19.06.2019

Fragen und Antworten zu der EU Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz

Vorbemerkung

Die europäischen und der deutsche Gesetzgeber haben das Datenschutzrecht auf neue rechtliche Grundlagen gestellt. Ab dem 25.05.2018 gilt die EU-Datenschutz-Grundverordnung (DS-GVO); gleichzeitig tritt das neue Bundesdatenschutzgesetz (BDSG n.F.) in Kraft.

Die neuen Rechtsgrundlagen stellen keinen Paradigmenwechsel dar. Viele Grundsätze der DS-GVO gab es schon in der EU-Datenschutzrichtlinie von 1995, die durch das bisher geltende BDSG a.F. umgesetzt wurde. Dazu gehören u.a. die Datenvermeidung und Datensparsamkeit, die Zweckbindung der Datenverarbeitung und das grundsätzliche Verbot der Datenverarbeitung mit Erlaubnisvorbehalt. Die Unterschiede zwischen dem neuen und dem bisherigen Recht liegen vor allem in einer erheblich gesteigerten Dokumentations- und Nachweispflicht („Accountability“) sowie in der Verschärfung des Haftungsregimes und der Erhöhung des Bußgeldrahmens. Außerdem weitet die DS-GVO den Datenschutz in gewissen Konstellationen auf Datenverarbeitungen auch außerhalb der EU aus.

Neu ist außerdem, dass die für den Datenschutz Verantwortlichen bei der Wahl der Schutzmaßnahmen vielfach selbst einschätzen müssen, wie weitreichend eine Schutzmaßnahme sein muss, um dem drohenden Risiko der Datenschutzverletzung entgegenzuwirken. Dieser sog. risikobasierte Ansatz soll den Verantwortlichen Spielraum verschaffen, die für ihre Risikosituation passenden Maßnahmen zu ergreifen. Selbstverantwortung kann allerdings zu Fehleinschätzungen führen, die nunmehr hohe Bußgeldzahlungen nach sich ziehen können.

Mit dem vorliegenden Papier soll den in Deutschland tätigen WP in Form von Fragen und Antworten ein Überblick über die wichtigsten Regelungsinhalte vermittelt werden. Dadurch soll ihnen eine praktische Hilfestellung bei der Vorbereitung auf das neue Datenschutzregime und bei dessen weiteren Anwendung an die Hand gegeben werden.

Die Antworten und Hinweise in diesem Papier reflektieren den Erkenntnis- und Diskussionsstand zum Zeitpunkt seiner Veröffentlichung. Bei Fragen, zu denen es noch keine

endgültige Antwort gibt, wird zunächst die in den Fachgremien des IDW vorläufig abgestimmte Auffassung wiedergegeben. Es ist geplant, das Papier weiterzuentwickeln und bei Anlass zu aktualisieren.

Wir weisen darauf hin, dass die gegebenen Empfehlungen und Hinweise weder Anspruch auf Vollständigkeit erheben, noch in allen Fällen zwingend erforderliche Handlungsvorgaben darstellen.

1. Definitionen und Anwendungsbereich

1.1. Gilt das neue Bundesdatenschutzgesetz oder die DS-GVO?

Beide. Es gelten sowohl die DS-GVO als auch das DSAnpUG (im Folgenden: BDSG n.F.) nebeneinander. Im Unterschied zur alten EU-Datenschutzrichtlinie (RL 95/46 EG), die mit Wirksamwerden der DS-GVO außer Kraft treten wird, handelt es sich bei der DS-GVO um eine EU-Rechtsverordnung, die unmittelbar in allen EU-Mitgliedstaaten Geltung besitzt und keiner Umsetzung in nationales Recht bedarf, um wirksam zu werden. Daneben gilt auch das BDSG n.F. Das BDSG n.F. füllt Gestaltungsspielräume aus, die die DS-GVO den nationalen Gesetzgebern in sog. Öffnungsklauseln lässt.

1.2. Welches Recht ist im Kollisionsfall anwendbar – DS-GVO oder BDSG n.F.?

Im Kollisionsfall, d.h. wenn sich die DS-GVO und das BDSG n.F. widersprechen, geht die DS-GVO als übergeordnetes Recht vor und ist damit vorrangig anzuwenden. Dementsprechend regelt § 1 BDSG n.F. in Abs. 5, dass die Vorschriften des Gesetzes keine Anwendung finden, soweit das Recht der DS-GVO in der jeweils geltenden Fassung unmittelbar gilt.

1.3. Wer ist „betroffene Person“?

Betroffene Person i.S. des Artikels 4 Nr. 1 DS-GVO ist jede natürliche Person, deren personenbezogene Daten verarbeitet werden.

Beispiele:

Zu den betroffenen Personen i.S. des Artikels 4 Nr. 1 DS-GVO zählen in der Praxis insb. die folgenden Personen: die Beschäftigten (z.B. Angestellte, freie Mitarbeiter) des WP oder der WPG, Mandanten, soweit es sich um natürliche Personen handelt, Kontaktpersonen, Ansprechpartner und z.B. Geschäftsführer bei Mandanten, die juristische Personen sind, die Ansprechpartner und Beschäftigten von sonstigen Vertragspartnern des WP oder der WPG (z.B. Beschäftigte der Dienstleister, Lieferanten, IT Service Provider etc.). Darüber hinaus können aus Sicht des WP zu den betroffenen Personen auch z.B. Geschäftspartner und Beschäftigte des Mandanten gehören.

Der Schutz der DS-GVO gilt nur für lebende natürliche, nicht aber für verstorbene Personen.

1.4. Werden auch Unternehmensdaten durch die DS-GVO geschützt?

Nein, die DS-GVO schützt nur natürliche Personen. Angaben zu einer juristischen Person einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person fallen grundsätzlich nicht in den Anwendungsbereich der DS-GVO (Erwägungsgrund 14).

1.5. Welche Daten werden durch die DS-GVO geschützt?

Geschützt werden nur personenbezogene Daten. Der Begriff der „personenbezogenen Daten“, der den sachlichen Anwendungsbereich der DS-GVO nach Artikel 1 maßgeblich bestimmt, wird in Artikel 4 Nr. 1 DS-GVO definiert.

1.6. Welche Informationen unterfallen dem Begriff „personenbezogene Daten“?

Nach der Definition in Artikel 4 Nr. 1 DS-GVO sind – der bisherigen Rechtslage entsprechend – personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine natürliche Person ist nach der Definition identifizierbar, wenn die Person direkt oder indirekt identifiziert werden kann, insb. mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu Merkmalen, die Ausdruck der physischen, physiologischen, wirtschaftlichen, kulturellen oder sozialen Identität der betroffenen Person sind.

Beispiele:

Der Begriff der personenbezogenen Daten ist sehr weit gefasst. Er erfasst neben den typischen direkten Identifikationsmerkmalen, mit denen die Identität einer Person festgestellt werden kann (wie Namen, Anschrift, Telefonnummern, Geburtsdatum, Angabe von Alter und Geschlecht, E-Mail-Adressen etc.), auch solche Informationen, die eine Zuordnung zu einer bestimmten Person erlauben, wie z.B. Konto- und Kreditkartennummern, Steueridentifikationsnummern, Sozialversicherungsnummern, Ausweisnummern, Personalnummern oder Kundennummern. Hierzu gehören auch Login-Informationen und ebenso IP-Adressen, also die individuelle Kennung eines Computeranschlusses.

Darüber hinaus umfasst der Begriff der personenbezogenen Daten auch Angaben zur beruflichen, familiären oder sozialen Identität der betroffenen Person. Hierzu gehören u.a. die berufliche Position, Angaben zum Arbeitgeber, Beteiligung an Handelsgesellschaften, Angaben über die familiäre Situation (Personenstand, Anzahl der Kinder, Verwandtschaftsverhältnisse), Angaben über Wohnverhältnisse, Angaben über die Mitgliedschaft und Betätigung in Organisationen sowie Angaben über Vermögens- und Einkommensverhältnisse.

Geschützt sind weiterhin Informationen zu körperlichen Merkmalen und Zuständen, z.B. Angaben zum Gesundheitszustand (Krankheiten, ärztliche Untersuchungsergebnisse), Standortdaten und Aufenthaltsangaben, biometrische Informationen sowie Informationen zu rechtlichen Beziehungen (Verträge, Eigentum, Vertragspartner).

1.7. Wer ist „Verantwortlicher“ i.S. der DS-GVO?

Nach Artikel 4 Nr. 7 DS-GVO ist „Verantwortlicher“ jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Damit ist grundsätzlich jeder, der personenbezogene Daten natürlicher Personen für eigene Zwecke und mit eigenen Datenverarbeitungsmitteln verarbeitet, Verantwortlicher i.S. des Artikels 4 Nr. 7 DS-GVO. So ist z.B. ein einzelner WP in eigener Praxis Verantwortlicher i.S. des Datenschutzrechts. Im Fall einer WPG ist dagegen allein die Gesellschaft Verantwortlicher i.S. des Datenschutzrechts, nicht aber die einzelnen WP, die als Angestellte bei der WPG tätig sind. Dies gilt unabhängig von der Rechtsform, insb. auch für Sozietäten in der Form der GbR oder andere Formen der beruflichen Zusammenarbeit als Personenvereinigung ohne eigene Rechtspersönlichkeit.

1.8. Ist ein WP „Verantwortlicher“ i.S. der DS-GVO?

Ja, i.d.R. ist der WP bzw. die WPG sowohl in prüfender als auch in beratender Funktion Verantwortlicher i.S. der DS-GVO (Artikel 4 Nr. 7 DS-GVO).

1.9. Was bedeutet „Verarbeitung“?

Verarbeitung ist nach der Definition in Artikel 4 Nr. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Reihe von solchen Vorgängen im Zusammenhang mit personenbezogenen Daten.

Der Begriff der Verarbeitung ist damit sehr weit gefasst und erfasst jede Tätigkeit, bei der personenbezogene Daten in irgendeiner Weise zur Kenntnis genommen und genutzt werden.

1.10. Welche Tätigkeiten fallen unter den Begriff der „Verarbeitung“?

Die Definition des Begriffs der „Verarbeitung“ in Artikel 4 Nr. 2 DS-GVO nennt beispielhaft als wesentliche Verarbeitungstätigkeiten das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten.

1.11. Findet das Datenschutzrecht auch Anwendung, wenn die Daten nicht automatisiert verarbeitet werden?

Ja. Nach Artikel 2 Abs. 1 DS-GVO erfasst der sachliche Anwendungsbereich der DS-GVO zum einen die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Darüber hinaus ist auch die nichtautomatisierte Verarbeitung personenbezogener Daten in den Anwendungsbereich der DS-GVO einbezogen, wenn die betroffenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Der sachliche Anwendungsbereich wird in Erwägungsgrund 15 der DS-GVO konkretisiert. Danach ist der Schutz von personenbezogenen Daten grundsätzlich technologieneutral und erfasst jede Form der automatisierten Verarbeitung unabhängig von der verwendeten Technik. Um eine Umgehung der Vorschriften der DS-GVO zu vermeiden, soll außerdem auch die manuelle Verarbeitung in den Anwendungsbereich einbezogen werden, jedoch nur wenn und soweit die betroffenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Beispiele:

Zu den vom Anwendungsbereich erfassten manuellen Verarbeitungen gehören i.d.R. auch (Papier-)Aktensammlungen. Dies gilt jedenfalls dann, wenn diese einer gewissen Ablagestruktur unterliegen. In aller Regel sind daher sämtliche Akten des täglichen Geschäfts eines WP dem Anwendungsbereich unterworfen, da sie bspw. alphabetisch sortiert oder durchnummeriert sind. Selbst unsortierte Dokumente, wie etwa Belege, die demnächst abgelegt und damit sortiert werden sollen, sind von der DS-GVO umfasst. Lediglich unstrukturierte Notizen und ähnliche Informationen unterfallen nicht dem Anwendungsbereich der DS-GVO.

Aber auch in Bezug auf diese ergibt sich eine Gegenausnahme. Wie schon bisher nach § 32 BDSG a.F. unterfallen dem Beschäftigtendatenschutz nach § 26 Abs. 7 BDSG n.F. auch solche personenbezogene Daten von Beschäftigten dem Datenschutzrecht, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Dies bedeutet, dass im Hinblick auf personenbezogene Beschäftigtendaten jede – auch eine unstrukturierte – Form der Datenverarbeitung datenschutzrechtlich relevant ist.

1.12. Wo ist das EU-Datenschutzrecht anwendbar (Marktortprinzip, Artikel 3)?

Das EU-Datenschutzrecht ist nicht nur für WP und WPG anwendbar, die ihren Sitz in der EU haben, sondern kann auch Anwendung finden für WP und WPG, die außerhalb der EU ansässig sind.

1.12.1. Nach Artikel 3 Abs. 1 DS-GVO ist das EU-Datenschutzrecht zunächst ausnahmslos auf die Verarbeitung von personenbezogenen Daten anwendbar, wenn diese

im Rahmen der Tätigkeiten einer Niederlassung des Verantwortlichen oder des Auftragsverarbeiters in der EU stattfindet.

Dies gilt unabhängig davon, ob die Verarbeitung selbst in der EU stattfindet oder nicht.

Die DS-GVO besitzt somit auch Geltung, wenn der WP bzw. die WPG seinen bzw. ihren Sitz oder eine Niederlassung zwar in der Union hat, die Verarbeitung personenbezogener Daten jedoch außerhalb der Union erfolgt (z.B. wenn die Verarbeitung auf Servern außerhalb der Union erfolgt oder durch Dienstleister außerhalb der Union durchgeführt wird).

Beispiele:

Die DS-GVO ist in den folgenden Fällen anwendbar:

Die WPG hat ihren Sitz in der Union,

- die Verarbeitung findet in einer Niederlassung der WPG außerhalb der Union statt; oder
- die Verarbeitung findet durch einen Dienstleister mit Sitz außerhalb der Union statt; oder
- die Verarbeitung findet für eine WPG-Niederlassung in der Union statt, jedoch auf Servern außerhalb der Union.

1.12.2. Darüber hinaus unterfallen Verantwortliche oder Auftragsverarbeiter, die nicht in der EU ansässig sind, ebenfalls der DS-GVO, wenn sie Waren und Dienstleistungen an betroffene Personen in der EU anbieten und in diesem Zusammenhang deren Daten verarbeiten, sowie wenn die Verarbeitungstätigkeiten von außerhalb der EU ansässigen Verantwortlicher oder Auftragsverarbeitern die Beobachtung des Verhaltens von Betroffenen in der EU umfassen.

Die DS-GVO besitzt daher Geltung, wenn die Verarbeitung in einer Niederlassung einer außereuropäischen WPG in der Union erfolgt. Dies betrifft Fälle, in denen eine außereuropäische WPG eine oder mehrere Niederlassungen in der Union hat und dort die Verarbeitung stattfindet. Auch hier kommt es nicht darauf an, ob die Verarbeitung technisch in der Union erfolgt oder nicht, sondern dass sie im Rahmen der Tätigkeiten der WPG-Niederlassung in der Union erfolgt.

1.13. Ist das EU-Datenschutzrecht neben dem Berufsrecht für WP und WPG anwendbar?

Ja. Das Datenschutzrecht gemäß DS-GVO und BDSG n.F. wird durch das Berufsrecht für WP und WPG nicht verdrängt. Soweit Mandantendaten verarbeitet werden, geht das Berufsrecht im Falle einer Kollision mit der DS-GVO als lex specialis (s. auch u. 1.15.) vor. Die DS-GVO bleibt z.B. in den Bereichen anwendbar, in denen personenbezogene

Daten z.B. von Beschäftigten des WP oder der WPG oder von Beschäftigten von Dienstleistern oder Lieferanten verarbeitet werden (also außerhalb eines Mandatsverhältnisses).

Beispiele für personenbezogene Daten siehe **Anhang**.

1.14. Ändert die DS-GVO und das BDSG die berufliche Verschwiegenheitspflicht?

Nein, die DS-GVO und das BDSG n.F. ändern die berufliche Verschwiegenheitspflicht grundsätzlich nicht.

Die DS-GVO enthält keine unmittelbaren Regelungen zu berufsrechtlichen Verschwiegenheitspflichten. Der deutsche Gesetzgeber hat jedoch von einer Öffnungsklausel Gebrauch gemacht und in § 29 Abs. 1 BDSG n.F. einige Ausnahmen von insb. den Informations- und Transparenzpflichten aufgenommen, wenn durch deren Erfüllung das Berufsgeheimnis gefährdet oder verletzt würde. Zudem wurden die Befugnisse der Datenschutzaufsichtsbehörden eingeschränkt. Hierzu s.u. 5.2., 5.4. und 5.5.

1.15. Haben die berufsrechtlichen Regeln Vorrang vor dem Datenschutzrecht?

Die gesetzlichen und verordnungsrechtlichen Regelungen zur berufsrechtlichen Verschwiegenheitspflicht sind im Verhältnis zum allgemeinen Datenschutzrecht spezialgesetzliche Regelungen und damit vorrangig anwendbar.

