EU-Datenschutz-Grundverordnung: Das müssen Sie wissen

Nach langen Verhandlungen erfolgte im Dezember 2015 die europäische Einigung auf eine **EU-Datenschutz-Grundverordnung (EU-DSGVO).** Diese wird zu einer weitgehenden Vereinheitlichung europäischen Datenschutzrechtes führen. Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie doch erhebliche Unterschiede bestanden, wird die Datenschutz-Grundverordnung direkt geltendes Recht in allen Mitgliedsstaaten sein. Geringe Unterschiede sind allenfalls durch die Möglichkeit sog. „Öffnungsklauseln“ zu erwarten. Öffnungsklauseln bieten nationalen Gesetzgebern die Möglichkeit, eigene nationale Regelungen zu erlassen.

Zeitplan der EU-Datenschutz-Grundverordnung

Bis zu der Anwendbarkeit sind noch einige Schritte erforderlich. Der Zeitplan sieht derzeit wie folgt aus:

- März 2016: offizielle deutsche Fassung der EU-DSGVO
- April 2016: Beratung des EU-Ministerrats, danach Abstimmung im Europäischen Parlament
- **25. Mai 2018: Anwendbarkeit der EU-Datenschutz-Grundverordnung**

Ziele und Grundsätze

Die Ziele der EU-DSGVO sind der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO (http://dsgvo-gesetz.de/art-1-dsgvo/)) und der freie Verkehr personenbezogener Daten (Art. 1 Abs. 3 DSGVO (http://dsgvo-gesetz.de/art-1-dsgvo/)).

Die vorangestellten Ziele sollen durch die in Art. 5 DSGVO (http://dsgvo-gesetz.de/art-5-dsgvo/) festgelegten Grundsätze der Verarbeitung personenbezogener Daten erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Die Datenschutz-Grundverordnung wird das europäische Datenschutzrecht nicht völlig umwälzen, weist aber eine Reihe von in der Praxis erheblichen

Sachlicher Anwendungsbereich: Die DSGVO gilt, wenn…

Gut ein Jahr vor dem Start der Datenschutz-Grundverordnung (DSGVO) sollten Sie wissen, unter welchen grundlegenden Voraussetzungen die DSGVO gilt. In zwei Teilen soll deshalb zunächst der sachliche und später auch der räumliche Anwendungsbereich der DSGVO dargestellt werden. Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Sachlicher Anwendungsbereich nach Art. 2 DSGVO

Ausgangspunkt für die Bestimmung des sachlichen Anwendungsbereichs ist Art. 2 Abs. 1 DSGVO: (https://dsgvo-gesetz.de/art-2-dsgvo/)

> *„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“.*

Grundsatz: Weiter sachlicher Anwendungsbereich zwingt zur Vorsicht

Nach Art. 2 Abs. 1 DSGVO kommt es darauf an, ob personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden oder ob bei einer nichtautomatisierten Verarbeitung eine Speicherung in einem Dateisystem erfolgen (soll). Hierzu ist es erforderlich, grundlegende Begriffe zu kennen. Dabei hilft Art. 4 DSGVO (https://dsgvo-gesetz.de/art-4-dsgvo/).

Wesentlich sind folgende Begriffe:

Personenbezogene Daten

Soweit keine personenbezogenen Daten betroffen sind, ist die Datenschutz-Grundverordnung nicht anzuwenden. Der Begriff der personenbezogenen Daten ist allerdings sehr weit gefasst (Art. 4 Nr. 1 DSGVO) und umfasst beispielsweise Informationen wie Name, Adresse, Telefonnummer, Autokennzeichen oder aber auch die IP-Adresse einer Person. Ausreichend ist es, wenn die Informationen einer Person lediglich irgendwie zugeordnet und damit ein Personenbezug hergestellt werden kann.

Automatisierte und nicht automatisierte Verarbeitung

Die DSGVO bezieht schließlich jede automatisierte Verarbeitung und jede nichtautomatisierte Verarbeitung bei Speicherung in einem Dateisystem mit ein.

Bei einer automatisierten Verarbeitung werden beispielsweise Computer, Smartphones, Kameras, Webcams, Dashcams, Scanner oder Kopierer erfasst. Jede Benutzung von Computer, Internet, E-Mail kann also zur Anwendbarkeit der Datenschutz-Grundverordnung führen, wenn personenbezogene Daten betroffen sind.

Eine nichtautomatisierte Verarbeitung liegt insbesondere bei handschriftlichen Aufzeichnungen vor.

Ein Dateisystem ist nach Art. 4 Nr. 6 DSGVO (https://dsgvo-gesetz.de/art-4-dsgvo/)

> *„(…) jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung, zentral, dezentral oder funktionalen oder geografischen Gesichtspunkten zugeordnet geführt wird. Damit sind etwa Akten, Aktensysteme oder Deckblätter erfasst“.*

Dass insbesondere bei handschriftlichen Aufzeichnungen noch ein weiter Anwendungsbereich der DSGVO angestrebt wurde, verdeutlicht die Formulierung „gespeichert werden sollen“ in Art. 2 Abs. 1 DSGVO. Hierbei reicht bereits die Absicht aus, dass personenbezogene Daten in ein Dateisystem aufgenommen werden. Wer etwa eine Aktenverwaltung plant, muss künftig vorsichtig sein.

Verarbeitung

Auch der Begriff der Verarbeitung wird definiert. Die Verarbeitung umfasst nach Art. 4 Nr. 2 DSGVO (https://dsgvo-gesetz.de/art-4-dsgvo/) dabei

> *(…) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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.*

Wenige Ausnahmen außerhalb des privaten und familiären Lebensbereichs

Nach Art. 2 Abs. 2 DSGVO findet die Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten, wenn

- die Tätigkeit nicht in den Anwendungsbereich des Unionsrechts fällt,
- im Rahmen von Tätigkeiten durch die Mitgliedstaaten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
- natürliche Personen ausschließlich persönliche oder familiäre Tätigkeiten ausüben oder
- die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit tätig werden – hierfür ist die neue Richtlinie 2016/680/EU maßgeblich.

Interessant ist, dass die Datenschutz-Grundverordnung nur wenige Ausnahmen zulässt. Unter den Ausnahmen ist regelmäßig nur diejenige interessant, die den privaten und familiären Lebensbereich ausnimmt. Hierunter fällt beispielsweise privater Schriftverkehr, ein privates Anschriftenverzeichnis oder die private Nutzung sozialer Netze und private Online-Tätigkeiten (vgl. Erwägungsgrund 18 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-18/)).

Etwas komplizierter ist darüber hinaus auch das Verhältnis zur sog. ePrivacy-Richtlinie zum Schutz der Vertraulichkeit und der Privatsphäre im Bereich der elektronischen Kommunikation (RL 2002/58/EG (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:de:PDF), vgl. auch §§ 91 ff. TKG (https://www.gesetze-im-internet.de/tkg_2004/__91.html)) ausgestaltet, das von Artikel 95 DSGVO (https://dsgvo-gesetz.de/art-95-dsgvo/) normiert wird.

Sonderbereiche

In Art. 2 Abs. 3 DSGVO wird die Datenverarbeitung durch Organe und Einrichtungen der Union geregelt, für die weiterhin die VO (EG) Nr. 45/2001 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:de:PDF) gilt.

Das Verhältnis zur Richtlinie über den elektronischen Geschäftsverkehr (sog. E-Commerce-Richtlinie, Richtlinie 2000/31/EG (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:DE:PDF)) bestimmt Art. 2 Abs. 4 DSGVO für die Verantwortlichkeit von Vermittlern, beispielsweise bei der reinen Durchleitung, beim Caching oder beim Hosting (vgl. §§ 7 ff. TMG (https://www.gesetze-im-internet.de/tmg/__7.html)).

Teilweise ist jedoch eine Überprüfung der rechtlichen Vorgaben des Datenschutzes durch die Kommission vorgesehen, um einen einheitlichen und kohärenten Datenschutz sicherzustellen (vgl. Art. 98 DSGVO (https://dsgvo-gesetz.de/art-98-dsgvo/)).

Räumlicher Anwendungsbereich: Wo gilt die DSGVO?

Mit Einführung der Datenschutzgrundverordnung (DSGVO) ergibt sich im Vergleich zur Datenschutzrichtlinie 95/46/EG ein deutlich weiterer räumlicher Anwendungsbereich, sodass sich die Frage stellt, wo die DSGVO gilt. Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/?utm_source=dsb&utm_medium=banner&utm_content=sidebar&utm_campaign=jede-seite). Gleichzeitig schließt sich der Artikel an unseren Fachbeitrag zum sachlichen Anwendungsbereich (https://www.datenschutzbeauftragter-info.de/sachlicher-anwendungsbereich-die-dsgvo-gilt-wenn/) der DSGVO an.

Räumlicher Anwendungsbereichs nach Art. 3 DSGVO

Ausgangspunkt für die Bestimmung des räumlichen Anwendungsbereichs ist Art. 3 DSGVO. (https://dsgvo-gesetz.de/art-3-dsgvo/)

Der räumliche Anwendungsbereich der DSGVO ergibt sich also grundsätzlich bei der Verarbeitung personenbezogenen Daten,

- soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet (Art. 3 Abs. 1 DSGVO).

Sofern die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter sattfindet, muss die Datenverarbeitung nach Art. 3 Abs. 2 DSGVO im Zusammenhang stehen damit, dass

- gegenüber betroffenen Personen in der Union Waren oder Dienstleistungen – unabhängig von einer Zahlungspflicht – angeboten werden oder
- das Verhalten betroffener Personen beobachten werden soll, soweit ihr Verhalten in der Union erfolgt.

Die DSGVO findet auch auf einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort Anwendung, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt (Art. 3 Abs. 3 DSGVO). Der räumliche Anwendungsbereich kann vertraglich nicht geändert werden. Eine Rechtswahlklausel ist damit nicht möglich. Hat ein Mitgliedstaat jedoch im Rahmen einer Öffnungsklausel eine nationale Datenschutzregelung

getroffen, ist grundsätzlich das Datenschutzrecht des jeweiligen Mitgliedstaats maßgeblich.

Niederlassung innerhalb der EU

Nach Art. 3 Abs. 1 DSGVO (https://dsgvo-gesetz.de/art-3-dsgvo/)ist zunächst das **Vorhandensein einer Niederlassung** in der Union maßgeblich, wobei der tatsächliche Ort der Datenverarbeitung unerheblich ist.

