.	*Frage*	*Anm. Auditor*
4.2	Bitte benennen Sie, sofern nicht in 4.1 enthalten, die zentralen Standorte von Datenverarbeitungssystemen und deren Hauptaufgaben.	
4.3	Werden die Standorte regelmäßig einer externen Prüfung unterzogen (z. B. ISO 27001, IT-Grundschutz, geprüftes Rechenzentrum)? Bitte legen Sie die jeweils aktuellen Prüfberichte vor.[36]	
4.4	Unterziehen Sie Systeme regelmäßigen Sicherheitsüberprüfungen (z. B. Penetration-Tests oder Security Audit Trails)? Bitte legen Sie aktuelle Prüfberichte oder Logs vor.	
4.5	Setzen Sie eine zentrale Unternehmenssoftware (ERP-System) ein? Falls ja, welche?[37]	
4.6	Sofern Sie eine ERP-Software einsetzen, wird diese auf eigenen Systemen (intern oder Housing), auf fremden Systemen (Hosting) oder als SaaS-Lösung betrieben?[38]	
4.7	Besteht ein externer Zugriff auf einzelne oder alle Systeme im Netzwerk (z. B. für Home Office, E-Mail-Abruf oder Fernwartung)? Bitte listen Sie auf, welche Nutzergruppen auf welche Systeme Zugriff haben und wie dieser Zugriff abgesichert wird.[39]	
4.8	Können Mitarbeiter auf Ihren Clients, Laptops oder Tablets eigenständig Software installieren?[40]	
4.9	Werden die Festplatten/Speichereinheiten mobiler Geräte verschlüsselt?[41]	
4.10	Setzen Sie ein Mobile Device Management ein?[42] Falls ja, welches?	
4.11	Nutzt das Unternehmen oder nutzen Mitarbeiter und Abteilungen Cloud-Speicherdienste wie Google Drive, Dropbox oder Microsoft OneDrive?[43]	
4.12	Nutzt das Unternehmen Cloud-Services wie Salesforce (CRM), Datapine (Data Analytics) oder ähnliche Dienste?[44]	
4.13	Besteht ein IT-Sicherheitskonzept?[45] Bitte legen Sie dieses vor.	

Anmerkungen

1. Organigramm. Anhand des Organigramms kann der Auditor sich einen ersten Überblick über das Unternehmen, die Abteilungen und die verantwortlichen Perso-

nen verschaffen. Bei der Prüfung des Verzeichnisses der Verarbeitungstätigkeiten kann abgeglichen werden, ob die Verantwortlichkeiten richtig benannt sind und der Auditor wird in die Lage versetzt, zielgerichtet Fragen an die verantwortlichen Personen zu stellen.

2. Standorte. Die Frage nach Unternehmensstandorten ermöglicht dem Auditor eine Orientierung, ob regelmäßig oder dauerhaft Datenaustausch zwischen Standorten erfolgt. Bei verschiedenen Standorten ist z. B. im Rahmen der Prüfung der technischen und organisatorischen Maßnahmen insbesondere zu beachten, ob diese an den verschiedenen Standorten unterschiedlich ist. Häufig bestehen mindestens beim Zugang zu Gebäuden und Datenverarbeitungsanlagen Unterschiede. Ein Datenaustausch zwischen verschiedenen Standorten eines Unternehmens führt regelmäßig auch dazu, dass der Auditor besonderes Augenmerk auf die Sicherheit des Datenaustausches zwischen den Standorten richten muss (Art. 32 DS-GVO). Handelt es sich bei den verschiedenen Standorten sogar um unterschiedliche Unternehmen, so sind die Anforderungen an eine rechtmäßige Übermittlung zu erfüllen oder es bedarf entsprechender Vereinbarungen zur Auftragsverarbeitung (Art. 28 DS-GVO), dazu → G.I.

3. Drittstaaten. Erfolgt ein Datenaustausch mit Konzerngesellschaften in einem Drittland, muss jeweils die Rechtsgrundlage dafür gesondert geprüft werden (z. B. Einwilligung, EU-Standardvertragsklauseln, EU-US Privacy Shield oder verbindliche interne Datenschutzvorschriften nach Art. 47 DS-GVO), dazu → G.VII.

4. Größe der Standorte. In der Regel hat die Größe eines Standortes datenschutzrechtlich keine Auswirkung, für den Auditor ist sie vor allem bei kleinen Standorten, in denen einzelne Personen möglicherweise mehrere Funktionen ausüben und daher ggf. auch mit umfassenden Rechten ausgestattet sind, von Bedeutung, da er hier ggf. konkret prüfen muss, wie Vier-Augen-Prozesse und innerbetriebliche Kontrollen ausgestaltet sind.

5. Produkte und Dienstleistungen. In gut strukturierten Unternehmen sollte die Frage unnötig sein, da sich alle Datenverarbeitungen unmittelbar aus dem Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) ergeben sollten. Häufig ist dies jedoch nicht der Fall, so dass die Abfrage von Produkten und Dienstleistungen im Freitext dem Auditor regelmäßig wichtige Hinweise auf datenschutzrechtlich relevante Vorgänge gibt.

6. Besondere Kategorien personenbezogener Daten. In der Personalabteilung fallen regelmäßig Angaben zur Gewerkschaftszugehörigkeit oder der Gesundheit an. Für den Auditor ist es wichtig zu wissen, ob außerhalb der Personalabteilung ebenfalls mit besonderen Kategorien personenbezogener Daten umgegangen wird. Die Verarbeitung solcher Daten setzt voraus, dass eine Einwilligung des Betroffenen vorliegt oder einer der aufgeführten Ausnahmetatbestände des Art. 9 Abs. 2–4 DS-GVO vorliegt. Zudem gelten diese Daten als besonders sensibel und bedürfen eines besonderen Schutzes (ErwG 51 DS-GVO), was der Auditor bei seiner Bewertung entsprechend berücksichtigen muss.

7. Automatisierte Einzelfallentscheidungen. Die zunehmende Automatisierung in Unternehmen führ dazu, dass auch immer mehr Entscheidungen in Unternehmen durch – entsprechend parametrisierte – Software getroffen werden. Schon Art. 15