Dementsprechend regelt § 1 Abs. 2 BDSG n.F. grundsätzlich, dass andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG n.F. vorgehen. Wird ein Sachverhalt, für den ein solches Spezialgesetz gilt, allerdings nicht oder nicht abschließend durch die Vorgaben des Spezialgesetzes geregelt, finden die Vorschriften des BDSG n.F. Anwendung. Insb. bleibt auch die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt. Hierzu können bspw. vertragliche Geheimhaltungspflichten ebenso zählen wie derartige Pflichten aus Satzungen oder auch Verordnungen.

1.16. Welche Befugnisse haben die datenschutzrechtlichen Aufsichtsbehörden gegenüber WP und WPG?

Der Umfang der Befugnisse der Datenschutzaufsicht ergibt sich grundsätzlich aus Artikel 58 DS-GVO. Allerdings erlaubt Artikel 90 Abs. 1 DS-GVO den nationalen Gesetzgebern, die Befugnisse der datenschutzrechtlichen Aufsichtsbehörden nach Artikel 58 Abs. 1 Buchst. e und f DS-GVO einzuschränken.

Das hat der Gesetzgeber in § 29 BDSG n.F. getan. Nach § 29 Abs. 3 BDSG n.F. besteht

- das Recht der Datenschutzaufsicht auf Zugang zu allen personenbezogenen

Daten und Informationen (Artikel 58 Abs. 1 Buchst. e) sowie

- das Recht der Datenschutzaufsicht auf Zugang zu den Geschäftsräumen einschließlich aller Datenverarbeitungsanlagen und -geräte des Verantwortlichen und Auftragsverarbeiters (Artikel 58 Abs. 1 Buchst. f)

nicht gegenüber den in § 203 Abs. 1, 2a und 3 des Strafgesetzbuches genannten Personen, zu denen die WP gehören, und ihren Auftragsverarbeitern, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde.

Die Einschränkungen der Befugnisse der Datenschutzaufsicht gegenüber WP und WPG gelten auch für die Auftragsverarbeiter von Berufsgeheimnisträgern. Damit will der Gesetzgeber dem Umstand Rechnung tragen, dass Berufsgeheimnisträger sich vermehrt externer IT-Dienstleister bedienen und diese vertraglich zur Verschwiegenheit verpflichten. Dem soll Rechnung getragen werden, indem die Befugnisse der Behörde nicht nur gegenüber den Berufsgeheimnisträgern selbst, sondern auch gegenüber deren Auftragsverarbeitern gleichermaßen eingeschränkt sind.

Beispiele:

Untersuchungen der Datenschutzaufsichtsbehörden können daher für diejenigen Bereiche verweigert werden, in denen personenbezogene Daten verarbeitet werden, die im Rahmen einer der Geheimhaltungspflicht unterliegenden Tätigkeit erhoben wurden und zu Zwecken einer der Geheimhaltungspflicht unterliegenden Tätigkeit genutzt werden.

- Zugriff auf Systeme, in denen mandatsbezogene Informationen gespeichert und verarbeitet werden, soweit eine Beschränkung des Zugriffs auf nicht-mandatsbezogene Daten nicht möglich ist
- Zugriff auf zur Abrechnung von Mandaten genutzte Systeme
- Zugriff auf Datenbanken mit Informationen zu Mandanten, die im Rahmen der Bearbeitung von Mandaten genutzt werden
- Zugriff auf Mandatsakten
- Zugriff auf E-Mail-Systeme, mit denen Mandantenkorrespondenz geführt wird.

1.17. Erfassen die Informationspflichten gegenüber Betroffenen nach DS-GVO auch Informationen, die dem Berufsgeheimnis unterfallen?

Nein. Die DS-GVO selbst schränkt in Artikel 14 Abs. 5 Buchst. d die Informationspflichten gegenüber den Betroffenen ein, wenn die personenbezogenen Daten nach Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis – einschließlich einer satzungsmäßigen Geheimhaltungspflicht – unterliegen und deshalb vertraulich behandelt

werden müssen. In diesem Fall finden die Informationspflichten nach Artikel 14 Abs. 1 bis 4 DS-GVO keine Anwendung.

2. Auftragsverarbeiter (Artikel 28 DS-GVO)

2.1. Was ist Auftragsverarbeitung?

Die grundlegenden Prinzipien einer Auftragsverarbeitung (im bisherigen BDSG "Auftragsdatenverarbeitung") bleiben auch im Rahmen der DS-GVO weitgehend gleich. Auftragsverarbeiter ist gemäß Artikel 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Das Konstrukt der Auftragsverarbeitung erleichtert in rechtlicher Hinsicht das „Outsourcing" technischer Verarbeitungsvorgänge.

Eine Auftragsverarbeitung liegt i.d.R. dann vor, wenn die Datenverarbeitung durch den Auftragnehmer nicht eigenen Zwecken, sondern überwiegend den Zwecken des Auftraggebers dient und kein eigenes, fachlich-inhaltliches Interesse des Auftragsverarbeiters an der Verarbeitung vorliegt. I.d.R. betrifft eine Auftragsverarbeitung deshalb lediglich die technische Unterstützung bei einer Datenverarbeitung und keine eigenständige fachliche Leistung. Der Auftraggeber bestimmt Umfang und Art der Verarbeitung und der Auftragsverarbeiter erbringt für diesen mit der Dienstleistung lediglich eine technische Hilfs- und Unterstützungsfunktion und unterliegt dabei den Weisungen des Auftraggebers.

Ein Auftragsverarbeiter ist deshalb wie bisher datenschutzrechtlich nicht als „Dritter" anzusehen (Artikel 4 Nr. 10 DS-GVO), d.h. eine eigenständige Rechtsgrundlage außerhalb der Auftragsverarbeitung ist für die Weitergabe personenbezogener Daten an Auftragsverarbeiter nicht erforderlich. Der Auftragsverarbeiter ist ebenfalls weiter im Rahmen des Auftrags kein „Verantwortlicher" i.S. des Artikels 4 Abs. 7 DS-GVO, d.h. von der Datenverarbeitung Betroffene müssen ihre Rechte (Artikel 15 ff. DS-GVO) bei einer Auftragsverarbeitung gegenüber dem Auftraggeber/datenschutzrechtlich „Verantwortlichen" geltend machen.

Eine Regelung zum Umgang mit (Fern-)Wartungstätigkeiten wie § 11 Abs. 5 BDSG enthält die DS-GVO nicht. Bei bestimmten Tätigkeiten, wie bei einer rein technischen Wartung, kann dies u.U. nicht zu einer Qualifikation als Auftragsverarbeiter und damit nicht zu einer Anwendung von Artikel 28 DS-GVO führen. Ist Auftragsgegenstand der (Fern-)Wartung allerdings gerade der Umgang mit Datensätzen mit personenbezogenen Daten, so handelt es sich weiter um eine Auftragsverarbeitung nach Artikel 28 DS-GVO (vgl. Bayerisches Landesamt für Datenschutz, Kurzpapier Auftragsverarbeitung nach der DS-GVO, https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf).

2.2. Kann der WP Auftragsverarbeiter sein?

Ja, aber nur in Ausnahmefällen. Der Tatbestand der weisungsgebundenen Datenverarbeitung, den auch die DS-GVO für eine Auftragsverarbeitung voraussetzt, ist wegen der berufsrechtlich vorgegebenen Eigenverantwortlichkeit des WP nicht erfüllt, wenn dieser personenbezogene Daten im erforderlichen Umfang zur Durchführung seiner fachlichen Tätigkeiten im Rahmen von § 2 WPO verarbeitet. Hier wird der WP gegenüber dem Mandanten in eigener Verantwortung, nach eigenem Ermessen und nicht weisungsgebunden tätig.

Anders kann dies ggf. zu beurteilen sein, wenn der WP als Schwerpunkt seiner Leistung eine technische Plattform zur Verfügung stellt, wie z.B. im Rahmen von Forensic-Aufträgen eine Plattform zur Analyse von E-Mails, die im Rahmen der Leistungserbringung vom Mandanten und von von ihm beauftragten Anwälten genutzt wird.

Abzugrenzen ist die Auftragsverarbeitung künftig auch von der gemeinsamen Verantwortung zweier datenschutzrechtlich Verantwortlicher („Joint Control“, Artikel 26 DS-GVO). Inwieweit im Verhältnis zwischen WP und Mandanten diese für das deutsche Recht noch neue Rechtsfigur der gemeinsamen Verantwortlichkeit (Artikel 26 DS-GVO) in der Praxis Anwendung finden kann, ist derzeit noch nicht abzusehen. Ausgangspunkt einer gemeinsamen Verantwortlichkeit gemäß Artikel 26 DS-GVO soll jedenfalls ein (nicht zwingend gleichrangiger) tatsächlicher Einfluss mehrerer Parteien auf Festlegung und Durchführung der Datenverarbeitung sein. Da der WP seinen Beruf gemäß § 43 Abs. 1 WPO, § 12 Berufssatzung eigenverantwortlich auszuüben hat, ist jedoch nach wie vor davon auszugehen, dass er in aller Regel weiterhin alleinverantwortliche Stelle bleibt.

Unabhängig hiervon kann ohnehin wie bisher auch immer in Erwägung gezogen werden, dem Mandanten die datenschutzrechtlichen Verpflichtungen, denen der WP als Verantwortlicher unterliegt, in einer schriftlichen Vereinbarung zuzusichern, die die berufsrechtliche Verschwiegenheitspflicht, der der WP unterliegt, entsprechend berücksichtigt.

2.3. Welche Regeln hat der Auftragsverarbeiter zu beachten?

Bisher durch § 11 BDSG a.F. nur auf nationaler Ebene in eine detaillierte Regelung gefasst, regelt nun Artikel 28 DS-GVO die Auftragsverarbeitung (BDSG a.F.: „Auftragsdatenverarbeitung“) ausführlich.

Die grundlegenden Prinzipien einer Auftragsverarbeitung bleiben weitgehend gleich. Der Inhalt der Vereinbarung, die mit dem Auftragsverarbeiter zu schließen ist, wird – ähnlich dem bisherigen § 11 Abs. 2 BDSG a.F. – in Artikel 28 Abs. 3 DS-GVO vorgeschrieben und ist schriftlich oder in elektronischer Form (Artikel 28 Abs. 9 DS-GVO) festzuhalten.

Der Auftragsverarbeiter muss u.a. dem Auftraggeber die gemäß Artikel 32 DS-GVO

getroffenen Maßnahmen zur Datensicherheit nachweisen und zusichern (Artikel 28 Abs. 3 Buchst. c DS-GVO) sowie sich diesbezüglich auch der Kontrolle durch den Auftraggeber unterwerfen (Artikel 28 Abs. 3 Buchst. h DS-GVO). Setzt der Auftragsverarbeiter zur Auftragserfüllung Unterauftragnehmer ein, ist er verpflichtet, diesen dieselben Datenschutzpflichten aufzuerlegen, die er mit dem Auftragnehmer vereinbart hat, und steht auch für deren Einhaltung ein (Artikel 28 Abs. 4 DS-GVO). Der Auftragsverarbeiter ist schließlich vollumfänglich an die Weisungen des Auftraggebers gebunden (Artikel 29 DS-GVO).

2.4. Existieren künftig Standardvertragsklauseln für Auftragsverarbeitungsverträge?

Artikel 28 Abs. 7 und 8 DS-GVO ermächtigen sowohl Kommission als auch Aufsichtsbehörden, künftig Standardvertragsklauseln für Auftragsverarbeitungsverhältnisse zu veröffentlichen. Bisher haben Kommission und/oder Aufsichtsbehörden hiervon jedoch noch keinen Gebrauch gemacht.

Auf Verbandsebene (z.B. Bitkom e.V.) wurden wie auch schon in der Vergangenheit Vertragsmuster zur Auftragsverarbeitung gemäß DS-GVO veröffentlicht, die eine Orientierung bezüglich der Umsetzung der gesetzlichen Anforderungen bieten können.

2.5. Inwieweit ist der Auftragsverarbeiter auch ggü. Betroffenen, Aufsichtsbehörden etc. verantwortlich?

Im Vergleich zur bisherigen Rechtslage erhöht die DS-GVO die Verantwortung des Auftragsverarbeiters, der nunmehr nicht mehr nur ausschließlich im Innenverhältnis ggü. dem Auftraggeber rechenschaftspflichtig ist.

So muss dieser z.B. ein eigenes Verarbeitungsverzeichnis führen (Artikel 30 Abs. 2 DS-GVO, siehe auch unten 3.3.), ein solches der Aufsichtsbehörde vorlegen (Artikel 30 Abs. 4 DS-GVO) und unterliegt dem Sanktionsregime der Artikel 82 ff. DS-GVO (siehe Kapitel 14).

Auch kann ein Auftragsverarbeiter bei Verstößen auf Schadensersatz haften (Artikel 82 Abs. 1 DS-GVO). Auftraggeber bzw. Verantwortlicher und Auftragnehmer bzw. Auftragsverarbeiter haften gegenüber Betroffenen bei Schäden, die aus einer Auftragsverarbeitung resultieren, ggf. als Gesamtschuldner (Artikel 82 Abs. 4 DS-GVO).

2.6. Cloud-Anbieter als Auftragsverarbeiter?

Gängige Cloud-Dienstleistungen – wie z.B. Software as a Service (SaaS) oder Infrastructure as a Service (IaaS) – sind regelmäßig reine technische Hilfs- und Unterstützungstätigkeiten zur Auslagerung von Datenverarbeitungsprozessen und werden somit i.d.R. als Auftragsverarbeitung gemäß Artikel 28 DS-GVO einzustufen sein.

Besonders zu beachten ist hier die regelmäßig mit der Cloud-Nutzung einhergehende Verarbeitung der auftragsgegenständlichen Daten durch gängige Cloud-Anbieter außerhalb der EU bzw. des EWR. Hier bleibt insb. relevant, dass regelmäßig zwar ein Datencenter des Cloud-Anbieters gewählt werden kann, in dem die Daten innerhalb der EU bzw. des EWR gespeichert werden, im Rahmen globaler Wartungs- und Supportkonzepte der Cloud-Anbieter jedoch oftmals auf die gespeicherten Daten von Stellen außerhalb der EU bzw. des EWR zugreifen kann. Grundsätzlich gilt wie bisher, dass die verantwortliche Stelle ein angemessenes Datenschutzniveau (siehe hierzu auch Frage 12.9.) entlang der gesamten Kette aller in die Auftragsverarbeitung einbezogenen Parteien sicherzustellen hat. Zum rechtskonformen Einsatz von Cloud-Anbietern hat auch der Düsseldorfer Kreis eine Stellungnahme veröffentlicht (https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf; hier sind ebenfalls § 203 StGB und § 50a WPO zu beachten).

3. Datenschutzmanagement (DSM)

3.1. Was sind die zwingenden Bestandteile eines DSM?

Ein DSM ist ein Corporate-Governance-Instrument i.S. eines IKS. Es besteht aus einem Managementsystem, um systematisch die spezifischen Ziele des Datenschutzes zu erreichen. Optional kann dies im Wege eines integrierten Managementsystems (IMS) erreicht werden. Kernprozesse der Ablauforganisation des DSM sind z.B.:

- Datenschutzkonforme Datenverarbeitung (weiterer Inhalt dieses Kapitels)
- Sicherstellung der Betroffenenrechte (siehe Kapitel 4 – Informations- und Auskunftspflichten)
- Handhabung von Datenschutzverletzungen (siehe Kapitel 12 – Breach Notification), aufbauend auf einem IMS.

3.2. Findet sich das Prinzip der Datensparsamkeit auch in der DS-GVO wieder?

Das bereits im BDSG a.F. fest verankerte Prinzip der „Datensparsamkeit“ (s.u. Frage 9.2.) bleibt auch nach der DS-GVO eines der zentralen Prinzipien des Datenschutzes – auch wenn es nunmehr unter dem neuen Titel der „Datenminimierung“ Eingang in die DS-GVO (Artikel 5 Abs. 1 Buchst. c) gefunden hat. Mit Ausnahme der Betitelung hat sich jedoch zum bereits bekannten Prinzip der „Datensparsamkeit“ nichts geändert. Somit ist auch nach der DS-GVO die Verarbeitung von personenbezogenen Daten auf das für den Zweck der Datenverarbeitung notwendige Maß zu beschränken. Dabei kann ein solcher Zweck u.a. auch in der Erfüllung gesetzlicher Aufbewahrungspflichten liegen, wonach die betreffenden personenbezogenen Daten so lange gespeichert werden müssen, wie es

die (verschiedenen) gesetzlichen Aufbewahrungsfristen vorsehen. Ist die gesetzliche Aufbewahrungsfrist hingegen abgelaufen und besteht darüber hinaus kein legitimer Zweck, die Daten weiterhin zu speichern, sind die Daten nach dem Fristablauf zwingend zu löschen.

