DS-GVO:

Datenschutz im Unternehmen

FAQ-Liste

in

Zusammenarbeit

mit den IHKs und HWKs

1. Was ist im Unternehmen wirklich umzusetzen?

Bei der Umsetzung der DS-GVO gibt es keine Ausnahmen hinsichtlich des Umfangs der Umsetzungspflichten. Die DS-GVO ist vollumfänglich zu beachten. Zusätzlich dazu auch die Bestimmungen des BDSG, soweit in der DS-GVO eine Öffnungsklausel dafür besteht.

Eckpunkte der Umsetzung sollten auf jeden Fall sein:

- Erstellung eines Verarbeitungsverzeichnisses
- Informationspflichten
- Wahrung der Rechte der betroffenen Person
- Prüfung der Notwendigkeit eines DSB
- Auftragsverarbeitung

Nicht erforderlich ist es, pauschal eine Einwilligung in die Datenverarbeitung von jedem Kunden einzuholen.
Es ist auch nicht erforderlich, dass der Kunde die zu Verfügung gestellten Informationen nach Art. 13/14 DS-GVO unterschreiben oder anderweitig bestätigen muss.

2. Gibt es „Datenschutzfallen“ wie die angebliche Anforderung von Datenschutz-Musterformularen gegen Gebühr?

Dazu kann der TLfDI nicht Stellung nehmen, da hier keine erweiterten Kenntnisse über das am Markt erhältliche Angebot oder dessen Qualität bestehen.

Der TLfDI hält auf seiner Webseite jedenfalls eine Vielzahl von Mustern und Beispielen unentgeltlich zum Download bereit (siehe bitte unter www.tlfdi.de) z.B. Formulierungshilfe zum Auftragsverarbeitungsvertrag (AVV), Formulierungshilfe zur Einwilligung, Muster für die Erstellung eines Verarbeitungsverzeichnisses.

3. Müssen bestehende Einwilligungserklärungen, Auftragsverträge und Verarbeitungsdokumentationen geändert werden? (z.B. Zusätze gemäß DS-GVO: hinsichtlich Widerrufbarkeit, zwingende Regelung zur Unterbeauftragung im Auftragsverarbeitungsvertrag (AVV), Anpassung Technisch-Organisatorischer Maßnahmen (TOM) in Verarbeitungsverzeichnissen)

Im Rahmen der Umstellung auf die DS-GVO ist es notwendig, alle im Unternehmen benutzten Erklärungsvordrucke, Verträge und Dokumentationen hinsichtlich ihrer weiteren Gültigkeit und Übertragbarkeit auf die Anforderungen der DS-GVO hin zu prüfen.

Bestehende Einwilligungen behalten nur dann ihre Gültigkeit weiter, wenn sie schon den Anforderungen an die DS-GVO entsprachen, also einen Hinweis auf die jederzeitige Widerrufbarkeit enthalten und auch sonst dem Art. 7 DS-GVO entsprechen. Sie müssen zudem hinreichend transparent sein, zweckgebunden und dürfen nicht pauschal erteilt sein. Weiterhin sollte der Verantwortliche prüfen, ob er hinsichtlich der Einwilligungen seiner Nachweispflicht nachkommen kann.

Auftragsverarbeitungsverträge sind ebenfalls an die neuen Bestimmungen der DS-GVO anzupassen. Zum einen, weil es die Normen, auf die sich in den Vertragswerken bezogen wird, nicht mehr gibt, da das BDSG in seiner alten Fassung nicht mehr gültig ist, zum anderen, weil Art. 28 DS-GVO Mindestanforderungen an den Inhalt eines AVVs stellt. (eine Formulierungshilfe für einen AVV befindet sich auf der Webseite des TLfDI; siehe unter 2.) Hinsichtlich der Verarbeitungsdokumentationen sind die Beschreibungen der technischen und organisatorischen Maßnahmen weitestgehend ähnlich oder gelichgeblieben. Es muss nur darauf geachtet werden, dass ein Verarbeitungsverzeichnis nach Art. 30 DS-GVO mehr beinhaltet als nur eine Auflistung der TOMs.

4. Wo muss der Betrieb besonders sensibel reagieren?

Grundsätzlich sind die Anforderungen an die Datenverarbeitung gleich, egal um welche Art von Daten es sich handelt. Auch die Erhebung von Daten mittels optisch-elektronischen Einrichtungen (Video) o.ä. unterfallen der Anwendbarkeit der DS-GVO. Bei besonderen Kategorien personenbezogener Daten, wie z.B. Gesundheitsdaten, Daten zur religiösen Überzeugung, Daten zur ethnischen Herkunft, Daten zur sexuellen Orientierung, Daten über strafrechtliche Verurteilungen usw, ist zu beachten, dass diese zusätzlich zu Art. 6 DS-GVO den besonderen Voraussetzungen nach Art. 9 und 10 DS-GVO unterliegen, wonach grundsätzlich eine ausdrückliche Einwilligung für die Verarbeitung notwendig ist. Zudem ist ggf. in diesen Fällen auch eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 3 lit. b) DS-GVO). Hinweise hierzu befinden sich in den Kurzpapieren Nr. 5 und 18 der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und in der „Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich – Art. 35 DS-GVO“ vom TLfDI : https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/ .

5. Wie sehen die wesentlichen Informationspflichten für einen Handwerksbetrieb aus?

Der Inhalt der Informationspflichten ergibt sich aus Art. 13 bzw. 14 DS-GVO. Gemäß Art.13 DS-GVO muss der Betroffene informiert werden, wenn die Daten direkt bei ihm erhoben werden. Weiterhin enthält Art.14 DS-GVO die Informationspflichten gegenüber dem Betroffenen bei einer indirekten Erhebung, also nicht beim Betroffenen selbst.

Die einzelnen Angaben im Rahmen des Art. 13 DS-GVO, die der Verantwortliche zum Zeitpunkt der Erhebung der Daten zur Verfügung stellen muss sind dort explizit und erschöpfend genannt. Im Einzelnen sind das folgende:

a. den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b. gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c. die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e. gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f. gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b. das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c. wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e. ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Bei einer Information nach Art. 14 DS-GVO an den Betroffenen muss zusätzlich mitgeteilt werden, aus welcher Quelle die Daten stammen und ob sie ggf. aus öffentlich zugänglichen Quellen stammen.

6. Ist das Einstellen der Informationen auf der Homepage des Handwerksunternehmens/-organisation ausreichend?

Gemäß Art. 13 DS-GVO sind die Informationen dem Betroffenen bei Erhebung der Daten vom Verantwortlichen zur Verfügung zu stellen. Würde mit dem Betroffenen ausschließlich elektronisch kommuniziert und würden auf diesem Wege Daten erhoben, kann die Verweisung auf eine Website auf der die Informationen nach Art. 13/14 DS-GVO hinterlegt sind, ausreichend sein. Wenn der Verantwortliche mit dem Betroffenen nur schriftlich oder persönlich kommuniziert, muss er die Informationen durch Übergabe an den Betroffenen oder durch Aushänge im Ladengeschäft o.ä. gewährleisten. Die Informationen müssen sich auf jeden Fall auf den jeweiligen Verantwortlichen beziehen und konkret genug sein. Ob sich dies durch einen Verweis auf die Homepage einer Handwerksorganisation verwirklichen lässt erscheint daher höchst zweifelhaft.

7. Was ist der Unterschied zwischen Einwilligung und Informationspflicht; wo ist Beides erforderlich?

Die Informationspflicht besteht gem. Art. 13/14 DS-GVO, sobald Daten von einer Person erhoben werden. Sei es durch Abfragen von Name und Adresse oder weitere Angaben zur Person. Immer dann ist dem Betroffenen die weitere Verarbeitung transparent darzulegen. Dies geschieht anhand der Informationen die ich als Verantwortlicher zur Verfügung stellen muss. Damit weiß der Betroffenen wer die Daten verarbeitet, zu welchen Zwecken, an wen sie übermittelt werden, wie lange sie gespeichert werden usw.

Eine Einwilligung hingegen ist eine Rechtsgrundlage gem. Art 6 Abs. 1 S. 1 lit. a) DS-GVO aufgrund derer Daten verarbeitet werden können. Auch wenn ich eine Einwilligung zur Verarbeitung einhole, muss man noch auch die Informationspflichten nach Art. 13/14 DS-GVO erfüllen.

8. Was sind personenbezogene Daten und wie gehe ich mit diesen um?

Was personenbezogenen Daten sind, ist in Art. 4 Nr. 1 DS-GVO definiert.

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder **indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Darunter fallen alle mit einer natürlichen Person in Verbindung zu bringenden Informationen.

9. Gibt es beim Umgang mit personenbezogenen Daten einen Unterschied zwischen der Speicherung in elektronischer Form und Papier?

Nein. Es gibt keinen Unterschied. Die DS-GVO ist anwendbar unabhängig von der Verarbeitungsweise und folgt daher in Art. 2 Abs. 1 DS-GVO einem technikneutralen Ansatz. Sie findet daher sowohl bei automatisierter wie auch bei nichtautomatisierter Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, Anwendung. Ein Dateisystem ist gem. Art. 4 Nr. 6 DS-GVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon,

ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Ob die Datei dann in Papierform (z.B. Karteikarten oder Aktenordner) oder in rein elektronischer Form geführt wird (z.B. Mitgliederverzeichnis oder ein Custumer-Relationship-Management (CRM)) ist für die Anwendung der DS-GVO nicht von Belang.

10. Welche Empfehlung gibt es zum Umgang mit Personalausweiskopien?

Personalausweiskopien können zur Identifizierung einer natürlichen Person gegenüber nichtöffentlichen Stellen (Unternehmen) genutzt werden. Dies obliegt nur dem Ausweisinhaber. Er allein kann die Daten zur Verfügung stellen oder eine Kopie des Ausweises anfertigen oder seine Einwilligung dazu erteilen. Die Einzelheiten sind in § 20 PAuswG näher geregelt.

§ 20 Verwendung durch öffentliche und nichtöffentliche Stellen

(1) Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

(3) Die Seriennummern, die Sperrkennwörter und die Sperrmerkmale dürfen nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist. Dies gilt nicht für den Abgleich von Sperrmerkmalen durch Diensteanbieter zum Zweck der Überprüfung, ob ein elektronischer Identitätsnachweis gesperrt ist.

(4) Beförderungsunternehmen dürfen personenbezogene Daten aus der maschinenlesbaren Zone des Personalausweises elektronisch nur auslesen und verarbeiten, soweit sie auf Grund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind. Biometrische Daten dürfen nicht ausgelesen werden. Die Daten sind unverzüglich zu löschen, wenn sie für die Erfüllung dieser Pflichten nicht mehr erforderlich sind.

(5) Zum Zwecke des Jugendschutzes und mit Einwilligung des Ausweisinhabers dürfen die in § 5 Absatz 4 Satz 2 Nummer 6 und 7 genannten Daten aus der maschinenlesbaren Zone des Personalausweises erhoben werden, um das Alter des Ausweisinhabers und die Gültigkeit des Ausweises zu überprüfen. Eine Speicherung der Daten ist unzulässig.