Hat der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung in der Union, ist die DSGVO räumlich anwendbar, wenn es sich um eine Niederlassung im Sinne von Art 3 Abs. 1 DSGVO handelt.

Ob eine Niederlassung im Sinne des von Art. 3 Abs. 1 DSGVO vorliegt, kann aus Erwägungsgrund 22 der DSGVO (https://dsgvo-gesetz.de/erwaegungsgruende/nr-22/) abgeleitet werden:

> *„Jede Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union sollte gemäß dieser Verordnung erfolgen, gleich, ob die Verarbeitung in oder außerhalb der Union stattfindet. Eine Niederlassung setzt die **effektive und tatsächliche Ausübung** einer Tätigkeit durch eine **feste Einrichtung** voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend.“*

Für eine Niederlassung ist demnach kennzeichnend, dass eine feste Einrichtung eine effektive und tatsächliche Ausübung einer Tätigkeit erlaubt. Die praktische Schwierigkeit liegt in der Feststellung, was hierunter im Einzelfall zu verstehen ist. Mitunter werden sogar interne Abteilungen innerhalb eines Unternehmens als „Niederlassung“ im rechtlichen Sinne betrachtet. Nach wie vor muss allerdings die Datenverarbeitung der Niederlassung „im Rahmen der Tätigkeit“ der Niederlassung erfolgen – die Datenverarbeitung muss demnach einen Bezug zur Niederlassung aufweisen. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend (vgl. hierzu Erwägungsgrund 22)

Niederlassung außerhalb der EU

Sofern innerhalb der EU keine Niederlassung vorhanden ist, ist Art. 3 Abs. 2 und Abs. 3 DSGVO (https://dsgvo-gesetz.de/art-3-dsgvo/) zu beachten.

Interessant ist hierbei zunächst, dass sich die Verarbeitung

personenbezogener Daten von betroffenen Personen nach Art. 3 Abs. 2 DSGVO im Gegensatz zu Art. 3 Abs. 1 DSGVO darauf beziehen muss, dass sich die betroffenen Personen örtlich innerhalb der Union befinden. Dabei reicht es aus, wenn sich die betroffenen Personen – auch nur kurzfristig – in der Union aufzuhalten. Auf die Staatsangehörigkeit oder den Status als Unionsbürger kommt es demnach nicht an.

Datenverarbeitung im Zusammenhang mit Angebot von Waren oder Dienstleistungen

Nach Art. 3 Abs. 2 lit. a) DSGVO muss die Datenverarbeitung im Zusammenhang damit stehen, dass der betroffenen Person in der Union Waren oder Dienstleistungen -unabhängig einer Zahlungspflicht- angeboten werden sollen. Ein konkretes Angebot ist damit nicht erforderlich.

Besonders interessant ist hierbei die Frage, wann Waren oder Dienstleistungen „in der Union“ angeboten werden. Nach Erwägungsgrund 23 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-23/) ist hierfür entscheidend, ob der Verantwortliche oder Auftragsverarbeiter das Anbieten von Waren bzw. Dienstleistungen in der Union „offensichtlich beabsichtigt“ hat:

> *„(…) Um festzustellen, ob dieser Verantwortliche oder Auftragsverarbeiter betroffenen Personen, die sich in der Union befinden, Waren oder Dienstleistungen anbietet, sollte festgestellt werden, ob der Verantwortliche oder Auftragsverarbeiter offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten (…).“*

Demnach muss sich aus dem Waren- bzw. Dienstleistungsangebot mit einer gewissen Eindeutigkeit ergeben, dass die Waren oder Dienstleistungen in der Union angeboten werden sollen. Ein Hinweis, dass etwaige Angebote nicht auf die Union gerichtet sind, soll aber genügen. Darüber hinaus soll es jedoch nicht ausreichend sein, dass die Webseite in der Union oder die Kontaktdaten innerhalb der Union abrufbar sind. Auch die verwendete Sprache bietet keine ausreichenden Anhaltspunkte für den Bezug zur Union. Letztlich bleibt vielmehr eine Gesamtschau notwendig, aus welcher sich die offensichtliche Absicht für das Anbieten von Waren oder Dienstleistungen innerhalb der Union ergibt.

Datenverarbeitung im Zusammenhang mit einer Verhaltensbeobachtung

Nach Art. 3 Abs. 2 lit. b) (https://dsgvo-gesetz.de/art-3-dsgvo/) ist die DSGVO auf diejenigen Verantwortlichen und Auftragsverarbeiter anzuwenden, die im Rahmen der Datenverarbeitung das Verhalten betroffener Personen innerhalb der Union beobachten. Grundsätzlich

werden hiervon nur Beobachtungen im Zusammenhang mit Internetaktivitäten, wie etwa das Profiling oder das Tracking erfasst (vgl. hierzu auch Erwägungsgrund 24 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-24/)):

> *„(…) Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.“*

Zu beachten ist dabei, dass jede Verhaltensbeobachtung zu einer Anwendung der DSGVO führt, wodurch insofern weltweit die Vorgaben DSGVO einzuhalten sind.

Räumlicher Anwendungsbereich aufgrund völkerrechtlicher Vorgaben

Schließlich kann die DSGVO auch dann anwendbar sein, wenn die Datenverarbeitung durch den Verantwortlichen an einem Ort erfolgt, der aufgrund des Völkerrechts dem Recht eines Mitgliedstaats unterliegt. Hierunter fallen etwa diplomatische oder konsularische Vertretungen eines Mitgliedstaats (Erwägungsgrund 25 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-25/)).

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/?utm_source=dsb&utm_medium=banner&utm_content=sidebar&utm_campaign=jede-seite).

Veröffentlicht am: 15. Mai 2017 | **Von** Dr. Datenschutz (https://www.datenschutzbeauftragter-info.de/ziel-und-inhalt-dieser-website/) | **Kategorie:** Fachbeitrag

Tags: Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/), europäische Datenschutzstandards (https://www.datenschutzbeauftragter-info.de/tag/europaeische-datenschutzstandards/), europäischer Datenschutz (https://www.datenschutzbeauftragter-info.de/tag/europaeischer-datenschutz/)

Datenschutz-Grundverordnung: Pflichten für Unternehmen

Die EU-Datenschutz-Grundverordnung statuiert neben altbekannten Pflichten auch neue Pflichten für Unternehmen im Bereich Datenschutz. Als erfreulich ist die Pflicht zu verbraucher- und datenschutzfreundlichen Voreinstellungen z. B. bei elektronischen Geräten einzuschätzen. Allerdings könnte vor allem die vorgesehene Pflicht zur Datenschutz-Folgenabschätzung sowie die sich daran evtl. anschließende Konsultation der zuständigen Aufsichtsbehörde zu noch nicht abschätzbaren (negativen) Auswirkungen und zu vermehrter Bürokratie führen. Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/?utm_source=dsb&utm_medium=banner&utm_content=sidebar&utm_campaign=jede-seite).

I. Technischer Datenschutz

Was versteht man unter den für die Verarbeitung Verantwortlichen nach Art. 24 EU-DSGVO?

Darunter fällt jede natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 4 Nr. 7 EU-DSGVO.

Wozu werden Unternehmen nach Art. 24 EU-DSGVO verpflichtet?

Unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten haben die für die Verarbeitung verantwortlichen Unternehmen **geeignete technische und organisatorische Maßnahmen** zu installieren.

Was bedeuten die Vorgaben des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen nach Art. 25 EU-DSGVO?

Der für die Verarbeitung Verantwortliche sollte interne Strategien festlegen und Maßnahmen treffen, die insbesondere dem Grundsatz des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default)

sicherstellen. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Datenverarbeitung zu überwachen, und der für die Verarbeitung Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern, vgl. Erwägungsgrund 61 EU-DSGVO.

Was sollte das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO beinhalten?

- Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen (ggf. auch Vertreter und Datenschutzbeauftragter)
- Zwecke der Verarbeitung
- Kategorien von betroffenen Personen und personenbezogenen Daten
- Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden (auch in Drittländern)
- Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation
- Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Näheres hierzu finden Sie in unserem Beitrag: Verzeichnis von Verarbeitungstätigkeiten – Infos & Tipps zur Umsetzung (https://www.datenschutzbeauftragter-info.de/verzeichnis-von-verarbeitungstaetigkeiten-infos-tipps-zur-umsetzung/)

Wann muss ich mit der Aufsichtsbehörde zusammenarbeiten?

Nach Art. 29 EU-DSGVO dann, wenn es die Aufsichtsbehörde zur Erfüllung ihrer Aufgaben verlangt.

II. Meldepflicht

Müssen Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemeldet werden?

Nach Art. 33 EU-DSGVO grundsätzlich ja.

Gilt die Meldepflicht ausnahmslos immer?

Nein. Es entsteht keine Meldepflicht, wenn ein Risiko für Rechte und Freiheiten von Individuen unwahrscheinlich ist.

Gibt es eine Frist für die Meldepflicht?

Ja, nach Art. 33 EU-DSGVO unverzüglich und ohne unangemessene Verzögerung. Möglichst binnen höchstens 72 Stunden, nachdem die Verletzung bekannt wurde.

Gilt die Meldepflicht auch für öffentliche Stellen?

Ja. Allerdings bleibt abzuwarten, wie der öffentlich-rechtliche Grundsatz der Polizeifestigkeit von Hoheitsträgern mit den Vorgaben der EU-Datenschutz-Grundverordnung in Einklang zu bringen ist. Zudem bleibt den Mitgliedstaaten in diesem Bereich ein großzügiger Handlungsspielraum durch nationale Regelungen.

Muss auch der Betroffene der Datenschutzverletzung benachrichtigt werden?

Nach Art. 34 EU-DSGVO grundsätzlich ja.

Muss der Betroffene nach Art. 34 EU-DSGVO ausnahmslos immer benachrichtigt werden?

Nein, der Betroffene muss nicht benachrichtigt werden, wenn technische oder organisatorische Maßnahmen wie z. B. eine Verschlüsselung die Kenntnisnahme von personenbezogenen Daten verhindern oder sichergestellt ist, dass kein hohes Risiko besteht.

Wie muss der Betroffene benachrichtigt werden?

Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten und so rasch wie nach allgemeinem Ermessen möglich geschehen, vgl. Erwägungsgrund 67a EU-DSGVO.