Die Herangehensweise und Ausgestaltung des Löschens unterliegt der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO. Zum Beispiel gibt DIN 66398 (Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogenen Daten) Hinweise zu Löschkonzepten.

3.3. Worin besteht der Unterschied zwischen dem bisherigen Verfahrensverzeichnis und dem Verzeichnis von Verarbeitungstätigkeiten?

Wenn man die Regelungen des Artikels 30 DS-GVO mit den Festlegungen zum bisherigen Verfahrensverzeichnis im BDSG a.F. (§§ 4g Abs. 2, 4e BDSG) vergleicht, kann man feststellen, dass sich die jeweiligen Anforderungen inhaltlich stark ähneln. War jedoch bislang ein Verstoß gegen die Pflicht zur Führung eines Verfahrensverzeichnisses nicht direkt bußgeldbewehrt, ändert sich dies mit Einführung der DS-GVO (Artikel 83 Abs. 4 Buchst. a DS-GVO).

Weiterhin ist nach der DS-GVO nunmehr auch der Auftragsverarbeiter verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten (VVT) zu führen (vgl. Artikel 30 Abs. 2 DS-GVO). Dahingegen sieht die DS-GVO auch teilweise Befreiungen von der Pflicht zur Führung des VVT (Artikel 30 Abs. 5 DS-GVO) für Unternehmen oder Einrichtungen vor, die weniger als 250 Mitarbeiter beschäftigen. Allerdings greift eine solche Befreiung nur solange, wie die von diesen Unternehmen vorgenommene Verarbeitung nicht mit einem Risiko für die Betroffenen verbunden ist, die Verarbeitung nur gelegentlich erfolgt oder keine besonderen Kategorien personenbezogener Daten (Artikel 9 DS-GVO) verarbeitet werden.

Ein weiterer Unterschied besteht in der Zugänglichkeit der Verzeichnisse. Während das Verfahrensverzeichnis nach dem BDSG in weiten Teilen noch auf Antrag jedermann zugänglich gemacht werden musste, besteht diese Pflicht bei den Verzeichnissen nach der DS-GVO nur noch gegenüber den Aufsichtsbehörden. Zeitgleich entfallen sind die (noch) im BDSG enthaltenen etwaigen Meldepflichten (§§ 4d, 4e BDSG).

Schließlich werden in den Verzeichnissen nach der DS-GVO nunmehr auch Angaben im Hinblick auf eine Übermittlung personenbezogener Daten in ein Drittland verlangt. Hierzu ist insb. zu dokumentieren, durch welche Maßnahmen ein angemessenes Datenschutzniveau in dem betreffenden Land gewährleistet wird.

3.4. Was ist die Datenschutz-Folgenabschätzung und wann ist sie durchzuführen?

Die Datenschutz-Folgenabschätzung (Artikel 35 DS-GVO) ist ein zu dokumentierender und damit nachprüfbarer Risikomanagement-Prozess, der aus dem Blickwinkel der Betroffenen heraus die vorhandenen Risiken für die Freiheiten und Rechte der Betroffenen analysiert. Der Prozess ist zwingend durchzuführen z.B.

a) bei Einführung/Verwendung neuer Technologien (wie bspw. Fingerabdrucksensoren oder einer Technologie zur Gesichtserkennung),

b) wenn die Art, der Umfang, die Umstände oder die Zwecke der Verarbeitung ein hohes Risiko für die Betroffenen darstellen,

c) bei der Verarbeitung besonders schützenswerter Kategorien von personenbezogenen Daten (wie bspw. Daten zur rassischen und ethnischen Herkunft, politische Meinungen, religiöse Überzeugungen, Informationen über die Gewerkschaftszugehörigkeit, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben einer natürlichen Person, vgl. Artikel 9 Abs. 1 DS-GVO).

Die Datenschutz-Folgenabschätzung ist damit vergleichbar mit der bereits aus dem BDSG bekannten Vorabkontrolle, wonach schon bislang bestimmte automatisierte Verfahren vor ihrer erstmaligen Verwendung vom Datenschutzbeauftragten dahingehend zu überprüfen sind, ob die datenschutzrechtlichen Vorgaben eingehalten werden und die technisch-organisatorischen Maßnahmen ausreichen, um dem – in diesem Fall – besonderen Anspruch an die Datensicherheit zu genügen. Auch die Datenschutz-Folgenabschätzung erfordert neben der Risikoeinschätzung eine Festlegung der zur Bewältigung der jeweiligen Risiken geeigneten Abhilfemaßnahmen, insb. technisch-organisatorischer Art. Geht aus der Datenschutz-Folgenabschätzung des Datenschutzbeauftragten hervor, dass die Risiken der Betroffenen nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten einzudämmen sind, sollte die Datenschutzaufsichtsbehörde konsultiert werden (vgl. Artikel 36 DS-GVO), sofern an dem Gedanken, das betreffende Verfahren einzusetzen, festgehalten wird.

3.5. Was ist das Datenschutzaudit bzw. die Datenschutzzertifizierung und wann sind sie durchzuführen?

Für den Nachweis, dass die Anforderungen der DS-GVO eingehalten werden, müssen geeignete Kontrollmechanismen angewandt werden. Diese Pflicht trifft sowohl den WP für Verarbeitungen, die intern bei ihm stattfinden oder vorbereitet werden, als auch (zusätzlich) den Auftragsverarbeiter. Beide (sowohl WP als auch Auftragsverarbeiter) haben in diesem Fall die Einhaltung ihrer technisch-organisatorischen Sicherheitsmaßnahmen (TOMs) nachzuweisen.

Zwei Instrumente, nämlich die Auditierung und die Zertifizierung, können ein sinnvolles Mittel für den WP und den Auftragsverarbeiter darstellen, den entsprechenden Nachweis zu erbringen.

3.6. Kann der WP als Datenschutz-Auditor fungieren?

Ja, der WP kann, neben der zuvor erwähnten eigenen Pflicht, Kontrollmechanismen zu installieren, auch als Datenschutz-Auditor bei Dritten fungieren, die keine Auftragsverarbeiter des WP sind, um dort – als unabhängige Instanz – über die Umsetzung geeigneter Kontrollmechanismen ein Audit durchzuführen.

4. Informations- und Auskunftspflichten

4.1. Welche Informationspflichten gegenüber Betroffenen gelten nach der DS-GVO?

Artikel 13 und 14 der DS-GVO sehen umfangreiche Informationspflichten des Verantwortlichen gegenüber den von der Datenverarbeitung betroffenen Personen vor. Artikel 13 und 14 DS-GVO sehen dabei weitestgehend die gleichen Informationspflichten vor, unterscheiden aber nach der Situation der Erhebung von Daten bei der betroffenen Person selbst (Artikel 13) und bei Dritten (Artikel 14).

Grundsätzlich sind (bei Artikel 13 DS-GVO zum Zeitpunkt der Erhebung) die folgenden Angaben mitzuteilen (Ausnahmen s.u. 4.2.):

- der Name und die Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf der Grundlage eines berechtigten Interesses des Verantwortlichen oder eines Dritten erfolgt, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (dies gilt in Fällen, in denen die betroffenen Daten von dem Verantwortlichen an Dritte, wie z.B. Dienstleister, weitergegeben werden)
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, einschließlich Informationen zur Angemessenheit des Datenschutzniveaus im Empfängerland
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls

dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

- das Bestehen der Betroffenenrechte (Recht auf Auskunft, Recht auf Berichtigung, Recht auf Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit)
- soweit vorhanden, Recht auf Widerruf einer Einwilligung in die Datenverarbeitung
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob eine Verpflichtung zur Angabe der Daten besteht und Folgen der Nichtangabe
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- bei Zweckänderung: Informationen über diesen anderen Zweck.

4.2. Gelten die Informationspflichten uneingeschränkt für Berufsgeheimnisträger?

Nein, sowohl die DS-GVO selbst als auch das BDSG n.F. schränken die Informationspflichten ein, soweit es sich bei den betroffenen Informationen um Berufsgeheimnisse handelt.

Die DS-GVO selbst schränkt in Artikel 14 Abs. 5 Buchst. d die Informationspflichten gegenüber den Betroffenen ein, wenn die personenbezogenen Daten nach Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und deshalb vertraulich behandelt werden müssen. In diesem Fall finden die Informationspflichten nach Artikel 14 Abs. 1 bis 4 DS-GVO keine Anwendung.

Beispiele:

Artikel 14 DS-GVO sieht grundsätzlich vor, dass ein Verantwortlicher (z.B. WP/WPG), der personenbezogene Daten von einem Dritten (z.B. vom Mandanten) erhält, die Betroffenen, d.h. die Personen, deren Daten er erhält (dies können z.B. Beschäftigte des Mandanten oder Kunden sein), hierüber informieren muss, indem er die im Katalog des Artikels 14 DS-GVO vorgesehenen Mindestinformationen an den Betroffenen mitteilt.

Diese Pflicht gilt jedoch nicht für WP oder WPG, wenn diese im Zuge eines Mandatsverhältnisses personenbezogene Daten über Dritte von einem Mandanten erhalten. Eine solche Übertragung von personenbezogenen Daten von dritten Betroffenen kann in verschiedenen Mandatssituationen vorkommen, z.B. wenn

- im Rahmen einer Prüfung personenbezogene Daten entweder des Mandanten oder eines Dritten von einem WP/einer WPG eingesehen werden müssen bzw. diese an WP/WPG übermittelt werden (hierzu können bspw. personenbezogene

Daten zu Beschäftigten des Mandanten oder personenbezogene Daten aus Kundendatenbanken des Mandanten gehören); oder wenn

- im Rahmen der Betreuung einer Unternehmenstransaktion Mitarbeiterlisten des Käufers/Verkäufers (also des Mandanten) übermittelt werden.

Darüber hinaus hat der deutsche Gesetzgeber die Öffnungsklauseln in Artikel 23 Abs. 1 Buchst. i DS-GVO genutzt und die Informationspflichten bei überwiegendem Geheimhaltungsinteresse eingeschränkt. Insb. die Regelung des § 29 Abs. 2 BDSG n.F. schränkt die datenschutzrechtliche Informationspflicht nach Artikel 13 Abs. 3 DS-GVO ein, wenn Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt werden, soweit der betroffene Dritte kein überwiegendes Interesse an der Informationserteilung hat. Diese Ausnahme betrifft die WP und WPG nur indirekt.

Beispiele:

So muss ein Mandant, der eine Beratungsdienstleistung im Rahmen einer Unternehmenstransaktion in Anspruch nimmt und in diesem Rahmen Beschäftigtenlisten an die beratenden WP/WPG übermittelt, die hiervon betroffenen Beschäftigten nicht über die Übermittlung, den/die empfangende/n WP/WPG und die Zwecke der Datenverarbeitung informieren. Auch gelten die Informations- und Hinweispflichten bspw. dann nicht uneingeschränkt, wenn Ziel einer Sonderprüfung die Aufklärung dolosen Verhaltens von Mitarbeitern ist. Für derartige Fälle schränkt § 29 Abs. 1 BDSG n.F. die Informations- und Hinweispflichten ebenfalls ein.

Die Ausnahmen in Artikel 14 Abs. 5 DS-GVO und § 29 Abs. 1 BDSG n.F. schützen die ungehinderte Kommunikation zwischen Mandant und Berufsgeheimnisträger. Der besondere Schutz des Mandatsverhältnisses wäre nach der Begründung des BDSG-n.F.-Entwurfs nicht mehr gewährleistet, wenn Berufsgeheimnisträger und Mandant in jedem Fall sämtliche durch die Datenübermittlung an einen Berufsgeheimnisträger betroffenen Personen informieren müsste.

4.3. Müssen Verletzungen des Schutzes personenbezogener Daten der Datenschutzaufsicht gemeldet werden?

Ja, grundsätzlich müssen derartige Verletzungen (Datenvorfall, Data Breach) gemeldet werden (bisher § 42a BDSG a.F.).

Artikel 33 DS-GVO sieht eine Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten vor (Meldepflicht bei Datenvorfällen), Artikel 34 DS-GVO eine entsprechende Benachrichtigung der von einem solchen Datenvorfall Betroffenen.

Eine Benachrichtigung des Betroffenen kann unter bestimmten Voraussetzungen

unterbleiben, insb. wenn der Verantwortliche geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten auf die betroffenen Daten angewandt hat, sowie wenn er nachfolgend durch geeignete Maßnahmen sicherstellt, dass das durch den Datenvorfall bestehende Risiko für den Betroffenen aller Wahrscheinlichkeit nach nicht mehr besteht (s.u. Frage 13.2.).

4.4. Gibt es Ausnahmen von den Meldepflichten nach Artikel 33, 34 DS-GVO für WP und WPG?

Ja. Auf der Grundlage der Öffnungsklausel in Artikel 23 Abs. 1 Buchst. i DS-GVO hat der deutsche Gesetzgeber die Benachrichtigungspflichten nach Artikel 34 weiter eingeschränkt. So besteht nach § 29 Abs. 1 BDSG n.F. die Pflicht zur Benachrichtigung gemäß Artikel 34 DS-GVO nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insb. wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Anderes gilt nur, wenn die Interessen der betroffenen Person, insb. unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

Während Artikel 34 DS-GVO selbst allgemeine Fälle regelt, in denen die Benachrichtigungspflicht des Verantwortlichen nach Artikel 34 nicht besteht, sieht § 29 Abs. 1 Satz 3 BDSG n.F. spezielle Ausnahmen für die Meldung von solchen Informationen vor, die einem besonderen Geheimnisschutz unterliegen.

Hierdurch erfasst werden zum einen Informationen, die nach einer Rechtsvorschrift geheim gehalten werden müssen. Hierzu gehören die Regelungen zu den berufsrechtlichen Verschwiegenheitspflichten in den einschlägigen berufsrechtlichen Gesetzen und Satzungen. Zum anderen sind auch Informationen erfasst, die ihrem Wesen nach, insb. wegen der überwiegenden Interessen eines Dritten, geheim gehalten werden müssen.

Eine Ausnahme von der Befreiung von der Meldepflicht besteht jedoch dann, wenn der betroffenen Person bspw. durch den Datenvorfall Schäden drohen, die ihr Informationsinteresse gegenüber dem Geheimhaltungsinteresse überwiegen lassen.

4.5. Dürfen Informationen aus Meldungen von Datenvorfällen in Straf- oder Ordnungswidrigkeitenverfahren verwendet werden?

Bezüglich der Melde- bzw. Benachrichtigungspflichten nach Artikel 33 und Artikel 34 DS-GVO sehen § 42 bzw. § 43 BDSG n.F. jeweils vor, dass eine entsprechende Meldung oder Benachrichtigung in einem Strafverfahren (§ 42 BDSG n.F.) oder einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen die meldepflichtige oder benachrichtigende Person oder einen ihrer in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der Meldepflichtigen oder Benachrichtigenden verwendet werden dürfen.

4.6. Informationspflicht gegenüber Mandanten

S.u. Frage 13.5.

5. Aufsichtsbehörde (Artikel 51 ff.)

5.1. Wer ist Aufsichtsbehörde und welche Arten von Befugnissen haben die Aufsichtsbehörden nach der DS-GVO?

Aufsichtsbehörde i.S. der DS-GVO ist diejenige Behörde, welche der Mitgliedstaat als unabhängige staatliche Stelle einrichtet (Artikel 4 Nr. 21 DS-GVO). In Deutschland sind und bleiben dies die Bundes- und Landesdatenschutzbeauftragten (vgl. § 8 BDSG und die Landesdatenschutzgesetze).

Die bisherigen Befugnisse der Aufsichtsbehörden nach dem BDSG a.F. werden durch die DS-GVO erweitert. So listet alleine der Artikel 58 DS-GVO insgesamt 22 Befugnisse auf, die sich der Art nach in Untersuchungsbefugnisse (Abs. 1), Abhilfebefugnisse (Abs. 2) sowie Genehmigungs- und beratende Befugnisse (Abs. 3) einteilen lassen. Daneben, d.h. zusätzlich oder anstelle der vorgenannten Maßnahmen, können Verstöße gegen die DS-GVO von den Aufsichtsbehörden mit Geldbußen (Artikel 83 DS-GVO) geahndet und die angeordneten Maßnahmen mit Zwangsmitteln durchgesetzt werden. Soweit es in der Öffnungsklausel des Artikels 58 Abs. 6 DS-GVO dem nationalen Gesetzgeber ermöglicht wurde, den Aufsichtsbehörden zusätzliche Befugnisse einzuräumen, ist davon bislang in der Neufassung des BDSG kein Gebrauch gemacht worden.

Hinsichtlich der Daten, die der berufsrechtlichen Verschwiegenheit unterliegen, ergeben sich aufgrund des Artikels 90 DS-GVO i.V.m. § 29 Abs. 3 Satz 1 BDSG n.F. Einschränkungen bestimmter Untersuchungsbefugnisse der Aufsichtsbehörden (s.u. Frage 5.4.).

