Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Angst vor der EU-Datenschutz-grundverordnung? – Nicht mit uns!

Prof. Dr. Dagmar Gesmann-Nuissl & Dipl.-Jur. Univ. Gernot Kirchner

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Impressum

Herausgeber:

Mittelstand 4.0-Kompetenzzentrum Chemnitz
Geschäftsstelle
c/o Technische Universität Chemnitz
Prof. Dr.-Ing. Egon Müller
DE – 09107 Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935

E-Mail: info@betrieb-machen.de
Web: www.betrieb-machen.de
www.kompetenzzentrum-chemnitz.digital

Redaktion & Gestaltung:

Prof. Dr. Dagmar Gesmann-Nuissl
Dipl.-Jur. Univ. Gernot Kirchner
Romy Kertzsch

Bildnachweis Titel:

Pixabay, JanBaby

Informationsveranstaltung ist keine Rechtsberatung!

Bitte beachten Sie, dass die Informationsveranstaltung (Basisworkshop) sowie die vorliegenden veranstaltungsbegleitenden Unterlagen lediglich dem unverbindlichen Informationszweck dienen und keine Rechtsberatung darstellen.

Die erteilten abstrakten Informationen können, sollen und dürfen eine individuelle und verbindliche Rechtsberatung nicht ersetzen. Es ist damit insbesondere nicht möglich, die in diesem Zusammenhang erteilten Informationen auf den jeweiligen konkreten Einzelfall – unproblematisch – zu übertragen.

So kann insbesondere keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit der bereitgestellten Informationen übernommen werden, zumal das Recht – und vor allem auch das Datenschutzrecht – einer ständigen Dynamik unterliegt.

Prof. Dr. Dagmar Gesmann-Nuissl

Dipl.-Jur. Univ. Gernot Kirchner

Inhalt

Geltungsbereich der DSGVO

Nach der ab dem 25. Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO) stehen wesentlich mehr Vorschriften als nach dem derzeit geltenden Bundesdatenschutzgesetz (BDSG) unter einer Bußgeldandrohung, die zudem nunmehr bis zu 20.000.000 EUR bzw. 4 % des globalen Jahresumsatzes betragen kann (vgl. Art. 83 Abs. 5, 6 DSGVO). Die DSGVO gilt dabei allgemein, unmittelbar und verbindlich (Art. 288 Abs. 2 AEUV), beinhaltet jedoch selbst zahlreiche Öffnungsklauseln, die wiederum beispielsweise durch das am 25. Mai 2018 in Kraft getretene BDSG neue Fassung (n. F.) ausgestaltet werden (z.B. § 38 BDSG n. F. in Bezug auf den Datenschutzbeauftragten). Das Gesetz zur Anpassung landesrechtlicher Vorschriften an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (vgl. Sächsisches Datenschutzgesetz und Sächsisches Datenschutzdurchführungsgesetz) betrifft zwar primär u. a. Behörden und sonstige öffentliche Stellen des Freistaates Sachsen, ist jedoch beispielsweise in Bezug auf die Bestimmung der Aufsichtsbehörde auch im Übrigen relevant (vgl. § 40 BDSG n. F.).

Datenschutz geht jeden an! – Wer ist Adressat?

Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO/§ 46 Nr. 7 BDSG n. F. ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam [vgl. Art. 26 DSGVO] mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Was wird eigentlich geschützt?

Geschützt werden sog. personenbezogene Daten. Personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO/§ 46 Nr. 1 BDSG n. F. sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetisch, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann.

Nicht umfasst werden daher **rein statistische** Daten und solche, die anonymisiert vorliegen, wobei hinterfragt werden muss, inwiefern eine tatsächliche **Anonymisierung** überhaupt stattfinden kann. Dies ist anhand der für jedermann (str.) verhältnismäßig zugänglichen Mittel zu bestimmen. Dabei ist u. a. zu fragen, welchen zeitlichen, finanziellen, technischen Aufwand jemand aller Wahrscheinlichkeit nach betreiben würde, um die dahinterstehende natürliche Person zu identifizieren. Im Zweifel sollte eine Anonymisierung eher verneint werden. Eine bloße Pseudonymisierung – d. h. es sind zusätzliche gesondert aufzubewahrende Informationen zur Identifizierung erforderlich, Art. 3 Nr. 5 DSGVO/§ 46 Nr. 5 BDSG n. F. – ist jedenfalls in der Regel nicht ausreichend. Beispielsweise zu nennen sind Online-Kennungen oder Pseudonyme.