Zu beachten ist allerdings auch in diesem Zusammenhang die Zweckbindung und Datenminimierung, Art. 5 Abs. 1 lit. b) und c) DS-GVO. Es dürfen immer nur die Daten erhoben werden, die dem festgelegten, eindeutigen und legitimen Zweck angemessen und erheblich sind. Außerdem bedarf es auch immer einer Rechtsgrundlage zur Erhebung der Ausweisdaten. Je, nach dem, auf welcher Rechtsgrundlage aus Art. 6 Abs. 1 Satz 1 DS-GVO die Datenerhebung erfolgt, ist auch die Erforderlichkeit der Datenverarbeitung zu prüfen. Zur Identifizierung einer Person reichen gewöhnlich der Name und die Adresse, ggf. noch das Geburtsdatum aus. Alle anderen Angaben sind daher nicht zu erheben und müssen ggf. mit einer Schablone abgedeckt werden oder der Betroffene kann gleich eine geschwärzte Kopie einreichen.

11. Welche Alternative gibt es, um der Identität der Person sicher zu sein? (Personalausweisgesetz ist den meisten kleinen Betrieben nicht bekannt)

Nach dem Personalausweisgesetz ist es möglich, dass der Ausweisinhaber selbst eine Kopie des Ausweises anfertigen oder die Einwilligung in die Fertigung einer solchen geben kann. In den Fällen, in denen eine Identitätsprüfung notwendig ist, z.B. vor einer Auskunftserteilung nach Art.15 DS-GVO, kann es notwendig sein, eine Personalausweiskopie vom Betroffenen zu verlangen, wenn dieser sich nicht anderweitig legitimieren kann. Dabei ist jedoch zu beachten, dass diese nur für die notwendigen Daten erstellt werden darf, der Rest des Ausweises daher geschwärzt werden kann. In der Regel sind daher nur der Name, Vorname, ggf. Geb.Datum (wenn relevant) und die Adresse maßgeblich. Alle anderen Daten sind entweder durch eine Schablone beim Kopiervorgang oder bereits durch die Einreichung einer geschwärzten Kopie unkenntlich zu machen. Eine Alternative zur Ausweiskopie als Identifizierung einer natürlichen Person stellt auch die reine Vorlage des Ausweises dar. Dass der Ausweis vorgelegen hat, wird in solchen Fällen beim Verantwortlichen vermerkt, ohne dass eine Kopie gefertigt werden muss.

12. Wie sieht der datenschutzkonforme Umgang bei der Kommunikation über WhatsApp zwischen Kunden und Handwerksbetrieb aus?

Wie in Nr. 31 weiter ausgeführt, ist das wesentliche Problem bei der Nutzung von WhatsApp die regelmäßige Übermittlung der Kontaktdaten des Adressbuchs an WhatsApp (siehe auch: https://www.heise.de/newsticker/meldung/Thueringens-Datenschuetzer-Whatsapp-wird-meist-rechtswidrig-genutzt-3983437.html). Hierbei werden auch Kontaktdaten von Personen übertragen, die nicht Nutzer von WhatsApp sind. Eine Einwilligung der Betroffenen in diese

Übermittlung liegt indes in der Regel nicht vor. Um WhatsApp nutzen zu können, ist der vollständige Abgleich der Kontakte jedoch nicht notwendig. Für die datenschutzkonforme Nutzung von WhatsApp bieten sich daher verschiedene Möglichkeiten an:

1. Auf dem Smartphone werden nur Kontaktdaten von Personen gespeichert, die in die WhatsApp Nutzung eingewilligt haben.
2. Das Adressbuch wird nicht mit Kontakten befüllt.
3. Der Zugriff von WhatsApp auf das Adressbuch wird blockiert. Diese Zugriffssperre ist bei Smartphones mit Android-Betriebssystem ab Version 6.0 in den Berechtigungseinstellungen für die App jederzeit aktivierbar. Bei iOS Endgeräten wird das Zugriffsrecht beim ersten Start von WhatsApp festgelegt, kann aber auch nachträglich (wie bei Android) wieder entzogen werden. Ist der Zugriff auf das Adressbuch untersagt, sieht man dann bei den Anrufen nur noch die Telefonnummern, nie den Namen.

13. Müssen alle Handwerksbetriebe ein Verzeichnis von Verarbeitungstätigkeiten führen?

Grundsätzlich, ja.

Im Verzeichnis von Verarbeitungstätigkeiten hat der Verantwortliche nach Art. 30 Abs. 1 DS-GVO alle Verarbeitungstätigkeiten mit folgende Angaben schriftlich[1] aufzuführen:

„a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (nachfolgend „pD“ abgekürzt);

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

[1] DS-GVO, Artikel 30, (3)

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1."

Die Pflicht zum Führen des Verzeichnisses besteht auch für Unternehmen unter 250 Mitarbeitern, …

- bei denen die Verarbeitung von personenbezogenen Daten ein Risiko für die Rechte und Freiheiten natürlicher Personen birgt,
- in denen die Verarbeitung nicht nur gelegentlich erfolgt,
- sobald eine Verarbeitung von personenbezogenen Daten gem. Art. 9 Abs. 1 erfolgt sowie
- bei der Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO

14. Wie sieht die Beschreibung der technischen und organisatorischen Maßnahmen aus?

Die technischen und organisatorischen Maßnahmen (TOMs) sind in allgemeiner Form – bestenfalls mit Verweise auf konkrete Regelungen – zusammenfassend zu dokumentieren. Gemäß Art. 32 Abs. 1 und 2 DS-GVO ist durch den Verantwortlichen sowie den Auftragsverarbeiter die Sicherheit der Verarbeitung bei der Verarbeitung personenbezogener Daten zu gewährleisten. Zu treffende Maßnahmen können bspw. dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellten Grundschutz Kompendium entnommen werden (siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html). Muster zu Konzepten der Maßnahmen kann man über eine Suche im Internet finden. Aufgrund der unternehmerischen Vielfältigkeit und der Neutralität des TLfDI kann aber kein spezielles Muster empfohlen werden. Hier muss jeder Verantwortliche für sich entscheiden, ob der Umfang und die Struktur für ihn passend ist.

Bedient sich der Verantwortliche eines Auftragsverarbeiters, so müssen gem. Art. 28 DS-GVO geeignete technische und organisatorische Maßnahmen durchgeführt werden, sodass die Verarbeitung im Einklang mit der DS-GVO erfolgen kann und die Rechte der betroffenen Person gewahrt werden. Diese müssen sowohl im Auftragsverarbeitungsvertrag (AVV) als auch im eigenen Maßnahmenkonzept dokumentiert werden. Dabei sind folgende Aspekte relevant:

a) **Verschlüsselung**

Dabei geht es um den Schutz der personenbezogenen Daten vor unberechtigtem Zugang. Der Verantwortliche sollte folgende Fragen beantworten können:

Wird eine Verschlüsselung beim Verantwortlichen und/oder Auftragsverarbeiter eingesetzt, um technische Vorkehrungen bzgl. unberechtigtem Zugang zu treffen? Wenn ja, an welcher Stelle wird diese Maßnahme eingesetzt (detaillierte Beschreibung im IT- Maßnahmenkonzept zur Datensicherheit erforderlich)?

b) Gewährleistung der **Vertraulichkeit**

Dabei geht es um den Zutritt und Zugang zu Datenverarbeitungsanlagen (Servern, Räumen mit Datenverarbeitungs-Technik). Es muss gewährleistet sein, dass nur Berechtigte Zutritt und Zugang haben. Zutritt bedeutet dabei, dass Räume mit Datenverarbeitungstechnik betreten werden können, während Zugang bedeutet, dass man auf elektronischem Weg Zugriff auf die Daten erhalten kann.

Der Verantwortliche sollte folgende Fragen beantworten können:

Wie wird der Zutritt sowie Zugang beim Verantwortlichen und/oder dem Auftragsverarbeiter geregelt, um Unberechtigten den Zutritt / Zugang zu verwehren? An welchen Stellen des Verarbeitungsprozesses werden diese Maßnahmen eingesetzt (detaillierte Beschreibung im Managementkonzept zur Datensicherheit erforderlich)?

c) Gewährleistung der **Integrität**

Integrität bedeutet einmal, dass Daten nur von berechtigten Personen verändert werden dürfen (d.h. die Authentizität ist gewahrt – ein Arztbrief sollte z.B. nur von einem Arzt unterschrieben werden dürfen) und von unberechtigten Personen nicht verändert werden können. Authentizität bedeutet dabei, dass der Ersteller der Informationen echt, überprüfbar und vertrauenswürdig ist.

Der Verantwortliche sollte folgende Fragen beantworten können:

Wie gewährleisten Sie / Ihr Auftragsverarbeiter, dass die Daten, die Sie verarbeiten, richtig sind und nicht böswillig oder durch technisches Versagen verändert sind? Wie steuern Sie / Ihr Auftragsverarbeiter Änderungen und/oder Löschungen sowie Sperren für Datensätze (Stichwort gem. DS-GVO „Einschränkung der Verarbeitung“)?

Zusätzlicher Hinweis zur Gewährleistung von Vertraulichkeit und Integrität:

Die Gewährleistungsziele „Vertraulichkeit“ und „Integrität“ können über Verschlüsselungsmaßnahmen umgesetzt werden. Dazu müssen aber Verfahren genutzt werden, welche als sicher

eingestuft sind. Dazu gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Technischen Richtlinie TR-02102-2 Empfehlungen für den Einsatz kryptographischer Verfahren und der damit zusammenhängenden Transportsicherheit [Transport Layer Security (TLS)] (Richtlinie siehe vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7). Im Kern gibt die Richtlinie einsetzbare Verschlüsselungstechnologien UND deren korrekte Parametrisierung vor. Viel Wert wird dabei auf die Transportverschlüsselung (Transport Layer Security (TLS), früher bekannt als Secure Socket Layer (SSL)) gelegt. Diese ermöglicht die sichere Übertragung von Informationen aus der Anwendungsschicht (zum Beispiel Browser über HTTPS, Dateitransport über SFTP oder Mailempfang über IMAPS) über das Internet. Allerdings kann man die gleichen Verfahren auch zur Verschlüsselung von Daten auf dem eigenen Rechner nutzen. Sie können als technische Empfehlungen zur Umsetzung der Forderungen Art. 32 DS-GVO in Bezug auf die Übermittlung von personenbezogenen Daten gelten und sind „Stand der Technik“ (Januar 2019).

d) Gewährleistung der **Verfügbarkeit**

Die Verfügbarkeit charakterisiert, zu welchen Zeiten ein System dem Nutzer zur Verfügung steht und wie oft Ausfälle oder langsame Reaktionszeiten auftreten. Bei der Dokumentation der Verfügbarkeit sollten Verantwortliche folgende Fragen beantworten können:

Wie gewährleisten Sie / Ihr Auftragsverarbeiter bei technischen Vorfällen (Defekten, Ausfällen, wie z.B. bei einem Stromausfall, Angriff durch Verschlüsselungstrojaner) die Verfügbarkeit der Daten? Wie lang sind maximale Ausfallzeiten? Können Daten unumkehrbar verlorengehen?