5.2. Haben die Aufsichtsbehörden das Recht, Geschäftsräume des WP zu betreten und sich Zugang zu den Daten und Informationen zu verschaffen, die personenbezogene Daten enthalten?

Befugnisse der Aufsichtsbehörden, sich Zugang zu personenbezogenen Daten zu verschaffen, sind in den Untersuchungsbefugnissen nach Artikel 58 Abs. 1 Buchst. a, e und f DS-GVO geregelt. Bei der Ausübung ihrer Befugnisse hat die Aufsichtsbehörde allerdings den Grundsatz der Verhältnismäßigkeit zu beachten. Zudem bestehen nach Artikel 90 DS-GVO i.V.m. § 29 Abs. 3 Satz 1 BDSG n.F. Einschränkungen des Zugangs hinsichtlich solcher Daten, die der berufsrechtlichen Verschwiegenheit unterliegen (s. hierzu Fragen 5.4. und 5.7.), sodass insoweit zwischen diesen und sonstigen personenbezogenen Daten zu differenzieren ist.

5.2.1. Befugnis der Aufsichtsbehörde nach Artikel 58 Abs. 1 Buchst. a DS-GVO

Die Aufsichtsbehörde kann nach Artikel 58 Abs. 1 Buchst. a DS-GVO die Bereitstellung von Informationen verlangen. Dieser Auskunftsanspruch der Aufsichtsbehörde erstreckt sich auf alle Informationen und Angaben, die die Behörde zur Erfüllung ihrer Aufgaben benötigt. Die vorgenannte Öffnungsklausel des Artikels 90 DS-GVO erwähnt zwar ausdrücklich nur die Befugnisse der Aufsichtsbehörden nach Artikel 58 Abs. 1 Buchst. e und f DS-GVO (Erhalt des Zugangs zu personenbezogenen Daten und zu Geschäftsräumen und Datenverarbeitungsanlagen) als Befugnisse, die der nationale Gesetzgeber zugunsten des Schutzes von Berufsgeheimnissen ausschließen darf (s. dazu nachstehend in Ziff. 5.2.2 und Ziff. 5.2.3). Diese Ausschlussmöglichkeit könnte jedoch leerlaufen, wenn die eingangs genannte Bereitstellungsverpflichtung auch Berufsgeheimnisse umfassen würde. Es spricht daher viel dafür, dass die Bereitstellungsverpflichtung entsprechend begrenzt ist, wenn der nationale Gesetzgeber von der Öffnungsklausel des Artikels 90 DS-GVO Gebrauch gemacht hat (wie in der Neufassung des BDSG geschehen, s. nachstehend Ziff. 5.2.2 und 5.2.3).

5.2.2. Befugnis der Aufsichtsbehörde nach Artikel 58 Abs. 1 Buchst. e DS-GVO

Artikel 58 Abs. 1 Buchst. e DS-GVO gestattet der Aufsichtsbehörde, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen zu erhalten, die zur Erfüllung ihrer Aufgaben notwendig sind. Hinsichtlich solcher personenbezogenen Daten, die der WP als Verantwortlicher oder Auftragsverarbeiter bei seiner beruflichen Tätigkeit erlangt oder erhoben hat, entfällt dem WP gegenüber aber die Zugangsbefugnis nach § 29 Abs. 3 BDSG n.F.

5.2.3. Befugnis der Aufsichtsbehörde nach Artikel 58 Abs. 1 Buchst. f DS-GVO

Artikel 58 Abs. 1 Buchst. f DS-GVO regelt ausdrücklich ein Zugangsrecht der Aufsichtsbehörden zu den Geschäftsräumen und Datenverarbeitungsanlagen (sog. vor-Ort-Prüfung) des Verantwortlichen und des Auftragsverarbeiters, was mithin auch alle zur Datenverarbeitung eingesetzten Geräte umfasst.

Durch diese der Aufsichtsbehörde eingeräumten Befugnisse wird der Adressat verpflichtet, die genannten Maßnahmen zu dulden und diese in begrenztem Umfang zu unterstützen. Der Verpflichtete hat der Aufsichtsbehörde daher den Zugang zu Räumen, Anlagen und Geräten zu verschaffen. Bei automatisierten Datenverarbeitungen ist er zugleich verpflichtet, das jeweilige Verfahren zu starten, Anwendungen auszuführen und gespeicherte Daten einschließlich Protokolldaten sichtbar zu machen.

Hinsichtlich der personenbezogenen Daten, die der WP als Verantwortlicher oder Auftragsverarbeiter bei seiner beruflichen Tätigkeit erlangt oder erhoben hat, entfällt dem WP gegenüber aber wiederum die Zugangsbefugnis nach § 29 Abs. 3 BDSG n.F.

5.3. Was ist beim Betreten der Praxisräume des WP zu beachten?

Wie die Differenzierung zwischen den mandatsbezogenen und nicht-mandatsbezogenen Daten im Hinblick auf das Zugangsrecht zu den Geschäftsräumen und Datenverarbeitungsanlagen eines WP umgesetzt werden kann, lässt sich angesichts der Vielfalt denkbarer tatsächlicher Sachverhalte nicht abschließend beantworten. Vorstellbar ist folgende Differenzierung:

Das ausschließliche Betreten von Empfangsräumen oder Räumen, in denen sich lediglich betriebs- und nicht-mandatsbezogene Daten des WP befinden, wird man als zulässig ansehen müssen. Unzulässig dürfte wohl das Betreten von Räumen sein, die der Mandatsbearbeitung dienen, sofern sich dort mandatsbezogene Unterlagen befinden und die Möglichkeit der Kenntnisnahme durch die Aufsichtsbehörde besteht (zulässig lediglich, wenn die Mandantenakten komplett in Schränken weggeschlossen sind oder die Kenntnisnahmemöglichkeit von mandatsbezogenen Daten der Aufsichtsbehörden durch geeignete Maßnahmen ausgeschlossen werden kann; anders wiederum bei gerade im Betretenszeitpunkt physisch oder am PC bearbeiteten Akten). Dient das Betreten ausschließlich der Verschaffung des Zugangs zu betriebsbezogenen, d.h. nicht-mandatsbezogenen personenbezogenen Daten, ist der Zugang auf diese Räumlichkeiten beschränkt, „Umwege“ bzw. ein „Hindurchgehen“ durch der Mandatsbearbeitung dienende Räumlichkeiten sind regelmäßig als nicht gestattet anzusehen und vom WP zu untersagen.

5.4. Welche Einschränkungen der Untersuchungsbefugnisse ergeben sich für WP aufgrund des Artikels 90 DS-GVO i.V.m. § 29 Abs. 3 Satz 1 BDSG n.F.?

Der deutsche Gesetzgeber hat im Rahmen der Neuregelung des Bundesdatenschutzgesetzes in § 29 Abs. 3 Satz 1 BDSG n.F. die Befugnisse der Aufsichtsbehörde insoweit eingeschränkt, als ihr die Untersuchungsbefugnisse nach Artikel 58 Abs. 1 Buchst. e und f DS-GVO nicht zustehen, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflicht des WP führen würde. Die Begründung des Gesetzes weist zutreffend darauf hin, dass es ohne diese Regelung zu einer Kollision der Pflichten des Geheimnisträgers gekommen wäre, was gerade bei den freien Berufen zu einer Unsicherheit im Mandatsverhältnis darüber geführt hätte, inwieweit die berufsrechtliche Schweigepflicht die Vertraulichkeit noch schützt. Die Untersuchungsbefugnisse der Aufsichtsbehörden bestehen danach dem WP bzw. der WPG gegenüber nicht, soweit die geschützten Daten unter der bindenden Pflicht zur Geheimhaltung erlangt oder erhoben wurden und die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Person führen würde.

Rein betriebsbezogene personenbezogene Daten des WP bzw. der WPG ohne Mandatsbezug unterliegen dagegen den vollen Zugriffsrechten der Aufsichtsbehörde.

Dasselbe gilt für personenbezogene Daten mit Mandatsbezug, wenn der Mandant eingewilligt hat und sich die konkrete Ausübung des Zugriffsrechts allein auf diese Daten beschränken lässt (vgl. Ziff. 1.16 a.E. und Ziff. 5.3).

Hat der WP Zweifel an der Rechtmäßigkeit einer entsprechenden Anordnung der Aufsichtsbehörden, kann er – wie bisher – Rechtsschutz im verwaltungsgerichtlichen Verfahren suchen.

5.5. Gibt es neben Artikel 90 DS-GVO i.V.m. § 29 Abs. 3 Satz 1 BDSG n.F. weitere, auch für den WP relevante Einschränkungen der Untersuchungsbefugnisse der Aufsichtsbehörden?

Neben den vorstehend beschriebenen Beschränkungen der Untersuchungsbefugnisse aufgrund des Artikels 90 DS-GVO i.V.m. § 29 Abs. 3 Satz 1 BDSG n.F. ist zu berücksichtigen, dass nach deutschem Strafverfahrensrecht der Nemo-tenetur-Grundsatz gilt, wonach sich niemand wegen einer Straftat oder Ordnungswidrigkeit selbst belasten muss (§ 136 Abs. 1 Satz 2, § 55 Abs. 1 StPO). Gleiches wird für Personen angenommen, die zur Verweigerung des Zeugnisses berechtigt sind.

Dieser Grundsatz gilt über den Verweis auf das nationale Verfahrensrecht in Artikel 58 Abs. 4 DS-GVO auch für die Untersuchungsbefugnisse nach Artikel 58 Abs. 1 und ist auch in § 40 Abs. 4 Satz 2 BDSG n.F. zusätzlich noch einmal allgemein für das Auskunftsrecht enthalten. Voraussetzung ist, dass sich das Auskunftsverlangen auf ein Verhalten bezieht, dass selbst den Tatbestand einer Straftat oder Ordnungswidrigkeit erfüllen kann. Ob auch der Fall erfasst ist (mithin ein Auskunftsverweigerungsrecht besteht), wenn die Beantwortung des Ersuchens selbst eine Straftat oder Ordnungswidrigkeit (etwa wegen Verstoßes gegen die Verschwiegenheitspflicht nach § 203 StGB) darstellen könnte, ist streitig.

5.6. Wer ist zur Auskunft gegenüber den Aufsichtsbehörden verpflichtet, wenn diese von den ihnen eingeräumten Befugnissen Gebrauch machen?

Wenn Aufsichtsbehörden von den ihnen eingeräumten Befugnissen, insb. den Untersuchungsbefugnissen nach Artikel 58 Abs. 1 Buchst. a, e und f DS-GVO Gebrauch machen und Auskunft verlangen, sind der Verantwortliche oder Auftragsverarbeiter sowie deren Vertreter auskunftspflichtig. Bei juristischen Personen sind dies deren Organe oder die von ihnen bevollmächtigten Personen.

5.7. Was passiert mit den Daten, von denen die Behörde ohne Befugnis Kenntnis erhält?

§ 29 Abs. 3 Satz 2 BDSG n.F. sieht vor, dass für eine Aufsichtsbehörde, die im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht i.S. des Satzes

1 unterliegen, erlangt hat, die Geheimhaltungspflicht ebenfalls gilt. Die Geheimhaltungspflicht wird somit auf die Aufsichtsbehörde gewissermaßen verlängert. Dies wird man mithin dahingehend auslegen müssen, dass der Behörde dann eine Offenbarung der Daten an Dritte ebenso wenig bzw. nur in dem Umfang und nur unter den Voraussetzungen möglich sein wird wie dem WP selbst, sodass die diesen insoweit treffenden Regelungen entsprechend zur Anwendung kommen.

Die durch das IDW angeregte Ergänzung des § 29 Abs. 3 Satz 2 BDSG-E um eine Löschungspflicht der Aufsichtsbehörde hat keinen Eingang in das neue Gesetz gefunden.

6. Datenschutzbeauftragter

6.1. Wer benötigt einen Datenschutzbeauftragten?

Schon unter bisher geltendem Recht (§ 4f Abs. 1 BDSG a.F.) mussten öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz schriftlich bestellen. Diese Anforderung wird nunmehr von der DS-GVO europaweit für Unternehmen eingeführt, deren Kerntätigkeit die Verarbeitung von personenbezogenen Daten mit umfangreicher oder systematischer Überwachung von Personen oder mit umfangreicher Verarbeitung besonderer Kategorien von Daten ist (Artikel 37 Abs. 1 Buchst. b und c).

Ergänzend zur DS-GVO gilt § 38 BDSG n.F., der grundsätzlich die bisherige Regelung des BDSG-alt in Deutschland fortführt. Hiernach benennen der Verantwortliche und der Auftragsverarbeiter einen Datenschutzbeauftragten, soweit sie i.d.R. mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Es sind hierbei weiterhin alle (Sach-)Bearbeiter einer verantwortlichen Stelle zusammenzuzählen, die personenbezogene Daten verarbeiten (also z.B. Mitarbeiter aus Personalabteilung, Finance, Marketing etc.).

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO 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 einen Datenschutzbeauftragten zu benennen.

6.2. Welche (Kern-)Pflichten hat der Datenschutzbeauftragte?

Der Datenschutzbeauftragte hat gemäß Artikel 39 DS-GVO folgende Aufgaben:

- Unterrichtung und Beratung zu Pflichten gemäß der DS-GVO, BDSG n.F. sowie sonstigen einschlägigen Datenschutzvorschriften

- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften sowie der Strategien für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der beteiligten Mitarbeiter und entsprechender Überprüfungen
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DS-GVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DS-GVO.

6.3. Wer darf Datenschutzbeauftragter werden?

Gemäß Artikel 37 Abs. 6 DS-GVO wird der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insb. 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.

Der Datenschutzbeauftragte sollte folgende Fachkenntnisse besitzen:

- Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle
- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen der DS-GVO und des BDSG, auch technischer und organisatorischer Art
- umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen etc.)
- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle)
- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z.B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

6.4. Welche Stellung hat der Datenschutzbeauftragte?

Die Stellung des Datenschutzbeauftragten ist in Artikel 38 DS-GVO festgeschrieben. Danach muss der Datenschutzbeauftragte frühzeitig in alle Datenschutzfragen eingebunden werden. Er muss bei der Erfüllung seiner Aufgaben mit den erforderlichen Ressourcen, einem Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie zur Erhaltung seines Fachwissens unterstützt werden. Der Verantwortliche muss die Weisungsfreiheit des Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben sicherstellen, z.B. durch eine vertragliche Zusicherung.

Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen. Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben zur Wahrung der Vertraulichkeit verpflichtet. Der Verantwortliche muss zudem sicherstellen, dass bei einem nebenamtlichen Datenschutzbeauftragten keine Interessenkonflikte auftreten.

6.5. Wer darf nicht Datenschutzbeauftragter werden?

In der Praxis hat sich eine große Vielfalt von gleichzeitig mit dem Amt des (Teilzeit-) Datenschutzbeauftragten ausgeübten Tätigkeiten in Unternehmen ergeben. Zum Teil stellen sie eine sinnvolle Ergänzung dar, wenn juristische oder technische Fähigkeiten im Amt genutzt werden können. Eventuelle Interessenkonflikte können allerdings als mangelnde Zuverlässigkeit bewertet werden. Diese wird immer dann anzunehmen sein, wenn der Teilzeit-Datenschutzbeauftragte sich aufgrund seiner weiteren Aufgaben selbst kontrollieren müsste. Dies ist nach der herrschenden Meinung zum BDSG a.F. überwiegend bei Leitern der Abteilungen IT, Personal, Recht, Marketing/Vertrieb und Revision zu bejahen.

Aufgrund des stärkeren Interesses am wirtschaftlichen Erfolg der WPG ist die Bestellung eines Anteilseigners (Equity Partners) als Datenschutzbeauftragten eine entsprechend zu begründende Einzelfallentscheidung.

6.6. Wer darf externer Datenschutzbeauftragter sein?

Die Bestellung eines externen Datenschutzbeauftragten ist zulässig. Gemäß Artikel37 Abs. 6 DS-GVO kann der Datenschutzbeauftragte Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

Soll ein externer Datenschutzbeauftragter eingesetzt werden, muss dessen Qualifikation (s.o. Frage 6.3.) umfassend vorab geprüft werden, da die Leitung der verantwortlichen Stelle diesen oftmals vorher nicht kennt. Im Rahmen dieser Prüfung sollten auch

mögliche Interessenkonflikte ausgeschlossen werden, wenn der Anbieter z.B. schon bei einem Konkurrenten bestellt wurde oder aber der Anbieter bereits IT-Dienstleistungen für die verantwortliche Stelle erbringt.

Sofern eine juristische Person bestellt werden soll, so sollte im Vertrag gleichwohl ein dortiger zentraler Mitarbeiter benannt werden, der die Aufgaben des Datenschutzbeauftragten wahrnimmt. Die verantwortliche Stelle sollte einen Genehmigungsvorbehalt vereinbaren, sofern dieser Mitarbeiter durch die juristische Person ausgetauscht werden soll.