III. Datenschutz-Folgenabschätzung

Wann muss ein Unternehmen eine Datenschutz-Folgenabschätzung nach Art. 35 EU-DSGVO vornehmen?

Dann, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko verursacht, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke.

Was sind Beispiele für derartige neue Technologien?

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen aufgrund automatisierter Verarbeitung
- Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche

Verurteilungen und Straftaten

- Systematische weiträumige Überwachung öffentlich zugänglicher Bereiche

Wann muss die Aufsichtsbehörde konsultiert werden?

Nach Art. 36 EU-DSGVO dann, wenn die Datenschutz-Folgeabschätzung (https://www.datenschutzbeauftragter-info.de/datenschutz-folgenabschaetzung/) nach Art. 35 EU-DSGVO ergibt, dass eine Datenverarbeitung ohne Maßnahmen ein hohes Risiko bedeutet.

Sind die Aufsichtsbehörden auch schon vorab in die Datenschutz-Folgenabschätzung eingebunden?

Ja, sie werden vorab Positiv-/Negativ-Listen zu umfassten Technologien veröffentlichen.

Müssen auch die Betroffenen an der Datenschutz-Folgenabschätzung beteiligt werden?

Ja und zwar dann, wenn es als angemessen erscheint.

Was passiert, wenn die Aufsichtsbehörde der Auffassung ist, die Maßnahme verstoße gegen die EU-DSGVO?

Es erfolgt ein schriftlicher Rat der Aufsichtsbehörde mit einer Frist von acht Wochen.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/?utm_source=dsb&utm_medium=banner&utm_content=sidebar&utm_campaign=jede-seite).

Veröffentlicht am: 15. März 2016 | **Von** Dr. Datenschutz (https://www.datenschutzbeauftragter-info.de/ziel-und-inhalt-dieser-website/) | **Kategorie:** Fachbeitrag

Tags: Datenschutz (https://www.datenschutzbeauftragter-info.de/tag/datenschutz/), Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), Datenschutzverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutzverordnung/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/), EU-Verordnung (https://www.datenschutzbeauftragter-info.de/tag/eu-verordnung/), Unternehmen (https://www.datenschutzbeauftragter-info.de/tag/unternehmen/)

EU-Datenschutz-Grundverordnung: Neues zur Videoüberwachung?

Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/) und soll klären, ob und wenn welche Änderungen die ab Frühsommer 2018 geltende EU-Datenschutz-Grundverordnung (EU-DSGVO) für die **Zulässigkeit einer Videoüberwachung** hat.

Wie ist die bisherige Rechtslage?

Wir haben die Grundsätze zur Zulässigkeit von Videoüberwachung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/videoueberwachung-und-datenschutz/) bereits umfangreich dargestellt. Hier nochmals kurz die wesentlichen Eckpunkte:

Derzeit richtet sich die datenschutzrechtliche Zulässigkeit nach § 6b Bundesdatenschutzgesetz (BDSG). Demnach ist eine Videoüberwachung **nur zu bestimmten** – in § 6b BDSG aufgelisteten – **Zwecken zulässig**. Zudem muss auf die Überwachung mit Videokameras hingewiesen und die verantwortliche Stelle benannt werden. Weiter ist es so, dass zwischen dem reinen Monitoring / Beobachten und dem Speichern von Aufnahmen unterschieden wird. Letzteres bedarf einer besonderen Rechtfertigung und es müssen verbindliche Löschungsfristen für die Aufnahmen festgelegt werden. Zudem darf nur eine bestimmte Personengruppe Zugriff auf die Überwachungsbilder haben. Auch dies ist verbindlich festzulegen.

Alle diese Voraussetzungen werden derzeit in Rahmen einer stets erforderlichen **„Vorabkontrolle“** geprüft. Die Vorabkontrolle wird entweder durch die Aufsichtsbehörden oder den betrieblichen Datenschutzbeauftragten durchgeführt. Dies hat sich in der Praxis als wirksames Mittel gegen eine Ausuferung von Videoüberwachungen bewährt, da häufig noch durch Änderung des Kamerawinkelns oder Verpixelungsmöglichkeiten ein besserer **Schutz vor Eingriffen in Persönlichkeitsrechte** erreicht werden kann.

Welche Regelungen zur Videoüberwachung enthält die EU-DSGVO?

Im Gegensatz zum BDSG enthält die EU-Datenschutz-Grundverordnung keine konkrete Regelung zur Zulässigkeit von Videoüberwachung. Erwähnung findet diese lediglich in Artikel 35 EU-DSGVO. Dieser regelt die

Notwendigkeit einer sog. „**Datenschutz-Folgenabschätzung**“. Die Datenschutz-Folgenabschätzung ist wohl einer Vorabkontrolle gleichzustellen und soll in Konstellationen, in denen die Datenverarbeitung ein erhöhtes Eingriffspotential aufweist, den Schutz erhöhen.

Künftig geringere rechtliche Anforderungen an die Zulässigkeit?

Es besteht tatsächlich die Möglichkeit, dass **künftig geringere datenschutzrechtliche Anforderungen** an die **Zulässigkeit einer Videoüberwachung** gestellt werden. Jedenfalls lassen dies die „sparsamen“ Regelungen in der EU-DSGVO vermuten.

Während bislang stets eine Vorabkontrolle durchzuführen ist, kann dem Wortlaut der EU-Datenschutz-Grundverordnung entnommen werden, dass die Notwendigkeit einer Datenschutz-Folgenabschätzung nicht generell bei jeder Videoüberwachung erforderlich sein wird, sondern nur dann, wenn eine *„systematische“* und *„umfangreiche“* Überwachung stattfindet.

Unterscheidet die EU-DSGVO zwischen verschiedenen Arten der Videoüberwachung?

Was genau unter den Voraussetzungen *„systematisch“* und *„weiträumig“* zu verstehen ist, geht aus der EU-Datenschutz-Grundverordnung nicht hervor. Jedenfalls lassen die Begriffe einen erheblichen Interpretationsspielraum zu. Da mittlerweile praktisch jede Überwachung unter Einsatz automatisierter Verfahren vorgenommen wird, kann es aus Sicht des eingesetzten Verfahrens wohl keine „unsystematische“ Überwachung geben. Wegen der Verwendung dieses konkreten Begriffs, geht der europäische Gesetzgeber offensichtlich gleichwohl davon aus, dass nicht jede automatisierte Überwachung *„systematisch“* ist. Was hierunter jedoch genau zu verstehen ist, bleibt offen. Gleiches gilt für den Begriff *„weiträumig“*. Soll hier z.B. von der Größe der überwachten Fläche ausgegangen werden? Und falls ja: Wie groß muss diese Fläche sein?

Auch der Umkehrschluss ist interessant: Da die EU-DSGVO nur unter den vorbezeichneten Voraussetzungen eine Datenschutz-Folgenabschätzung für erforderlich hält, geht der europäische Gesetzgeber offenbar davon aus, dass nicht jede Videoüberwachung einen erheblichen Eingriff in die Rechte der Betroffenen darstellt. Dieser Wertung kann entnommen werden, dass die EU-Datenschutz-Grundverordnung bestimmte Formen der Videoüberwachung für nicht besonders risikobehaftet erachtet und diese Formen künftig leichter möglich sein werden.

Verdeckte oder offene Beobachtung – Hinweis auf Videoüberwachung?

Eine Videoüberwachung stellt einen erheblichen Eingriff in die

Persönlichkeitsrechte der Betroffenen dar. Als besonders intensiv wird der Eingriff erachtet, wenn eine diese verdeckt; also ohne Wissen des Betroffenen stattfinden könnte. Falls eine verdeckte und damit heimliche Überwachung möglich wäre, könnte sich faktisch niemand mehr sicher sein, ob er nicht gerade überwacht wird. Aus diesem Grund ist nach der derzeitigen Rechtslage die verdeckte Videoüberwachung von öffentlichen Räumen untersagt und § 6b Abs. 2 BDSG verlangt, dass über die Überwachung informiert und auf einem Hinweisschild auch die verantwortliche Stelle genannt wird.

In der EU-DSGVO fehlt eine derartige eindeutige Regelung. Es ist daher nach unserer Auffassung nicht ausgeschlossen, dass das Verbot der verdeckten Überwachung von öffentlichen Räumen daher – jedenfalls in gewissen Konstellationen – entfällt und eine verdeckte Überwachung auch öffentlicher Räume mit der Anwendbarkeit der EU-Datenschutz-Grundverordnung daher möglich wird.

Regelungen zur Videoüberwachung von Mitarbeitern?

Die Frage nach der Zulässigkeit von Videoüberwachung von Mitarbeitern / Arbeitnehmern ist eine der in der Praxis wichtigsten Fragen. Derzeit ist die Rechtslage zusammengefasst so:

- Am Arbeitsplatz ist – unter den Voraussetzungen des § 6b BDSG – eine offene Videoüberwachung möglich.
- In engen Ausnahmefällen ist auch eine verdeckte Videoüberwachung gestattet. Allerdings nur, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers vorliegen, weniger einschneidende Mittel müssen ausgeschöpft sind, die Videoüberwachung als einziges Mittel verbleibt und sie insgesamt **nicht unverhältnismäßig** ist.
- Sozialräume dürfen grundsätzlich nicht überwacht werden.

Aufgrund der hohen Praxisrelevanz wäre zu wünschen gewesen, dass die EU-DSGVO konkreten Regelungen zur Zulässigkeit einer **Videoüberwachung von Mitarbeitern** aufweist. In einer Entwurfsversion zu EU-DSGVO (http://www.europarl.europa.eu/sides /getDoc.do;jsessionid=5A20FB49505FBD792382AE8EF2F94F66.node2?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//en) waren solche konkreten Regelungen noch vorgesehen. Dort sollte in Artikel 82 EU-DSGVO ausdrücklich das Verbot zur Überwachung von Sozialräumen geregelt werden. Zudem war ein generelles Verbot einer verdeckten Videoüberwachung vorgesehen. In der nun verabschiedeten Fassung der EU-Datenschutz-Grundverordnung sind allerdings leider Regelungen zur Zulässigkeit einer Videoüberwachung von Arbeitnehmern nicht zu finden.