Haben Sie Vorgehensweisen bei einem Zwischenfall, der z.B. alle ihre Daten auf einem Server löscht? Wenn ja, wie ist eine schnelle Wiederherstellung geregelt?

Das Maßnahmekonzept zur Datensicherheit fordert dabei nur die Dokumentation, welche Maßnahmen zur Sicherstellung der Verfügbarkeit getroffen sind. Eine Dokumentation der tatsächlich eingetretenen Vorfälle erfolgt dort nicht. Es kann als Maßnahme zusätzlich vorgesehen sein, ein „Havarie-Handbuch“ oder ähnliches zu führen (dies wird als Maßnahme durch das BSI auch empfohlen, um einen Überblick zu bekommen), wird aber separat vom Managementkonzept zur Datensicherheit geführt. Ein Beispielformular für die Erfassung eines Havarie-Falles ist z.B. hier zu finden: https://www.its.uni-bayreuth.de/pool/ITS_PDF/Ordnungen_Formulare/Formular_Meldung_IT-Sicherheitsereignis.pdf .

e) Gewährleistung der **Belastbarkeit der Systeme**

Führen Sie / Ihr Auftragsverarbeiter regelmäßige Prüfungen durch, ob technische Systeme bei höherer Belastung entsprechend dimensioniert und auch gegen Sicherheitsvorfälle sicher sind? Wenn ja, wie erfolgt dies (detailliert im Managementkonzept zur Datensicherheit beschreiben)?

15. Bislang besteht wenig Verständnis für die Erstellung und Erforderlichkeit von datenschutzrechtlichen Auftragsverträgen, insbesondere bei den IT-Firmen und anderen Dienstleistern an Handwerksbetriebe. Dies wird eher als zusätzliche Belastung empfunden. Was ist der Sinn und Nutzen solcher Verträge zur Auftragsverarbeitung? Warum sind diese notwendig?

Als Auftragsverarbeiter wird nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezeichnet, die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet.

Der Verantwortliche ist dabei das Unternehmen. Wenn dieses beispielsweise einen IT Dienstleister mit der Wartung und Pflege des Systems beauftragt, dann ist für die Durchführung des Auftrages und ggf. für die Administrierung der Systeme, Zugang zu den Systemen erforderlich. Dabei können auch alle darin gespeicherten und erfassten Daten eingesehen werden. Diese Daten wurden allerdings nur dem Verantwortlichen gegenüber von Kunden, Auftraggebern oder auch den eigenen Mitarbeitern zur Verfügung gestellt. Wenn nunmehr ein Dritter wie es der IT Dienstleister ist, im Rahmen der Systemwartung und Pflege solche Daten zur Kenntnis nehmen kann, wäre dies eine unbefugte Übermittlung an Dritte, für die der Unternehmer verantwortlich ist und datenschutzrechtlich zur Verantwortung gezogen werden kann.

Um hier datenschutzkonforme Zustände herzustellen, benötigt der Unternehmer **neben seinem eigentlichen Dienstleistungsvertrag** mit dem IT Dienstleister einen besonderen Auftragsverarbeitungsvertrag (AVV). In diesem Vertrag werden die Bedingungen und Anforderungen an die Datenverarbeitung gegenüber dem Auftragsverarbeiter (IT Dienstleister) festgeschrieben. Bei deren Verletzung haftet der Auftragnehmer. Der Inhalt eines solchen Vertrages ist ebenfalls **in der DS-GVO in Art. 28** genau geregelt. Ein **Muster** für einen solchen Auftragsverarbeitungsvertrag (AVV) ist auf der Webseite des TLfDI ebenfalls zu finden: https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf .

16. Muss der Handwerksbetrieb alle Kunden anschreiben und nach deren Einwilligung zur Speicherung von personenbezogenen Daten fragen?

Nein, für die meisten Verarbeitungen von Daten gibt es eine andere Rechtsgrundlage, sodass auf die Einwilligung nur als letztes Mittel und in wenigen Fällen zurückgegriffen werden muss.

Die wichtigste Rechtsgrundlage für Unternehmen ist nach wie vor, die Verarbeitung aufgrund oder in Erfüllung eines Vertrages oder im Rahmen von vorvertraglichen Maßnahmen, gem. Art. 6 Abs. 1 Satz 1 lit. b) DS-GVO und die Verarbeitung aufgrund berechtigter Interessen des Verantwortlichen gem. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO. Im Rahmen des Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO ist allerdings immer zu prüfen, ob die Verarbeitung der Daten durch den Verantwortlichen zur Wahrung seiner berechtigten Interessen erforderlich ist. Erst wenn diese Voraussetzung gegeben ist, erfolgt die Interessenabwägung zwischen dem berechtigten Interesse des Verantwortlichen und dem schutzwürdigen Interesse des Betroffenen. Wenn das schutzwürdige Interesse überwiegt, kann die Verarbeitung nicht auf Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO gestützt werden.

17. Wunsch nach einer sicheren einheitlichen verschlüsselten Datenübertragung zwischen öffentlichen und nicht öffentlichen Stellen; viele verschiedene Verschlüsselungsmethoden erschweren die sichere Datenübermittlung

Der Wunsch nach einer einheitlichen sicheren Verschlüsselungsmethode ist nachvollziehbar. Zudem hat sich der Versuch, eine relativ sichere Datenübermittlung seitens der Bundesregierung bereitzustellen, nicht wirklich flächendeckend durchgesetzt. So wird DE-Mail, nach Kenntnisstand des TLfDI, von vielen nicht genutzt.

Erschwerend kommt - wie bei DE-Mail oder anderen technisch ähnlichen Verfahren – hinzu, dass auch dort nicht nur der Absender, sondern auch der Empfänger über das jeweilige Verschlüsselungsverfahren Kenntnis haben muss. Weiterhin sind technische Voraussetzungen für eine so erfolgende Übertragung zu schaffen und aufrecht zu erhalten (Installation von Software, Updates, Wartung). Nach aktuellem Kenntnisstand des TLfDI scheint GnuPG als auch PGP einen relativ hohen Verbreitungsgrad zu haben. Hinweise zum Einsatz dieser Verfahren hat das Bundesamt für Sicherheit in der Informationstechnik bereitgestellt. Siehe hierzu

https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptotechnologie/Gpg4win/gpg4win_node.html .

18. Welche Unternehmen sind verpflichtet, einen Datenschutzbeauftragten zu benennen? Hier insbesondere Versicherungsvermittler (Einzelunternehmen), die z.B. gesundheitsbezogene Daten der Kunden verarbeiten (Krankenversicherung, Berufsunfähigkeitsversicherung, etc.).

Die Pflicht zur Benennung des Datenschutzbeauftragten ergibt sich aus verschiedenen Regelungen.

Zunächst ergibt sich die Pflicht aus Art. 37 Abs. 1 DS-GVO. Danach ist ein DSB immer dann zu benennen, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln, die **Kerntätigkeit** des Verantwortlichen (siehe auch nachfolgende Absätze)) oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9, also Daten aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürliche Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

Aus § 38 BDSG ergeben sich zusätzliche Sachverhalte, aus denen sich eine Bennennungspflicht ergibt:

Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der DS-GVO benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **zwanzig Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer **Datenschutz-Folgenabschätzung** (DS-FA) nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Für eine Beurteilung, ob eine Pflicht zur Benennung eines DSB besteht, muss jeder Verantwortliche die Benennungsvoraussetzungen hinsichtlich der Pflicht zur Benennung eines Datenschutzbeauftragten aus Art. 37 DS-GVO und aus § 38 BDSG mit der bei Ihm vorliegenden Situation abgleichen. (Grundlegend zur Bestellpflicht von Datenschutzbeauftragten siehe auch das Kurzpapier Nr. 12 der Datenschutzkonferenz welches unter https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_12_datenschutzbeauftragter.pdf eingestellt ist)

Nach Art. 37 Abs. 1 lit. c) DS-GVO besteht die Pflicht dann, wenn die **Kerntätigkeit** in der umfangreichen Verarbeitung besonderer Kategorien von Daten nach Art. 9 DS-GVO besteht. Kerntätigkeit ist dabei die Haupttätigkeit eines Verantwortlichen, die ihn untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwG 97). Als Kerntätigkeit lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind. Dazu gehören auch sämtliche Tätigkeiten, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen oder des Auftragsverarbeiters darstellt. (siehe Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 rev.01 (zu finden unter dem Link: https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf). Die Tätigkeit eines Versicherungsvermittlers oder Maklers besteht darin, für interessierte Kunden eine auf ihre Bedürfnisse und Voraussetzungen abgestimmte Versicherung zu finden und einen Vertragsabschluss vorzubereiten. Dazu ist es notwendig, dass der Kunde alle notwendigen Informationen, je nach dem versicherten Risiko auch umfangreiche Angaben zu besonderen Kategorien personenbezogener Daten gem. Art. 9 DS-GVO, im Versicherungsantrag angibt. Dieser Antrag wird durch den Versicherungsmakler an die Versicherung weitergeleitet. Hier verbleibt zudem eine Kopie dieses Antrags beim Makler selbst. Dies wird zu Dokumentationszwecken oder zur Sicherstellung einer individuellen Kundenberatung begründet. Wenn dem so ist, zählt dies aber auch auf jeden Fall zur Kerntätigkeit des Verantwortlichen. Ebenso verhält es sich, wenn zu Kundenbindungszwecken als sog. Kundenservice die Übernahme der Regulierungsabwicklung von Versicherungsfällen für die Kunden übernommen wird. Auch derartige Verarbeitungen sind dann selbstverständlich zur Kerntätigkeit zu rechnen. Weiterhin müsste die Verarbeitung auch umfangreich sein. Umfangreiche Bearbeitung ist in der DS-GVO nicht direkt definiert. Bei der Klärung der Frage, ob eine umfangreiche Verarbeitung vorliegt, sind gem. WP 243 rev.01 (https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf) und dem ErwG 91 folgende Faktoren zu berücksichtigen: die Zahl der betroffenen Personen, das Datenvolumen oder das Spektrum an in Bearbeitung befindlichen Daten, die Dauer oder Permanenz der Datenverarbeitung und die geografische Ausdehnung der Verarbeitungstätigkeit auf regionaler, nationaler oder supranationaler Ebene. Von einer umfangreichen Verarbeitung kann beim einzelnen Makler im Regelfall wohl nicht

ausgegangen werden. Sobald jedoch mehrere Makler in einem Versicherungsvermittler/Maklerbüro tätig sind, sind die Voraussetzungen anders zu bewerten und zu prüfen.

