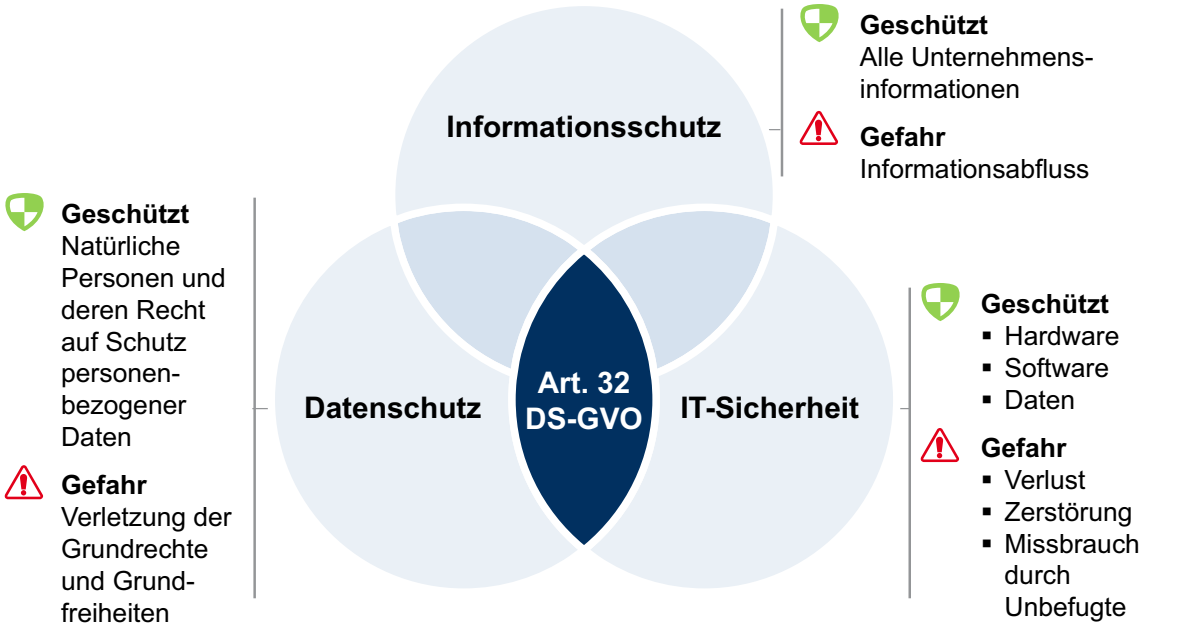

Abb. 3: Datenschutz und Datensicherheit (Art. 32 DS-GVO)

4.3 Der sachliche Schutzbereich der DS-GVO (Art. 2 DS-GVO)

Primär richtet sich der Schutz des Einzelnen gegen die Gefahren für sein Persönlichkeitsrecht, die von einer **automatisierten Verarbeitung** personenbezogener Daten ausgeht. Einbezogen sind aber auch personenbezogene Daten, die für oder in einem manuell geführten Dateisystem verarbeitet werden, worunter eine in Art. 4 Nr. 6 DS-GVO definierte manuelle Verarbeitung in einem strukturierten Ablagesystem zu verstehen ist.

Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare „natürliche“ Person[1] (betroffene Person) beziehen. Damit gilt die Verordnung zum einen nicht für personenbezogene Daten Verstorbener. Zum anderen erstreckt die Verordnung ihren Schutz nicht auf juristische Personen und insbesondere nicht– wie Erwägungsgrund 14 S. 2 DS-GVObetont – auf als juristische Person gegründete Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.

Bestimmbar ist die von den Daten tangierte Person, wenn sie direkt oder indirekt von dem Verantwortlichen identifiziert werden kann, wenn er dazu zusätzliche Informationen heranzieht, wie es ihm nach allgemeinem Ermessen möglich ist. Damit fallen auch pseudonymisierte Daten in den Anwendungsbereich der DS-GVO, da die Möglichkeit der Wiedererkennung ausreicht. Das gilt zwar für den Verantwortlichen, der die Pseudonymisierung vorgenommen hat, nicht jedoch für einen Dritten, dem die pseudonymisierten Daten übermittelt wurden und der keine Möglichkeit der Entpseudonymisierung hat.

Nicht geschützt werden aggregierte oder anonymisierte Daten. Auch sonstige geheime Daten, wie Geschäfts- und Betriebsgeheimnisse werden nicht durch die DS-GVO, sondern durch anderweitige Normen geschützt.

Der Begriff der Verarbeitung erfasst jede Form des „Umgangs“ mit personenbezoge-

1. „natürliche Person“ = Mensch, im Gegensatz zur „juristischen Person“ = Firma, Verein, Partei etc.