Das Fehlen von konkreten Regelungen ist deshalb so bedauerlich, weil die

Frage nach einer solchen Zulässigkeit für den Bereich des **Arbeitnehmerdatenschutz (https://www.datenschutzbeauftragter-info.de/fachbeitraege/arbeitnehmerdatenschutz/)** in der Praxis eine hohe Relevanz hat. Da im Spannungsfeld „Videoüberwachung von Mitarbeitern“ sich anerkennenswerte Interessen von Arbeitgebern und Mitarbeitern oft nahezu gleichrangig gegenüberstehen, wäre es hilfreich gewesen, hier klare gesetzliche Vorgaben zu schaffen.

Welchen Einfluss haben die Aufsichtsbehörden?

Eine abschließende Bewertung der Frage zu den künftigen datenschutzrechtlichen Anforderungen an die Zulässigkeit einer Videoüberwachung ist selbstverständlich zu diesem Zeitpunkt nicht möglich. Vielmehr wird man die Umsetzung in der Praxis abwarten müssen.

Eine erhebliche Rolle für deren Handhabung wird voraussichtlich den datenschutzrechtlichen Aufsichtsbehörden zufallen. Gemäß Artikel 35 Abs. 4 EU-DSGVO ist es Aufgabe der jeweiligen Aufsichtsbehörden eine Liste mit Datenverarbeitungsprozessen zu erstellen, die einer Datenschutz-Folgenabschätzung unterworfen werden müssen. Denkbar ist, dass hier die Begriffe *„systematisch“* und *„weiträumig“* in einer Form ausgelegt werden, die faktisch dann doch – wieder – dazu führen, dass faktisch jede Videoüberwachung einer besonderen Kontrolle unterliegt. Zwar ist es so, dass im Grundsatz die Aufsichtsbehörden nicht ermächtigt sind, Vorgaben zu definieren, die strengere Maßstäbe als die EU-DSGVO beinhalten. Da aber – wie dargestellt – die Voraussetzungen einen erheblichen Interpretationsspielraum bieten, verstößt eine enge Auslegung der Begriffe nicht per se gegen diesen Grundsatz.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Veröffentlicht am: 16. März 2016 | **Von** Dr. Datenschutz (https://www.datenschutzbeauftragter-info.de/ziel-und-inhalt-dieser-website/) | **Kategorie:** Fachbeitrag

Tags: Arbeitnehmerdatenschutz (https://www.datenschutzbeauftragter-info.de/tag/arbeitnehmerdatenschutz/), Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/), Mitarbeiter (https://www.datenschutzbeauftragter-info.de/tag/mitarbeiter/), Videokamera (https://www.datenschutzbeauftragter-info.de/tag/videokamera/), Videoüberwachung (https://www.datenschutzbeauftragter-info.de/tag/videoueberwachung/)

Auftragsdatenverarbeitung und Datenschutz-Grundverordnung

In der Datenschutz-Grundverordnung wird die Auftragsdatenverarbeitung europaweit einheitlich geregelt. Obwohl sich die neuen Regelungen inhaltlich an dem bekannten § 11 BDSG orientieren und diesen im Prinzip auf ein europäisches Level heben, sind einige Unterschiede zu beachten. Die Neuregelungen möchten wir nun einmal vorstellen. Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Was ist Auftragsdatenverarbeitung?

Die Auftragsdatenverarbeitung ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragnehmer gemäß den Weisungen der verantwortlichen Stelle (Auftraggeber) auf Grundlage eines schriftlichen Vertrags. Über die derzeit in § 11 BDSG geregelten Anforderungen können Sie sich hier informieren (https://www.datenschutzbeauftragter-info.de/fachbeitraege/auftragsdatenverarbeitung/). Eine entsprechende europaweite Vorschrift existiert bislang in Art 17 der Datenschutzrichtlinie nur ansatzweise. **Mit Art. 28 ff. EU-DSGVO erfährt nun auch die Auftragsdatenverarbeitung eine detaillierte gesetzliche Regelung**.

Was sind die grundsätzlichen Änderungen und Anforderungen?

Zunächst werden einige sprachliche Änderungen eingeführt. Die Verordnung spricht von Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen. Wie bisher ist eine vertragliche Regelung erforderlich, die nicht mehr ausschließlich schriftlich vorliegen muss sondern auch in einem elektronischen Format abgeschlossen werden kann.

Analog zu § 11 BDSG muss der Auftragsverarbeiter sorgfältig und unter besonderer Berücksichtigung der technischen und organisatorischen Maßnahmen ausgewählt werden. Wie bisher darf der Auftragsverarbeiter nach Art 29 EU-DSGVO die Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten. Verstößt der Auftragsverarbeiter dagegen, indem er z.B. Zwecke der Verarbeitung selbst bestimmt, wird er nach Art. 28 Abs. 10 EU-DSGVO selbst zum Verantwortlichen.

Neu ist, dass eine **Datenverarbeitung im Auftrag auch außerhalb der EU** stattfinden kann. Nach Art. 3 EU-DSGVO findet sie

> *„Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.“*

Was muss in einem Vertrag zur Auftragsdatenverarbeitung beachtet werden?

Auch die inhaltlichen Anforderungen an einen Vertrag zur Datenverarbeitung im Auftrag orientieren sich sehr stark an den in Deutschland bereits bekannten Punkten. Nach Art. 28 Abs. 3 EU-DSGVO sind zu regeln:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Wer ist für die Datenverarbeitung verantwortlich?

Grundsätzlich wird auch künftig der für die Verarbeitung Verantwortliche und nicht der Auftragsverarbeiter erster Ansprechpartner für Betroffene und für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich sein.

Die Datenverarbeitung im Auftrag muss insoweit von den in Art. 26 EU-DSGVO geregelten **gemeinsam für die Verarbeitung Verantwortlichen, der sog. „Joint Control“** unterschieden werden. Hierbei legen zwei oder mehrere Verantwortliche die Zwecke und Mittel zur Verarbeitung personenbezogener Daten gleichberechtig und gemeinsam transparent fest.

Bei diesem Modell, das dem BDSG unbekannt ist, kann der Betroffene seine Rechte gegenüber jedem für die Verarbeitung Verantwortlichen geltend machen.

Wer haftet bei Datenschutzverstößen?

Anders als im BDSG, wo gegenüber den Betroffenen nur eine Haftung des Auftraggebers auf Schadensersatz vorgesehen ist, finden sich in Art 82 EU-DSGVO insbesondere für Auftragsverarbeiter schärfere Haftungsregeln:

> *„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder moralischer Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.“*

Grundsätzlich haften der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter gegenüber dem Betroffenen gemeinsam. Jedoch beschränkt sich die Haftung des Auftragsverarbeiters auf Verstöße gegen speziell den Auftragsverarbeitern auferlegten Pflichten. Beiden Parteien steht die Möglichkeit der Exkulpation zur Verfügung. Dazu müssen sie nachweisen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind.

Welche besonderen Pflichten hat der für die Verarbeitung Verantwortliche?

Für deutsche Unternehmen, die Auftragsverarbeiter einsetzen, ergeben sich keine besonderen neuen Verpflichtungen, da die Regelungen der EU-DSGVO die derzeitigen Anforderungen des BDSG nahezu vollständig übernommen.

Welche besonderen Pflichten hat der Auftragsverarbeiter?

Für Auftragsverarbeiter werden künftig einige neue Regelungen und Pflichten zu beachten sein. Gemäß Art. 30 Abs. 2 DSGVO müssen auch Auftragsverarbeiter ein Verzeichnis über die Verarbeitungstätigkeiten führen, die sie für den für die Verarbeitung Verantwortlichen durchführen. Dieses Verzeichnis, das inhaltlich dem aus dem BDSG bekannten Verfahrensverzeichnis ähnelt, musste bislang nur von Auftraggebern geführt werden. Daneben bestehen die bekannten Meldepflichten aus dem BDSG grundsätzlich fort.

Welche Sanktionen drohen Unternehmen?

Bei Verstößen gegen die Verpflichtungen der Art. 28 ff. EU-DSGVO drohen

den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern nach Art. 83 EU-DSGVO **Geldbußen in Höhe von bis zu 10 Millionen Euro oder 2%** des gesamten weltweit erzielten Jahresumsatzes, je nachdem welcher Betrag höher ist. Dies ist eine empfindliche Verschärfung. Unternehmen sollten daher besonderes Augenmerk auf eine rechtskonforme Ausgestaltung legen.

Was sollten Unternehmen beachten?

Dazu sollten sie bereits in der Übergangsphase ihre **bestehenden Prozesse und Verträge zur Datenverarbeitung im Auftrag überprüfen und erforderliche Änderungen** vornehmen. Neu abzuschließende Verträge sollten dann bereits die künftige Rechtslage berücksichtigen.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Veröffentlicht am: 17. März 2016 | **Autor:** Felix Hudy (https://www.datenschutzbeauftragter-info.de/author/fhudy/) | **Kategorie:** Fachbeitrag

Tags: § 11 BDSG (https://www.datenschutzbeauftragter-info.de/tag/11-bdsg/), Auftragsdatenverarbeitung (https://www.datenschutzbeauftragter-info.de/tag/auftragsdatenverarbeitung/), Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/)

Wartungsarbeiten – Ist das eine Auftragsverarbeitung nach der DSGVO?

Das (unbeliebte) Thema Auftragsdatenverarbeitung ist aus dem Alltag eines Datenschutzbeauftragten nicht wegzudenken. Häufig ist es sehr mühsam, die Dienstleister davon zu überzeugen, dass zusätzlich zu bzw. statt einer Geheimhaltungsvereinbarung eine Vereinbarung zur Auftragsdatenverarbeitung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/auftragsdatenverarbeitung/) i.S.d. § 11 BDSG abzuschließen ist. Insbesondere Dienstleister, die lediglich Wartungsarbeiten an einem Tool durchführen und dabei den Zugriff auf personenbezogenen Daten des Auftraggebers gar nicht benötigen, stellen sich quer. Dieser Artikel ist Teil unserer Reihe zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

(Noch) Aktuelle Rechtslage

Gemäß § 11 BDSG (https://www.gesetze-im-internet.de/bdsg_1990/__11.html) hat der Auftraggeber mit dem Auftragnehmer, der in seinem Auftrag personenbezogenen Daten erhebt, verarbeitet oder nutzt, eine Vereinbarung zur Auftragsdatenverarbeitung abzuschließen (kurz ADV). Nach § 11 Abs. 5 BDSG gilt dies auch für die Fälle, in denen der Dienstleister lediglich mit der Prüfung oder Wartung automatisierter Verfahren (diverse Tools) oder von Datenverarbeitungsanlagen (z.B. Server) beauftragt wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Das heißt, dass nach dem BDSG mit dem Anbieter einer Software auch dann eine ADV abzuschließen ist, wenn dieser nur gelegentlich per Fernwartung oder dann vor Ort technische Fehler der Software behebt. In der Regel hat der Dienstleister überhaupt kein Interesse auf die personenbezogenen Daten zuzugreifen, da er diese für die Behebung der Fehler gar nicht braucht. Um eine Auftragsdatenverarbeitung wird er trotzdem nicht herumkommen.