Beispiele für eine umfangreiche Verarbeitung sind die Verarbeitung von Kundendaten im gewöhnlichen Geschäftsbetrieb eines Versicherungsunternehmens oder einer Bank. (WP 243 rev.01; https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf)

Weiterhin ist Art 37 Abs. 1 lit. b) DS-GVO zu prüfen, da dieser eine Bestellpflicht für den Fall vorsieht, dass die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen erforderlich machen, da auch dann eine Benennungspflicht besteht. Auch der Begriff der regelmäßigen und systematischen Überwachung ist in der DS-GVO nicht definiert, erstreckt sich jedoch auf jede Form der Verfolgung und Profilerstellung im Internet, beschränkt sich aber nicht darauf. (WP 243 rev.01; https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf) Als regelmäßig wird die Verarbeitung gesehen, wenn sie fortlaufend oder in bestimmten Zeitabständen vorkommend, immer wieder wiederholend, ständig oder regelmäßig auftritt. Als systematisch wird die Verarbeitung gesehen, wenn sie organisiert, methodisch, im Rahmen eines allgemeinen Datenerfassungsplans erfolgend oder im Rahmen einer Strategie erfolgt. (WP 243 rev. 01, 2.1.4; https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf) Beispiele dafür sind die Typisierung und Scoring zu Zwecken der Risikobewertung bei der Kreditvergabe oder zur Festlegung von Versicherungsprämien.

Auch für den Fall der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DS-FA) muss ein Datenschutzbeauftragter durch den Verantwortlichen bestellt werden, § 38 Abs. 1 BDSG.

Die Verpflichtung zur Durchführung einer DS-FA ergibt sich gem. Art. 35 Abs. 1 DS-GVO, wenn die Form der Verarbeitung insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge haben wird. Ein hohes Risiko besteht immer dann, wenn die Eintrittswahrscheinlichkeit und die Schwere für die Beeinträchtigung oder Verletzung der persönlichen Rechte und Freiheiten der betroffenen Personen als hoch einzustufen sind, ErwG 90.

Zusätzlich kann sich die Verpflichtung zur Durchführung einer DS-FA auch aus der sog. Blacklist der Datenschutzaufsichtsbehörden gem. Art 35 Abs. 4 DS-GVO ergeben, da hier eine Liste von Verarbeitungstätigkeiten erstellt wurde, für die verpflichtend die Durchführung einer DS-FA für die Verantwortlichen festgeschrieben wurde. Diese Blacklist finden Sie auf der Webseite des TLfDI unter https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/. Wenn eine Verpflichtung

zur Durchführung einer DS-FA besteht, dann ergibt sich daraus auch die zwangsläufige Pflicht zur Benennung eines Datenschutzbeauftragten, § 38 Abs. 1 BDSG.

So verarbeiten Versicherungsmakler umfangreiche Angaben auch zu besonderen Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO, wonach die Durchführung einer DS-FA aufgrund der Art der Daten und des Umfangs notwendig zu prüfen wäre. Die Personen- und Vertragsdaten der Versicherungs- und/oder Vorsorgeverträge aller Kunden werden zunächst beim Makler gespeichert und dann ggf. per E-Mail versendet und zusätzlich an die Versicherungsgesellschaft übermittelt und dort gespeichert und in einem Maklerpool gesammelt und verwaltet. Allein diese **Art** der Weiterleitung und Speicherung von Kundendaten und darunter auch von besonderen Kategorien von Daten macht gem. Art. 35 Abs. 1 und Abs. 3 lit. b) DS-GVO wohl eine Datenschutz-Folgeabschätzung dringend notwendig, da diese voraussichtlich ein hohes Risiko für die Rechte der betroffenen Personen darstellen, welche im Rahmen der DS-FA beseitigt werden müssen. Demnach bestünde hier auch die Pflicht zur Benennung eines DSB.

19. Wer darf zum Datenschutzbeauftragten bestellt werden (Qualifikation)?

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DS-GVO genannten Aufgaben. Diese umfassen gem. Art. 39 DS-GVO die Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten hinsichtlich ihrer Pflichten nach der DS-GVO sowie sonstigen Datenschutzvorschriften der Mitgliedstaaten, die Überwachung der Einhaltung der DS-GVO, einschließlich der Überwachung der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter und diesbezügliche Überprüfungen, auf Anfrage Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung der Durchführung, Zusammenarbeit mit der Aufsichtsbehörde, Anlaufstelle zu sein für die Aufsichtsbehörde bei Fragen und im Rahmen von vorherigen Konsultationen gem. Art. 36 DS-GVO und ggf. Beratung zu allen sonstigen Fragen.

Das erforderliche Fachwissen muss bereits zum Zeitpunkt der Übernahme der Aufgaben des Datenschutzbeauftragten vorliegen. Das erforderliche Niveau des Fachwissens kann sich der Datenschutzbeauftragte durch entsprechende Lehrgänge aneignen und ist dazu angehalten, dieses Wissen auch ständig durch geeignete Fortbildungen auf einem aktuellen Stand zu halten. Hierzu muss dem Datenschutzbeauftragten vom Verantwortlichen genügend Möglichkeit, wie Zeit und Mittel für entsprechende Weiterbildung, eingeräumt werden, Art. 38 Abs. 2 DS-GVO.

Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

20. Besteht die Möglichkeit durch den TLfDI eine zentrale Plattform mit einer Übersicht aller externer Datenschutzbeauftragten zu erstellen?

Ist dies zumindest für den Freistaat Thüringen möglich?

Nein, eine derartige Möglichkeit gibt es beim TLfDI nicht und ist auch nicht geplant. Externe Datenschutzbeauftragte sind wirtschaftlich selbständige Unternehmer und sind für ihre Präsenz am Markt eigenständig verantwortlich. Möglicherweise können aber derartige Übersichten über die Berufsverbände der Datenschutzbeauftragten eingeholt werden.

21. Dürfen die Informationspflichten nach Artikel 13 DS-GVO in Allgemeinen Geschäftsbedingungen aufgeführt werden?

Grundsätzlich ja, aber nicht ausschließlich! Die Informationen nach Art. 13 DS-GVO sind dem Betroffenen bei Erhebung der Daten zur Verfügung zu stellen, d.h. im Zweifel auch auszuhändigen. Bei der weiteren Verarbeitung der erhobenen Daten ist diese Information nicht nochmals notwendig, wenn die Erstinformation die Zwecke der Verarbeitung vollständig aufführt. Eine erneute Information ist lediglich dann notwendig, wenn neue Daten erhoben werden oder sich die Zwecke der Verarbeitung verändern, Art. 13 Abs. 3 DS-GVO. Die AGBs sind zumeist sehr umfangreich und eine Aushändigung an den Kunden ist hier nicht vorgesehen, da die AGBs automatisch Bestandteil des Vertrages werden. Bei schriftlicher Korrespondenz sind die Informationen daher dem Schriftstück beizufügen, bei elektronischer Korrespondenz kann ein Hinweis auf eine Webseite genügen. Die bessere Variante ist aber auch hier die Informationen innerhalb der Bestätigungsmail, oder eines zu erstellenden Angebotes o.ä. zu übersenden.

22. Wann kann ein Datenschutzbeauftragter abberufen werden?

Die Abberufung eines Datenschutzbeauftragten ist nicht ausdrücklich in der DS-GVO geregelt. Der Datenschutzbeauftragte darf auch nicht wegen der Erfüllung seiner Aufgaben abberufen oder benachteiligt werden, Art. 38 Abs. 3 DS-GVO. Die Abberufung ist aber grundsätzlich aus Gründen möglich, die nicht im Zusammenhang mit der Erfüllung seiner Pflichten als DSB stehen (Bsp.: grobes Fehlverhalten, Diebstahl u. ä.), siehe WP 243 rev.01, 3.4. In § 38 Abs. 2 BDSG wird auf § 6 Abs. 4, 5 Satz 2 und Abs. 6 BDSG verwiesen und diese auch für den nichtöffentlichen Bereich für anwendbar erklärt. Die Abberufung ist daher in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches (BGB) zulässig und damit aus den

gleichen Gründen möglich, die auch eine außerordentliche Kündigung des Arbeitsverhältnisses rechtfertigen würden. Die Abberufung als DSB führt allerdings nicht automatisch zu einer Kündigung des Arbeitsverhältnisses, § 6 Abs. 4 Satz 2. Diese beiden Verhältnisse sind zu trennen.

23. Gibt es für externe Datenschutzbeauftragte eine Gebührenordnung oder ähnliches oder unterliegt das Honorar der freien Vereinbarung der Vertragsparteien?

Nein, es gibt keine Gebührenordnung für externe Datenschutzbeauftragte. Das Honorar für die Dienstleistungen ist frei verhandelbar.

24. Darf der Arbeitgeber ohne Verdachtsgründe E-Mails lesen oder Telefonate abhören?

Grundsätzlich Nein!

Ohne Verdachtsgründe kann das Lesen von E-Mails nicht auf § 26 Abs. 1 Satz 2 Bundesdatenschutzgesetz gestützt werden. Dazu müsste der konkrete Verdacht auf das Begehen von Straftaten vorliegen.

Ansonsten muss differenziert werden:

- Zunächst muss konstatiert werden, dass es sich um den E-Mail-Account des Betriebs handelt, der einem Mitarbeiter zur Erledigung seiner Arbeit zur Verfügung gestellt wird. Dienstliche E-Mails stehen grundsätzlich dem Arbeitgeber zu. Auf diese kann aber durch den Arbeitgeber ausnahmsweise und nur dann, wenn die private Nutzung des Accounts ausgeschlossen ist, **aber auch nur in Einzelfällen und nicht zur Leistungs- und Verhaltenskontrolle** zugegriffen werden. Voraussetzung hierfür sind konkrete Regelungen in Form einer Betriebsvereinbarung oder, falls ein Betriebsrat nicht vorhanden ist, durch Betriebsanweisung. Es sind Festlegungen zu treffen, ob aus zu konkret zu benennenden Anlässen (z. B. unvorhersehbare Abwesenheiten) durch eine bestimmte Person, besser nach dem Mehr-Augen-Prinzip unter Einbindung des betrieblichen Datenschutzbeauftragten und/oder des Betriebsrats, soweit solche vorhanden sind, zugegriffen werden kann, damit eine erforderliche Erledigung der Arbeit möglich ist. Ist die Nutzung des Accounts auch zu privaten Zwecken zugelassen, muss sichergestellt sein, dass auf diese Mails nicht zugegriffen wird. Möglicherweise ergibt sich dies aus dem Adressaten oder Absender der Mail. Der Inhalt der Mails darf nicht geöffnet und zur Kenntnis genommen werden.

Nähere Ausführungen enthält die Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und Internetdiensten am Arbeitsplatz, die unter https://www.tlfdi.de/tlfdi/gesetze/orientierungshilfen/ abgerufen werden kann. Diese stammt

zwar aus dem Jahr 2016 und ist noch nicht an die DS-GVO angepasst, jedoch gelten die Ausführungen weitestgehend auch nach neuem Recht.