Der Vertrag mit dem externen Datenschutzbeauftragten muss so ausgestaltet sein, dass die Aufgaben des Datenschutzbeauftragten tatsächlich auch unabhängig wahrgenommen werden können. Hierzu bedarf es Regelungen zu angemessenen Vertragslaufzeiten, Kündigungsrechten, Zahlungsmodalitäten, Haftungsbegrenzungen und Dokumentationspflichten.

6.7. Darf der WP externer Datenschutzbeauftragter sein?

Bei seinen Abschlussprüfungsmandanten darf der WP aufgrund von Unabhängigkeitsanforderungen nicht externer Datenschutzbeauftragter sein.[1]

Bei Nicht-Abschlussprüfungsmandanten darf der WP beauftragt werden.[2]

6.8. Muss der interne Datenschutzbeauftragte einer WPG ein Berufsangehöriger sein?

Nein, es reichen entsprechende datenschutzrechtliche Kenntnisse sowie ein Verständnis der berufsrechtlichen Besonderheiten.

6.9. Müssen die Kontaktdaten des Datenschutzbeauftragten veröffentlicht werden?

Ja, Artikel 37 Abs. 7 DS-GVO verlangt vom Verantwortlichen und vom Auftragsverarbeiter, dass die Kontaktdaten des Datenschutzbeauftragten veröffentlicht werden. Dies kann z.B. auf der Website des WP oder der WPG erfolgen. Zudem müssen die Kontaktdaten der zuständigen Aufsichtsbehörde mitgeteilt werden.

7. Erlaubnistatbestände

Wie bereits aus dem BDSG a.F. bekannt, normiert auch die DS-GVO als allgemeinen Grundsatz ein Verbot mit Erlaubnisvorbehalt (Artikel 6 DS-GVO). Dieses Verbot besteht

[1] Vgl. auch IDW, WPH Edition, Kap. A Tz. 113.
[2] Vgl. auch IDW, WPH Edition, Kap. A Tz. 79.

allerdings nur solange, wie keine Einwilligung des Betroffenen in eine Verarbeitung seiner Daten vorliegt, vgl. Artikel 6 Nr. 1 Buchst. a DS-GVO (siehe Kapitel 8), oder ein gesetzlicher Ausnahmetatbestand eine Verarbeitung legitimiert, vgl. Artikel 6 Nr. 1 Buchst. b bis f DS-GVO.

8. Einwilligung (Artikel 7)

8.1. Wann ist die datenschutzrechtliche Einwilligung nach der DS-GVO für den WP relevant?

Nach der DS-GVO wie nach dem BDSG a.F. (siehe Kapitel 7) stellt die Einwilligung einen Erlaubnistatbestand für eine Datenverarbeitung personenbezogener Daten dar (Artikel 6 Nr. 1 Buchst. a DS-GVO). Für den WP wird die datenschutzrechtliche Einwilligung als Erlaubnistatbestand allerdings nur dann relevant, wenn die Datenverarbeitung nicht schon aufgrund einer gesetzlichen Rechtsgrundlage (z.B. Artikel 6 Abs. 1 Buchst. b bis f DS-GVO, insb. aufgrund eines Vertrags über Wirtschaftsprüfungsleistungen oder eines berechtigten Interesses) legitimiert ist. Generell gilt es bei einer auf eine Einwilligung gestützten Verarbeitung zu berücksichtigen, dass eine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann und danach eine weitere Verarbeitung der betreffenden Daten nicht mehr legitim und folglich verboten wäre.

8.2. Was sind die Bedingungen für eine wirksame Einwilligung?

In Artikel 7 DS-GVO werden die „Bedingungen für die Einwilligung“ aufgeführt. Dies sind die Nachweisbarkeit der Einwilligung (Nr. 1), die Hervorhebung, Verständlichkeit und Zugänglichkeit bei mehreren Sachverhalten (Nr. 2), die Widerrufbarkeit der Einwilligung und die Belehrung hierüber (Nr. 3) sowie die Freiwilligkeit (Nr. 4).

8.3. Welcher Form bedarf die Einwilligung?

Die DS-GVO macht hinsichtlich der Form einer Einwilligung keine konkreten Vorgaben. Notwendig ist eine „unmissverständlich abgegebene Willensbekundung“ und damit eine aktive Handlung.

Daher kann der WP die Einwilligung schriftlich, mündlich, elektronisch oder per E-Mail einholen. Zu beachten ist dabei, dass die Einwilligung stets vor Beginn der Datenverarbeitung eingeholt werden muss.

Da Artikel 7 Nr. 1 DS-GVO die Nachweisbarkeit der Einwilligung vom Verantwortlichen verlangt, trägt der WP als Verantwortlicher die Beweislast für das Vorliegen der Einwilligung. Daher sollte der WP die Einwilligung in einem speicherungsfähigen Format, z.B. Schrift- oder Textform, einholen. Zudem sollte der Erhalt dokumentiert werden.

An die elektronische Einwilligung werden dabei keine anderen Anforderungen gestellt als an die nicht-elektronische, vorbehaltlich Erwägungsgrund 32 Satz 6 DS-GVO, der für die Einwilligung auf elektronischem Weg fordert, dass die Aufforderung zur Abgabe der Einwilligung „in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird," erfolgen muss.

Der deutsche Gesetzgeber fordert derzeit in § 13 Abs. 2 Telemediengesetz (TMG) bei elektronischen Einwilligungen bei Telemedien, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

§ 13 Abs. 2 TMG wird aufgrund des Anwendungsvorrangs der DS-GVO ab dem 25.05.2018 keine Anwendung mehr finden, da die DS-GVO den Schutz natürlicher Personen technologieneutral (vgl. Erwägungsgrund 15 DS-GVO) und – mangels Öffnungsklausel – abschließend regelt.

Aufgrund des Nachweisbarkeitserfordernisses (Artikel 7 Nr. 1 DS-GVO) ist dem WP dennoch zu raten, die Einwilligung zu protokollieren. Zu beachten ist zudem, dass bereits vom WP vorab angekreuzte Kästchen nach Erwägungsgrund 32 unzureichend sind.

Da mit der DS-GVO auch die ePrivacy-Verordnung in Kraft treten soll[3], ist diese im Fall von elektronischen Einwilligungen vom WP zu beachten. Der derzeitige Entwurf für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG sieht für die elektronische Einwilligung bspw. in Artikel 9 Abs. 3 vor, dass Endnutzer in regelmäßigen Abständen von sechs Monaten an die Möglichkeit des jederzeitigen Widerrufs der Einwilligung zu erinnern sind, solange die Verarbeitung andauert.

8.4. Was ist bei Einholung einer schriftlichen Einwilligung zu beachten?

Möchte der WP die Einwilligung (z.B. für eine Marketingaktivität, einen Newsletter) schriftlich im Rahmen eines Dokuments, das noch andere Sachverhalte betrifft, bspw. im Rahmen eines Vertrags über Wirtschaftsprüfungsleistungen, auch durch AGB-Regelungen, einholen, so hat er neben den §§ 305 ff. BGB Artikel 7 Nr. 2 DS-GVO zu beachten.

Danach muss der WP den Abschnitt, mit dem um die Einwilligung gebeten wird, „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" so gestalten, dass dieser „von den anderen Sachverhalten klar zu unterscheiden ist". Dies kann durch eine eindeutige Überschrift, z.B. „datenschutzrechtliche Einwilligung", sowie

[3] Verordnungsvorschlag KOM(2017)10 vom 10.01.2017; EU-Gesetzgebungsverfahren noch nicht abgeschlossen.

eine deutliche Hervorhebung des Texts, z.B. durch Fettdruck, erfolgen. Zudem sollte der WP Alltagssprache und kein unnötiges Fachvokabular verwenden.

Zudem muss der WP darauf achten, dass für den Betroffenen keinerlei Zwang i.S. des Artikels 7 Abs. 4 DS-GVO (sog. Koppelungsverbot) für die Erteilung der Einwilligung besteht. Wie dies im Rahmen eines Vertrags gewährleistet werden kann, ist aufgrund des unklaren Umfangs des Koppelungsverbots fraglich. Daher sollte der WP im Zweifel die Einwilligung nicht im Rahmen eines Vertrags, sondern davon separat einholen (s. dazu auch Frage 8.8.).

8.5. Wann ist eine Einwilligung freiwillig abgegeben?

Der Betroffene erteilt die Einwilligung freiwillig, wenn er diese ohne Druck oder Zwang abgibt und eine echte oder freie Wahl hat.

Hierbei hat der WP die Pflicht, im Einwilligungstext den Betroffenen über die Freiwilligkeit und die Möglichkeit eines jederzeitigen Widerrufs für die Zukunft zu informieren, sowie darüber, dass der Betroffene durch die Verweigerung oder den Widerruf keine Nachteile zu befürchten hat. Der Betroffene ist zudem auf die Wirkung einer Verweigerung der Einwilligung hinzuweisen, wenn es den Umständen nach erforderlich ist oder der Betroffene dies verlangt (§ 51 Abs. 4 Satz 3 BDSG n.F.).

8.6. Wie bestimmt muss die Einwilligung sein? Kann eine Blanko-Einwilligung eingeholt werden?

Die Einwilligung muss sich auf einen oder mehrere bestimmte Zwecke (Artikel 6 Abs. 1 Buchst. a DS-GVO) sowie auf einen bestimmten Fall der Verarbeitung von Daten beziehen (Artikel 4 Nr. 11 DS-GVO). Daher ist auch unter der DS-GVO eine Einholung von Blanko-Einwilligungen nicht zulässig und somit unwirksam.

8.7. Was gilt für die Einwilligung von Arbeitnehmern/Beschäftigten?

Auch nach dem 25.05.2018 können personenbezogene Daten von Arbeitnehmern im Beschäftigungsverhältnis für alle Datenverarbeitungszwecke verarbeitet werden, die der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses dienen oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist (§ 26 Abs. 1 BDSG n.F.).

Möchte der WP personenbezogene Daten seiner Beschäftigten für andere Zwecke verwenden, wie bspw. die Veröffentlichung von Bildern seiner Beschäftigten im Intranet oder Anfertigung einer Geburtstagsliste seiner Beschäftigten, benötigt er die Einwilligung der betroffenen Beschäftigten. Nach § 26 Abs. 2 BDSG n.F. muss die Einwilligung freiwillig erteilt werden. Vom WP ist bei der Einholung einer Einwilligung zu beachten, dass

der Beschäftigte vor Erteilung der Einwilligung über die Freiwilligkeit informiert wird und darüber, dass die Verweigerung der Einwilligung keine nachteiligen Folgen für das Beschäftigungsverhältnis mit sich bringt.

Für die Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, sind nach § 26 Abs. 2 BDSG n.F. insb. die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Freiwilligkeit kann insb. dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Der WP muss als Arbeitgeber nach § 26 Abs. 2 Satz 3 BDSG n.F. die Einwilligung – abweichend von Artikel 7 DS-GVO – grundsätzlich schriftlich einholen, es sei denn, es ist wegen besonderer Umstände eine andere Form angemessen. Zudem ist die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Abs. 3 DS-GVO in Textform aufzuklären (vgl. § 26 Abs. 2 Satz 4 BDSG n.F.).

8.8. Sind Verknüpfungen von Einwilligungen mit Gegenleistungen möglich?

Aus Artikel 7 Abs. 4 DS-GVO sowie Erwägungsgrund 43 DS-GVO ergibt sich ein allgemeines Koppelungsverbot. Dies bedeutet, dass es unzulässig ist, u.a. den Abschluss eines Vertrags einschließlich der Erbringung von Dienstleistungen von einer Einwilligung des Betroffenen abhängig zu machen, die sich auf personenbezogene Daten erstreckt, die für die Erfüllung des Vertrags nicht erforderlich sind. Einer solchen Einwilligung fehlt die Freiwilligkeit. Zudem ergibt sich aus Erwägungsgrund 42 DS-GVO, dass jeder mögliche Nachteil, der mit der Nichterteilung der Einwilligung verbunden ist, die Einwilligung unfreiwillig und danach unwirksam machen kann.

Daher ist für den WP wichtig, dass er die Einwilligung nicht mittels einer Einwilligungserklärung innerhalb eines Vertrags einholt, sondern durch eine separate Einwilligungserklärung. Dabei ist zu beachten, dass dem Betroffenen eine echte oder freie Wahl gegeben wird, die dieser, ohne Nachteile zu erleiden, treffen kann. Bspw. wäre es unzulässig, wenn der WP vom Kunden eine Einwilligung in die Referenznennung von einem Preisnachlass für die Dienstleistung abhängig machen würde.

8.9. Bleiben bereits erteilte Einwilligungen nach dem 25.05.2018 wirksam?

Die DS-GVO enthält zwar keine Regelung dazu, was für bereits erteilte Einwilligungen nach dem Inkrafttreten der DS-GVO gilt. Aus dem Erwägungsgrund 171 Satz 3 DS-GVO ergibt sich jedoch, dass bereits erteilte Einwilligungen wirksam bleiben, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht. Nach dem

Beschluss der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis; Datenschutzkonferenz) vom 13./14.09.2016 erfüllen bisher rechtswirksame Einwilligungen grundsätzlich diese Bedingungen. Nach diesem Beschluss verdienen allerdings die Bedingung der Freiwilligkeit (Koppelungsverbot, Artikel 7 Abs. 4 i.V.m. Erwägungsgrund 43 DS-GVO) sowie die Altersgrenze 16 Jahre i.S. des Artikels 8 Abs. 1 DS-GVO besondere Beachtung. Sind diese Bedingungen nicht erfüllt, gelten bereits erteilte Einwilligungen nicht fort. Fraglich ist jedoch zum jetzigen Zeitpunkt, ob diese Aufzählung abschließend ist. Da sich aus dem Erwägungsgrund 171 DS-GVO nicht ergibt, wann die “Art“ einer Einwilligung den Bedingungen der DS-GVO entspricht, ist dem WP anzuraten, bereits vorhandene Einwilligungen bis zum 25.05.2018 an die Voraussetzungen der DS-GVO anzupassen.

8.10. Was sind die Folgen der Einwilligung?

Möchte der WP personenbezogene Daten verarbeiten, die er nicht mittels einer anderen entsprechenden Rechtsgrundlage nach der DS-GVO (z.B. Artikel 6 Abs. 1 Buchst. b bis f), wie z.B. einem Vertrag über Wirtschaftsprüfungsleistungen oder berechtigtes Interesse, legitimieren kann, so kann er eine solche Verarbeitung auf eine wirksame Einwilligung stützen.

9. Datenschutz durch Technik und datenschutzfreundliche Voreinstellung

9.1. Was bedeutet Datenschutz durch Technik und datenschutzfreundliche Voreinstellung i.S.v. Artikel 25 DS-GVO?

Datenschutz muss bereits in die Programmierung und Konzipierung der Datenverarbeitungsvorgänge und -technik integriert sein und bei deren Entwicklung Berücksichtigung finden („privacy by design“). Damit wird der Datenschutz bereits Bestandteil der technischen Systementwicklung.

Durch die datenschutzfreundliche Voreinstellung („privacy by default“) soll gewährleistet werden, dass grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den Verarbeitungszweck erforderlich sind. Dabei ist zu achten auf die Menge der erhobenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit der Daten.

9.2. Gab es die Pflicht zum Datenschutz durch Technik und zur datenschutzfreundlichen Voreinstellung schon im bisherigen deutschen Datenschutzrecht?

Den Grundgedanken gab es schon im bisherigen Recht. Artikel 25 DS-GVO konkretisiert den Grundsatz der Datenminimierung aus Artikel 5 Abs. 1 Buchst. c DS-GVO, der in

Deutschland im Grundsatz der Datenvermeidung und Datensparsamkeit in § 3a BDSG a.F. verankert ist, und entspricht dem § 9 BDSG a.F. einschließlich seiner Anlage.

9.3. Ist es nicht Aufgabe der Hersteller von Datenverarbeitungssoft- und -hardware, auf die datenschutzrelevante Technik und Voreinstellung zu achten?

Nein, die Verantwortung für die Beachtung der datenschutzrechtlichen Vorgaben liegt beim Verantwortlichen, d.h. demjenigen, der über die Zwecke und Mittel der Datenverarbeitung entscheidet (Artikel 4 Nr. 7 DS-GVO). Wenn Hersteller von Datenverarbeitungssoftware und -hardware ihre Produkte zertifizieren lassen (s.o. Frage 3.5.), bieten sie dem Verantwortlichen den Vorteil, dass er ein Produkt kaufen kann, bei welchem die Datenschutzrechtskonformität indiziert ist.