Am 25. Mai 2018 wird das BDSG durch die Datenschutz-Grundverordnung (DSGVO) (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/) abgelöst.

Wartungsarbeiten auch nach der DSGVO eine Auftragsverarbeitung?

Diese Frage ist schon jetzt bei den Juristen umstritten. Einigkeit besteht

lediglich darin, dass die DSGVO im Gegensatz zu BDSG keine Sonderregelung für die Wartung oder Prüfung von automatischen Verfahren enthält.

1. Auffassung: Es liegt eine Auftragsverarbeitung vor, Art. 28 DSGVO findet direkte Anwendung

Schmidt/Freund in ZD 2017, 14 (16) sind der Ansicht, dass es bei der Systemverwaltung unproblematisch um eine Auftragsverarbeitung nach Art. 28 DSGVO (https://dsgvo-gesetz.de/art-28-dsgvo/) vorliegt:

> *„Die Regelungen des Art. 28 DSGVO sind direkt auf die Systemwartung anzuwenden. Bei der Systemwartung erhält der Dienstleister in der Regel die Möglichkeit, auf personenbezogenen Daten zuzugreifen. Es handelt sich dabei um eine Verarbeitung i.S.d. Art. 4 Nr. 4 DSGVO. Ob Systemverwaltung dabei eine Offenlegung „durch Übermittlung“, „Verarbeitung“ oder „eine andere Form der Bereitstellung“ ist, kann als akademische Frage offen bleiben.*
>
> *All dies sind nach Art. 4 Nr. 2 DSGVO (https://dsgvo-gesetz.de /art-4-dsgvo/) aber nur Beispiele für die eigentliche Definition der Verarbeitung als „Vorgang … im Zusammengang mit personenbezogenen Daten“. Diese Definition erfüllt die Wartung eines IT-Systems in jedem Fall. Die Verarbeitung der personenbezogenen Daten erfolgt auch im Auftrag des Verantwortlichen. Auch nach dem gesetzlichen Schutzzweck kann ein solcher Vorgang nicht dem Anwendungsbereich der DSGVO entzogen werden, sofern er mit einer Zugriffsmöglichkeit auf die personenbezogenen Daten und damit mit einer Gefahr für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden ist.*
>
> *Diese Verarbeitung erfolgt auch im Auftrag des Verantwortlichen. Es handelt sich damit um einen Fall der Auftragsverarbeitung gem. Art. 28 Abs. 1 DSGVO, die unter den Voraussetzungen des Art. 28 DSGVO zulässig ist.“*

Müthlein in RDV 2016, 74 (83) ist der Auffassung, dass die Regelungen über die Auftragsverarbeitung in Art. 28 DSGVO analog anzuwenden sind.

2. Auffassung: Es liegt eine Auftragsverarbeitung vor, Art. 28 DSGVO findet analoge Anwendung

Müthlein in RDV 2016, 74 (83) ist der Auffassung, dass die Regelungen über die Auftragsverarbeitung in Art. 28 DSGVO analog anzuwenden sind, da DSGVO eine der § 11 Abs. 5 BDSG vergleichbare Regelung nicht enthält.

3. Auffassung: Keine Auftragsverarbeitung nach Art. 28 DSGVO

Lissner im Tagungsband der Herbstakademie der DSRI 2016, 401 (414) stellt es auf den Willensmoment des Dienstleisters an:

> *„Die DSGVO enthält im Vergleich zum BDSG einen deutlich weiter gefassten Begriff der Datenverarbeitung. Mit Art. 4 Nr. 2 DSGVO bezeichnet der Ausdruck „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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.*
>
> *Die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen zielt nicht auf eine „Datenverarbeitung“ ab – die Möglichkeit, Daten zur Kenntnis zu nehmen, ist vielmehr nur ein – nicht auszuschließendes – „Beiwerk“. Trotz der deutlich weiter gefassten Definition des Verarbeitungsbegriffs der DSGVO dürfte es schwer fallen, derartige Konstellationen unter den Begriff der „Verarbeitung“ zu subsumieren. Die bloße Möglichkeit der Kenntnisnahme könnte allenfalls als „Offenlegung durch Verbreitung oder eine andere Form der Bereitstellung“ oder als „Auslesen“ eingestuft werden. Diese Begriffe setzten jedoch rein vom Wortlaut her allesamt ein Willensmoment auf Seitens des Verarbeiters voraus – dies liegt im Falle eines Vertrags zur Prüfung oder Wartung automatisierter Verfahren und Datenverarbeitungsanlagen jedoch gerade nicht vor, da ein solcher Zugriff nicht beabsichtigt ist. Die besseren Gründe sprechen daher wohl dafür, derartige Konstellationen zukünftig nicht mehr unter die Vorgaben der Auftragsverarbeitung zu fassen. Ein Schutzdefizit auf Seiten der Betroffenen sollte damit nicht verbunden sein, da ein Dienstleister, der sich unbefugt Zugriff auf personenbezogene Daten verschafft, als „verantwortliche Stelle“ einzustufen sein dürfte.“*

4. Auffassung: Es liegt eine Übermittlung vor, sodass eine Rechtsgrundlage erforderlich ist

Es könnte auch überlegt werden, ob die Wartung oder Prüfung von Soft- oder Hardwaresystemen künftig als datenschutzrechtlich rechtfertigungsbedürftiger Vorgang anzusehen ist. Als Folge bräuchte man für die Tätigkeit der Dienstleister eine Rechtsgrundlage, da dieser selbst zum Verantwortlichen in Sinne der DSGVO wird. Als Rechtsgrundlage für die Wartung oder Prüfung von Soft- oder Hardwaresystemen könnte Art. 6 Abs. 1 f) DSGVO (https://dsgvo-gesetz.de/art-6-dsgvo/) in Betracht kommen. Danach ist die Verarbeitung von personenbezogenen Daten zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und keine Interessen und Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen.

Stellungnahme

Bei der Wartung und Prüfung von Soft- oder Hardwaresystemen handelt es sich um keine Auftragsverarbeitung nach Art. 28 DSGVO. Diese Hilfstätigkeit bzw. technische Unterstützung betrifft im Kern nicht die Verarbeitung der

personenbezogenen Daten. Vielmehr ist eine Verarbeitung von personenbezogenen Daten von den Parteien gar nicht gewollt. Daher kann auch nicht von einer Datenverarbeitung nach Weisungen gesprochen werden. Dem Recht auf informationelle Selbstbestimmung der betroffenen Personen wird genüge getan, wenn mit den Wartungs- und Prüfungsdienstleistern ordentliche Dienstleistungsverträge abgeschlossen werden. Im Dienstleistungsvertrag muss insbesondere die Art und der Umfang von Wartungsarbeiten geregelt werden, einschließlich der jeweiligen Auslöser von Wartungsaktivitäten, der Informationswege zur Bestellung, der Durchführung und Abrechnung der Wartung sowie der Protokollierung der Wartungsaktivitäten. Wichtig ist zudem, dass eine Vertraulichkeitsvereinbarung abgeschlossen wird, die sich auf alle Arten der Daten bezieht. Hält sich der Dienstleister nicht an die vertraglichen Vorgaben, haftet er für seine unrechtmäßige Handlung wie ein Verantwortlicher.

Wie ist Ihre Meinung?

Ihre Meinung bzw. Rechtsauffassung ist gefragt! Was meinen Sie, sollten die Dienstleister im Bereich der Wartung und Pflege von Soft- und Hardware unter Art. 28 DSGVO fallen? Wir freuen uns auf Ihren Kommentar.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Veröffentlicht am: 23. Januar 2017 | **Autor:** Katrin Rammo (https://www.datenschutzbeauftragter-info.de/author/krammo/) | **Kategorie:** Fachbeitrag

Tags: Art. 28 DSGVO (https://www.datenschutzbeauftragter-info.de/tag/art-28-dsgvo/), Auftragsdatenverarbeitung (https://www.datenschutzbeauftragter-info.de/tag/auftragsdatenverarbeitung/), Auftragsverarbeitung (https://www.datenschutzbeauftragter-info.de/tag/auftragsverarbeitung/), Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/), Fernwartung (https://www.datenschutzbeauftragter-info.de/tag/fernwartung/), IT-Systeme (https://www.datenschutzbeauftragter-info.de/tag/it-systeme/)

Datenschutz-Grundverordnung (DSGVO) – Datenschutzbeauftragter

Ein betrieblicher Datenschutzbeauftragter muss mit dem in Kraft treten der Datenschutz-Grundverordnung (DSGVO) europaweit spätestens bis Mai 2018 von Unternehmen bestellt werden, deren Tätigkeit einer besonderen Kontrolle bedarf (Art. 35 ff. DSGVO). Damit schafft die DSGVO eine Funktion, die vielerorts unbekannt ist. Dieser Artikel ist Teil unserer Reihe zur Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Bestellung eines Datenschutzbeauftragten

Wann besteht eine Bestellpflicht nach der Datenschutz-Grundverordnung?

Ab 2018 gilt die Datenschutz-Grundverordnung und es wird erstmals eine europaweit geltende Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten geben (Art. 35 ff. DSGVO). Diese ist bindend sofern ein Unternehmen einer Tätigkeit nachgeht, die aus datenschutzrechtlicher Sicht einer besonderen Kontrolle bedarf. Darüber hinaus kann jedes Unternehmen einen Datenschutzbeauftragten freiwillig bestellen.