- **Telefonate abhören ist strafbar (§201 StGB**) und kann strafrechtlich nur mit richterlicher Anordnung erfolgen. Um einen solcher Antrag bei Strafverfolgungsbehörden zu stellen, müssen erhebliche Verdachtsmomente vorliegen.

Ist eine Tätigkeit aber rein über Telefon abzuwickeln (z. B. Callcenter), können innerbetrieblichen Festlegungen (Betriebsvereinbarungen, die nach § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz eine Rechtsgrundlage bilden können) die Möglichkeit des Mithörens zum Zweck der Qualitätsverbesserung vorsehen. Eine Betriebsvereinbarung darf aber das Niveau der DS-GVO nicht unterschreiten (Art. 88 Abs. 2 DS-GVO, § 26 Abs. 4 BDSG). Vor allem darf damit keine vollständige Leistungs- und Verhaltenskontrolle eingeführt werden. Zunächst bedarf es einer Prüfung, ob dies zur Durchführung des Arbeitsverhältnisses nach § 26 Abs. 1 Bundesdatenschutzgesetz erforderlich ist. Diese Festlegungen sind einer strengen Kontrolle im Hinblick auf die Erforderlichkeit zu unterziehen. Die Kunden müssen aufgeklärt werden, denn auch sie werden von anderen „abgehört“ und können ggf. einwilligen. Fehlt die Einwilligung, ist das Mithören nicht zulässig. Wird ein Gespräch aufgezeichnet (z. B. zum Nachweis eines Vertragsabschlusses), muss dies ebenfalls für alle Seiten transparent sein.

25. Ist das Verzeichnis der Verarbeitungstätigkeiten für jedermann einsehbar?

Nein, das Verzeichnis dient der Aufsichtsbehörde dazu, sich einen Überblick über die Datenverarbeitungen im Unternehmen zu verschaffen. Es kann zu Prüfzwecken jederzeit angefordert werden. Ein Einsichtsrecht für „jedermann“ besteht aber nicht.

26. Wann ist eine Verschwiegenheitserklärung vom AN zu unterzeichnen?

Das Datengeheimnis ist von der Weisungsgebundenheit des Arbeitgebers umfasst. Zu den Schritten, die der Verantwortliche oder der Auftragsverarbeiter unternehmen **müssen,** um Art. 29 zu erfüllen, gehört die Verpflichtungserklärung der Beschäftigten (zur Verschwiegenheit) bevor eine Verarbeitung personenbezogener Daten aufgenommen wird (siehe Simitis, Kommentar zur DS-GVO, Art. 32, Rdn.69). Siehe hierzu Datenschutzbeauftragtenkonferenz Kurzpapier und Muster: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf .

27. Kann die Weigerung einer Unterschrift unter eine Verschwiegenheitserklärung zur Kündigung des Arbeitnehmers führen?

Dies ist eine arbeitsrechtliche und keine datenschutzrechtliche Frage und daher nicht vom TLfDI abschließend zu beantworten. Unter Berücksichtigung der Ausführungen zu Frage 28 wird man annehmen müssen, dass die Möglichkeit besteht.

28. Für welche Räume eines Unternehmens ist eine Videoüberwachung generell verboten?

Die Videoüberwachung ist als eine Art der Datenverarbeitung grundsätzlich immer je nach Unternehmen individuell zu prüfen und die Zulässigkeit ist einzelfallbezogen zu bewerten.

Es gibt jedoch grundsätzliche Umstände in denen eine Überwachung von vorn herein als unzulässig anzusehen ist. Dies betrifft Bereiche, in denen die Intim- und Privatsphäre der Beschäftigten verletzt wird. Eine Videoüberwachung beispielsweise in Toilettenräumen, im Duschbereich und in Umkleidebereichen ist grundsätzlich verboten. Auch die Pausen- und Aufenthaltsräume dürfen nicht von einer Videoüberwachung erfasst werden. Raucherbereiche ebenfalls nicht. Die Zugänge zu diesen Bereichen sind auch von der Videoüberwachung auszunehmen. Eine dauerhafte verdachtsunabhängige Überwachung der Arbeitsplätze von Beschäftigten darf ebenso nicht erfolgen.

29. Darf ich in meinem Unternehmen WhatsApp nutzen?

WhatsApp selbst schreibt in seinen Nutzungsbedingungen (https://www.whatsapp.com/legal/?eea=1#Dienstbedingungen), dass eine nicht-private Nutzung nicht rechtmäßig ist, außer sie wurde von WhatsApp genehmigt. Zum generellen Einsatz von WhatsApp hat der TLfDI auch in seinem Tätigkeitsbericht für das Jahr 2018 (siehe: https://www.tlfdi.de/mam/tlfdi/datenschutz/taetigkeitsbericht/1._tatigkeitsbericht_2018_zum_datenschutz_nach_der_dsgvo.pdf) an verschiedenen Stellen die Problematik aufgegriffen, insbesondere in Kap. 5.35.

Aus Sicht des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) ist die Nutzung von WhatsApp problematisch, da WhatsApp standardmäßig die kompletten Kontaktdaten eines Kommunikationsgerätes ausliest. Somit auch Kontaktdaten von Personen aus dem eigenen Telefonbuch, die selbst nicht bei WhatsApp registriert sind. Begründet wird dies damit, dass man kundenorientiert bei Kontaktaufnahme sofort den Namen, also nicht die Telefonnummer, anzeigen möchte. Wenn man diese Einstellung deaktiviert, wer-

den dann allerdings nicht mehr die Namen, sondern nur noch die Telefonnummern des Kontaktes angezeigt. Problematisch ist aus Sicht des TLfDI, dass eben auch Kontaktdaten von Nicht-WhatsApp-Nutzern aus dem Adressbuch des Gerätes ausgelesen werden, wofür es keine Einwilligung der betroffenen Personen gibt.

Für eine rechtmäßige Übermittlung der Kontaktdaten aus dem Adressbuch an WhatsApp bedarf es einer Rechtsgrundlage nach Art. 6 DS-GVO. Für Unternehmen kommt Art. 6 Abs. 1, Satz 1, lit. f) DS.GVO (berechtigtes Interesse) in Betracht. Hierbei kann jedoch ein berechtigtes Interesse an der Übermittlung der Kontaktdaten an WhatsApp nur für bereits registrierte Nutzer unterstellt werden, wenn deren schutzwürdige Interessen nicht überwiegen. In Einzelfällen kann die Interessensabwägung durchaus auch zugunsten eines bereits registrierten Nutzers erfolgen. Für nicht-registrierte Nutzer kann regelmäßig angenommen werden, dass die Interessen von WhatsApp nicht überwiegen. Im Fall, dass die Interessensabwägung zugunsten des Inhabers der Telefonnummer erfolgt, darf diese nicht auf Basis von Art. 6 Abs. 1, Satz 1, lit. f) DS.GVO an WhatsApp übermittelt werden. Die Übermittlung von Kontaktdaten solcher Personen ist nur rechtmäßig, wenn sie auf Grundlage einer Einwilligung nach Art. 6 Abs. 1, Satz 1, lit. a) DS-GVO in Verbindung mit Art. 7 u. 8 DS-GVO erfolgt. Ohne eine solche Einwilligung begeht der Dienste-Nutzer gegenüber diesen Kontaktpersonen eine deliktische Handlung, die zu einer kostenpflichtigen Abmahnung führen kann (vergleiche Amtsgericht Bad Hersfeld, Az.: F120/17EASO).

30. Kann ich den PC-Arbeitsplatz meiner Angestellten überwachen lassen?

Siehe Antwort zu Frage 26 (§ 26 Abs. 1 Satz 2 BDSG) bei konkretem Verdacht gegen eine Person.

31. Was muss ich beachten, wenn ich eine externe Firma mit der Vernichtung von Dokumenten beauftrage?

Jeder, der selbst oder im Auftrag vertrauliche, personenbezogene und/oder besondere Daten (pD) verarbeitet, hat eine datenschutzgerechte und sichere Vernichtung der Datenträger mit solchen Daten sicherzustellen. Sicher vernichtet bedeutet in diesem Zusammenhang, dass die Datenträger, auf denen schutzbedürftige Informationen dargestellt sind, so zu vernichten sind, dass die Reproduktion der auf ihnen wiedergegebenen Informationen entweder unmöglich oder nur mit erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist. Hierbei muss berücksichtigt werden, dass der Grad der Schutzbedürftigkeit von Informationen und die physikalischen Eigenschaften von Datenträgern unterschiedlich sind.

Der Schutzbedarf des Inhalts der zu vernichtenden Datenträger richtet sich nach den Eigenschaften von Daten und Informationen, welche unter Berücksichtigung der bei einer Verletzung der Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit zu erwartenden Schäden die Notwendigkeit beschreibt, diese Daten und Informationen vor einer Verletzung dieser Grundwerte zu bewahren.

Das Vernichten von Datenträgern ist gleichzeitig an geeignete technisch-organisatorische Maßnahme zur Gewährleistung der Datensicherheit, insbesondere zur Verhinderung der Kenntnisnahme pD durch Unbefugte (Sicherung der Vertraulichkeit). Insofern sind die Regelungen des Art. 32 DS-GVO mit Blick auf die technischen und organisatorischen Maßnahmen zu beachten. Danach müssen die Maßnahme dem Schutzbedarf der Daten angemessen sein (vgl. hierzu Ausführungen zu TOM in Frage 13). Ihre Umsetzung hat sich nach den im Einzelfall zu betrachtenden Risiken und dem Stand der Technik zu richten. In der DIN 66399 beschreiben sieben Sicherheitsstufen Anforderungen an die Wirksamkeit der Vernichtung, d. h. die Höhe des Aufwands für Angreifer, vernichtete Datenträger bzw. darauf gespeicherte Daten wiederherzustellen und Informationen zur Kenntnis nehmen zu können. Die Norm bestimmt für diverse Materialklassen (wie Papier u. a.) Grenzwerte für Teilchengrößen, die bei der Vernichtung eines Datenträgers eingehalten werden müssen, um die Wiederherstellung von Informationen aus dem nach der Vernichtung vorliegenden Restmaterial zu verhindern oder zumindest zu erschweren.

Sofern ein externer Dienstleister mit der Vernichtung beauftragt wird, ist zudem Folgendes zu beachten: Sobald externe Dienstleister personenbezogenen Daten aufbewahren, liegt eine Verarbeitung im Auftrag eines Verantwortlichen vor. Hierfür ist ein Vertrag erforderlich, der die Anforderungen des Art. 28 DS-GVO erfüllen muss (Auftragsverarbeitungsvertrag).