Erläuterung der DS-GVO nach Sachgebieten

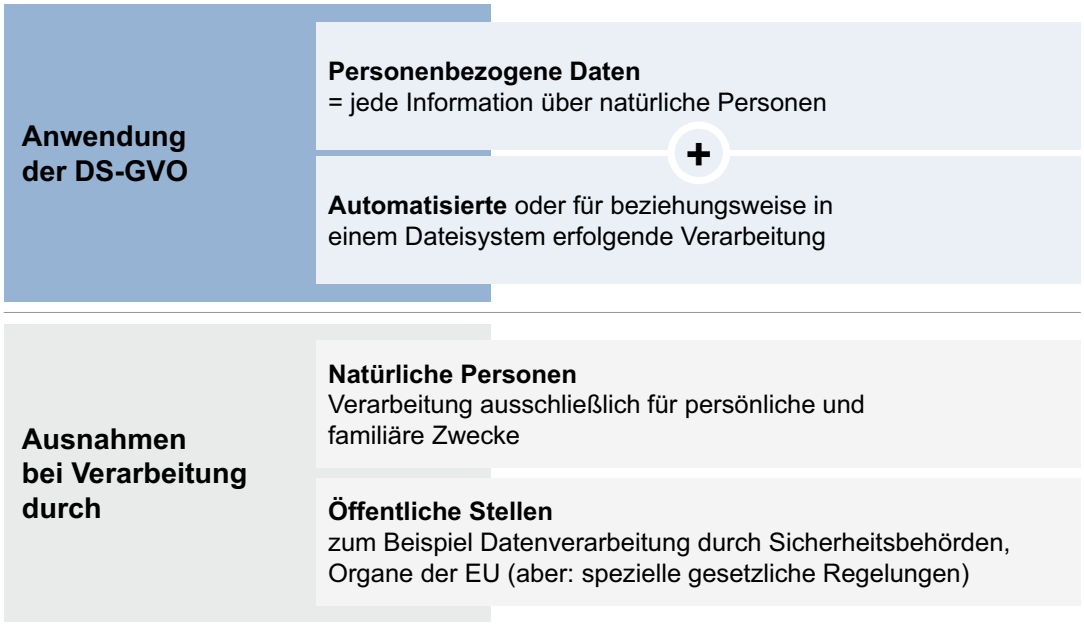

Abb. 4: Anwendung der DS-GVO

nen Daten, beginnend mit der Erhebung und endend mit der Löschung. Trotz eines erheblich erweiterten Definitionskatalogs werden die bisherigen „klassischen“ Erscheinungsformen der Verarbeitung nicht mehr definiert, obwohl sie, wie zum Beispiel das Übermitteln oder Löschen, im Einzelnen geregelt werden. Eine Ausnahme gilt für das „Sperren“ von Daten (Art. 4 Nr. 3 DS-GVO), das nunmehr als „Recht auf Einschränkung der Verarbeitung**“** bezeichnet wird (Art. 18 DS-GVO).

Für einige Anwendungen bestehen jedoch Ausnahmen (Art. 2 Abs. 2 DS-GVO).

Die Verordnung gilt insbesondere im öffentlichen Bereich dort nicht, wo die EU keine Regelungskompetenz hat oder der Datenschutz speziell geregelt ist.

Bei Verarbeitungen durch natürliche Personen gilt die Verordnung nicht, wenn diese Verarbeitungen ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeit (Haushalts- beziehungsweise Familienprivileg) erfolgen.

Der DS-GVO vorrangige EU-Regelungen sind die parallel mit der DS-GVO verabschiedeten Richtlinien „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“ ((EU) 2016/680) und „über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität“ ((EU) 206/681).

Ferner gilt bis auf weiteres fort die sogenannte E-Privacy-Richtlinie[2]), die den Datenschutz im Informations- und Kommunikationsbereich (IuK) regelt und umgesetzt ist im Telekommunikationsgesetz, im Telemediengesetz und im Gesetz gegen den unlauteren Wettbewerb.

2. Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie) (ABl. EG Nr. L 201 S. 37

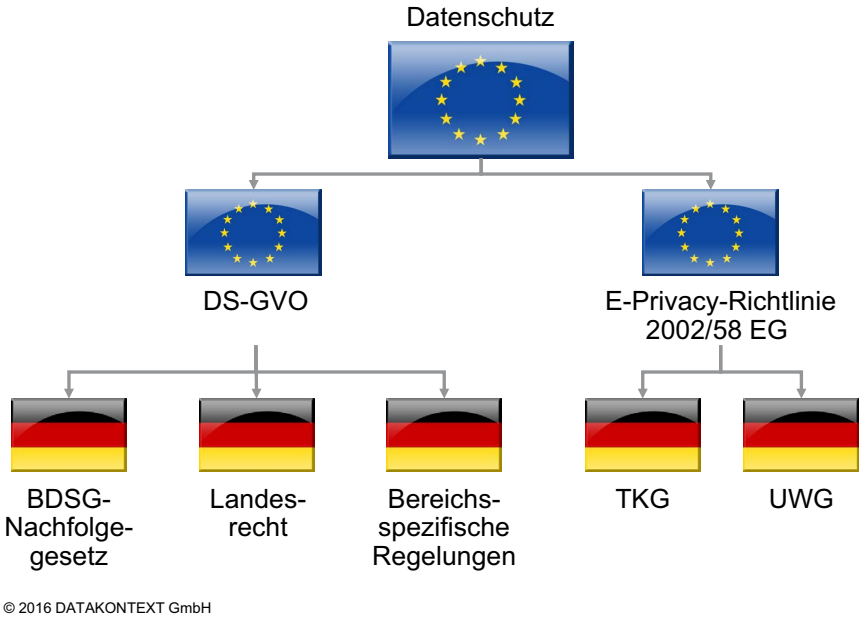

Abb. 5: Das Verhältnis europäischer Datenschutzregelungen zueinander

4.4 Räumlicher Geltungsbereich (Art. 3 DS-GVO)

Die Verordnung findet Anwendung, wenn die Verarbeitung von einem mit einer Niederlassung in der EU ansässigen Verantwortlichen oder Auftragsverarbeiter initiiert wird, gleichgültig, ob die Verarbeitung selbst in der Union stattfindet.