Daten, die ausschließlich **juristische Personen** betreffen, werden demnach von der DSGVO nicht geschützt. Es ist insoweit jedoch streng im jeweiligen Einzelfall zu prüfen, ob nicht doch gegebenenfalls die dahinterstehende natürliche Person identifiziert werden kann und folglich ein personenbezogenes Datum vorliegt. Die DSGVO selbst differenziert nämlich gerade nicht zwischen Datenverarbeitungsvorgängen zwischen einem Unternehmer und einem Verbraucher (B2C) und solchen zwischen Unternehmern (B2B), so dass für beide Konstellationen die DSGVO-Vorgaben zu beachten sind, sobald ein personenbezogenes Datum i.S.d. Art. 4 Nr. 1 DSGVO/§ 46 Nr. 1 BDSG n. F. vorliegt.

Wofür findet die DSGVO Anwendung?

Der **sachliche Anwendungsbereich** der DSGVO wird durch Art. 2 Abs. 1 DSGVO wie folgt bestimmt: 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. Ergänzend ist zudem § 1 Abs. 1 S. 2 BDSG n. F. zu zitieren: Für nichtöffentliche Stellen gilt dieses Gesetz [BDSG n. F.] für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (vgl. auch Art. 2 Abs. 2 lit. c) DSGVO).

Welche Vorgänge sind betroffen?

Eine **Datenverarbeitung** i.S.d. Art. 4 Nr. 2 DSGVO/§ 46 Nr. 2 BDSG n. F. ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Wo findet die DSGVO überhaupt Anwendung?

Der **räumliche Anwendungsbereich** der DSGVO bestimmt sich nach Art. 3 Abs. 1, 2 DSGVO (vgl. auch § 1 Abs. 4 BDSG n. F.) und umfasst zum einen Unternehmen mit **Niederlassung in der EU** (unabhängig vom Datenverarbeitungsort). Ebenso erfasst sind nach dem **sogenannten Marktortprinzip** aber auch Unternehmen ohne Niederlassung in der EU, wenn die Verarbeitung personenbezogener Daten Personen in der EU betrifft und im Zusammenhang damit steht, (a) betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist bzw. (b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der EU erfolgt. Irrelevant ist die Staatsangehörigkeit oder Unionsbürgerschaft des/der Betroffenen.

Überblick über den Inhalt der DSGVO

Kapitel 1	Allgemeine Bestimmungen
Kapitel 2	Grundsätze
Kapitel 3	Rechte der betroffenen Person
Kapitel 4	Verantwortlicher und Auftragsverarbeiter
Kapitel 5	Übermittlungen an Drittländer oder internationale Organisationen
Kapitel 6	Unabhängige Aufsichtsbehörden
Kapitel 7	Zusammenarbeit/Kohärenz (Aufsichtsbehörden/Kommission)
Kapitel 8	Rechtsbehelfe, Haftung und Sanktionen
Kapitel 9	Vorschriften für besondere Verarbeitungssituationen
Kapitel 10	Delegierte Rechtsakte und Durchführungsrechtsakte
Kapitel 11	Schlussbestimmungen

Grundprinzipien, Art. 5 DSGVO/§ 47 BDSG n. F.

1. Rechtmäßigkeitsgrundsatz

Für jede Datenverarbeitung ist eine rechtliche Grundlage erforderlich (»auf rechtmäßige Weise«). Es handelt sich dabei um ein **Verbot mit Erlaubnisvorbehalt** (Art. 6 DSGVO), so dass grundsätzlich von der Rechtswidrigkeit auszugehen ist, sofern kein Erlaubnisgrund vorliegt.

Erlaubnisgründe können nach Art. 6 Abs. 1 DSGVO sein:

a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die **Erfüllung eines Vertrags,** dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher

Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Gemäß Art. 6 Abs. 1 lit. c) DSGVO tritt somit beispielsweise das grundsätzlich bestehende Datenverarbeitungsverbot hinter die Erfüllung einer **rechtlichen Verpflichtung** (z.B. aus HGB, AO, UStG, EStG, GWG etc.) zurück. Dies betrifft zum Beispiel die gesetzliche Aufbewahrungspflicht für E-Mails, die Handelsbriefe oder Buchungsbelege i.S.d. § 257 Abs. 1 Nr. 2, 4 HGB darstellen.

Im Falle der **Direktwerbung** (z.B. Postwurfsendungen, Sonderangebote etc.) bestimmt Art. 21 Abs. 1 DSGVO i.V.m. Art. 6 Abs. 1 lit. f) DSGVO i.V.m. Erwägungsgrund 47 der DSGVO, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse (Informationspflicht, gem. Art. 13 Abs. 1 lit. d) bzw. Art. 14 Abs. 2 lit. b) DSGVO) dienende Verarbeitung betrachtet werden kann. In jedem Fall muss aber eine **Interessenabwägung** vorgenommen werden, so dass nur dann von einer Zulässigkeit ausgegangen werden kann, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Abs. 1 lit. f) DSGVO), z.B. Widerspruch i.S.d. Art. 21 DSGVO (Informationspflicht, gem. Art. 21 Abs. 4 DSGVO). Im Verhältnis zwischen Unternehmern (B2B) wird die Interessenabwägung aber regelmäßig für das überwiegende berechtigte Interesse an der geschäftsbezogenen Direktwerbung sprechen, was eine Einzelfallprüfung aber nicht entbehrlich macht. Ergänzend soll ferner auf § 7 Abs. 2

Nr. 2 und 3 UWG hingewiesen werden: Eine unzumutbare Belästigung ist stets anzunehmen, bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige **ausdrückliche Einwilligung** oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest **mutmaßliche Einwilligung** bzw. bei Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgerätes oder elektronischer Post, ohne dass eine vorherige **ausdrückliche Einwilligung** des Adressaten vorliegt.