Das Unternehmen bleibt auch bei einer Aufbewahrung beim Auftragsverarbeiter Verantwortlicher und muss diesen daher in den Geschäftsprozess einbeziehen. Alle möglichen Problemfelder müssen bei der Entscheidung, ob ein Unternehmen die Aufbewahrung selbst durchführt oder auslagert, bedacht werden. Ein Auftrag darf gemäß Art. 28 Abs. 1 DS-GVO nur an Auftragsverarbeiter erteilt werden, wenn sichergestellt ist, dass diese hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Berufs- und Amtsgeheimnisträgern hat der Gesetzgeber besondere Geheimhaltungspflichten auferlegt. Davon erfasst werden Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den sie betreffen, ein schutzwürdiges Interesse hat. Auch der Name eines Ratsuchenden und die Tatsache, dass er überhaupt den

Berufsgeheimnisträger aufgesucht hat, gehören zu dem geschützten Geheimnis. Zu den Berufsgeheimnisträgern gehören u. a. Ärzte, Berufspsychologen und Rechtsanwälte. Den **Berufsgeheimnisträgern** ist die Auslagerung solcher Unterlagen nicht grundsätzlich verwehrt, aber nur unter bestimmten sehr engen Bedingungen erlaubt. Werden diese nicht beachtet, laufen die Geheimnisträger Gefahr, eine Straftat nach § 203 StGB zu begehen.

In diesem Zusammenhang verweist der TLfDI außerdem auf seine entsprechende Orientierungshilfe: https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/datentragervernichtung.pdf . Zu beachten dabei ist, dass für Daten die dem Berufs- und Amtsgeheimnis (z.B. Patientenakten, Akten von Rechtsanwälten usw.) unterliegen, die Sicherheitsstufe 5 anzuwenden ist.

32. Muss ich einen Vertrag über Auftragsverarbeitung (AVV) abschließen, wenn ich ein externes Unternehmen mit der Versendung von Briefen beauftrage?

Bei der Inanspruchnahme von Postdienstleistern, die ähnlich der Deutschen Post AG die Post lediglich befördern, muss kein AVV geschlossen werden, da der Postdienstleister als eigenständiger Verantwortlicher bei der Beförderung von Postsendungen gilt. Die Datenverarbeitung hinsichtlich des Versenders ergibt sich aufgrund des Vertrages über die Beförderung, die Adressdatenverarbeitung erfolgt aufgrund berechtigten Interesses nach Art. 6 Abs.1 Satz 1 lit. f) DS-GVO, da es ein berechtigtes Interesse des Beförderers ist, die Post ordnungsgemäß zustellen zu können. Die Nutzung der zustellfähigen Adresse ist auch erforderlich. Das schutzwürdige Interesse des Adressaten ist in diesem Fall auch nicht höher zu gewichten, da auch dem Adressaten an der Zustellung von Post an sich selbst gelegen ist.

Anders ist es aber zu beurteilen, wenn ein externer Dienstleister mit der Erstellung und Kuvertierung von Briefen beauftragt wird und ihm dazu die Adressdaten und die Inhalte, die gedruckt werden, zur Verfügung gestellt werden. Dies stellt regelmäßig eine Verarbeitung im Auftrag des Verantwortlichen dar. Da hier aber für die Übermittlung der Daten der betroffenen Personen an den Dritten (externer Dienstleister) keine rechtliche Grundlage existiert, muss der Dritte eingebunden werden. Der Abschluss eines Vertrages über die Auftragsverarbeitung gem. Art. 28 DS-GVO ist daher notwendig.

33. Benötige ich für die Verarbeitung von Personaldaten die Einwilligung meiner Angestellten?

Es kommt darauf an, welche Verarbeitungsrechtfertigungsnorm des Art. 6 DS-GVO herangezogen wird. Art. 6 Abs. 1 Satz 1 lit. b) DS-GVO bzw. § 26 BDSG erlaubt die Verarbeitung aller für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlicher Daten. Auch kann eine Verpflichtung zur Verarbeitung der Daten nach § 6 Abs. 1 Satz 1 lit. c) DS-GVO bestehen (Übermittlung an Krankenkassen, Rentenversicherung, Steuern). Erst wenn keine andere Rechtfertigungsnorm greift, wird eine Einwilligung erforderlich

Im Kurzpapier Nr. 14 der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, wird ausführlich dargelegt, in welchen Fällen und unter welchen Umständen eine Einwilligung im Beschäftigungsverhältnis überhaupt wirksam eingeholt werden kann; https://www.datenschutzkonferenz-online.de

Beschäftigte können gem. § 26 Abs. 2 BDSG dann freiwillig in eine Datenverarbeitung einwilligen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Dasselbe gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Im Hinblick auf diese gesetzlichen Regelvermutungen sind aufgrund des Über-/Unterordnungsverhältnisses jedoch hohe Anforderungen an den Zweck der Einwilligung zu stellen, falls eine Verarbeitung von Beschäftigtendaten im Einzelfall hierauf gestützt werden soll.

34. Darf ich personenbezogene Daten aus öffentlichen Quellen zu Werbezwecken verwenden?

Um personenbezogene Daten aus öffentlichen Quellen für Werbezwecke zu verarbeiten, bedarf es einer Rechtsgrundlage. Diese müsste sich aus Art. 6 Abs. 1 Satz 1 lit. a) bis f) DS-GVO ergeben. Da eine Verwendung öffentlich zugänglicher Adressen aus Telefonbüchern oder anderen Verzeichnissen nicht aufgrund Vertrages oder einer Einwilligung erfolgt, kommt nur die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO in Betracht. Hier ist das berechtigte Interesse des Verantwortlichen an der werblichen Ansprache gegen das Interesse des Betroffenen abzuwägen. Diese Abwägung fällt im Rahmen der sog. Akquisewerbung, der Ansprache mit Werbung, ohne dass der Betroffene jemals mit dem Werbenden in einer Beziehung stand, regelmäßig zugunsten des Betroffenen aus. Der Betroffene muss nicht damit rechnen, dass seine Daten dazu verwendet werden, dass er mit Werbung jedweder Art durch jedweden Verantwortlichen angesprochen wird, nur, weil seine Adressdaten aus einer öffentlichen Quelle stammen. Er wäre dadurch auch gezwungen sich aktiv mittels eine Widerspruches an den Verantwortlichen zu wenden und tätig zu werden, wenn er die Werbung nicht

erhalten möchte. Dies würde unweigerlich dazu führen, dass der Betroffene sich gegen etwas wehren muss, dass er aber gar nicht selbst veranlasst hat.

Zur Zulässigkeit von Werbemaßnahmen durch Verantwortliche hat die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, eine Orientierungshilfe erstellt, in der weitere umfangreiche Ausführungen zu allen Fragen rund um die Werbung im Unternehmen und auch in Hinblick auf die Wechselwirkungen mit dem UWG festgehalten sind. Es werden Hinweise zu den rechtlichen Grundlagen der postalischen Werbung, der Telefonwerbung oder der Werbung per E-Mail detailliert dargelegt und erläutert. Diese Orientierungshilfe ist auf der Webseite der Datenschutzkonferenz unter dem nachfolgenden Link zu finden: https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf .

35. Muss man mit dem Steuerberater einen Vertrag gem. Art. 28 DS-GVO über Auftragsverarbeitung abschließen?

Hierzu gibt es keine übereinstimmende Ansicht unter den Aufsichtsbehörden in Deutschland. Derzeit gilt für Thüringen, dass ein solcher Vertrag auf jeden Fall notwendig ist, wenn der Steuerberater neben der steuerlichen Beratung des Unternehmens/des Unternehmers auch die Lohn- und Gehaltsberechung/Lohnbuchhaltung für diesen übernimmt. Die Übermittlung aller Daten der Mitarbeiter des Unternehmens kann auf keine rechtliche Grundlage gestützt werden. Auch der Art. 6 Abs. 1, Satz 1 lit. f) DS-GVO ist nicht einschlägig, da es sich bei den Abrechnungsdaten auch um besondere Kategorien personenbezogener Daten handelt, die nach Art. 9 DS-GVO ausschließlich mittels Einwilligung des Betroffenen verarbeitet werden können. Durch den Abschluss eines Auftragsverarbeitungsvertrages allerdings ist der Steuerberater im Rahmen der Gehaltsberechnung/ Lohnbuchhaltung kein Dritter mehr und die Verarbeitung der personenbezogenen Daten im Auftrag des Verantwortlichen ist daher zulässig.(https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf) Auch ein Vertrag nach Art. 26 DS-GVO zur gemeinsamen Verantwortlichkeit zwischen dem Steuerberater und dem Unternehmer hilft in dieser Situation nicht weiter. Auch hier fehlt es an einer Übermittlungsnorm für die Arbeitnehmerdaten vom Unternehmer zum Steuerberater, da der Steuerberater von sich aus, nicht über die Daten der Mitarbeiter verfügt.

36. Ist eine mündliche Einwilligung in eine Datenerhebung möglich oder muss sie stets schriftlich vereinbart werden?

Die Einwilligung ist nach der DS-GVO grundsätzlich formfrei erteilbar. Es ist jedoch zu beachten, dass der Verantwortliche nach der DS-GVO auch eine **Nachweispflicht,** gem. Art. 7 Abs. 1 DS-GVO für die Erteilung der Einwilligung hat. Unter diesem Aspekt ist eine schriftliche Einwilligung von Vorteil, da diese damit dem Verantwortlichen auch gegenüber der Aufsichtsbehörde als Nachweis dienen kann.

37. Darf ich noch Daten über meine Kunden bei Creditreform anfordern?

Die Abfrage von Daten über Betroffene bei einer Auskunftei bedarf einer Rechtsgrundlage. Diese kann sich daher nur aus Art. 6 DS-GVO ergeben. Wenn der Kunde ausdrücklich eine Einwilligung erteilt, ist eine Abfrage möglich oder wenn die Abfrage zur Wahrung des berechtigten Interesses des Abfragenden gem. Art. 6 Abs. 1 Satz1 lit. f) DS-GVO erforderlich ist. Dieses ist allerdings erst dann zu bejahen, wenn auch wirklich ein Ausfallrisiko besteht, d.h. erst wenn bei einem Bezahlvorgang auch eine Zahlungsweise gewählt wurde, die ein solches Risiko birgt, wie z.B. Kauf auf Rechnung. Ist ein derartiges Risiko nicht gegeben, z.B. Zahlung per Paypal, per Nachnahme oder Vorkasse, dann ist eine Abfrage bei einer Auskunftei nicht erforderlich und daher widerrechtlich. Zur allgemeinen „Vorabüberprüfung“ des Betroffenen bevor noch geschäftliche Kontakte aufgenommen wurden, ist jedenfalls eine solche Abfrage unzulässig, da hier keine Erforderlichkeit zur Wahrung der Interessen besteht.