Werden personenbezogene Daten von natürlichen Personen, die sich in der EU aufhalten, durch einen nicht in der EU niedergelassen Verantwortlichen oder Auftragsverarbeiter verarbeitet, fallen die betroffenen Personen unter den Schutz der Verordnung, wenn

- ⇨ ihnen Waren oder Dienstleistungen angeboten werden oder
- ⇨ ihr Verhalten beobachtet wird.

Das Verhalten wird beobachtet zum Beispiel bei Registrierung der Internetnutzung, der Auswertung von Postings aber auch der Auswertung von Mitarbeiterdaten von Konzerntöchtern durch die Konzernmutter.

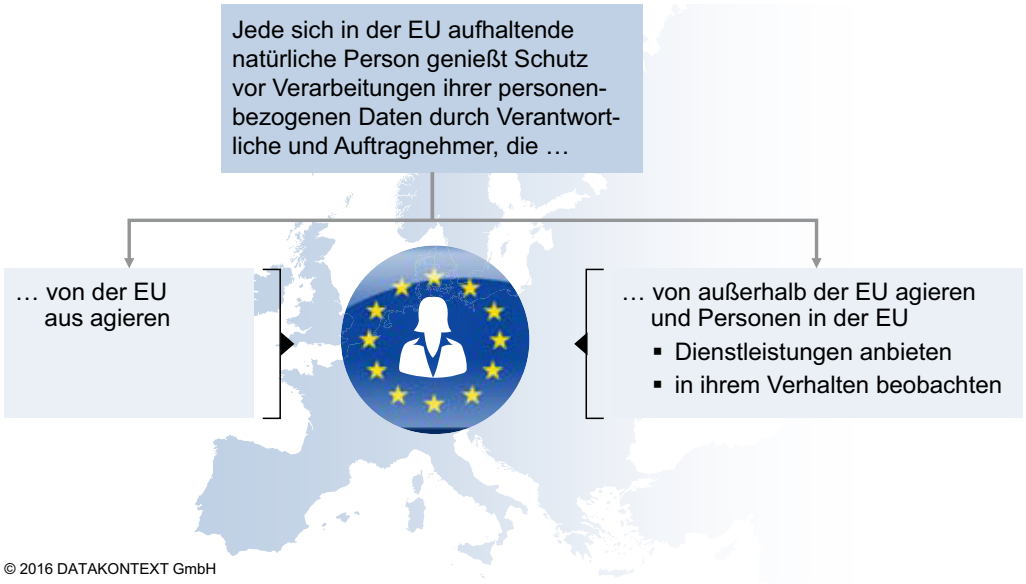

Abb. 6: Räumlicher Schutzbereich

4.5 Der Verantwortliche als Adressat der Verordnung (Art. 3 DS-GVO)

Abb. 7: An der Datenverarbeitung Beteiligte

Primärer Adressat der Verordnung ist der sogenannte Verantwortliche, das heißt die natürliche oder juristische Person, Behörde oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DS-GVO). Er hat für die Zulässigkeit der Verarbeitung und insbesondere für die Weitergabe der Daten der betroffenen Person an Dritte einzustehen, hat Auftragsverarbeiter sorgfältig auszuwählen und zu überwachen, hat die Rechte der Betroffenen zu erfüllen und unterliegt der Aufsicht staatlicher Aufsichtsbehörden.

Grundlage des gemeinsamen Verfahrens mehrerer Verantwortlicher bildet Art. 26 DS-GVO. Danach können zwei oder mehr Verantwortliche per Vertrag gemeinsame Zwecke und Mittel zur Verarbeitung personenbezogener Daten festlegen. Vertragsinhalt muss insbesondere auch sein, wer von ihnen welche Aufgaben wahrnimmt, die ihnen nach der Verordnung obliegen, und wer insbesondere die für die Erfüllung der Rechte der betroffenen Personen erforderlichen Maßnahmen ergreift.

Die Verordnung enthält auch Regelungen, die sich an Verantwortliche richten, die als Unternehmen zu verstehen sind. Als Unternehmen ist nach Art. 4 Nr. 18 jede natürliche und juristische Person einschließlich Personengesellschaften oder Vereinigungen zu verstehen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgeht.