Einen **Sonderfall** bildet die **Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO**. Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt. Ausgenommen sind dabei die in Art. 9 Abs. 2 DSGVO geschilderten Fälle, u. a.: (a) die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke **ausdrücklich eingewilligt**, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Abs. 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden.

2. Transparenzgebot (Grundsatz von Treu und Glauben)

Das Transparenzgebot verlangt, dass der Betroffene die Datenverarbeitung nachvollziehen können muss (»Was passiert mit meinen Daten?«). Auch insoweit ist nach dem **risikobasierten Ansatz in der DSGVO** vorzugehen, mithin ein verhältnismäßiger Ausgleich zwischen den zu veranlassenden Maßnahmen und dem drohenden Risiko vorzunehmen (u. a. Informationsverpflichtungen).

3. Zweckbindungsgrundsatz

Personenbezogene Daten müssen für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt nicht als unvereinbar mit den ursprünglichen Zwecken, vgl. Art. 89 Abs. 1 DSGVO. Eng damit verwoben ist die **Erforderlichkeits- und Verhältnismäßigkeitsprüfung**, so dass die Datenverarbeitung u. a. dem Verarbeitungszweck entsprechend

und für die Zweckerreichung erforderlich sein muss und nicht außer Verhältnis zum zu erreichenden Zweck stehen darf.

Nur ausnahmsweise sind dagegen nachträgliche Zweckänderungen gem. Art. 6 Abs. 4 DSGVO zulässig (vgl. insbes. § 24 BDSG n. F.). Besonders zu nennen ist die Datenverarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen, § 24 Abs. 1 Nr. 2 BDSG n. F. Im Übrigen ist eine **Vereinbarkeitsprüfung** im Hinblick auf den ursprünglichen Zweck durchzuführen, wobei unter anderem folgende Punkte zu berücksichtigen sind (Art. 6 Abs. 4 DSGVO):

a) jede **Verbindung** zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den **Zusammenhang**, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die **Art der personenbezogenen Daten**, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO verarbeitet werden,

d) die **möglichen Folgen** der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das **Vorhandensein geeigneter Garantien**, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

4. Richtigkeitsgrundsatz

Darüber hinausgehend müssen die personenbezogenen Daten **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sein. Dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (Löschungs- und Berichtigungspflicht, Art. 16 f. DSGVO).

5. Grundsatz der Datenminimierung/-sparsamkeit

Die personenbezogenen Daten müssen im Übrigen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Auch insoweit ist daher unter anderem eine **Verhältnismäßigkeitsprüfung** in Bezug auf den legitimen Zweck und die Datenquantität anzustellen.

6. Speicherbegrenzungsgrundsatz

Personenbezogene Daten dürfen zudem nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht. Es obliegt damit jedem Einzelnen selbst, die Erforderlichkeit zur Zweckerreichung auch unter diesem Gesichtspunkt (z.B. Speicherdauer) zu überprüfen.

7. Datensicherheitsgrundsatz

Im Übrigen muss der Verantwortliche dafür Sorge tragen, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten gewährleistet. Hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

8. Rechenschaftspflicht

Ergänzt werden die bis hierhin dargestellten Datenverarbeitungsgrundprinzipien durch die Rechenschaftspflicht des Verantwortlichen. Der Verantwortliche ist demnach für die Einhaltung des Art. 5 Abs. 1 DSGVO verantwortlich und muss dessen Einhaltung nachweisen können. Angesprochen wird damit indirekt auch ein Datenschutzmanagementsystem nach Art. 24, 30 DSGVO. So verlangt beispielsweise Art. 30 Abs. 1 S. 1 DSGVO (vgl. auch § 70 BDSG n. F.): Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung (Art. 30 Abs. 3 DSGVO, § 70 Abs. 4 BDSG n. F.). Eine Ausnahme von der Erstellung eines Verarbeitungsverzeichnisses (Pflichten aus Art. 30 Abs. 1, 2 DSGVO) besteht für

Unternehmen oder Einrichtungen, die **weniger als 250 Mitarbeiter beschäftigen**, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (besonderer Kategorien personenbezogener Daten) bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO.