38. Können meine Kunden auf die Informationspflichten verzichten?

Dem Betroffenen sind die Informationen gem. Art. 12 Abs. 1 DS-GVO zur Verfügung zu stellen. Ob dieser sie dann tatsächlich auch zur Kenntnis nimmt oder nicht, oder ganz darauf verzichten möchte, obliegt dem Betroffenen selbst. Die DS-GVO sieht nur eine Pflicht des Verantwortlichen vor, die Informationen zur Verfügung zu stellen (Art. 12 Abs. 1, Art. 13 Abs. 1 und Abs. 2, Art. 14 Abs. 1 und Abs. 2), aber keine Pflicht des Betroffenen, diese auch tatsächlich zur Kenntnis zu nehmen. Der Verantwortliche muss jedoch jederzeit **nachweisen** können, dass er die notwendigen Informationen zur Verfügung gestellt hat, gem. Art. 5 Abs. 2 DS-GVO.

39. Gelten Einwilligungen der Kunden zur E-Mail-Werbung nach altem Recht auch nach dem 25. Mai 2018 fort?

Die Einwilligungen, die unter Geltung des alten BDSG für die Zusendung von Werbung erteilt worden sind, gelten grundsätzlich dann weiter fort, wenn sie den Voraussetzungen des Art. 7 DS-GVO genügen. Oftmals entsprechen sie den Voraussetzungen jedoch nicht, da es am Widerrufsvorbehalt fehlt. Auf das Widerrufsrecht hinsichtlich der Einwilligung ist jedoch explizit hinzuweisen.

40. Unter welchen Voraussetzungen ist das Anfertigen und Verbreiten personenbezogener Fotografien auf Messen, Verkaufsveranstaltungen oder Volksfesten jetzt noch zulässig?

Der Umgang mit Fotografien ist ein komplexes Thema. Der TLfDI hat dazu in seinem 1. Tätigkeitsbericht zum Datenschutz nach der DS-GVO 2018 einen ausführlichen Beitrag gestaltet, bei dem alle möglichen Varianten umfangreich beleuchtet wurden. Zu finden ist der Beitrag 5.21 Veröffentlichung von Fotos und Filmaufnahmen, unter dem folgenden Link: https://www.tlfdi.de/mam/tlfdi/datenschutz/taetigkeitsbericht/1._tatigkeitsbericht_2018_zum_datenschutz_nach_der_ds-gvo.pdf .

41. Kundendaten werden oft an Dritte übermittelt (z.B. Auskunfteien oder Logistikdienstleister). In welchen Fällen muss mit dem Dritten eine Vereinbarung zur Auftragsverarbeitung geschlossen werden? Wann muss eine Einwilligung vorliegen?

Die Datenübermittlung an Dritte bedarf immer einer rechtlichen Grundlage. Diese kann sich nur aus Art. 6 DS-GVO ergeben. Eine Möglichkeit ist daher auch die Einwilligung. Da die Einwilligung allerdings jederzeit für die Zukunft widerrufen werden kann, sollte zunächst geprüft werden, ob nicht auch eine vertragliche Grundlage zur Datenübermittlung vorliegt.

Die Übermittlung der Adressdaten einer Lieferung an den Logistikunternehmer zur reinen Zustellung ist von einem berechtigten Interesse des Verantwortlichen gem. Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO gedeckt, welcher die Lieferung oder die Ware an den jeweiligen Adressaten versenden möchte. Das schutzwürdige Interesse des Bestellers ist hier auch nicht höher zu bewerten, da er ja den Kauf und die Lieferung der Ware an seine Adresse möchte und dies auch beim Versendungskauf ein vertraglicher Bestandteil ist. Davon zu unterscheiden ist allerdings die Übermittlung der Telefonnummer oder Emailadresse an das Logistikunternehmen z.B. für das Pakettracking, da diese regelmäßig nicht zur Zustellung der Ware an die Adresse

notwendig ist. Sollte dies dennoch erfolgen, wäre hierfür eine Einwilligung des Betroffenen vom Verantwortlichen einzuholen.

Die Abfrage bei Auskunfteien und die Übermittlung von Daten dorthin, kann vom Verantwortlichen, wenn kein vertragliches Verhältnis vorliegt, dass zum Abruf berechtigen würde, nur aufgrund einer Einwilligung erfolgen. Für den Fall dass ein Vertragsverhältnis besteht, könnte eine Abfrage bei einer Auskunftei von einem berechtigten Interesse des Verantwortlichen gedeckt sein. In Frage kommt hier ein wirtschaftliches Interesse daran, das Ausfallrisiko besonders gering zu halten. Eine Abfrage bei einer Auskunftei kommt daher auch nur dann in Frage, wenn ein solches Risiko tatsächlich besteht. Dies ist nur bei Zahlungsarten der Fall, die dem Verantwortlichen eine Vorausleistung abverlangen, wie Kauf auf Raten oder Kauf auf Rechnung. Bei Käufen per paypal, Vorkasse, Überweisung o.ä. besteht daher regelmäßig kein Ausfallrisiko seitens des Verantwortlichen, und daher auch kein berechtigtes Interesse an einer Abfrage, siehe auch unter Nr. 37.

Im Fall von Mietverhältnissen und deren Anbahnung, besteht das berechtigte Interesse des Vermieters an einer Selbstauskunft des Mieters bzw. an einer Abfrage des Mieters bei einer Auskunftei auch erst in dem Moment, in dem eine Anmietung der Wohnung überhaupt möglich erscheint. Dies ist regelmäßig erst nach der Besichtigung und nach der Bekanntgabe des Willens des Mieters, diese Wohnung auch anmieten zu wollen, zu bejahen. Keinesfalls besteht ein berechtigtes Interesse des Vermieters bereits bei einer bloßen Interessenbekundung eines potentiellen Mieters an der Anmietung einer Wohnung. Einer derartige Vorverlagerung eines angeblichen berechtigten Interesses des Vermieters stehen auf jeden Fall die schutzwürdigen Interessen des Mieters entgegen. Dieses Thema wird auch in einer Orientierungshilfe der Datenschutzkonferenz, dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zur Einholung einer Selbstauskunft bei MietinteressentInnen umfassend behandelt. Die Orientierungshilfe ist unter dem folgenden Link zu finden: https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf.

Als Auftragsverarbeiter wird nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle bezeichnet, die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Der Auftragsverarbeiter ist nicht Dritter, sondern wird zur Sphäre des Verantwortlichen gerechnet. Für die erfolgreiche Auftragsverarbeitung ist allerdings ein an bestimmte Inhalte gebundener Auftragsverarbeitungsvertrag (AVV) mit technischen und organisatorischen Maßnahmen unabdinglich. (https://www.tlfdi.de/mam/tlfdi/themen/tlfdi_formulierungshilfe_fur_auftragsverarbeitungsvertraege.pdf)

42. Wie können die Informationspflichten nach Art. 13 DS-GVO erfüllt werden, wenn der Erstkontakt mit dem Kunden telefonisch erfolgt (z.B. telefonische Bestellung von Heizöl).

Der Kunde ist dann bereits am Telefon darauf hinzuweisen, dass seine Daten zur Bestellung bzw. Lieferung gespeichert werden. Die ausführlichen Informationen nach Art. 13 DS-GVO sollten dann schriftlich auf der Auftragsbestätigung, dem Lieferschein oder der Rechnung hinterlegt sein. Wenn der Kunde wiederholt bestellt und seine Daten dafür schon beim Unternehmen hinterlegt sind, ist bei einer weiteren Bestellung eine Information in der Regel nicht noch einmal nötig, gem. Art. 13 Abs. 4 DS-GVO, da der Kunde bereits über die Informationen verfügt.

43. Müssen Kunden, deren Daten vor dem 25. Mai 2018 rechtmäßig erhoben wurden, jetzt nochmal die umfangreichen Informationen nach Art. 13 DS-GVO erhalten?

Ja. Die Informationen sind auch an Bestandskunden mitzuteilen, da auch diesen die Rechte aus der DS-GVO zustehen und sie wissen müssen, wer Verantwortlicher der Datenverarbeitung ist und welche Rechte sie geltend machen können. Die Kunden sollten daher bei nächster Gelegenheit die Informationen zur Verfügung gestellt bekommen.

Die DS-GVO sieht eine Angleichungsfrist von 2 Jahren vor, also bis zum 25.05.2020. Dies ergibt sich aus dem ErwG 171 der DS-GVO.

44. Ist eine aktive Tracking-Zustimmung vor dem Setzen des ersten Cookies (z.B. der Google Analytics Cookies) erforderlich?

Als Kurzantwort: ja, eine wirksame Einwilligung ist bei der Nutzung von Google-Analytics notwendig. Dies gilt aber nicht pauschal für alle Cookies. Grundsätzlich sind technisch notwendige Cookies nicht einwilligungspflichtig, während Cookies zu Trackingzwecken dies meist sind. Technisch notwendige Cookies sind solche Cookies, ohne deren Nutzung die Website nicht mehr korrekt funktionieren würde. Zusätzliche Komfortfunktionen oder Zusatzfunktionen jeder Art werden nicht als technisch notwendig erachtet. Hier muss die Funktion jedes Cookies einzeln betrachtet werden. Zu Komfortfunktionen zählen z.B. bei Online-Shops die Anzeige von favorisierten Produktkategorien oder die Anzeige der zuletzt gekauften Artikel. Auch Chat-Assistenten bei Support-Bereichen einer Website sind Komfortfunktionen. Zusatzfunktionen währen Online-Betrachter von PDF-Dokumenten, die Anzeige von Videos, Trackingverfahren oder z.B. Umfragen, welche sich bei der Nutzung der Website einblenden.

Im Detail: Die DSK hat in ihrer „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ (OH TMG) (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf) derzeit wie folgt positioniert:

„Nach dem Verständnis der Aufsichtsbehörden handelt es sich bei „Tracking“ um Datenverarbeitungen zur – in der Regel website- übergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzern. Dieses Begriffsverständnis entspricht dem, welches von den europäischen Aufsichtsbehörden in Veröffentlichungen zugrunde gelegt wird. Für die Bewertung der Zulässigkeit ist allein entscheidend, ob eine bestimmte Verarbeitungstätigkeit rechtmäßig durchgeführt wird und der Verantwortliche allen datenschutzrechtlichen Pflichten der DS-GVO nachkommt. Die Datenverarbeitung ist nur dann rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 DS-GVO vorliegt.

Sämtliche Erlaubnistatbestände der DSGVO sind als gleichrangig und gleichwertig zu betrachten. In Art. 6 DSGVO werden die Bedingungen für die rechtmäßige Verarbeitung personenbezogener Daten festgelegt und sechs Rechtsgrundlagen beschrieben, auf die sich Verantwortliche stützen können. Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche bei der Erbringung von Telemediendiensten kommen insbesondere folgende Erlaubnistatbestände in Betracht:

a) Art. 6 Abs. 1 Satz 1 lit. a) DSGVO - Einwilligung

b) Art. 6 Abs. 1 Satz 1 lit. b) DSGVO - Vertrag

c) Art. 6 Abs. 1 Satz 1 lit. f) DSGVO - Interessenabwägung „

Zur Prüfung, welche der genannten Rechtsgrundlagen für welchen Cookie eingesetzt werden kann, wird an dieser Stelle auf die Ausführungen der „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“, Seiten 8 bis 12 verwiesen, da dies eine komplexe Materie für sich ist.