9.4. Was ändert sich gegenüber der bisherigen Rechtslage (§ 9 BDSG a.F. und Anlage 1)?

a) Der Datenschutz durch datenschutzfreundliche Voreinstellungen wird ausdrücklich erfasst; eine inhaltliche Änderung ergibt sich daraus jedoch nicht, da die datenschutzfreundliche Voreinstellung im BDSG durch den Grundsatz der Datensparsamkeit angelegt war (§ 3a BDSG a.F., s.o. Frage 9.2.).

b) Die Verpflichtung zum Datenschutz durch Technikgestaltung muss nach wie vor in einem angemessenen Verhältnis zum Aufwand stehen, den die technischen und organisatorischen Maßnahmen erfordern. Neu ist allerdings, was unter Aufwand zu verstehen ist. Bisher waren als Aufwand sämtliche Kosten zu verstehen, die von der Planungs- und Entwicklungsphase bis hin zur Einführung entstehen, sowie alle anfallenden Betriebskosten und eventuell hiermit verbundenen Leistungseinbußen der Verarbeitungskapazität. Mit Artikel 25 DS-GVO wird hingegen nur noch auf die Implementierungskosten abgestellt.

c) Bisher konnte nur sanktioniert werden, wenn sich der Verantwortliche einer vorangegangenen behördlichen Anordnung widersetzte (§ 43 Abs. 1 Nr. 11 BDSG a.F.). Das ist gemäß Artikel 83 Abs. 6 DS-GVO nach wie vor möglich. Nunmehr können aber auch Verstöße gegen Artikel 25 DS-GVO als solche unmittelbar mit Geldbuße belegt werden (Artikel 83 Abs. 4 Buchst. a DS-GVO).

9.5. Was ist mit technischen Maßnahmen gemeint?

Wie i.S. des § 9 BDSG a.F sind mit technischen Maßnahmen alle Vorkehrungen gemeint, die sich auf den Vorgang der Datenverarbeitung erstrecken, wie z.B. das Wegschließen von Datenträgern, bauliche Maßnahmen, die den Zutritt Unbefugter verhindern sollen, oder Steuerungen des Software- oder Hardwareprozesses der Verarbeitung,

etwa Zugriffs- oder Weitergabekontrolle wie Verschlüsselungen oder Passwortsicherung. Weitere Maßnahmen können z.B. sein: Pseudonymisierung, Anonymisierung, Datenaggregation, Datensynthese, Nutzerauthentifizierung.

9.6. Was sind organisatorische Maßnahmen?

Sie richten sich auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses, etwa Vier-Augen-Prinzip, Protokollierung von Tätigkeiten und Stichprobenroutinen oder aber auch Mitarbeiterschulungen.

9.7. Wer überwacht die korrekte Anwendung der Vorschriften zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung?

Die nationale Aufsichtsbehörde (s.o. Frage 5.1.) überwacht die korrekte Anwendung der Vorschriften zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung (Artikel 57 Abs. 1 Buchst. a DS-GVO). Die Behörde kann Anweisungen erteilen, um Datenrechtskonformität herzustellen (Artikel 58 Abs. 2 Buchst. d DS-GVO).

9.8. Wenn man auf Maßnahmen zurückgreift, die zertifiziert sind, hat man dann alles Notwendige getan?

Die Anwendung zertifizierter technischer und organisatorischer Maßnahmen bedeutet nicht automatisch, dass der Verantwortliche bzw. der Auftragsverarbeiter den gesetzlichen Anforderungen genügt hat. Zertifikate stellen aber ein starkes Indiz für Gesetzeskonformität dar (s.o. Frage 3.5.). Sie mindern aber nicht die Verantwortung des Verantwortlichen bzw. des Auftragsverarbeiters für die Einhaltung der gesetzlichen Vorschriften (vgl. Artikel 42 Abs. 4 DS-GVO).

9.9. Was geschieht, wenn ein Verantwortlicher die Vorschriften zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung nicht beachtet?

Die Aufsichtsbehörde kann gegen den Verantwortlichen ein Bußgeld allein aufgrund der Verletzung der Vorschrift des Artikels 25 DS-GVO verhängen (Artikel 83 Abs. 4 Buchst. a DS-GVO). Hier beträgt die Höhe des Bußgeldes bis zu 10 Mio. € bzw. bis zu 2% des weltweit erzielten Jahresumsatzes.

Hat die Aufsichtsbehörde dem Verantwortlichen eine Anweisung gegeben, wie er die Verletzung der Vorschriften des Artikels 25 DS-GVO beheben kann, und hat der Verantwortliche die Anweisung nicht befolgt, kann die Aufsichtsbehörde auch dafür eine Geldbuße verhängen (Artikel 83 Abs. 6 DS-GVO). Hier beträgt die Höhe des Bußgeldes bis zu 20 Mio. € bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes.

9.10. Welche Folgen hat ein Verstoß für den Betroffenen?

Die betroffene Person kann gemäß Artikel 82 DS-GVO wegen eines Verstoßes gegen Artikel 25 DS-GVO materielle und immaterielle Schäden ersetzt bekommen. Ein Schadensersatzanspruch entsteht nicht nur, wenn Artikel 25 DS-GVO gar nicht, sondern auch, wenn er nicht ausreichend erfüllt wird. Begrenzend auf die Schadensersatzpflicht wirkt sich aus, dass bei der Bestimmung der Datenschutzpflichten nach Artikel 25 DS-GVO der Stand der Technik, die Implementierungskosten und Art, Umfang, Umstand und Zwecke der Datenverarbeitung in Betracht gezogen werden müssen.

10. Netzwerkgesellschaften

10.1. Eine WPG ist Mitglied eines Netzwerks. Ein Netzwerkmitglied begeht einen Datenschutzverstoß. Können andere Netzwerkmitglieder für diesen Datenschutzverstoß zur Verantwortung gezogen werden, obschon sie mit der betreffenden Datenverarbeitung nichts zu tun hatten?

Nein. Bei der Verarbeitung personenbezogener Daten ist grundsätzlich der für die Verarbeitung „verantwortliche“ Adressat für die Einhaltung der Vorschriften der DS-GVO. Verantwortlich ist innerhalb eines Netzwerks diejenige Netzwerkgesellschaft, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Artikel 4 Nr. 7 DS-GVO). Einen Konzern- bzw. Netzwerkdatenschutz, wonach der Konzern oder das Netzwerk datenschutzrechtlich verantwortlich ist oder haftet, kennt Artikel 4 Nr. 7 DS-GVO demnach nicht. Ferner kommt eine Verantwortlichkeit und Haftung von Netzwerkmitgliedern nach Artikel 82 DS-GVO in Betracht, soweit sie als Auftragsverarbeiter tätig geworden sind und die diesbezüglichen spezifischen Voraussetzungen für eine eigene Verantwortlichkeit und/oder eine etwaige Haftung auf Schadensersatz vorliegen (s. dazu unter Ziff. 10.3). Andere nicht involvierte Netzwerkmitglieder können demgemäß nicht zur Verantwortung gezogen werden.

10.2. Gilt etwas anderes, wenn mehrere Netzwerkmitglieder gleichermaßen in den Verarbeitungsvorgang involviert waren?

Nein. Die datenschutzrechtliche Verantwortlichkeit und etwaige Haftung kann auch mehrere Netzwerkgesellschaften treffen. Legen zwei oder mehrere Netzwerkmitglieder gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemäß Artikel 26 Abs. 1 DS-GVO auch gemeinsam Verantwortliche, so dass eine von einem etwaigen Datenschutzverstoß betroffene Person ihre daraus resultierenden Rechte gegen jedes dieser Netzwerkmitglieder geltend machen kann; daneben haftet jedes dieser Netzwerkmitglieder für einen der betroffenen Person entstandenen Schaden gesamtschuldnerisch (vgl. Artikel 82 Abs. 4 DS-GVO). Voraussetzung für eine gemeinsame Verantwortlichkeit

ist, dass jeder der Beteiligten als „Herr der Daten“ auf den Verarbeitungsvorgang steuernd einwirken kann. Bei gemeinsam Verantwortlichen treffen alle Beteiligten wesentliche Entscheidungen über Zweck und Mittel der Datenverarbeitung. Anders als bei der Auftragsverarbeitung besteht dabei keine hierarchische Verteilung der Verantwortung bzw. keine weisungsgebundene Datenverarbeitung.

10.3. Welches Netzwerkmitglied trägt im Rahmen einer Auftragsverarbeitungskonstellation die Verantwortung für einen Datenschutzverstoß?

Findet der Datenschutzverstoß in einer Auftragsverarbeitungskonstellation (Artikel 28 DS-GVO) innerhalb des Netzwerks statt, ist grundsätzlich nur das als Auftraggeber tätig werdende Netzwerkmitglied Verantwortlicher, da es i.S. des Artikels 4 Nr. 7 DS-GVO derjenige ist, der die Zwecke und Mittel der Verarbeitung festgelegt hat. Überschreitet das als Auftragsverarbeiter handelnde Netzwerkmitglied allerdings seine Kompetenzen, indem es die Zwecke und Mittel der Verarbeitung bestimmt, so wird es nach Artikel 28 Abs. 10 DS-GVO in Bezug auf diese konkrete Verarbeitung selbst Verantwortlicher, so dass es selbst die weitergehenden Pflichten eines Verantwortlichen treffen.

Zu einer Haftung auch des Auftragsverarbeiters (und damit auch eines in dieser Funktion tätig gewordenen Netzwerkmitglieds) gegenüber dem Betroffenen auf Schadensersatz kann es nach Artikel 82 Abs. 2 Satz 2 DS-GVO dann kommen, wenn er seinen speziell ihm als Auftragsverarbeiter auferlegten datenschutzrechtlichen Pflichten (vgl. z.B. Artikel 28, 32, 44 DS-GVO) nicht nachgekommen ist oder er gegen die Anweisungen des für die Datenverarbeitung verantwortlichen Netzwerkmitglieds gehandelt hat. Verantwortlicher und Auftragsverarbeiter haften dann als Gesamtschuldner (Artikel 82 Abs. 4 DS-GVO).

10.4. Kann auch ein nicht innerhalb der EU niedergelassenes Netzwerkmitglied für einen EU-Datenschutzverstoß verantwortlich sein?

Eine Verantwortlichkeit eines Nicht-EU-Netzwerkmitglieds kommt zunächst nur dann in Betracht, wenn es sich um die Verarbeitung personenbezogener Daten von Personen handelt, die sich in der EU befinden (Artikel 3 Abs. 2 DS-GVO). Dafür ist keine Wohnsitz-Ansässigkeit der betroffenen Person erforderlich, vielmehr genügt bereits der tatsächliche Aufenthalt im Unionsgebiet (ohne zeitliche Mindestverweildauer).

Bezüglich solcher Daten ist ein außerhalb der EU niedergelassenes Netzwerkmitglied verantwortlich, wenn es Verantwortlicher i.S. des Artikels 4 Nr. 7 DS-GVO (s.o. Frage 10.1.) oder Auftragsdatenverarbeiter (dann in eingeschränktem Umfang, s.o. Frage 10.3.) ist und die Datenverarbeitung damit im Zusammenhang steht, dass

a) betroffenen Personen Waren oder Dienstleistungen angeboten werden oder

b) das Verhalten betroffener Personen beobachtet wird.

Für WPG wird regelmäßig insb. die vorstehende Alternative a) einschlägig sein können.

Erwägungsgrund 23 der DS-GVO wird man dahingehend verstehen müssen, dass es zur Feststellung, ob ein Anbieten i.S. des vorstehenden Buchst. a vorliegt, schon genügen kann, wenn festgestellt wird, dass das Netzwerkmitglied offensichtlich beabsichtigt, seine Dienstleistungen gegenüber Personen in der EU anzubieten. Wann wiederum dies der Fall ist, muss anhand von Hilfsfaktoren und Indizien bestimmt werden (vgl. Kurzpapier Nr. 7 der Datenschutzkonferenz zum Marktortprinzip: Regelungen für außereuropäische Unternehmen).

Für eine solche Absicht sprechen z.B. Faktoren wie

- die Verwendung der Sprache oder Währung eines Mitgliedstaats in Verbindung mit der Möglichkeit, Dienstleistungen abzurufen, oder
- die Erwähnung von anderen Kunden oder Nutzern, die sich in der EU befinden.

Zu beachten ist allerdings zusätzlich, dass eine ggf. vorausgegangene Übermittlung von EU-Daten in das Nicht-EU-Ausland durch ein EU-Netzwerkmitglied den Voraussetzungen der Artikel 44 ff. DS-GVO (Angemessenheitsbeschluss, Garantien etc.) genügen muss. Andernfalls begründet die unzulässige Übermittlung eine diesbezügliche datenschutzrechtliche Haftung der unrechtmäßig übermittelnden EU-Netzwerkgesellschaft.

10.5. Ist man für Datenschutzverstöße eines Subunternehmers bzw. eines als Subunternehmer eingesetzten Netzwerkmitglieds (EU und nicht-EU) verantwortlich?

Ob eine Verantwortlichkeit für Datenschutzverstöße des von einem WP beauftragten Subunternehmers (und damit auch eines als Subunternehmer eingesetzten Netzwerkmitglieds) besteht, beurteilt sich wiederum nach Artikel 4 Nr. 7 DS-GVO, mithin danach ob die WPG entweder allein oder gemeinsam mit dem Subunternehmer über die Zwecke und Mittel der Verarbeitung der betreffenden personenbezogenen Daten entscheidet. Eine gemeinsame (Mit-)Haftung für Datenschutzverstöße des Subunternehmers kommt daher nur in Betracht, wenn auch der beauftragende WP als „Herr der Daten“ steuernd in den Verarbeitungsvorgang beim Subunternehmer eingreifen kann. Dies wird regelmäßig eher nicht der Fall sein. Handelt es sich bei der beauftragten Dienstleistung aber um eine Auftragsverarbeitung des Subunternehmers, bleibt der beauftragende WP Verantwortlicher (vgl. § 62 Abs. 1 BDSG n.F.); daneben kann aber auch der Auftragsdatenverarbeiter-Subunternehmer Verantwortlicher und Haftender sein (wenn die diesbezüglichen Voraussetzungen des Artikels 28 Abs. 10 und Artikel 82 Abs. 2 Satz 2 DS-GVO vorliegen, s. o. Ziff. 10.3).

19.06.2019

11. Europäischer Vertreter von nicht in der EU niedergelassenen datenverarbeitenden Unternehmen (Artikel 27 DS-GVO)

11.1. Wann benötigt ein nicht in der EU ansässiges Unternehmen einen europäischen Vertreter i.S. des Artikels 27 DS-GVO? Gibt es hiervon auch Ausnahmen?

Liegt ein Fall des Artikels 3 Abs. 2 DS-GVO vor, d.h. eine Verarbeitung von personenbezogenen Daten von in der EU befindlichen Personen durch nicht in der EU Niedergelassene, so ist ein Vertreter in der Union zu benennen (bußgeldbewehrt, vgl. Artikel 83 Abs. 4 Buchst. a DS-GVO, bis zu 10.000.000 € oder bis zu 2 % des weltweit erzielten Jahresumsatzes).

Eine Verpflichtung zur Benennung eines Vertreters besteht jedoch dann nicht, wenn die betreffende Verarbeitung von personenbezogenen Daten nur „gelegentlich“ erfolgt (es sei denn, die Verarbeitung betrifft eine umfangreiche Verarbeitung der als besonders sensibel anzusehenden Daten i.S.d. Artikel 9 Abs. 1 oder Artikel 10 DS-GVO). Hierunter ist eine nur bisweilen bzw. vereinzelt erfolgende Verarbeitung zu verstehen. Nach einer Literaturauffassung soll dem der Fall gleichzustellen sein, dass sich ein Angebot einschlägiger Dienstleistungen nur zeitweise und vorübergehend auf Personen in der EU richtet. Da hier viele Grenzfälle denkbar sind, verbleibt eine nicht unbeträchtliche Rechtsunsicherheit.

11.2. Benötigt ein nicht in der EU niedergelassenes Netzwerkmitglied für die Erbringung steuerlicher Beratungsleistungen in der EU einen Vertreter i.S.d. Artikel 27 DS-GVO?

Ja, sofern das Nicht-EU-Netzwerkmitglied den Tatbestand des Artikels 27 DS-GVO erfüllt (s.o.). Denkbar ist dies bspw. für Expatriate Tax Services für Personen, die in die EU entsandt werden. Zu berücksichtigen ist aber, dass Expatriate Tax Services zwar im Ergebnis den sich im Ausland befindlichen Arbeitnehmern zugutekommen sollen, aber sehr häufig von den entsendenden Arbeitgebern beauftragt und bezahlt werden. Richtet sich das Angebot von vornherein explizit nur an Arbeitgeber, spricht viel dafür, insoweit die Erforderlichkeit der Benennung eines Vertreters zu verneinen.

11.3. Kann ein in Deutschland niedergelassener WP oder eine WPG für eine andere Netzwerkgesellschaft die von dieser ggf. vorzuhaltende Funktion eines Vertreters nach Artikel 27 DS-GVO übernehmen?