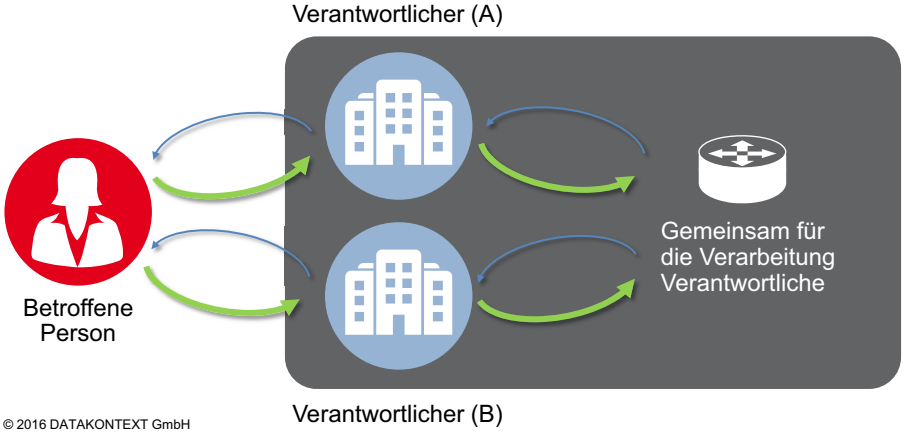

Abb. 8: Gemeinsam für die Verarbeitung Verantwortliche

Auch eine einzelne natürliche Person erfüllt bei Ausübung wirtschaftlicher Tätigkeit den Unternehmensbegriff. Mehrere der den obigen Begriff des Unternehmens erfüllende Verantwortliche können dann eine „Unternehmensgruppe“ bilden, sofern die Gruppe so strukturiert ist, dass sie aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht (Erwägungsgrund 37 DS-GVO). Bedeutung erlangen die Begriffe unter anderem im Rahmen der Regelung verbindlicher interner Datenschutzvorschriften (Art. 47 Abs. 1 lit. a DS-GVO), der gemeinsamen Bestellung eines Datenschutzbeauftragten (Art. 37 Abs. 2 DS-GVO) oder der Frage des Hineinlesens eines gewissen Konzernprivilegs in Art. 6 Abs. 1 lit. f DS-GVO gemäß Erwägungsgrund 48 DS-GVO.

4.6 Der Auftragsverarbeiter als Adressat der Verordnung

Setzt ein Verantwortlicher Auftragsverarbeiter ein, so ändert das an seiner primären Verantwortung für die Einhaltung der DS-GVO nichts. Gleichwohl werden unmittelbar auch im Auftrag tätig werdende Stellen mit Pflichten belegt, das heißt natürliche oder juristische Personen, Behörden oder sonstige Einrichtungen, die personenbezogene Daten weisungsgebunden im Auftrag des Verantwortlichen verarbeiten (Art. 4 Nr. 8, 29 DS-GVO). Neu ist unter anderem, dass der Auftragsverarbeiter gegebenenfalls gemeinsam mit seinem Auftraggeber für einen, infolge rechtswidriger Datenverarbeitung eingetretenen materiellen und immateriellen Schaden haftet (Art. 82 Abs. 1 DS-GVO). Setzt sich der Auftragnehmer über die ihm gegebenen Weisungen hinsichtlich der Bindung an die Zwecke und Mittel der Datenverarbeitung hinweg, ist er für diese unautorisierte Verarbeitung als der für die Verarbeitung Verantwortliche in Rechenschaft zu ziehen (Art. 28 Abs. 10 DS-GVO).

Auftragsverarbeiter dürfen nur mit Datenverarbeitungen betraut werden, zu denen der Auftragnehmer auch selbst befugt wäre. Damit ist die eigentliche Verarbeitung der Daten durch den Auftragsverarbeiter nicht erneut in Frage zu stellen. Auf seine Zulässigkeit zu prüfen ist jedoch der Vorgang der Weitergabe der Daten an den Auftragnehmer als „Empfänger“.

Unterschiedlich bewertet wird, ob der Auftragnehmer, nach der Verordnung gemäß seiner Weisungsgebundenheit (§ 29 DS-GVO) weiterhin „privilegierter“ Datenempfänger ist, oder ob er erst im Rahmen berechtigter Interessen des Auftraggebers nach Art. 6 Abs. 1 lit. f, DS-GVO zur Verarbeitung legitimiert werden kann, sofern nicht spezielle Geheimhaltungspflichten (zum Beispiel Art. 9 DS-GVO oder § 203 StGB) entgegenstehen. Die Auffassungen, die nunmehr nach der DS-GVO die Privilegierung verneinen, erscheinen nicht überzeugend (siehe Kap. Einleitung, 2.2)