Zusätzlich müssen die Nutzer dabei über die Erlaubnistatbestände für sämtliche Verarbeitungen ihrer personenbezogenen Daten informiert werden (Informationspflichten nach Art. 13 lit. f) DS-GVO).

Durch die Regelung in Art. 5 Abs. 3 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation), ist **in der Regel eine Einwilligung** zum Setzen von Cookies

notwendig. Grundsätzlich gelten die Datenschutzgrundverordnung und die Richtlinie 2002/58/EG unabhängig voneinander. Während laut DS-GVO noch die Möglichkeit besteht, sich bei Cookies auf Art. 6 Abs. 1 Satz 1 lit. a), b) und f) DS-GVO zu berufen, schränkt die Richtlinie diese Wahlfreiheit bei Cookies auf eine Einwilligung (nach 2002/58/EG Art. 5 Abs. 3) dann ein, wenn der Cookie nicht der Übertragung einer Nachricht dient bzw. der Cookie nicht technisch notwendig ist, um den Kommunikationsdienst zu erbringen. D.h. in den meisten Fällen ist eine Einwilligung aufgrund der Richtlinie notwendig. Entsprechend der Orientierungshilfe gilt es insbesondere bei der Einwilligung zu beachten:

Art. 4 Nr. 11 DS-GVO setzt für eine wirksame Einwilligung eine „unmissverständlich abgegebene Willensbekundung in Form einer „Erklärung“ oder eine sonstige eindeutige bestätigende Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten ausdrücklich einverstanden ist. Dies kann beispielweise durch Anklicken eines Kästchens beim Besuch einer Website, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder aktive Verhaltensweise (Opt-In-Verfahren) geschehen, mit der die betroffene Person eindeutig ihr Einverständnis hinsichtlich der angekündigten und beabsichtigten Datenverarbeitung ausdrückt. Wie dies technisch umgesetzt werden kann und was dabei zu beachten ist, ist in der o.g. „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ auf Seite 9 beschrieben. So kann z.B. ein Einwilligungsbanner vorgeschaltet werden, in welchem auch die nötigen Informationen zur Einwilligung vorhanden sind und welches aktiv durch den Nutzer ein Häkchen, Schalter oder ähnliches setzen lässt. Bevor der Nutzer einwilligt, sind alle Datenverarbeitungen zu unterlassen (Skripte, Zählpixel usw.) und erst nach Einwilligung zu aktivieren. Die Einwilligung muss dann ebenso einfach widerrufen werden können.

Ein Opt-Out-Verfahren, bei welchem von der Einwilligung des Nutzers ausgegangen wird und nur durch eine aktive Handlung wie z.B. der Abwahl eines Kontrollkästchens ein Widerspruch erfolgt, reicht als Einwilligung nicht aus. Insoweit führt Erwägungsgrund 32 DS-GVO explizit aus, dass konkludente Verhaltensweisen wie „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person“ keine Einwilligungen darstellen. Näheres hierzu findet sich ebenfalls auf Seite 9 der Orientierungshilfe. Diese Auffassung wird auch im aktuellen Urteil des Europäischen Gerichtshofs (Rechtssache C-673/17) vom 1. Oktober 2019 bestätigt.

45. Können auf der Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO Adressdaten von Unternehmern und Verbrauchern aus öffentlich zugänglichen Daten (z.B. Internet) für Marketingzwecke verarbeitet werden?

Auch im Bereich der Datenerhebung aus dem Internet gilt das Gleiche wie das zur Datenerhebung aus öffentlichen Verzeichnissen unter Nr. 36 Gesagte.

46. Ist der Verkauf dieser Adressdaten an andere Unternehmen auf der Grundlage von Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO möglich?

Nein. Ein Adressverkauf ist nicht aufgrund von Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO möglich. Ein Verkauf kann nur mit Einwilligung der betroffenen Person geschehen, denn das berechtigte Interesse an der Verarbeitung der Daten tritt hier hinter dem schutzwürdigen Interesse der betroffenen Person zurück. Auch von der Erwartungshaltung des Kunden aus rechnet dieser eher nicht damit, dass seine Daten an fremde Drittunternehmen weitergegeben werden.

Beim Lettershopverfahren handelt es sich um eine „Adressenvermietung“, da dort keine personenbezogenen Daten an einen Dritten übermittelt werden. Es werden dazu die personenbezogenen Daten (z.B. Adressen) bei einem Verantwortlichen genutzt, um für ein anderes Unternehmen Werbung zu machen. Dafür bleiben die Adressen beim ursprünglichen Verantwortlichen und dieser versendet dann die Werbematerialien (Briefe, Flyer) anderer Unternehmen an die bei ihm vorliegenden Adressen. Die werbenden Unternehmen erhalten die Adressen der Betroffenen aber selber nicht. Eine Weitergabe der Daten ist damit ausgeschlossen.

Beim Lettershopverfahren soll der Betroffene, der dann die Werbung eines Unternehmens erhält, auch auf den Werbenden im Werbeschreiben hingewiesen werden, sodass ein Werbewiderspruch auch ihm gegenüber erklärt werden kann und damit die Betroffenenrechte ungehindert ausgeübt werden können. Rechtsgrundlage für das Lettershopverfahren ist Art. 6 Abs. 1 Satz 1 lit. a) DS-GVO, also die Einwilligung. Es besteht zwar nach Art.6 Abs.1 Satz 1 lit.f) DS-GVO ein berechtigtes Interesse des Verantwortlichen und auch des Dritten (Werbenden) an der Datenverarbeitung für Werbezwecke und die Verarbeitung der Adressdaten wäre dafür auch erforderlich. Bei der Interessenabwägung ist allerdings zu beachten, dass es üblicherweise nicht der allgemeinen Erwartungshaltung der betroffenen Person entspricht, von diversen unbekannten Unternehmen Werbung zu erhalten. Betroffene Personen müssen daher nicht damit rechnen, von ihnen nicht bekannten Dritten, mit denen sie in keiner Beziehung stehen, Werbung zu erhalten.

47. Muss jedes Unternehmen, das seine Registrierkasse mit Videoüberwachung sichert, einen Datenschutzbeauftragten benennen?

Die Überwachung einer Registrierkasse mit einer Videokamera ohne Erfassung der daran arbeitenden Kassierer/innen und ohne dass Kunden ins Visier geraten, ist unproblematisch, denn diese Kamera erfasst keine personenbezogenen Daten mangels betroffener Personen. Werden jedoch mit der Registrierkasse das Kassenpersonal und Kunden erfasst, muss bei der Anschaffung der Technik auf die sichere und datenschutzfreundliche Gestaltung geachtet werden (Art. 32 und Art. 25 DS-GVO) und vor allem auch das Vorliegen der Zulässigkeitsvoraussetzungen nach Art. 6 Abs. 1 Satz 1 lit. f) DS-GVO geprüft werden. In die Interessensabwägung ist einzubeziehen, ob der Wahrung der berechtigten Interessen des Unternehmens ein überwiegendes Interesse der erfassten Personen gegenübersteht. Werden Mitarbeiter erfasst, ist ein strengerer Maßstab anzulegen. Es ist auszuschließen, dass eine vollständige Erfassung der Kassenmitarbeiter erfolgt, weil dies für den Zweck der Sicherung der Kasse grundsätzlich nicht erforderlich ist. Lediglich bei bestehendem Verdacht der Begehung von Straftaten kann eine Videoüberwachung auf eine bestimmte Person erfolgen, soweit die Voraussetzungen des § 26 Abs. 1 Satz 2 Bundesdatenschutzgesetz vorliegen. Weitere Ausführungen können dem Kurzpapier Nr. 15 „Videoüberwachung nach der Datenschutz-Grundverordnung“ https://www.tlfdi.de/tlfdi/europa/europaeischedsgvo/index.aspx und der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ https://www.tlfdi.de/tlfdi/gesetze/orientierungshilfen/ entnommen werden.

Eine Einwilligung des Arbeitnehmer kommt im Arbeitsverhältnis regelmäßig nicht in Betracht, da es wegen des Unter- Überordnungsverhältnisses im Arbeitsverhältnis an der Freiwilligkeit der Einwilligung mangelt, § 26 Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG). Eine Ausnahme von diesem Grundsatz nach § 26 Abs. 2 Satz 2 BDSG ist bei dieser Fallkonstellation nicht ersichtlich, da der Arbeitnehmer durch die Aufzeichnung offensichtlich keinen rechtlichen oder wirtschaftlichen Vorteil erlangt.

Unabhängig von der Prüfung der Zulässigkeit einer Videoüberwachung im Kassenbereich, sind die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten zu beachten. Siehe dazu unter Frage 20. Ein DSB ist wie oben bereits ausgeführt nur unter bestimmten Bedingungen zu benennen. Eine einzelne Überwachungskamera zieht ggf. noch keine Bestellpflicht nach sich. Anders kann dies natürlich bei einer gem. Art. 35 Abs. 3 lit. b) DS-GVO systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche sein, da dies regelmäßig eine Datenschutz-Folgenabschätzung nach sich zieht und daher eine Benennungspflicht auslöst. Danach wäre dann auch bei einer Videoüberwachung im Einzelhandel, so sie denn zulässig betrieben werden kann, ein DSB zu benennen.

48. Wie kann ich mein Unternehmen zertifizieren lassen?

Nach der DS-GVO können einzelne Verarbeitungsvorgänge zertifiziert werden, Art. 42 DS-GVO. Diese Zertifizierung wird wiederum von Unternehmen vorgenommen, die nach einem speziellen Verfahren durch die Aufsichtsbehörden in Zusammenarbeit mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) für ein vorab genehmigtes Zertifzierungsprogramm akkreditiert werden.

Das Unternehmen hat folglich nicht die Möglichkeit sich insgesamt zertifizieren zu lassen. Die Zertifizierung bezieht sich immer nur auf einen bestimmten Verarbeitungsvorgang.

Andere „Zertifizierungen“, die am Markt angeboten werden, z.B. mit der Aussage: „Zertifiziert nach der DS-GVO“, haben im Rahmen der datenschutzrechtlichen Prüfung möglicherweise keine Bindungswirkung für den TLfDI und anderer Datenschutzaufsichtsbehörden.

Durch eine Zertifizierung wird nicht die datenschutzrechtliche Verantwortung des Unternehmens für die Einhaltung der DS-GVO gemindert und sie schmälert auch nicht die Aufgaben und Befugnisse der Aufsichtsbehörden, Art. 42 Abs. 4 DSGVO. Eine Zertifizierung, die von einer nach der DS-GVO akkreditierten Stelle vergeben wird, erleichtert aber den Nachweis, dass die Anforderungen der DS-GVO eingehalten werden. Es sollte daher stets auch die Akkreditierungsurkunde überprüft werden.