Nach Art. 37 Abs. 1 DSGVO (https://dsgvo-gesetz.de/art-37-dsgvo/) ist ein betrieblicher Datenschutzbeauftragter unter bestimmten Bedingungen zu benennen:

> *„(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn […]*
>
> *b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder*
>
> *c) die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangsreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.“*

Stellungnahme der Artikel 29 Datenschutzgruppe zur „Kerntätigkeit“

Mittels der am 13. Dezember 2016 veröffentlichten Stellungnahme der Artikel 29 Gruppe (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf) gibt es bereits erste Klarstellungen was unter „Kerntätigkeit“ i.S.d. Art. 37 Abs. 1 b DSGVO zu verstehen ist. Im Zusammenhang mit Erwägungsgrund 97 (https://dsgvo-gesetz.de/erwaegungsgruende/nr-97/), ist hierunter demnach jede Tätigkeit zu verstehen, die essentiell für die Erreichung der Ziele des Unternehmens sind. Als Beispiel sei hier die Verarbeitung von Gesundheitsdaten in einem Krankenhaus genannt. Weitere finden Sie in der Stellungnahme sowie in den FAQs (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf).

Ziffer b) dürfte dabei insbesondere für Unternehmen, deren Kerngeschäft der Handel mit personenbezogenen Daten ist („Daten als Ware“), Auskunfteien oder Adresshändler gelten. Hierzu führt die Artikel 29 Gruppe einige Faktoren auf, die maßgeblich für das Merkmal „umfangreiche Verarbeitung“ i.S.d. Ziffern b) und c) sind:

- die Anzahl der Betroffenen
- die Menge der betroffenen Daten und/oder die Vielzahl der verschiedenen Datensätze
- die Dauer der Datenverarbeitung
- die geographische Reichweite der Datenverarbeitung.

Auch hier werden zahlreiche Beispiele zur Verdeutlichung genannt, u.a. die Verarbeitung von Gesundheitsdaten in einem Krankenhaus oder die Verarbeitung von personenbezogenen Daten für Werbezwecke durch Suchmaschinen für Verhaltensbedingte Werbevorschläge.

Unter Berücksichtigung von Erwägungsgrund 24 (https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-und-der-one-stop-shop/) kann man unter dem Merkmal „umfangreiche regelmäßige und systematische Überwachung“ alle Arten des Internettrackings und – profilings verstehen.

Welchen Einfluss haben Öffnungsklauseln für EU-Mitgliedstaaten?

Darüber hinaus gibt die DSGVO den EU-Mitgliedstaaten die Möglichkeit, nationale Sonderregelungen in Bezug auf die Bestellung eines betrieblichen Datenschutzbeauftragten zu schaffen. Ob und inwiefern die einzelnen EU-Mitgliedstaaten von dieser sog. Öffnungsklausel Gebrauch machen werden, ist noch nicht abschließend geklärt. Deutschland hat sich jedoch bereits als Befürworter ausgesprochen (https://www.gdd.de/aktuelles/startseite/news/copy_of_politische-einigung-im-trilog-zur-datenschutz-grundverordnung) und möchte ein ähnliches System, wie das bisherige,

weiterführen. Es wird erwartet, dass sich die zukünftige deutsche Regelung inhaltlich an der Bestellpflicht von § 4 f Abs. 1 BDSG orientieren (https://www.datenschutzbeauftragter-info.de/betrieblicher-datenschutzbeauftragter-wie-erfolgt-die-bestellung/) wird.

Ist weiterhin eine schriftliche Bestellung erforderlich?

Auch hier gibt es weitreichende Unterschiede zum bisherigen Verfahren. Bis dato muss nach dem BDSG ein betrieblicher Datenschutzbeauftragter schriftlich bestellt werden (vgl. § 4 f Abs. 1 S. 1 BDSG).

Der Wortlaut der Datenschutz-Grundverordnung spricht nur noch von einer „Benennung“ des Datenschutzbeauftragten. Eine tatsächliche schriftliche Bestellung ist nicht mehr erforderlich. Allerdings sieht die DSGVO in Art. 37 Abs. 7 vor, dass

> *„Der Verantwortliche oder der Auftragsverarbeiter […] die Kontaktdaten des Datenschutzbeauftragten [veröffentlicht] und […] diese Daten der Aufsichtsbehörde mit[teilt]“*

Die DSGVO erfordert zukünftig also die Benennung eines Datenschutzbeauftragten und die Mitteilung an die Aufsichtsbehörden, sofern eine „Benennungspflicht“ besteht.

Zwar ist es nach der Artikel 29 Gruppe hierfür ausreichend, dass den Betroffenen und/oder den Aufsichtsbehörden die Kontaktdaten des Datenschutzbeauftragten gegeben werden, die für eine Kontaktaufnahme „erforderlich“ sind und eine leichte Kommunikation ermöglichen – mithin also Anschrift, Telefonnummer und E-Mail. Es ist jedoch empfehlenswert, der Aufsichtsbehörde und den Mitarbeitern eines Unternehmens die konkreten Kontaktdaten des Datenschutzbeauftragten mitzuteilen. Auf der Webseite eines Unternehmens sei es hingegen ausreichend, wenn man beispielsweise eine Hotline oder spezifische Kontaktdaten veröffentlicht. Nicht erforderlich ist die Kundgabe des Namens des Datenschutzbeauftragten.

Ob das bisherige Schriftlichkeitserfordernis in Deutschland in Zukunft Bestand hat, hängt von der kommenden Sonderregelung in Bezug auf die Bestellung eines betrieblichen Datenschutzbeauftragten in Deutschland ab.

Kann ein Konzerndatenschutzbeauftragter bestellt werden?

Die Funktion eines Konzerndatenschutzbeauftragten ist dem BDSG unbekannt; gleichwohl untersagt das Gesetz die Bestellung eines solchen nicht. Die EU-Datenschutz-Grundverordnung nimmt hierzu hingegen klar in Art. 37 Abs. 2 DSGVO Stellung:

> *„Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.“*

Gehören zu einem Konzern auch Gesellschaften außerhalb der EU, sollte der Datenschutzbeauftragte seinen Sitz in einer konzernangehörigen Gesellschaft in der EU haben, um die leichte Erreichbarkeit zu gewährleisten.

Dies ist zwar keine zwingende Voraussetzung. Dennoch sollte der Datenschutzbeauftrage möglichst leicht für Aufsichtsbehörden, externe Betroffene und Mitarbeiter erreichbar sein. Ob dies bei einem Sitz in einer konzernangehörigen Gesellschaft außerhalb der EU effektiv gewährleistet werden kann, ist trotz der heutigen Technologien (E-Mail, Internet, Telefone) fragwürdig, aber jedoch nicht ausgeschlossen. Jedes Unternehmen sollte sich mit den Möglichkeiten auseinandersetzen.

Auch Behörden und öffentlich Stellen können zukünftig einen gemeinsamen Datenschutzbeauftragten bestellen (Absatz 3).

Interner oder externer Datenschutzbeauftragter?

Grundsätzlich kann ein Unternehmen wählen, ob die Position des betrieblichen Datenschutzbeauftragten intern oder extern besetzt wird. Viele Unternehmen bedienen sich heutzutage der Möglichkeit einen externen Datenschutzbeauftragten zu bestellen, um ihre eigenen internen Ressourcen besser nutzen zu können und von den Vorteilen des spezifischen Fachwissens eines externen Datenschutzbeauftragten zu profitieren.

Diese Möglichkeit regelt die Datenschutz-Grundverordnung nunmehr ebenfalls explizit in Art. 37 Abs. 6 DSGVO. Ein Unternehmen sollte daher die Vor- und Nachteile eines internen bzw. externen Datenschutzbeauftragten genau abwägen.

Welche Sanktionen drohen bei fehlender Bestellung eines Datenschutzbeauftragten?

Die vorsätzliche oder fahrlässige Versäumnis einen betrieblichen Datenschutzbeauftragten zu bestellen, diesen nicht in der vorgeschrieben Weise oder nicht rechtzeitig zu bestellen, stellt gemäß § 43 Abs. 1 Nr. 2 BDSG bereits heute eine Ordnungswidrigkeit dar, die mit einem Bußgeld in Höhe von bis zu 50.000 € belegt werden kann.

Die Datenschutz-Grundverordnung teilt diese Auffassung und sieht ein Bußgeld (https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-bussgelder-und-sanktionen/) von bis zu 10 Mio € oder 2 %

des weltweiten Jahresumsatzes vor, je nachdem, welcher Betrag höher ist (vgl. Art. 83 Abs. 4 lit. A DSGVO).

Anforderungen an einen Datenschutzbeauftragten

Welche Kriterien muss ein Datenschutzbeauftragter erfüllen?

Unabhängig davon ob sich ein Unternehmen für einen internen oder externen Datenschutzbeauftragten entschieden hat, sollte die auserwählte Person gewisse Anforderungen erfüllen, um das Unternehmen bei der Umsetzung etwaiger Datenschutzregelungen gezielt unterstützen zu können.

Die Datenschutz-Grundverordnung (Art. 37 Abs. 5 DSGVO) tut es hinsichtlich der Anforderungen an einen betrieblichen Datenschutzbeauftragten dem BDSG (§ 4f Abs. 2 S. 1 und 2 BDSG) gleich und fordert

- eine gewisse berufliche Qualifikation,
- das Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis und
- die Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben.

Durch stetige Neuentwicklungen werden Datenschutzbeauftragte ständig gefordert, so dass eine stete Weiterbildung im IT- und juristischen Bereich unerlässlich ist, um den immer komplexeren Fragestellungen gerecht werden zu können. Die Komplexität der Fragestellung wird dabei nicht nur durch technologische Neuentwicklungen, sondern auch durch die Komplexität der Datenverarbeitung und Größe des Betriebs definiert. Spätestens mit der Anwendbarkeit der noch komplexeren DSGVO sollte der Faktor der juristischen Qualifikation eines betrieblichen Datenschutzbeauftragten nicht unterschätzt werden, auch wenn grundsätzlich jedermann Datenschutzbeauftragter sein kann.

Darf wirklich „jedermann“ Datenschutzbeauftragter werden?

Unternehmen sollten jedoch auch darauf achten, dass kein Interessenskonflikt entsteht. Dies kann theoretisch hauptsächlich bei internen Datenschutzbeauftragten der Fall sein. Interessenkonflikte entstehen insbesondere dann, wenn der designierte Datenschutzbeauftragte zusätzlich einer anderen Tätigkeit nachgeht, was ihm grundsätzlich auch gestattet ist, und sich dann u.U. selbst kontrollieren muss. Dies wird insbesondere bei Mitarbeitern der IT-Abteilung, Personalabteilung und der Geschäftsführung angenommen. Auch die DSGVO nimmt diesen Punkt in Art. 38 Abs. 6 BDSG ausdrücklich mit auf.