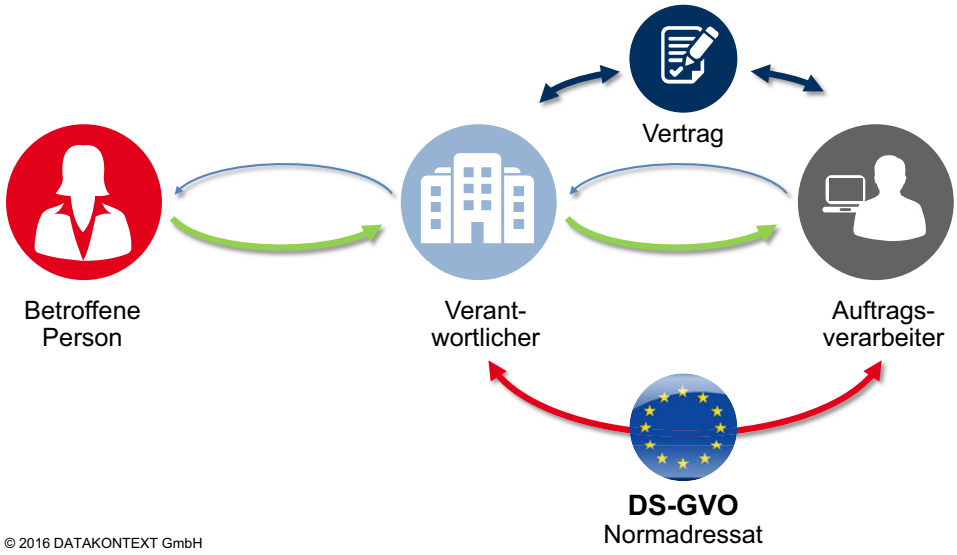

Abb. 9: Auftragsverarbeitung

4.7 Die bei der Datenverarbeitung Beschäftigten als Adressat der Verordnung

Die DS-GVO wendet sich in Art. 29 auch an Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, und gibt ihnen vor, personenbezogene Daten grundsätzlich nur auf Anweisung des für die Verarbeitung Verantwortlichen zu verarbeiten. Die entsprechende Verpflichtung des Verantwortlichen und des Auftragverarbeiters, die Mitarbeiter hierzu anzuhalten, findet sich in Art. 32 Abs. 4 DS-GVO. Eine Pflicht privater Arbeitgeber, die Beschäftigten bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten, besteht nunmehr jedoch nur noch indirekt, indem Auftragsverarbeiter sicherzustellen haben, dass die von ihnen zur Verarbeitung personenbezogener Daten autorisierten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DS-GVO). Andererseits wird der Verantwortliche im Rahmen der Datenschutzorganisation und seiner Unterweisungsverpflichtung die Beschäftigten auf ihre Vertraulichkeitspflichten besonders hinweisen müssen.

Die Beschäftigten müssen sich darüber hinaus bewusst sein, dass sie für die unbefugte Verwendung personenbezogener Daten einstehen müssen. Auch sie können – nach der zu erwartenden Änderung des OwiG – wie bisher wegen eines Verstoßes gegen die DS-GVO mit einer Geldbuße belegt werden. Schwere Verstöße können als Straftat geahndet werden. Ferner können sie der betroffenen Person und dem Arbeitgeber für eingetretene Schäden haftbar sein und letztendlich arbeitsrechtliche Konsequenzen zu fürchten haben.