Nach der Legaldefinition des Artikels 4 Nr. 17 DS-GVO kann sowohl eine natürliche als auch eine juristische Person Vertreter sein, sodass grundsätzlich auch eine Vertretung durch einen WP oder eine WPG in Betracht kommt. Für die berufsrechtliche Vereinbarkeit einer solchen Tätigkeit mit dem Berufsbild des WP spricht die Vergleichbarkeit der

Anforderungen mit der berufsrechtlich anerkannten Tätigkeit eines WP als Datenschutzbeauftragter. Ungeachtet dessen dürfte die Übernahme des „Amtes“ eines Vertreters i.S. des Artikels 27 DS-GVO nicht unbeträchtliche haftungsrechtliche Risiken bergen, sodass in jedem Fall mit dem Berufshaftpflichtversicherungsunternehmen geklärt werden sollte, ob diese Tätigkeit von der Versicherung ebenfalls gedeckt ist.

12. Internationale Zusammenarbeit

12.1. Für welche Drittländer hat die Kommission beschlossen, dass sie ein angemessenes Schutzniveau haben, und gelten diese Beschlüsse noch?

Angemessenheitsbeschlüsse der EU-Kommission gibt es für Andorra, Argentinien, die Färöer Inseln, Guernsey, die Insel Man, Israel, Jersey, Kanada (für privatrechtlich organisierte Empfänger, nicht jedoch öffentliche Stellen), Neuseeland, die Schweiz, Uruguay, Japan und die USA (zu USA s.u.: Frage 12.2.).

Die Beschlüsse der Kommission für diese Länder bleiben so lange in Kraft, bis sie die Beschlüsse aufhebt (Artikel 46 Abs. 5 Satz 2 DS-GVO). Bisher ist kein Beschluss aufgehoben worden.

12.2. Kann man aufgrund des Angemessenheitsbeschlusses bezüglich der USA personenbezogene Daten an jedes Unternehmen in den USA übermitteln?

Nein. Der Angemessenheitsbeschluss der EU-Kommission bezieht sich auf Datenübermittlungen in die USA, die im Rahmen des sog. EU-US-Datenschutzschildes (privacy shield) durchgeführt werden. Der EU-US-Datenschutzschild beruht auf einem System der Selbstzertifizierung von Unternehmen, die sich zu einem festgelegten Datenschutzniveau verpflichten. Diese selbstzertifizierten Unternehmen werden von der zuständigen EU-Behörde überprüft und kommen auf eine „Datenschutzschild-Liste“ des US-Handelsministeriums (https://www.privacyshield.gov/list). Die Datenübermittlung in die USA ist nur erlaubt, wenn die Daten an die Unternehmen der Datenschutzschild-Liste übermittelt werden (Artikel 1 Abs. 3 des Durchführungsbeschlusses vom 12.07.2016, ABl. EU Nr. L 207/1. Vor der Datenübermittlung müssen sich europäische Unternehmen vergewissern, dass die Ziel-Unternehmen in den USA auf der Liste stehen.

12.3. Kann man Daten an Verantwortliche oder Auftragsverarbeiter in Drittstaaten übermitteln, die nicht von der Kommission als angemessen angesehen werden?

Ja, die Angemessenheitserklärung der Kommission ist nur ein Weg, im Einklang mit dem EU-Datenschutz Daten in Drittländer zu übermitteln. Ohne Angemessenheitserklärung darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein

Drittland oder eine internationale Organisation allerdings nur übermitteln, sofern er „geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen“ (Artikel 46 Abs. 1 DS-GVO). Zu den „geeigneten Garantien“ gehören:

a) verbindliche und durchsetzbare Dokumente zwischen den Behörden der betroffenen Staaten

b) von der zuständigen öffentlichen Stelle genehmigte interne Datenschutzvorschriften („binding corporate rules“) des Verantwortlichen (Unternehmen) bzw. des Auftragsverarbeiters

c) Standardschutzklauseln (bisher “Standardvertragsklauseln“)

d) genehmigte Verhaltensregeln („codes of conduct“)

e) behördlich genehmigte Zertifizierung

f) behördlich genehmigte, von den Vertragspartnern erstellte Vertragsklauseln

g) behördlich genehmigte Bestimmungen, die in Verwaltungsvereinbarungen aufzunehmen sind und durchsetzbare und wirksame Rechte der Betroffenen enthalten.

12.4. Braucht man beim Vorliegen einer der „geeigneten Garantien“ noch zusätzlich eine behördliche Genehmigung?

Nein, für die Garantien nach Buchstaben a) bis e) ist keine weitere behördliche Genehmigung nötig. Die Verantwortlichen können sich für die Datenübermittlung direkt auf diese Garantien stützen.

12.5. Kann man allein aufgrund eines Angemessenheitsbeschlusses bzw. einer vorgenannten Garantie (s.o. Frage 12.3.) Daten ins Ausland schicken?

Nein, es gilt wie bisher eine Zweistufenprüfung. Zunächst muss geklärt werden, ob die Datenübermittlung als solche nach dem materiellen EU-Datenschutzrecht erlaubt ist. Das heißt, es muss geprüft werden, ob die Datenübermittlung in einem inländischen bzw. innereuropäischen Sachverhalt erlaubt wäre. Erst wenn dies bejaht ist, muss in einem zweiten Schritt geklärt werden, ob die Übermittlung in das konkrete Ausland erlaubt ist.

12.6. Welche Standarddatenschutzklauseln kann ich nutzen und gelten die bisherigen Klauseln noch?

Es gibt drei Standardklauselwerke.

Zwei davon betreffen Verträge zur Datenübermittlung von einem Verantwortlichen innerhalb des Geltungsbereichs der DS-GVO, d.h. EU und EWR, (sog. Datenexporteur) zu

einem Verantwortlichen außerhalb des Geltungsbereichs der DS-GVO (sog. Datenimporteur). Beide Klauselwerke stehen alternativ nebeneinander.

Ein Klauselwerk betrifft Verträge zur Datenübermittlung vom Verantwortlichen innerhalb des Geltungsbereichs der DS-GVO (sog. Datenexporteur) an einen Auftragsverarbeiter außerhalb des Geltungsbereichs der DS-GVO (sog. Datenimporteur).

Die Klauseln finden sich auf der Website der Europäischen Kommission (http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

Die Klauseln bleiben auch nach Erlass der DS-GVO gültig.

12.7. Warum gibt es verschiedene Klauseln für die Datenübermittlung zwischen zwei Verantwortlichen und welche Klauseln sollte man anwenden?

Welche Klauseln sich am besten eignen, muss im Einzelfall entschieden werden.

Der Haupt-Unterschied zwischen den beiden Werken liegt in den Haftungsregeln. Das ältere Klauselwerk (2004/915/EG), auch Set I genannt, enthält eine gesamtschuldnerische Haftung der Vertragsparteien (siehe Klausel 6). Das jüngere Klauselwerk (2010/87/EU), auch Set II genannt, sieht eine verursacherbezogene Haftung vor (Klausel III Buchst. a).

Set II ermöglicht in begrenztem Umfang Änderungen der Klauseln zu Aktualisierungszwecken (Klausel VII); Set I hingegen schließt diese Möglichkeit aus (Klausel 11).

Set II ist nach h.M. nicht für die Übermittlung von Arbeitnehmerdaten verwendbar.

12.8. Muss man die Standardvertragsklauseln auch im Verkehr mit Staaten nutzen, deren Datenschutz von der EU-Kommission als angemessen angesehen wird?

Nein. Die Standardvertragsklauseln sind ein Instrument, um über einen fehlenden Angemessenheitsbeschluss der EU-Kommission „hinwegzukommen“ (vgl. Artikel 46 Abs. 1 DS-GVO).

Hingegen bieten Standardvertragsklauseln dann einen Rechtsrahmen für den Datenaustausch, wenn Daten aus einem Drittstaat kommen ….. gilt auch, wenn Drittland-Daten in die EU gesendet werden, dort verarbeitet werden und ins Herkunftsdrittland zurückgesendet werden … …. Sobald Daten in den DSGVO-Bereich gelangen, gilt für sie das hohe Schutzniveau, auch wenn sie aus einem niedrigeren Niveau kommen. … Verarbeiter kann Daten dann nur mit Standardvertragsklauseln zurückschicken …

12.9. Darf ein Auftragsverarbeiter im Ausland Unteraufträge an einen Dienstleister im Ausland erteilen?

Grundsätzlich ja. Der Verantwortliche muss mit der Unterbeauftragung einverstanden sein. Als Daumenregel gilt, dass der Auftragsverarbeiter dem Subunternehmer (Unterauftragsverarbeiter) mittels einer schriftlichen Vereinbarung die gleichen Pflichten auferlegen muss, die auch er – der Auftragsverarbeiter – zu erfüllen hat. Dazu reicht es, wenn der Unterauftragsverarbeiter den Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter unterzeichnet.

12.10. Gelten die Vertragsklauseln auch, wenn nur der Subunternehmer im Drittland ist, der Verantwortliche und der Auftragsverarbeiter aber beide in der EU angesiedelt sind?

Nein, die Vertragsklauseln finden zwischen den in der EU angesiedelten Vertragspartnern keine Anwendung. In der genannten Konstellation muss der Verantwortliche mit dem Nicht-EU-Unterauftragnehmer den Standardklauselvertrag zur Auftragsverarbeitung abschließen, und zwar entweder selbst oder vertreten durch den Auftragsverarbeiter. Alternativ kommt ein behördlich genehmigter Vertrag, den die Vertragspartner selbst erstellen, in Betracht (Artikel 46 Abs. 3 Buchst. a DS-GVO).

12.11. Kann nur die Europäische Kommission Standarddatenschutzklauseln erlassen?

Nein, auch nationale Behörden können Standarddatenschutzklauseln annehmen, die allerdings von der Kommission genehmigt werden müssen (Artikel 46 Abs. 2 Buchst. d DS-GVO). Es gibt noch keine Standarddatenschutzklausel einer deutschen Behörde.

12.12. Wie muss sich eine international tätige WPG verhalten, wenn sie nach geltendem Recht eines Drittstaats zur Übermittlung von personenbezogenen "EU-Daten" hoheitlich, z.B. durch ein Urteil oder einen Verwaltungsakt, verpflichtet wird?

Die DS-GVO erlaubt in diesen Fällen eine Übermittlung nur, wenn es eine Übereinkunft zwischen den beiden betroffenen Staaten bzw. dem Drittstaat und der EU gibt (Artikel 48 DS-GVO). Besteht diese Übereinkunft nicht, bleibt nach der aktuellen Rechtslage nur die Wahl, das eine oder das andere Recht zu brechen und die Konsequenzen in Kauf zu nehmen.

12.13. Mit welchen Drittstaaten besteht eine Übereinkunft in Deutschland bzw. der EU, die eine Datenübermittlung in ein Drittland ermöglicht?

Deutschland hat mit den USA, Kanada und Australien zivilrechtliche wie auch strafrechtliche Rechtshilfeabkommen geschlossen, die Übereinkommen i.S. des Artikels 48 DS-

GVO sind. Ferner gibt es ein internationales Rechtshilfeübereinkommen des Europarats (1959) das für 50 Länder gilt. Ein weiteres internationales Abkommen ist das Haager Übereinkommen von 1970 mit 58 teilnehmenden Staaten.

13. Data Breach Notification

13.1. Wann liegt ein Datenvorfall/Data Breach („Verletzung des Schutzes personenbezogener Daten“) vor, der eine Mitteilung an die Aufsichtsbehörde oder die Betroffenen zur Folge haben kann?

Nach Artikel 4 Nr. 12 DS-GVO ist ein Data Breach „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. Beispiele für Data Breaches sind: Cyberangriffe, Einbruch in einen schlecht gesicherten Serverraum, der mit einem Verlust von Daten einhergeht, Verlust eines USB-Sticks, Diebstahl oder Verlust eines Smartphones bzw. sonstiger mobiler Hardware oder die unbefugte Weitergabe von Informationen durch Mitarbeiter – gleichgültig ob bewusst oder unbewusst. Data Breaches sind oftmals mit erheblichen Risiken, wie z.B. einer Rufschädigung oder einem Identitätsdiebstahl, für die Betroffenen sowie für die verantwortlichen Unternehmen verbunden. Beim Umgang mit Data Breaches müssen die Artikel 33 und 34 DS-GVO beachtet werden (s.o. Frage 4.3.).

13.2. Was ist unter der Meldepflicht gegenüber Behörden nach Artikel 33 DS-GVO zu verstehen und was ist von der Meldepflicht umfasst?

Eine Meldepflicht an die zuständige Aufsichtsbehörde besteht grundsätzlich nur dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Eine Beschränkung auf Risikodaten, wie die besonderen Arten von personenbezogenen Daten, gibt es nicht. Eine Ausnahme der Meldepflicht besteht dann, wenn das Risiko einer Verletzung bspw. durch eine geeignete Verschlüsselung personenbezogener Daten ausgeschlossen werden kann, da diese Verschlüsselung beim Verlust eines Datenträgers die Kenntnisnahme der Daten durch Dritte verhindert (s.o. Frage 4.3.).

Die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde hat unverzüglich, also ohne schuldhaftes Zögern, nach Kenntniserlangung zu erfolgen.

Nach Artikel 33 Abs. 1 DS-GVO wird bei der Meldung an die Aufsichtsbehörde nun zusätzlich ein gesetzlicher Richtwert von 72 Stunden für den Ablauf der Meldefrist

angenommen. Erfolgen Meldungen erst nach Ablauf dieser Frist, muss den Meldungen eine Begründung für diese Verzögerung beigefügt werden (vgl. Artikel 33 Abs. 1 Satz 2 DS-GVO). Dabei ist es unerheblich, wo innerhalb einer Organisation der Verstoß zuerst bekannt wurde. Es reicht aus, dass der Verstoß irgendjemandem innerhalb der Organisation bekannt wurde. Daher ist es wichtig, eine ganzheitliche Sensibilisierung für das Thema Data Breach zu schaffen und unternehmensinterne Meldeprozesse zu etablieren. Wenn der Verantwortliche nachweisen kann, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, kann die Meldung an die Aufsichtsbehörde unterbleiben (vgl. Artikel 33 Abs. 1 Satz 1 DS-GVO). Dies kann durch dokumentierte Tatsachen, wie bspw. ergriffene Verschlüsselungsmechanismen, aussagekräftige Zertifizierungen datenverarbeitender Systeme oder dem Nachweis von Schulungen der Mitarbeiter durch den Datenschutzbeauftragten belegt werden. Unter Berücksichtigung der Tatsache, dass bei jeder unterbliebenen Meldung an die Aufsichtsbehörde ein Bußgeld von bis zu 2 % des globalen Konzernumsatzes droht (vgl. Artikel 83 Abs. 4 Buchst. a DS-GVO), ist ein entsprechender lückenloser Prozess für Data Breaches unerlässlich, oder es muss grundsätzlich jede Verletzung gemeldet werden, um Sanktionen wegen Nicht-Meldung zu vermeiden.

13.3. Welche Mindestangaben muss die Meldung an die Aufsichtsbehörde gemäß Artikel 34 Abs. 2 DS-GVO enthalten?

a) Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (wenn möglich mit Angabe der Kategorien von Betroffenen und der Anzahl der betroffenen Personen [wenn nicht genau bezifferbar, reicht ein Schätzwert], der betroffenen Kategorien von Daten und der ungefähren Zahl der personenbezogenen Datensätze),

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,

d) eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten wie Auswirkungen der Verletzung und ergriffene Maßnahmen zur Abmilderung der Verletzung müssen künftig vom Datenschutzbeauftragten oder der dafür zuständigen Stelle innerhalb der Organisation dokumentiert

werden. Die Dokumentation dient der Aufsichtsbehörde zum einen dafür, einen ersten Überblick über den Data Breach zu bekommen, und zum anderen zur Überprüfung, ob der Verantwortliche seiner Meldepflicht korrekt nachgekommen ist (vgl. Artikel 33 Abs. 5 Satz 2 DS-GVO).

Gemäß Artikel 33 Abs. 4 DS-GVO ist es erlaubt, die konkreten Informationen zum Data Breach schrittweise zur Verfügung zu stellen, wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, sofern der Nachtrag zu diesen Informationen ohne unangemessene weitere Verzögerung erfolgt.

Sofern dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, muss dieser unverzüglich den Verantwortlichen kontaktieren und den Data Breach melden (vgl. Artikel 33 Abs. 2 DS-GVO).

13.4. Was ist unter der Meldepflicht gegenüber betroffenen Personen nach Artikel 34 DS-GVO zu verstehen und was ist von der Meldepflicht umfasst?