Ist die Unabhängigkeit des Datenschutzbeauftragten weiterhin gewährleistet?

Ja. Auch die Datenschutz-Grundverordnung stellt in Art. 38 Abs. 3 S. 1 die Weisungsfreiheit des betrieblichen Datenschutzbeauftragten sicher.

Auch zukünftig berichtet der betriebliche Datenschutzbeauftragte der Geschäftsleitung und ist gemäß Art. 38 Abs. 3 S. 3 DSGVO unmittelbar der höchsten Managementebene unterstellt, sofern es keine näheren Bestimmungen in nationalen Sonderregelungen gibt. Der Datenschutzbeauftragte hat auch weiterhin keine Entscheidungsbefugnis, sondern berät das Unternehmen lediglich im Rahmen seiner Aufgaben nach Art. 39 DSGVO

Datenschutzbeauftragter – Benachteiligungsverbot und Haftung

Nach Art. 38 Abs. 3 S. 3 DSGVO darf der betriebliche Datenschutzbeauftragte wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Hingegen findet man in der Datenschutz-Grundverordnung keinerlei Anhaltspunkte für einen Sonderkündigungsschutz, wie er derzeit in § 4f Abs. 3 S. 5 und 6 BDSG geregelt ist. Die in Art. 37 Abs. 4 DSGVO verankerte Öffnungsklausel zum Datenschutzbeauftragten findet hingegen keinerlei Anwendung auf das Benachteiligungsverbot.

Die mögliche persönliche Haftung des Datenschutzbeauftragten (https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-aufgaben-des-datenschutzbeauftragten/) bei Nichtbeachtung der Regelungen der DSGVO durch das Unternehmen oder bei Verstößen ist seit der Veröffentlichung der DSGVO sehr umstritten. Die Artikel 29 Gruppe stellt mit ihrer Stellungnahme vom 13. Dezember 2016 zwar eindeutig klar, dass das Unternehmen – ob Verantwortlicher oder Auftragsverarbeiter – selbst für die Einhaltung der Regelungen nach Artikel 24 Abs. 1 DSGVO verantwortlich ist. Trotzdem haftet der Datenschutzbeauftragte in seinem Verantwortungsbereich für Datenschutzverletzungen.

Welche Aufgaben und Pflichten hat ein Datenschutzbeauftragter nach der DSGVO?

Die Aufgaben und Pflichten eines betrieblichen Datenschutzbeauftragten sind in Art. 39 DSGVO geregelt und umfassen:

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten
- Überwachung der Einhaltung der DSGVO und nationalen Sonderregelungen
- Sensibilisierung und Schulung
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-

Folgenabschätzung (https://www.datenschutzbeauftragter-info.de/datenschutz-folgenabschaetzung/)

- Zusammenarbeit mit der Aufsichtsbehörde

Grundsätzlich bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften das Unternehmen selbst verantwortlich; der betriebliche Datenschutzbeauftragte wirkt insofern weiterhin in ausreichendem Maße auf die Einhaltung hin. Die Aufgaben ähneln denen aus dem BDSG bekannten sehr.

Um diesen Aufgaben und Pflichten nachkommen zu können, regelt die Datenschutz-Grundverordnung explizit, dass der Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ einzubinden ist (vgl. Art. 38 Abs. 1 DSGVO).

Was sollten Unternehmen jetzt tun?

Grundsätzlich empfiehlt es sich jedoch unabhängig von einer etwaigen Bestellpflicht einen betrieblichen Datenschutzbeauftragten zu bestellen, um so die Umsetzung der Datenschutz-Grundverordnung in ihrem Unternehmen auf die effektivste Weise voran zu treiben und startklar für Mai 2018 zu sein. Diese Empfehlung spricht auch die Artikel 29 Gruppe aus.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/).

Veröffentlicht am: 28. Juni 2016 | **Autor:** Cornelia M. Schmitt (https://www.datenschutzbeauftragter-info.de/author/cschmitt/) | **Kategorie:** Fachbeitrag

Tags: Bestellung (https://www.datenschutzbeauftragter-info.de/tag/bestellung/), Betrieblicher Datenschutzbeauftragter (https://www.datenschutzbeauftragter-info.de/tag/betrieblicher-datenschutzbeauftragter/), Datenschutzbeauftragter (https://www.datenschutzbeauftragter-info.de/tag/datenschutzbeauftragter/), EU-DSGVO (https://www.datenschutzbeauftragter-info.de/tag/eu-dsgvo/), Fachkunde (https://www.datenschutzbeauftragter-info.de/tag/fachkunde/), Konzerndatenschutz (https://www.datenschutzbeauftragter-info.de/tag/konzerndatenschutz/), Konzerndatenschutzbeauftragter (https://www.datenschutzbeauftragter-info.de/tag/konzerndatenschutzbeauftragter/), Zuverlässigkeit (https://www.datenschutzbeauftragter-info.de/tag/zuverlaessigkeit/)

Datenschutz-Grundverordnung und Datensicherheit

Im Zuge der **Datenschutz-Grundverordnung** (DSGVO) wurden auch die Bestimmungen zur **Datensicherheit** und damit zu den technischen und organisatorischen Maßnahmen überarbeitet. Welche Änderungen bei der „Sicherheit der Verarbeitung“ auf die Unternehmen und Verantwortlichen zukommen, wird in dem folgenden Artikel erklärt, der ein Teil unserer Reihe zur Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/) ist.

Wie ist die Datensicherheit in der Datenschutz-Grundverordnung verankert?

Die neuen Vorgaben für die „Sicherheit der Verarbeitung“ finden sich hauptsächlich in Art. 5 Abs. 1 f) DSGVO sowie in Art. 32 DSGVO. Zudem normieren weitere Bestimmungen wie z.B. Art. 24, 25, 36 DSGVO die Datensicherheit.

Wie sind die technischen und organisatorischen Maßnahmen geregelt?

§ 9 BDSG inklusive Anlage wird durch Art. 32 DSGVO ersetzt. In dieser Bestimmung finden sich Anhaltspunkte zur Umsetzung technischer und organisatorischer Maßnahmen und damit der Datensicherheit. Im ersten Absatz heißt es:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; …“*

Dabei ist die Beschreibung noch abstrakter als derzeit in § 9 BDSG geregelt. Denn konkrete Maßnahmen, wie in der Anlage zu § 9 BDSG aufgezählt, werden in Art. 32 Abs. 1 DSGVO (außer der Pseudonymisierung und Verschlüsselung) nicht genannt. Eine Aufzählung von Maßnahmen findet sich allerdings in § 58 Abs. 3 des Referentenentwurfes für das deutsche Ausführungsgesetz zur Datenschutz-Grundverordnung (https://www.datenschutzverein.de/wp-content/uploads/2016/11

/2016-11-11_DSAnpUG-EU-BDSG-neu_Entwurf-2_Ressortabstimmung.pdf), die stark an die Anlage zu § 9 BDSG erinnern und diese erweitern.

Ferner ist die Vorgehensweise die alte geblieben, denn auch nach dem BDSG heißt es in § 9 BDSG inkl. Anlage, dass der Aufwand je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen soll.

Neu verankert ist u.a., dass die umgesetzten Maßnahmen auf dem Stand der Technik sein sollen und bei der Beurteilung das drohende Risiko und dessen Eintrittswahrscheinlichkeit berücksichtig werden müssen.

Was versteht man unter „Stand der Technik“?

Was unter „Stand der Technik“ zu verstehen ist, wird ebenfalls in der Datenschutz-Grundverordnung nicht konkretisiert. Allerdings ist dieser Fachbegriff nicht neu. Bereits in der Anlage zu § 9 BDSG ist im letzten Satz geregelt, dass eine Verschlüsselung dem „Stand der Technik“ entsprechen soll. Demnach sollen technische Maßnahmen erhoben werden, die zur Verfügung stehen und die sich bereits in der Praxis bewährt haben. Gemeint sind also nicht Techniken, die gerade neu entwickelt wurde. Letztendlich muss die jeweilige Maßnahme ihre Geeignetheit und Effektivität in der Praxis bereits bewiesen haben und einen ausreichenden Sicherheitsstandard gewährleisten. Dabei impliziert der Begriff „Stand der Technik“, dass es sich um eine gegenwärtige Bewertung handelt und der Stand der Technik immer wieder geprüft werden muss, um die Datensicherheit gewährleisten zu können.

Aufgrund des IT-Sicherheitsgesetzes hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) eine Handreichung (https://www.all-about-security.de/fileadmin/micropages/Fachartikel_25/TeleTrusT-Handreichung_Stand_der_Technik.pdf) veröffentlicht, die den Verantwortlichen als Orientierung zur Ermittlung des Standes der Technik in der IT-Sicherheit dienen soll.

Wie beurteilt sich ein „angemessenes Schutzniveau“?

Wie bisher auch, orientiert sich das Schutzniveau an der Schutzbedürftigkeit der einzelnen gespeicherten personenbezogenen Daten. Es sollte also eine Schutzbedarfsfeststellung vorgenommen werden, indem der jeweilige Schutzbedarf der unterschiedlichen personenbezogenen Daten ermittelt wird. Dabei werden zunächst typische Schadenszenarien ermittelt und anschließend der Schutzbedarf für die einzelnen personenbezogenen Daten abgeleitet. Bewährt hat sich die Einteilung in Schutzbedarfskategorien, wobei eine Orientierung an z.B. die Kategorien des BSI-Standard 100-2 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen

/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile) in „normal, „hoch“ und „sehr hoch“ hilfreich sein kann.

Der Begriff „angemessen“ orientiert sich an dem Stand der Technik, den Implementierungskosten, der Art und dem Umfang der Umstände, dem Zweck der Verarbeitung sowie an den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Muss eine Risikobewertung durchgeführt werden?

Art. 32 Abs. 1 DSGVO regelt, dass die technischen und organisatorischen Maßnahmen unter Berücksichtigung des Risikos zur Beeinträchtigung von Persönlichkeits- und Freiheitsrechten erhoben werden sollen. Nun stehen personenbezogene Daten selbst im Fokus einer Risikobewertung. Dabei sollte eine Risikoinventur vorgenommen werden, indem alle möglichen Bedrohungen und Schwachstellen mit ihrer jeweiligen Eintrittswahrscheinlichkeit und der potenziellen Schwere des Schadens für die Rechte und Freiheiten natürlicher Personen identifiziert werden.