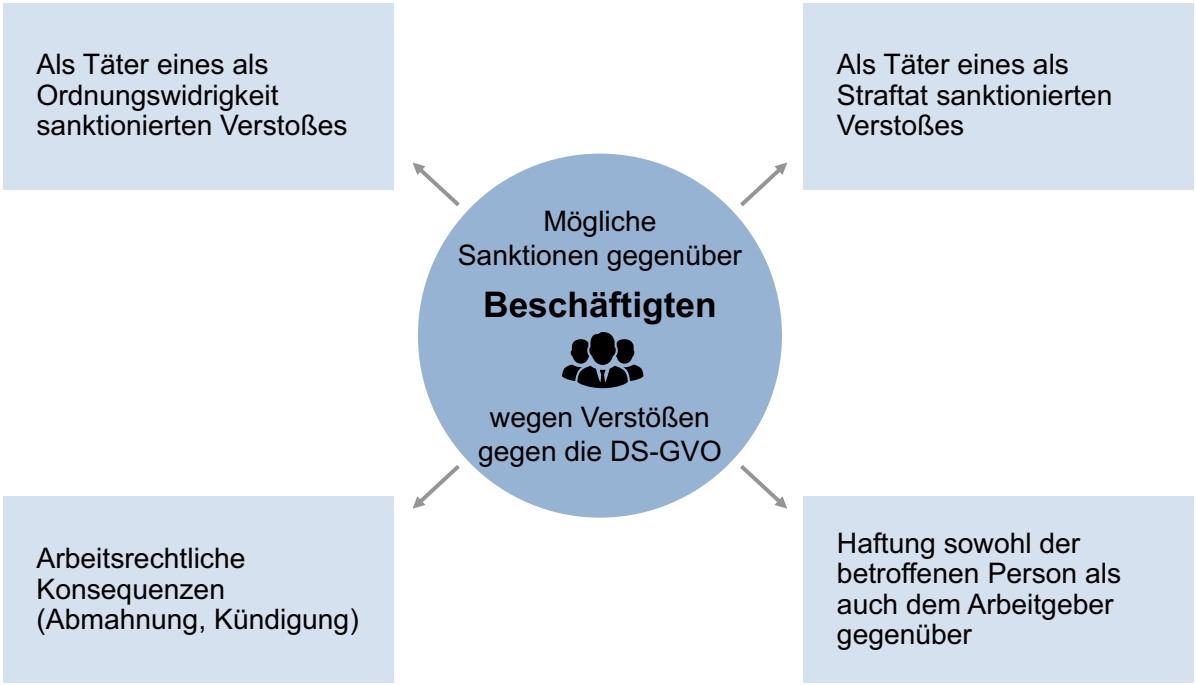

Abb. 10: Pflichtverstöße von Beschäftigten

4.8 Prinzipien der Datenverarbeitung

Bei der Verarbeitung personenbezogener Daten ist von den in Art. 5 DS-GVO festgelegten Grundsätzen auszugehen, die für die nachfolgenden diesbezüglichen Ausführungsbestimmungen den Rahmen vorgeben. Maßstäbe sind zunächst der Grundsatz von Treu und Glauben und die Gewährleistung der Transparenz der sie betreffenden Datenverarbeitungen gegenüber der betroffenen Person. Unaufgefordert zu informieren ist insbesondere über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Zudem sind die betroffen Personen über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können.

Die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Sie müssen angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, hat der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung der Speicherung vorzusehen. Zudem sind alle vertretbaren Schritte zu unternehmen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

4.9 Die sieben Grundregeln der DS-GVO

Die Gewährleistung des datenschutzgerechten Umgangs mit personenbezogenen Daten basiert auf folgenden sieben Grundregeln:

- **Rechtmäßigkeit**
  Die Rechtmäßigkeit der Verarbeitung bestimmt sich nach dem Verbotsprinzip des Art. 6 DS-GVO. Jeder Verarbeitungsschritt bedarf einer zweckbezogenen Erlaubnis (siehe Kap. 1.10).

- **Transparenz**
  Teil des Rechts auf informationelle Selbstbestimmung, das auch den Art. 8 GRCh ausfüllt ist, dass der Betroffene weiß, wer welche Daten zu welchen Zwecken über ihn verarbeitet. Die Verordnung konkretisiert den Transparenzgrundsatz in einem weit über die Regelungen des BDSG hinausgehenden Umfang unteranderem in den Art. 12 bis 15, 19 und 34.

- **Rechte der betroffenen Person**
  Zu den Rechten der betroffenen Person, gehört zunächst das Recht auf diejenigen Informationen, die die Transparenz der Datenverarbeitung sicherstellen. Korrekturrechte in Form der Berichtigung, der Löschung, der nur eingeschränkt erfolgenden Verarbeitung, der Datenübertragung (Art. 16-20 DS-GVO) sind Abwehrrechte gegen unzulässige Verarbeitungen. Abwehrrechte ergeben sich gegebenenfalls auch aus dem Widerspruchsrecht des Art. 21 DS-GVO. Einen Anspruch auf bei Wahrnehmung seiner Rechte gegebenenfalls auf erfor-

derliche Hilfestellung hat die betroffene Person gegenüber der Aufsichtsbehörde (Art. 77 DS-GVO) Die datenschutzrechtliche Haftungsnorm des Art. 82 DS-GVO für sowohl materieller als auch immaterieller Schädigungen, die infolge rechtswidriger Datenverarbeitung eingetreten sind, sichert die Rechtsstellung ab (siehe Kap. Einl. 2.8).

⇨ **Kontrolle**
Zunächst obliegt es dem Verantwortlichen, die etablierte Datenschutzorganisation erforderlichenfalls auch zu überprüfen und zu aktualisieren. Die Kontrolle der Einhaltung der Verordnung obliegt sodann der internen Kontrollinstanz des Datenschutzbeauftragten und der externen Kontrollinstanz in Gestalt der staatlichen Aufsichtsbehörde. Daneben ist es eine „Selbstpflicht" der betroffenen Person, durch Wahrnehmung ihrer Informations- und Korrekturrechte Zweifeln an der Korrektheit der Verarbeitung ihrer Daten nachzugehen und gegebenenfalls die ihr zustehenden Abwehrrechte zu nutzen.

⇨ **Sanktionen**
Abgesichert wird die Einhaltung der Verordnung durch die mögliche Ahndung von Verstößen durch Verhängung eines Bußgelds (Art. 83 DS-GVO) oder auch durch strafrechtliche Verfolgung im Rahmen nationalstaatlicher Strafnormen (Art. 84 DS-GVO). Bußgelder können verhängt werden gegen als Verantwortliche agierende natürliche Person beziehungsweise Unternehmen.

⇨ **Datenschutzkonforme Organisation**
Der Verantwortliche hat unter Beachtung des Verhältnismäßigkeitsgrundsatzes geeignete technische und organisatorische Maßnahmen zu treffen um sicherzustellen, dass die Verarbeitungen rechtmäßig verlaufen. Hierfür ist er nachweispflichtig (Art. 24 DS-GVO). Er hat solche Verarbeitungstechniken zu wählen, die den Datenschutzgrundsätzen der Datenminimierung und den Grundsätzen des Datenschutzes durch Technikgestaltung (data protection by design) oder durch datenschutzfreundliche Voreinstellungen (data protection by default) Rechnung tragen (Art. 25 DS-GVO; Erwägungsgrund 78).