Eine Meldepflicht gegenüber betroffenen Personen besteht, wenn der Data Breach voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge hat. Aus diesem Grund muss künftig eine Risikoabwägung stattfinden. Das Ergebnis dieser Risikoabwägung sollte dokumentiert werden. Die Benachrichtigung muss so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von der Aufsichtsbehörde oder von anderen zuständigen Behörden (bspw. Strafverfolgungsbehörden) erteilten Weisungen erfolgen. Erfolgt die Einschätzung, dass ein hohes Risiko für den Betroffenen besteht, muss dieser nach dem Ergebnis der Risikoabwägung unverzüglich benachrichtigt werden. Um das Risiko eines unmittelbaren Schadens mindern zu können, müssen Betroffene sofort benachrichtigt werden. Eine längere Benachrichtigungsfrist ist gerechtfertigt, wenn es darum geht, geeignete Maßnahmen gegen fortdauernde oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen, um z.B. weitere Folgen der Verletzung zu vermeiden oder zu minimieren (vgl. Erwägungsgrund 86 DS-GVO).

Welche Ausnahmen bestehen von der Pflicht zur Benachrichtigung des Betroffenen?

Nur in den in Artikel 34 Abs. 3 DS-GVO genannten Fällen kann von einer Benachrichtigung des Betroffenen abgesehen werden, wenn

a) geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen wurden (z.B. Verschlüsselung und dadurch die Sicherstellung, dass unbefugte Personen keinen Zugang zu Daten haben),

b) durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach

nicht mehr besteht, oder

c) die direkte Information der Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall ist jedoch eine öffentliche Bekanntmachung gefordert oder eine ähnliche Maßnahme, die die betroffenen Personen vergleichbar wirksam informiert.

Welche Mindestangaben muss die Meldung an den Betroffenen gemäß Artikel 34 Abs. 2 DS-GVO enthalten?

a) Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung (ggf. unter Berücksichtigung der Umstände der Verletzung, bspw. ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Datenmissbrauchs wirksam verringern),

d) eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Sollte der Verantwortliche zur Einschätzung kommen, dass eine Meldung an die betroffene Person nicht erfolgen muss, da die Verletzung nicht zu einem hohen Risiko für die Rechte und Freiheiten dieser natürlichen Person führt, die Aufsichtsbehörde aber der Auffassung ist, dass eine Meldung an die betroffene Person erfolgen muss, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Artikel 34 Abs. 3 DS-GVO genannten Voraussetzungen erfüllt sind (vgl. Artikel 34 Abs. 4 DS-GVO).

13.5. Gibt es eine zusätzliche Meldepflicht gegenüber Mandanten des WP (Vertragsverhältnis)?

Ggf. können sich aus dem Vertragsverhältnis zum Mandanten kürzere Meldefristen ergeben, die eingehalten werden müssen. Zu beachten ist, dass dies für den Mandanten keine Zeitersparnis zur Meldung eines Verstoßes an die Aufsichtsbehörde bedeutet. Die 72-Stunden-Frist zur Meldung eines Verstoßes an die Aufsichtsbehörde beginnt immer ab dem Zeitpunkt des Bekanntwerdens beim Verantwortlichen. Eine kürzere vertragliche Meldepflicht aus dem Mandantenverhältnis bedeutet für den Mandanten keinen Vorteil

im Hinblick auf die Reaktionszeit, wohl aber eine schnellere Reaktionszeit für den WP, welcher mit den Mandantendaten arbeitet, und folglich eine einwandfreie und lückenlose Datenschutzorganisation des WP. Ein einheitliches Reporting System für Data Breaches und darüber hinaus ein effizientes Vertragsmanagementsystem können sicherstellen, dass einschlägige Notifikationsfristen eingehalten werden. Um eine Übersicht über einzelne vertraglich geregelte Meldefristen zu bekommen, kann ein entsprechendes Register sachdienlich sein, das die Fristen der Mandanten enthält und bei einem Data Breach schnell zur Hand ist. Verstöße gegen vertraglich geregelte Fristen können zum einen mit Vertragsstrafen und Schadenersatzansprüchen der Mandanten verbunden sein und zum anderen zu einem erheblichen Reputationsschaden des WP führen.

13.6. Welche Maßnahmen sind einzuleiten nach Bekanntwerden eines Datenschutzverstoßes?

Ziel sollte die schnellstmögliche Bewertung eines Vorfalls sein hinsichtlich der Schwere, der Art, des Umfangs, der Bewältigung, der Hinzuziehung von Personen und der Abwendung von etwaigen Schäden für Betroffene, die Öffentlichkeit und das Unternehmen. Um dies zu erreichen, sollte unabhängig davon, wie kritisch einzelne Datenverarbeitungsvorgänge eines Verantwortlichen oder Auftragsverarbeiters sind bzw. welche Kategorien von Daten verarbeitet werden, ein nachhaltiges und effizientes Datenschutzmanagementsystem innerhalb des Unternehmensnetzwerks aufgebaut werden. Dieses stellt sicher, dass Geschäftsprozesse, Systeme und Strukturen einer Organisation einschließlich aller internen und externen Schnittstellen regelmäßig überprüft und angepasst werden. Dies dient auch im Falle eines Data Breach dazu, schnellstmöglich die notwendigen Maßnahmen zu ergreifen und Folgeschäden wie z.B. einen Reputationsschaden für das Unternehmen zu minimieren.

a) Information des Datenschutzbeauftragten

Die unverzügliche Information an den betrieblichen Datenschutzbeauftragten nach Bekanntwerden eines Verstoßes ist unabdingbar, da im Zweifel er der Einzige ist, der das nötige technische Verständnis und einen ganzheitlichen Überblick über Datenverarbeitungsvorgänge im Unternehmen hat. Darüber hinaus ist es seine Aufgabe, Risiken für betroffene Personen, die mit der Verarbeitung von personenbezogenen Daten einhergehen, zu erkennen und zu beurteilen (vgl. Artikel 39 DS-GVO – nicht abschließende Aufzählung der Aufgaben des Datenschutzbeauftragten).

b) Sammeln verfügbarer Informationen und Konsequenzen für die interne Organisation

Da bei Bekanntwerden eines Verstoßes meist vorerst lediglich Rumpfinformationen vorhanden sind, hat es Priorität, alle notwendigen Informationen bezüglich Art, Umfang, Kategorien von Daten, betroffener Systeme, betroffener Personen(-Gruppen) etc. zu

sammeln, um eine Aussage über die Schwere der Verletzung treffen zu können.

c) Review Data Breach

Im Review-Prozess des Data Breach steht die Risikoeinstufung des Vorfalls an erster Stelle. Die Einstufung ist maßgeblich dafür, ob durch die Verletzung ein (hohes) Risiko für die Rechte und Freiheiten einer natürlichen Person besteht, welches der Auslöser für die Meldepflicht gegenüber der Aufsichtsbehörde und der betroffenen Person ist. Der Risikoeinstufungsprozess sollte dokumentiert werden, um diesen auf Nachfrage der Aufsichtsbehörde zur Verfügung stellen zu können.

d) Meldung von Verletzungen des Schutzes personenbezogener Daten

Nach erfolgter Risikoeinschätzung erfolgt sodann die Meldung an die Aufsichtsbehörde/ den Mandanten und ggf. an den/die Betroffenen.

13.7. Kommt es bei Verlust eines Datenträgers (z.B. Laptop/USB-Sticks/Smartphones) zum Data Breach?

Zu einer unberechtigten Kenntnisnahme bei einem Verlust von Datenträgern kommt es i.d.R. nicht, wenn Verschlüsselungsmechanismen sicherstellen, dass die Daten vor Kenntnisnahme durch Unbefugte geschützt sind. Eine Verschlüsselung ist nach § 64 Abs. 3 Nr. 2 BDSG n.F. eine angemessene Maßnahme zur Sicherstellung der Datenträgerkontrolle und sollte beim Umgang mit personenbezogenen und vertraulichen Mandantendaten stets angewendet werden. Um eine generelle bestmögliche Verschlüsselung, auch von Systemen, und damit Sicherheit der Daten zu gewährleisten, sollten neben Standardverschlüsselungen zusätzliche Verschlüsselungen auf den Übertragungswegen und auf den Speichersystemen (Primär-, Sekundär- und Tertiärspeicher) i.S. einer Encryption in Transit und Encryption at Rest sichergestellt werden. Darüber hinaus bieten lange Schlüssellängen und die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als sicher eingestuften Algorithmen eine hohe Verschlüsselungssicherheit (Algorithmenkatalog des BSI abrufbar auf der Website des BSI).

14. Datenschutzrechtliche Haftung und Schadenersatzanspruch nach DS-GVO

14.1. Wo ist die Haftung für Schadensersatzansprüche in der DS-GVO geregelt?

Die Haftung und zivilrechtliche Schadenersatzansprüche sind in den Artikel 82 ff. der Verordnung geregelt. Jede Person, der wegen eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist, hat somit Anspruch auf Schadenersatz gegen den Verantwortlichen oder Auftragsverarbeiter (vgl. Artikel 82 Abs. 1 DS-GVO). Hierzu zählen etwa Verlust der Kontrolle über ihre personenbezogenen Daten, Einschränkung der Rechte der Betroffenen, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle

Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die Betroffenen (vgl. Erwägungsgrund 75 DS-GVO). Dabei trägt das Unternehmen nach Artikel 24 Abs. 1 DS-GVO die Beweislast, dass es die Vorgaben der Verordnung ordnungsgemäß umgesetzt hat. Unternehmen, Vorständen und dem Management drohen erhebliche finanzielle Risiken bei Verstößen gegen die Verordnung.

Haften wird in erster Linie das betroffene Unternehmen, d.h. der jeweilige Verantwortliche oder Auftragsverarbeiter. Es wird davon auszugehen sein, dass Unternehmen für Verstöße, die durch ihre Mitarbeiter begangen werden, grundsätzlich einstehen müssen und somit geahndet werden können.

14.2. Wie sind die Geldbußen und Sanktionen nach DS-GVO geregelt?

Die allgemeinen Bedingungen für die Verhängung von Geldbußen sind in Artikel 83 DS-GVO geregelt. Die Vorschriften über weitere Strafvorschriften und strafrechtliche Sanktionen für Verstöße, insb. jene, die keiner Geldbuße unterliegen, sind von den Mitgliedstaaten festzulegen (vgl. Erwägungsgrund 152, Artikel 84 DS-GVO). Die Sanktionen sollen von Datenschutzverstößen abhalten und daher wirksam, verhältnismäßig und abschreckend sein. Dies zeigt sich deutlich im Bußgeldrahmen der Verordnung, der bei einem Teil der Verstöße von 10 Mio. € oder bis zu 2 % des weltweit erzielten Jahresumsatzes, bei einem anderen Teil der Verstöße sogar bis zu 20 Mio. € oder bis zu 4 % des weltweit erzielten Jahresumsatzes reicht. Kriterien finden sich im Katalog in Artikel 83 Abs. 2 Buchst. a bis k DS-GVO.

Zuständig für die Verhängung von Geldbußen ist gemäß Artikel 55 Abs. 1 DS-GVO grundsätzlich jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats. Bei internationalen Datentransfers liegt die Zuständigkeit bei der federführenden Aufsichtsbehörde gemäß Artikel 56, 60 DS-GVO. Die Sanktionen können anstelle von oder zusätzlich zu den Anweisungen der Aufsichtsbehörde gemäß Artikel 58 DS-GVO verhängt werden. Die Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Abs. 2 DS-GVO wird ebenfalls mit einer Geldbuße von 20 Mio. € bzw. 4 % des weltweiten Jahresumsatzes geahndet.

Kriterien für die Verhängung von Geldbußen nach Artikel 83 Abs. 2 DS-GVO sind:

a) Art, Schwere, Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung sowie die Anzahl der Betroffenen und das Ausmaß des Schadens

b) Vorsatz oder Fahrlässigkeit

c) Maßnahmen zur Minimierung des entstandenen Schadens (z.B. auch, ob ein Privacy Impact Assessment durchgeführt wurde)

d) Grad der Verantwortung von Verantwortlichen und Auftragsverarbeitern unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen

e) frühere Verstöße

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern

g) Kategorien personenbezogener Daten, die betroffen sind

h) ob und in welchem Umfang der Verantwortliche oder Auftragsverarbeiter den Verstoß mitgeteilt hat

i) ob frühere angeordnete Maßnahmen umgesetzt wurden

j) Einhaltung von genehmigten Verhaltensregeln (Artikel 40 DS-GVO) oder genehmigten Zertifizierungsverfahren (Artikel 42 DS-GVO)

k) erschwerende oder mildernde Umstände wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste

19.06.2019

ANHANG ZU FRAGE 1.13.

Beispiele für personenbezogene Daten:

Beschäftigtendaten:

Kontaktdaten von Beschäftigten, z.B.:

- Name
- Privatanschrift
- private Telefonnummer und E-Mail-Adresse
- Bankverbindung

lohnsteuerrelevante und/oder sozialversicherungsbezogene Angaben von Beschäftigten, z.B.:

- Familienstand
- Religionszugehörigkeit
- Geburtsdatum/Alter des Beschäftigten
- Krankenversicherungsnummer sowie weitere Angaben zur Krankenversicherung
- Rentenversicherungsnummer
- Gehalt und sonstige Vergütungsbestandteile einschließlich Boni, Sonderzulagen etc.

Personenbezogene Informationen zum Beschäftigungsverhältnis, z.B.:

- Personalnummer
- dienstliche Kontaktdaten (Telefonnummer, E-Mail-Adresse)
- Eintrittsdatum und Dauer der Betriebszugehörigkeit
- Grad bzw. sonstige Einstufungen in der betrieblichen Hierarchie
- Gehalt und Gehaltsentwicklung
- dienstliche Beurteilungen und alle Informationen, die Bestandteil und/oder Grundlage einer solchen Beurteilung sind
- Zeugnisse und Zwischenzeugnisse
- Lebensläufe, Informationen zum beruflichen Werdegang
- Informationen zu schulischen und berufsqualifizierenden Abschlüssen, Hochschulabschlüsse, sonstige Qualifikationsnachweise

- sonstige Informationen in der Personalakte
- Informationen über einen Beschäftigten, die z.B. im Rahmen eines Vetting-Prozesses erhoben werden (z.B. Führungszeugnis etc.)
- Krankmeldungen, Angaben zu Dauer und Zeitpunkt von Erkrankungen, Angaben zur Art der Erkrankung
- Informationen zu betrieblichen Wiedereingliederungsmaßnahmen

sonstige Angaben, z.B.:

- Kreditkartennummer (z.B. der Firmenkreditkarte oder einer privaten Kreditkarte, die in Dienstreiseabrechnungen relevant ist)
- Fotos (z.B. im Firmenintranet oder auf Firmenwebsite, Bewerbungsfotos in Personalakten)
- Angaben zur Gewerkschaftszugehörigkeit
- Angaben zu Mitgliedschaft in politischen Parteien
- Aufzeichnungen aus der Videoüberwachung
- Logging von Zutrittsanlagen (z.B. Speicherung der Zutritte von Beschäftigten über Vereinzelungsanlagen in das Gebäude, zu bestimmten Räumen)
- Log-In-Informationen zu betrieblichen Rechnern, mobilen Geräten etc.
- Informationen im Rahmen der Handhabung der Nutzung von E-Mail und Internet am Arbeitsplatz (arbeitgeberseitiger Zugriff auf deren Inhalte)

Informationen zu ehemaligen Beschäftigten, z.B.:

- Kontaktdaten
- Geburtsdatum
- Dauer Betriebszugehörigkeit, Datum des Ausscheiden etc.
- Rentenbezüge einschließlich Betriebsrenten/sonstige Altersleistungen des Arbeitgebers

<u>Daten von Dienstleistern und Lieferanten:</u>

Kontaktdaten der Ansprechpartner/Beschäftigten bei Dienstleistern, z.B.:

- Name, dienstliche Anschrift
- dienstliche Telefonnummer und E-Mail-Adresse der konkreten Person
- Stellung/Funktion des Ansprechpartners im Unternehmen des Dienstleisters

- Nachweise zu Qualifikationen und Zuverlässigkeit der beim Dienstleister mit der konkreten Aufgabe betrauten Personen (z.B. Zeugnisse, Angaben zu beruflichem Werdegang, aber auch Ergebnisse von Sicherheitsüberprüfungen wie Führungszeugnisse/Mitteilungen über den Inhalt von Führungszeugnissen, Ergebnisse von Mitarbeiter-Screenings, Selbstauskünfte)
- bei Dienstleistern, die im Haus der WPG beschäftigt sind bzw. Zutritt zu den Dienstgebäuden der WPG haben: Logging von Zutrittsanlagen (z.B. Speicherung der Zutritte der Dienstleister, Aufzeichnungen aus der Videoüberwachung etc.)

ggf. Kontaktdaten von Sub-Unternehmern der Dienstleister:

- Name, dienstliche Anschrift
- dienstliche Telefonnummer und E-Mail-Adresse der konkreten Person/Stellung/Funktion des Ansprechpartners im Unternehmen des Dienstleisters.