Dieses Vorgehen ist bereits im IT-Risikomanagement bekannt, bei dem allerdings meist Informationen betrachtet werden, die nicht notwendigerweise personenbezogen sein müssen.

Das Ergebnis einer Risikobewertung ist nicht nur für die Datensicherheit wichtig, sondern auch für die Datenschutz-Folgenabschätzung (https://www.datenschutzbeauftragter-info.de/datenschutz-folgenabschaetzung/).

Werden auch konkrete Maßnahmen genannt?

Art. 32 Abs. 1 a) DSGVO erwähnt die Pseudonymisierung und die Verschlüsselung (https://www.datenschutzbeauftragter-info.de/verschluesselung-symmetrisch-asymmetrisch-oder-hybrid/) als Maßnahmen, die bei der Verarbeitung möglichst eingesetzt werden sollen. Erstaunlich ist, dass an dieser Stelle zwar die Pseudonymisierung jedoch nicht die Anonymisierung erwähnt wird, die durchaus bei einigen Verfahren eingesetzt werden kann.

In § 58 Abs. 3 des Referentenentwurf für das deutsche Ausführungsgesetz zur Datenschutz-Grundverordnung (https://www.datenschutzverein.de/wp-content/uploads/2016/11/2016-11-11_DSAnpUG-EU-BDSG-neu_Entwurf-2_Ressortabstimmung.pdf) werden folgende Maßnahmen aufgezählt: Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Zugangskontrolle (hierbei ist vermutlich das Berechtigungskonzept gemeint), Übertragungskontrolle, Eingabekontrolle, Transportkontrolle, Wiederherstellung, Datenintegrität, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle, Verschlüsselungsverfahren.

Welche Schutzziele sind in der DSGVO verankert?

In Art. 32 Abs. 1 b) DSGVO sind vier Schutzziele aufgelistet, die bei der Verarbeitung personenbezogener Daten sicherzustellen sind. Die ersten drei Schutzziele sind bereits aus der IT-Sicherheit bekannt:

- **Vertraulichkeit**, d.h. Daten sind für unberechtigte Dritte nicht zugänglich.
- **Integrität**, d.h. Daten können nicht verfälscht werden.
- **Verfügbarkeit**, d.h. Daten stehen zur Verfügung, wenn sie gebraucht werden.

Eine ausführliche Beschreibung der Schutzziele findet sich hier (https://www.datenschutzbeauftragter-info.de/unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/).

Als neues Schutzziel wird die „Belastbarkeit“ der Systeme und Dienste erwähnt, wobei auch hier keine nähere Definition oder konkrete Maßnahmen erwähnt werden. Gemeint sein könnte, dass Systeme und Dienste einer gewissen Beanspruchung standhalten müssen. Zur Lösung des Begriffes „Belastbarkeit“ sollte die englische Fassung hinzugezogen werden. Dort ist die Sprache von „resilience“. Ins Deutsche übersetzt, passen also eher die Begriffe Resilienz bzw. Widerstandsfähigkeit der System bzw. Dienste, die bereits aus dem Notfallmanagement bekannt sind.

Was versteht man unter einer raschen Wiederherstellbarkeit?

In Art. 32 Abs. 1 c) DSGVO ist normiert, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden sollen.

Um diese Anforderung der Datensicherheit erfüllen zu können, werden Verantwortliche nicht nur ein Notfallmanagement inkl. Notfallpläne oder entsprechende Leitfäden erstellen, sondern auch die Wiederherstellung regelmäßig testen müssen. Dazu gehört insbesondere die regelmäßige Prüfung, ob die erstellten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können.

Was allerdings unter dem Begriff „rasch“ zu verstehen ist, wird wohl noch interpretiert werden müssen. Es mag der deutschen (nicht amtlichen) Übersetzung geschuldet sein, dass sich ein umgangssprachliches Wort „rasch“ in der Verordnung findet. Ob damit „zeitnah“ oder „unverzüglich“ (also ohne schuldhaftes Zögern) gemeint ist, die sich bereits in der Praxis etabliert haben, wird abzuwarten sein.

Wie soll die Wirksamkeit der erhobenen Maßnahmen getestet werden?

Art. 32 Abs. 1 d) DSGVO regelt, dass nun auch die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen getestet werden muss. Dabei muss das Unternehmen ein Verfahren etablieren, das regelmäßig die Wirksamkeit der Maßnahmen bewertet und evaluiert. Ein solches mögliches Verfahren wäre z.B. das Durchführen von Penetrationstests (https://de.wikipedia.org/wiki/Penetrationstest_(Informatik)) oder die Einführung eines Qualitätsmanagements.

Was bedeutet “data protection by design” und “data protection by default”?

Art. 25 DSGVO erweitert die Vorgaben an technische und organisatorische Maßnahmen um die folgenden zwei Anforderungen:

1. Bei **Data protection by design** (Datenschutz durch Technik) sollen Datenschutz und Datensicherheit bereits in der Planung und Entwicklung von IT-Systemen berücksichtigt werden. Es soll vorgebeugt werden, dass die Vorgaben nach dem Datenschutz und Datensicherheit erst nach dem Bereitstellen von IT-Systemen durch teure und zeitaufwendige Zusatzprogrammierungen umgesetzt werden werden. Bereits bei der Herstellung sollten Möglichkeiten wie Deaktivierung von Funktionalitäten, Anonymisierung oder Pseudonymisierung aber auch an Authentisierung und Authentifizierung oder Verschlüsselungen berücksichtigt werden.

2. Bei **Data protection by default** (datenschutzfreundliche Einstellungen) sollen IT-Systeme datenschutzfreundlich voreingestellt sein, so dass nur die personenbezogenen Daten verarbeitet werden, die für den verfolgten Zweck erforderlich sind. Hintergrund dieser Regelung ist, dass viele Nutzer nicht über ausreichende IT Kenntnisse verfügen und somit keine Einstellungen zum Schutz ihrer personenbezogenen Daten vornehmen können. Darüber hinaus muss dem Nutzer Funktionalitäten zur Verfügung gestellt werden, mit denen er seine Privatsphäre schützen kann (z.B. Verschlüsselung).

Adressat dieser Vorschrift sind nicht nur Verantwortliche sondern auch die Entwickler von IT-Systemen und Produkten.

Ganz neu ist diese Anforderung nicht. Denn in § 3a BDSG, der die Datenvermeidung und Datensparsamkeit regelt, normiert, dass Datenverarbeitungssystemen an dem Ziel auszurichten seien, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Was ist bei der Einführung von IT-Systemen zu beachten?

Art. 38 Abs. 1 DSGVO regelt explizit, dass der Datenschutzbeauftragte (https://www.datenschutzbeauftragter-info.de/datenschutz-grundverordnung-datenschutzbeauftragter/) „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“

einzubinden ist. Falls dies also noch nicht im Unternehmen umgesetzt ist, muss ein Prozess etabliert werden, der rechtzeitig den Datenschutzbeauftragten in das Vorhaben einbezieht.

Außerdem muss gemäß Art. 35 DSGVO eine Folgenabschätzung vorgenommen werden, wenn die Verarbeitung der Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte. Das ist z.B. bei IT-Systemen denkbar, die besonderen personenbezogenen Daten verarbeiten.

Nach Art. 36 DSGVO muss sogar die Aufsichtsbehörde konsultiert werden, wenn die Folgeabschätzung ergibt, dass eine Datenverarbeitung ohne Maßnahmen ein hohes Risiko bedeutet.

Welche Sanktionen drohen bei unzureichender Datensicherheit?

In BDSG sind Verstöße gegen § 9 nicht sanktioniert. Das wird sich mit der DSGVO ändern. Sollten unzureichende oder ungeeignete technische und organisatorische Maßnahmen umgesetzt werden, fehlt eine Folgenabschätzung oder ausreichende Tests/Dokumentationen droht ein Bußgeld in Höhe von max. 10 Millionen Euro oder bis max. 2% des weltweit erzielten Jahresumsatzes.

Gibt es eine Rechenschaftspflicht?

Ja, der Verantwortliche muss nach Art. 5 Abs. 2 DSGVO die Einhaltung der Datensicherheit gewährleisten und nachweisen. Der Nachweispflicht wird der Verantwortliche wohl auch durch Zertifizierungen nachkommen können.

Welche Vorgehensweise ist anzuraten?

Angelehnt an das Informationsblatt (https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf) des Bayerischen Landesamtes für Datenschutzaufsicht zum Artikel 32, ist folgende Vorgehensweise anzuraten:

1. Etablieren eines Managements für Datensicherheit oder Informationssicherheit
2. Feststellen des Schutzbedarfes
3. Bewertung von Risiken
4. Treffen und Umsetzen der jeweiligen Maßnahmen
5. Führen von Dokumentationen und Nachweisen

Um Ihnen die Umsetzung dieser Anforderungen zu erleichtern, werden wir Sie in unserer Reihe „ISMS & DSGVO (https://www.datenschutzbeauftragter-info.de/tag/isms-dsgvo/)“ regelmäßig über die Umsetzung einzelner Punkte informieren.

Hier finden Sie weitere ausgewählte Artikel zur EU-Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/?utm_source=dsb&utm_medium=banner&utm_content=sidebar&utm_campaign=jede-seite).

Veröffentlicht am: 8. Juli 2016 | **Autor:** Agnieszka Czernik (https://www.datenschutzbeauftragter-info.de/author/aczernik/) | **Kategorie:** Fachbeitrag

Tags: angemessenes Datenschutzniveau (https://www.datenschutzbeauftragter-info.de/tag/angemessenes-datenschutzniveau/), Datenschutz-Grundverordnung (https://www.datenschutzbeauftragter-info.de/tag/datenschutz-grundverordnung/), Datensicherheit (https://www.datenschutzbeauftragter-info.de/tag/datensicherheit/), IT-Sicherheit (https://www.datenschutzbeauftragter-info.de/tag/it-sicherheit/), Technische und organisatorische Maßnahmen (https://www.datenschutzbeauftragter-info.de/tag/technische-und-organisatorische-massnahmen/)