⇨ **Öffnung**
Die Verordnung lässt an verschiedenen Stellen Raum für sie ergänzende oder präzisierende Reglungen, die sich jedoch an den Schutzzielen auszurichten haben (siehe Kap. Einl., 2.5)

Abb. 11: Grundlagen der DS-GVO

4.10 Das Verbot mit Erlaubnisvorbehalt

Die DS-GVO hält daran fest, dass jede Verarbeitung personenbezogener Daten in jeder ihrer Phasen auf Grund des damit verbundenen Eingriffs in das Persönlichkeitsrecht der betroffenen Person einer Erlaubnis bedarf. An erster Stelle steht unter dem Gesichtspunkt des Datenschutzes als Erlaubnis die Einwilligung (Art. 7 DS-GVO) der betroffenen Person (siehe Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a, Art. 22 Abs. 2 lit. c DS-GVO). Darüber hinaus erlaubt die DS-GVO aber auch Verarbeitungen personenbezogener Daten ohne oder gegen den Willen der Betroffenen. Ist die Verarbeitung der Daten durch keinen Erlaubnistatbestand legitimiert, so sind die unzulässig gespeicherten Daten zu löschen (Art.17 DS-GVO). Es bestehen gegebenenfalls Unterlassungs- und Schadensersatzansprüche (Art. 82 DS-GVO). Ferner liegt eine mit Bußgeld zu ahnende Ordnungswidrigkeit (Art. 83 DS-GVO) oder auch eine Straftat vor.

Art. 6 DS-GVO listet die regelmäßig geltenden Erlaubnistatbestände auf. Ein Sachverhalt kann durch mehrere der dort genannten Erlaubnistatbestände abgedeckt sein.

Beispiel: Die Speicherung und Verarbeitung der Lohn- und Gehaltsdaten von Mitarbeitern einer Firma zum Zwecke der Steuerabführung und Gehaltsabrechnung: Die Abführung der Steuer von dem Gehalt des Arbeitnehmers geschieht im Rahmen einer im Steuerrecht begründeten rechtlichen Verpflichtung und liegt zugleich im öffentlichen Interesse. Außerdem ist die ordnungsgemäße Gehaltsabrechnung eine bei der Durchführung des Arbeitsverhältnis anfallende Aufgabe.

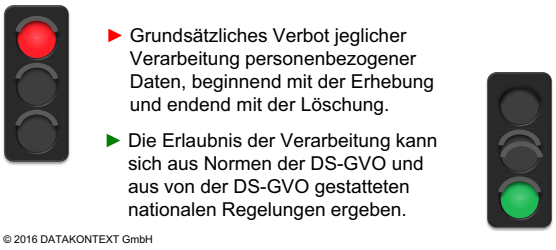

Abb. 12: Verbotsprinzip

Weitere durch konkrete Erlaubnisse aufzuhebende Verbotstatbestände enthält Art. 9 DS-GVO für die Verarbeitung besonderer Kategorien personenbezogener Daten und Art. 10 DS-GVO für die Verarbeitung von Angaben über Straftaten und strafrechtliche Verurteilungen. Art. 22 DS-GVO regelt automatisierte Einzelentscheidungen inklusive eines Profilings. Weitere Zulässigkeitsregelungen sind zu beachten, wenn personenbezogene Daten EU-grenzüberschreitend in Drittländer übermittelt werden sollen.

Sollen personenbezogene Daten in Länder außerhalb der EU (Drittländer) übermittelt werden, bedarf dieser Vorgang einer besonderen Erlaubnis.

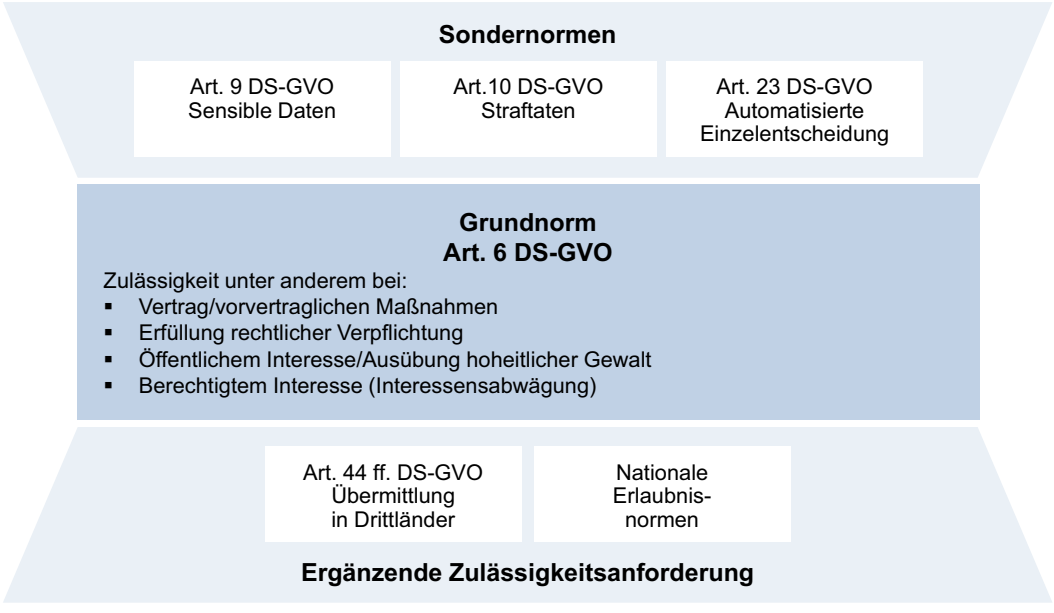

Abb. 13: Erlaubnistatbestände

4.11 Erfüllen der Rechenschaftspflicht durch Dokumentation

Ausgangspunkt für die Verarbeitungen personenbezogener Daten sind die in Art. 5 DS-GVO festgeschrieben und nachfolgend detailliert geregelten Grundsätze der Rechtmäßigkeit, der Beachtung von Treu und Glauben, der Transparenz, der Zweckbindung, der Datenminimierung und der Speicherbegrenzung sowie der Integrität und Vertraulichkeit. Der Verantwortliche ist für deren Einhaltung rechenschafts- und nachweispflichtig (Accountability) (Art. 5 Abs. 2 DS-GVO). Der Nachweis wird in der Regel anhand einer entsprechenden Dokumentation zu führen sein. Wiederholt wird diese Nachweispflicht insbesondere für die Installation der technischen und organisatorischen Maßnahmen, die die Einhaltung der Verordnung gewährleisten (Art. 24 Abs. 1 DS-GVO). Art. 7 Abs. 1 DS-GVO gibt vor, dass eine Einwilligung, die die Verarbeitung legitimiert, nachgewiesen werden können muss.

Als im Detail geregelte Dokumentationspflicht zu nennen ist unter anderem das von dem Verantwortlichen und gegebenenfalls parallel von den von ihm eigeschalteten Auftragsverarbeitern zu führende „Verzeichnis von Verarbeitungstätigkeiten“ (Art. 30 DS-GVO).

Abhängig von dem Risiko, das mit einer Verarbeitung verbunden ist, hat vor ihrer Einführung eine Datenschutz-Folgenabschätzung stattzufinden, die unter Hinzuziehung des Datenschutzbeauftragten und gegebenenfalls der Aufsichtsbehörde zu dokumentieren ist (Data Protection Impact Assessment) (Art. 35 DS-GVO). Bei einem Datentransfer in einen Drittstaat auf der Grundlage des Art. 49 Abs. 1 S. 2 DS-GVO sind die Risikoabschätzung und die ergriffenen Schutzmaßnahmen nach Art. 28 DS-GVO zu dokumentieren (Art. 49 Abs. 6 DS-GVO) und zum Gegenstand des Verfahrensverzeichnisses zu machen. Nachträglich aufgetretene und gegebenenfalls der Aufsichtsbehörde und den Betroffenen mitzuteilende Datenschutzverletzungen (Art. 33, 34 DS-GVO) sind, verbunden mit den ergriffenen Abwehrmaßnahmen, festzuhalten (Art. 34 Abs. 5 DS-GVO). Weitere umfangreiche Dokumentationspflichten bestehen zwecks Erfüllung der Transparenzregelungen gegenüber den Betroffenen (Art. 12, 13, 14, 15-22, 34 DS-GVO).

Verantwortliche müssen also jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Verarbeitungen nachweisen zu können. Das Fehlen einer Dokumentation kann mit einem Bußgeld belegt werden.

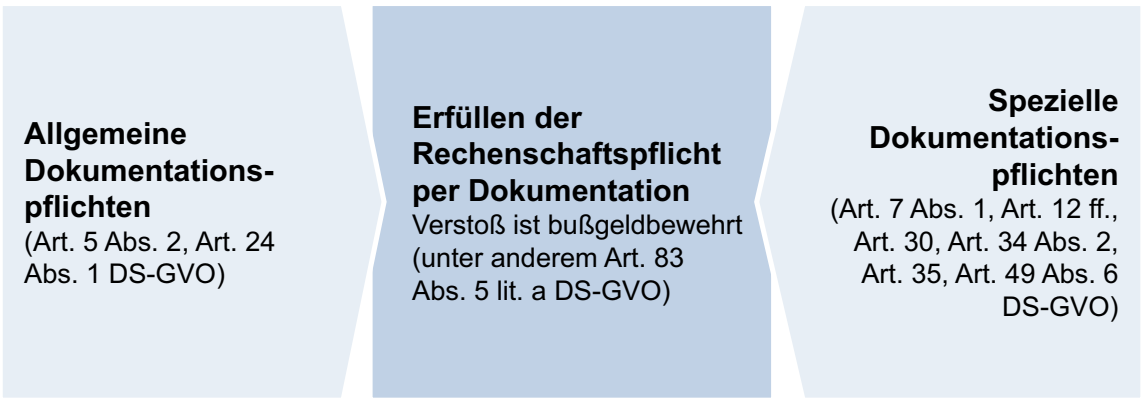

Abb. 14: Dokumentationspflichten