Ein vom Verantwortlichen (ggf. Vertreter) zu erstellendes Verarbeitungsverzeichnis i.S.d. Art. 30 Abs. 1 DSGVO enthält folgende Angaben:

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

b) die **Zwecke der Verarbeitung**;

c) eine **Beschreibung der Kategorien** betroffener Personen und der Kategorien personenbezogener Daten;

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

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

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

g) wenn möglich, eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Art. 32 Abs. 1 DSGVO.

Die Muster der deutschen Aufsichtsbehörden für ein solches Verarbeitungsverzeichnis i.S.d Art. 30 DSGVO können Sie hier abrufen: https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/.

Einwilligung, Art. 7 DSGVO/§ 51 BDSG n. F.

Unter einer Einwilligung versteht man gemäß Art. 4 Nr. 11 DSGVO/§ 46 Nr. 17 BDSG n. F. jede freiwillige für den bestimmten Fall, in informierter Weise (Informationspflicht) und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Nicht ausreichend ist damit das einfache Schweigen oder die »Opt-Out« Option (☑) im elektronischen Rechtsverkehr.

Die **Beweispflicht** für eine wirksame Einwilligungserklärung der betroffenen Person liegt dabei beim Verantwortlichen (§ 51 Abs. 1 BDSG n. F.).

Dabei ist die Einwilligung selbst grundsätzlich formfrei möglich. Im eigenen Interesse dürfte aber beispielsweise die Schriftform angezeigt sein. Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

Für die elektronische Kommunikation ist in Zukunft zudem die sog. ePrivacy-Verordnung zu berücksichtigen (Link zum Entwurf: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE). Aktuell regelt insoweit § 13 Abs. 2 TMG: Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Besondere Beachtung verdient des Weiteren die **Freiwilligkeit** in Bezug auf die erteilte Einwilligung. Eine solche ist im Zweifel zu verneinen, wenn ein gestörtes Gleichgewicht zwischen den Parteien vorliegt. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss ferner dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind (sog. Koppelungsverbot, Art. 7 Abs. 4 DSGVO).

Die betroffene Person hat gem. Art. 7 Abs. 3 DSGVO im Übrigen das Recht, ihre Einwilligung jederzeit zu **widerrufen**. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt (Informationspflicht). Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Bestehende Einwilligungserklärungen müssen folglich auf ihre **DSGVO-Konformität** hin überprüft und gegebenenfalls angepasst und erneuert werden. So gibt es beispielsweise zwar auch zukünftig kein »gesetzliches Verfallsdatum« einer einmal erklärten Einwilligung, rechtspraktisch ist eine regelmäßige Erneuerung aber zu empfehlen, wobei sich dies nach den Umständen des Einzelfalles bemisst.

Betroffenenrechte, Art. 12-23 DSGVO

1. Transparenz, Art. 12 DSGVO/§§ 32 f., 59 BDSG n. F.

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen und alle Mitteilungen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Zudem hat der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß der Art. 15 bis 22 zu erleichtern, vgl. Art. 12 Abs. 2 ff. DSGVO. Informationen gemäß der Art. 13 und 14 DSGVO sowie alle Mitteilungen und Maßnahmen gemäß der Art. 15 bis 22 und Art. 34 DSGVO werden unentgeltlich zur Verfügung gestellt. Ausnahmen gelten lediglich bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person, Art. 12 Abs. 5 S. 2 DSGVO.

2. Informationspflicht, Art. 13 f. DSGVO (vgl. § 56 BDSG n. F.)

Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten gemäß Art. 13 Abs. 2 DSGVO Folgendes mit:

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

b) gegebenenfalls die **Kontaktdaten** des Datenschutzbeauftragten;

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

d) wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f) beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

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

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

Zusätzlich zu diesen Informationen stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten gemäß Art. 13 Abs. 2 DSGVO folgende weitere Informationen zur Verfügung, die notwendig sind, um eine **faire und transparente Verarbeitung** zu gewährleisten:

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

b) das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichti-

gung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) DSGVO beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu **widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde;

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

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

Betreffend weitere Informationspflichten soll auf die Lektüre von Art. 13, 14 DSGVO verwiesen werden. Art. 13 DSGVO betrifft dabei die Informationspflicht bei Erhebung von personenbezogenen Daten **bei der betroffenen Person,** Art. 14 DSGVO dagegen die Informationspflicht, wenn die personenbezogenen Daten **nicht bei der betroffenen Person** erhoben wurden.

Die Informationspflichten reichen damit deutlich weiter als die Unterrichtungs- und Benachrichtigungspflichten aus den zuvor geltenden §§ 4 Abs. 3, 33 BDSG alte Fassung (a. F.).

3. Auskunftsrecht, Art. 15 DSGVO (§ 34 BDSG/§ 57 BDSG n. F.)

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, **ob** sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf **Auskunft** über diese personenbezogenen Daten und auf **folgende Informationen**:

a) die **Verarbeitungszwecke**;

b) die **Kategorien** personenbezogener Daten, die verarbeitet werden;

c) die **Empfänger oder Kategorien** von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante **Dauer**, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf **Berichtigung** oder **Löschung** der sie betreffenden personenbezogenen Daten oder auf **Einschränkung der Verarbeitung** durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines **Beschwerderechts** bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die **Herkunft der Daten**;

h) das Bestehen einer **automatisierten Entscheidungsfindung** einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Der Verantwortliche stellt gemäß Art. 15 Abs. 3 DSGVO eine **Kopie der personenbezogenen Daten**, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Folglich darf für die **erste Kopie kein Entgelt** verlangt werden. Insgesamt sollte aber gerade jener Art. 15 Abs. 3 DSGVO dazu veranlassen, über die eigene IT-Infrastruktur nachzudenken und gegebenenfalls erforderliche Anpassungen vorzunehmen, um die Verpflichtungen erfüllen zu können.

4. Berichtigungsanspruch, Art. 16 DSGVO (§ 58 BDSG n. F.)

Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die **Berichtigung** sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person zudem das Recht, die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen.

5. »Recht auf Vergessenwerden«, Art. 17 DSGVO (§ 58 BDSG n. F.)

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern beispielsweise gemäß Art. 17 Abs. 1 lit. a) DSGVO die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (**unverzügliche Löschungspflicht**). Hat der Verantwortliche die personenbezogenen Daten **öffentlich gemacht**, so trifft er angemessene Maßnahmen um für die Verantwortlichen, die die personenbezogenen Daten verarbeiten, **darüber zu informieren**, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

6. Verarbeitungseinschränkungsrecht, Art. 18 DSGVO (§ 58 BDSG n. F.)

Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen (vgl. bereits § 20 Abs. 3, 4 und § 35 Abs. 3, 4 BDSG a. F.), wenn beispielsweise gemäß Art. 18 Abs. 1 lit. a) DSGVO die **Richtigkeit** der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.

Dies betrifft gemäß den lit. b) bis d) ebenfalls folgende Fälle, wenn:

- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die **Einschränkung** der Nutzung der personenbezogenen Daten **verlangt**;

- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur

Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** benötigt, oder

- die betroffene Person **Widerspruch gegen die Verarbeitung** gemäß Art. 21 Abs. 1 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

7. Datenübertragbarkeitsrecht, Art. 20 DSGVO

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten, so dass gegebenenfalls Anpassungen am eigenen Datenverarbeitungssystem vorgenommen werden müssen. Sie hat ferner das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu **übermitteln**.

Voraussetzung für dieses Datenübertragbarkeitsrecht ist, dass die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) DSGVO (ausdrückliche Einwilligung) oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b) DSGVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Bei der Ausübung hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten **direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden**. Seine Grenze findet das Datenübertragbarkeitsrecht u. a. in den Rechten und Freiheiten anderer Personen (Art. 20 Abs. 4 DSGVO).

8. Widerspruchsrecht, Art. 21 DSGVO

Die betroffene Person hat das Recht, aus **Gründen, die sich aus ihrer besonderen Situation ergeben**, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e) oder f) DSGVO (öffentliches Interesse/öffentliche Gewalt bzw. berechtigte Interessen) erfolgt, Widerspruch einzulegen. Werden personenbezogene Daten verarbeitet, um **Direktwerbung** zu betreiben, so hat die betroffene Person das Recht, jederzeit – d. h. ohne besondere Begründung – Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen.

Die betroffene Person muss spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das Widerspruchsrecht hingewiesen werden. Der **Hinweis** hat in einer **verständlichen** und von anderen Informationen **getrennten Form** zu erfolgen.

9. Automatisierte Einzelfallentscheidungen, Art. 22 DSGVO

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Für die Leistungserbringung nach einem Versicherungsvertrag trifft § 37 BDSG n. F. abweichende Regelungen.

10. Beschränkbarkeit der Betroffenenrechte, Art. 23 DSGVO

Gemäß Art. 23 DSGVO können die Betroffenenrechte unter bestimmten Voraussetzungen im Wege von Gesetzgebungsmaßnahmen beschränkt werden. Legitime Zwecke sind dabei u. a. die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder auch die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Verantwortlicher, Art. 24 ff. DSGVO

1. Maßnahmen zur Sicherstellung DSGVO-Konformität, Art. 24 DSGVO

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (**Datenschutzmanagementsystem**). Im Vergleich zur aktuellen Gesetzeslage ergeben sich damit deutlich erweiterte Dokumentationspflichten.

So ist der Verantwortliche nicht nur für die Einhaltung der in Art. 5 Abs. 1 DSGVO genannten Datenverarbeitungsgrundsätze verantwortlich und muss deren Verantwortliche muss darüber hinausgehend auch noch die in Art. 24

DSGVO angesprochenen **geeigneten technischen und organisatorischen Maßnahmen** umsetzen sowie das in Art. 30 DSGVO aufgezeigte **Verzeichnis von Verarbeitungstätigkeiten** führen, sofern er davon nicht ausgenommen ist.

Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein **materieller oder immaterieller Schaden** entstanden ist, hat zudem Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Dabei gilt gemäß Art. 82 Abs. 2 DSGVO, dass jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden haftet, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Es rückt damit die Frage nach einem **Entlastungsbeweis** des Verantwortlichen in den Mittelpunkt.

Ebenso ist darauf hinzuweisen, dass auch im Falle der **Verhängung von Geldbußen** u. a. folgende Kriterien nach Art. 83 Abs. 2 DSGVO zur Bemessung zu berücksichtigen sind: Art, Schwere und Dauer des Verstoßes, Schadensminderungsmaßnahmen, Grad der Verantwortung unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen; Umfang der Zusammenarbeit mit der Aufsichtsbehörde etc.

2. »Privacy by Design and Default«, Art. 25 DSGVO und § 71 BDSG n. F.

Der Verantwortliche muss sowohl zum Zeitpunkt der **Festlegung der Mittel** für die Verarbeitung als auch zum Zeitpunkt der **eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen (**Privacy by Design**). Dabei bleibt ihm ein gewisser Ermessensspielraum, u. a. in Abhängigkeit des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung etc.

Des Weiteren hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch die **Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden (**Privacy by Default**). Dies betrifft unter anderem den Umfang der Verarbeitung, die Speicherfrist aber auch die Menge der erhobenen Daten.

3. Vereinbarung für gemeinsam Verantwortliche, Art. 26 DSGVO

Legen **zwei oder mehr Verantwortliche** gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer **Vereinbarung** in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.

Ungeachtet der Einzelheiten der Vereinbarung kann die betroffene Person ihre Rechte im Rahmen der DSGVO **bei und gegenüber jedem einzelnen der Verantwortlichen** geltend machen.

4. Auftrags(daten)verarbeitung, Art. 28 ff. DSGVO

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die **hinreichend Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines **Vertrags** oder eines anderen **Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten.

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf **Weisung des Verantwortlichen** verarbeiten (Weisungsgebundenheit), es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Unbeschadet der Art. 82, 83 und 84 DSGVO **gilt ein Auftragsverarbeiter**, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung **als Verantwortlicher**.

5. Datensicherheit, Art. 32 DSGVO/§ 64 BDSG n. F.

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 Maßnahmen**, um ein dem Risiko angemessenes **Schutzniveau** zu

gewährleisten. Beispielsweise zu nennen sind die Pseudonymisierung und die Verschlüsselung.

Darüber hinausgehend bestimmt § 64 Abs. 3 BDSG n. F., dass im Fall einer automatisierten Verarbeitung der Verantwortliche und der Auftragsverarbeiter nach einer **Risikobewertung** Maßnahmen zu ergreifen haben, die u. a. Folgendes bezwecken: Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übertragungs-, Eingabe-, Transportkontrolle, Widerherstellbarkeit, Zuverlässigkeit, Datenintegrität etc.

Vgl. Sie auch das diesbezügliche Muster der deutschen Aufsichtsbehörden: https://www.bvdnet.de/wp-content/up-loads/2017/06/Muster_Verz_der_Verarbeitungstätigkeiten_TOMs.pdf.

6. Verletzungsmeldung i.S.d. Art. 33 DSGVO (vgl. § 65 BDSG n. F.)

Eine **Verletzung des Schutzes personenbezogener Daten** liegt vor, wenn eine Verletzung der Sicherheit, zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde melden. Dies gilt nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Die Meldung an die Aufsichtsbehörde enthält zumindest folgende Informationen:

- eine **Beschreibung der Art der Verletzung** des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- den **Namen und die Kontaktdaten** des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

- eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten;

- eine Beschreibung der von dem Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Verletzungsmeldung i.S.d. Art. 34 DSGVO (§ 66 BDSG n. F.)

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche (zudem) die betroffene Person **unverzüglich** von der Verletzung. Im Begriffsverständnis unseres Bürgerlichen Gesetzbuches bedeutet unverzüglich dabei »ohne schuldhaftes Zögern«.

8. Neu: Datenschutzfolgenabschätzung, Art. 35 DSGVO/§ 67 BDSG n. F.

§ 4d Abs. 5 BDSG a. F. kennt bisher nur eine **sogenannte Vorabkontrolle**. Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie demnach der Prüfung vor Beginn der Verarbeitung. Eine Vorabkontrolle ist gemäß § 4d Abs. 5 BDSG a. F. insbesondere durchzuführen, wenn besondere Arten personenbezogener Daten verarbeitet werden oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens. Dies gilt nicht, wenn eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Art. 35 Abs. 1 DSGVO sieht dagegen nunmehr vor: Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (**Datenschutzfolgenabschätzung**).

Eine Datenschutzfolgenabschätzung ist insbesondere in folgenden Fällen er-

forderlich:

- **systematische und umfassende Bewertung persönlicher Aspekte** natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

- umfangreiche Verarbeitung **besonderer Kategorien** von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder

- **systematische umfangreiche Überwachung** öffentlich zugänglicher Bereiche.

Bei der Datenschutzfolgenabschätzung selbst sind sodann die **Mindestvorgaben nach Art. 35 DSGVO bzw. § 67 BDSG n. F.** zu berücksichtigen, u. a.: systematische Beschreibung der geplanten Verarbeitungsvorgänge, Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck, Bewertung der Gefahren für die Rechtsgüter der betroffenen Person etc.

9. Vorherige Konsultation Aufsichtsbehörde, Art. 36 DSGVO

Der Verantwortliche konsultiert vor der Verarbeitung die **Aufsichtsbehörde**, wenn aus einer Datenschutzfolgenabschätzung hervorgeht, dass die Verarbeitung ein **hohes Risiko** zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Der Verantwortliche stellt der Aufsichtsbehörde dabei folgende **Informationen** zur Verfügung:

- gegebenenfalls Angaben zu den jeweiligen **Zuständigkeiten** des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

- die **Zwecke und die Mittel** der beabsichtigten Verarbeitung;

- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen **Maßnahmen und Garantien**;
- gegebenenfalls die **Kontaktdaten** des Datenschutzbeauftragten;
- die **Datenschutzfolgenabschätzung** gemäß Art. 35 DSGVO und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung stünde, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Art. 58 DSGVO genannten Befugnisse (u. a. Untersuchungs- und Abhilfebefugnisse) ausüben.

Ergänzend ist auf die Anhörung **der oder des Bundesbeauftragten** gemäß § 69 BDSG n. F. hinzuweisen.

10. Datenschutzbeauftragter, Art. 37 ff. DSGVO

Gemäß Art. 37 Abs. 1 DSGVO hat der Verantwortliche und der Auftragsverarbeiter auf jeden Fall einen Datenschutzbeauftragten zu benennen, wenn u. a.

- 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
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** gemäß Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht.

Weiter reicht dagegen der auf nichtöffentliche Stellen anzuwendende § 38 BDSG n. F., der die Öffnungsklausel aus Art. 37 Abs. 4 DSGVO entsprechend ausgestaltet. Demnach ist eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter zu benennen, soweit der Verantwortliche bzw. der Auftragsverarbeiter in der Regel mindestens **zehn Personen** ständig mit der automatisierten

Verarbeitung personenbezogener Daten beschäftigt. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer **Datenschutzfolgenabschätzung** unterliegen, oder verarbeiten sie personenbezogene Daten **geschäftsmäßig** zum Zweck der **Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung**, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

§ 6 Abs. 4 (**Abberufungs-/Kündigungsschutz**), Abs. 5 S. 2 (**Verschwiegenheitsverpflichtung**) und Abs. 6 BDSG n. F. (**Zeugnisverweigerungsrecht und Beschlagnahmeverbot**) finden entsprechende Anwendung. § 6 Abs. 4 BDSG n. F. allerdings nur dann, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

Dem Datenschutzbeauftragten obliegen gemäß Art. 39 Abs. 1 DSGVO (vgl. auch § 7 BDSG n. F.) zumindest folgende Aufgaben:

- **Unterrichtung und Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

- **Überwachung** der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der **Zuweisung von Zuständigkeiten**, der **Sensibilisierung** und **Schulung** der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

- **Beratung** – auf Anfrage – im Zusammenhang mit der Datenschutzfolgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO;

- **Zusammenarbeit mit der Aufsichtsbehörde**;

- Tätigkeit als **Anlaufstelle** für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der **vorherigen Konsultation** gemäß Art. 36 DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

11. Ausarbeitung von Verhaltensregeln, Art. 40 f. DSGVO

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zur ordnungsgemäßen Anwendung dieser Verordnung beitragen sollen.

Der **Europäische Datenschutzausschuss** (vgl. in DSGVO: »Ausschuss«) wird als Einrichtung der Union mit eigener Rechtspersönlichkeit eingerichtet (zuvor: Art. 29-Datenschutzgruppe).

12. DSGVO-Zertifizierung, Art. 42 DSGVO (Selbstregulierung)

Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von **datenschutzspezifischen Zertifizierungsverfahren** sowie von **Datenschutzsiegeln und -prüfzeichen**, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen. Nicht verwechselt werden darf dabei aber die Zertifizierung im Sinne des Art. 42 DSGVO mit den bereits bestehenden ISO-Zertifizierungen.

13. Datenübermittlung Drittländer, Art. 44 ff. DSGVO/§§ 78 ff. BDSG n. F.

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig (**Verbot mit Erlaubnisvorbehalt**), wenn der Verantwortliche und der Auftragsverarbeiter die in den **Art. 44 bis 50 DSGVO niedergelegten Bedingungen** einhalten und auch die **sonstigen Bestimmungen dieser Verordnung** eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation.

Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung **gewährleistete Schutzniveau für natürliche Personen nicht untergraben** wird. Eine Datenübermittlung **innerhalb der EU** ist daher grundsätzlich unproblematisch. Für eine Datenübermittlung **an ein Drittland** sind dagegen vor allem die Anforderungen von Art. 45 DSGVO (Angemessenheitsbeschluss der EU-Kommission), Art. 46 DSGVO (geeignete Garan-

tien) sowie von Art. 49 DSGVO (Ausnahmen für bestimmte Fälle) zu beachten.

14. Videoüberwachung öffentlich zugänglicher Räume, § 4 BDSG n. F.

Die Videoüberwachung öffentlich zugänglicher Räume wird nunmehr neu in § 4 BDSG n. F. geregelt, ohne dass es eine ausdrückliche Entsprechung in der DS-GVO gibt, insoweit kann lediglich auf Art. 6 DSGVO Bezug genommen werden. Nach § 4 Abs. 1 BDSG n. F. ist die Videoüberwachung öffentlich zugänglicher Räume nur zulässig, soweit sie zur **Aufgabenerfüllung öffentlicher Stellen**, zur Wahrnehmung des **Hausrechts** oder zur Wahrnehmung **berechtigter Interessen** für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass **schutzwürdige Interessen der Betroffenen** überwiegen. Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Betreffend die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ist § 26 BDSG n. F. zu beachten.

15. Beschäftigtendatenschutz, Art. 88 DSGVO/§ 26 BDSG n. F.

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorsehen (**Öffnungsklausel**). Eine Definition für Beschäftigte liefert sodann § 26 Abs. 8 BDSG n. F.

Nach § 26 Abs. 1 S. 1 BDSG n. F. dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die **Begründung eines Beschäftigungsverhältnisses** oder nach Begründung des Beschäftigungsverhältnisses für dessen **Durchführung** oder **Beendigung** oder zur **Ausübung oder Erfüllung** der sich aus einem Gesetz oder einer Kollektivvereinbarung ergebenden **Rechte und Pflichten der Interessenvertretung** der Beschäftigten erforderlich ist. Besondere Voraussetzungen gelten nach § 26 Abs. 1 S. 2 BDSG n. F. für die Verwendung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten.

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der **Freiwilligkeit der Einwilligung** insbesondere die im Beschäftigungsverhältnis bestehende **Abhängigkeit der beschäftigten Person** sowie die **Umstände**, unter denen die

Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein **rechtlicher oder wirtschaftlicher Vorteil** erreicht wird oder Arbeitgeber und beschäftigte Person **gleichgelagerte Interessen** verfolgen. Die Einwilligung bedarf der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den **Zweck** der Datenverarbeitung und über ihr **Widerrufsrecht** nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären.

Abweichend von Art. 9 Abs. 1 DSGVO ist die **Verarbeitung besonderer Kategorien personenbezogener Daten** im Sinne des Art. 9 Abs. 1 DSGVO für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur **Ausübung von Rechten** oder zur **Erfüllung rechtlicher Pflichten** aus dem **Arbeitsrecht**, dem **Recht der sozialen Sicherheit** und des **Sozialschutzes** erforderlich ist und kein Grund zu der Annahme besteht, dass das **schutzwürdige Interesse** der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. § 26 Abs. 2 BDSG n. F. gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Abs. 2 BDSG n. F. gilt entsprechend, so dass angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen sind.

Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist ferner auf der Grundlage von **Kollektivvereinbarungen** zulässig. Dabei haben die Verhandlungspartner Art. 88 Abs. 2 DSGVO zu beachten. Das heißt, es sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde und der berechtigten Interessen und der Grundrechte der betroffenen Person zu treffen.

Haben Sie noch Fragen? – Gerne!

Prof. Dr. Dagmar Gesmann-Nuissl Sie ist Leiterin der Professur für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz mit einem Forschungsschwerpunkt auf dem Innovations- und Technikrecht. Als Konsortialpartnerin des Mittelstand 4.0-Kompetenzzentrum Chemnitz leitet sie außerdem den »Arbeitsgemeinschaft Recht 4.0« aller Mittelstand 4.0-Kompetenzzentren in Deutschland.

(+49) 0371/531 39233
dagmar.gesmann-nuissl@betrieb-machen.de

Dipl.-Jur. Univ. Gernot Kirchner ist wissenschaftlicher Mitarbeiter an der Professur für Privatrecht und Recht des geistigen Eigentums. Im Mittelstand 4.0-Kompetenzzentrum Chemnitz verantwortet er alle rechtlichen Themen in Bezug auf Digitalisierung und ist Experte für die EU-Datenschutzgrundverordnung.

(+49) 0371/531-30171
gernot.kirchner@betrieb-machen.de

Weitere Informationen

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de

Ihr schnellster Weg zu uns: