# Eine Praxiseinführung in die Datenschutz-Grundverordnung

## 1. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) stellte eines der ambitioniertesten legistischen Projekte der Europäischen Union der vergangenen Jahre dar. Sie ersetzte mit 25. Mai 2018 die EU-Datenschutzrichtlinie und machte die nationalen Datenschutzgesetze der 28 Mitgliedstaaten wenigstens im Grundsatz weitgehend obsolet.

Dass die DSGVO ernst zu nehmen ist, verdeutlichen nicht zuletzt die vorgesehenen harschen Strafen von bis zu 20 Millionen Euro oder 4 % des weltweiten Konzernjahresumsatzes. Die Verwaltungspraxis einiger nationalen Aufsichtsbehörden der letzten Jahre zeigt, dass auch in der Praxis vor hohen Strafen in zigfacher Millionenhöhe nicht zurückgeschreckt wird. Datenschutz wird so zu einem der größten Compliance-Risikofelder und damit notwendigerweise zu einer Priorität für jede Geschäftsleitung.

Die vorliegende Praxiseinführung dient dazu, sich rasch einen Überblick über die DSGVO und, soweit daneben noch relevant, das DSG oder einzelne ihrer Bereiche zu verschaffen. Hinsichtlich der Details verweist sie durch Angabe der entsprechenden Norm der DSGVO bzw einer Randziffer der Kommentierung des jeweiligen Artikels auf den Kommentarteil des vorliegenden Werkes.

## 2. Die wichtigsten Schritte zur DSGVO-Compliance

Um ein Mindestmaß an Compliance mit der DSGVO herzustellen, müssen Verantwortliche und Auftragsverarbeiter bereits frühzeitig Compliance-Schritte setzen. Wenn bisher Compliance-Schritte (immer noch) nicht gesetzt wurden, dann sollten diese nachgeholt werden.

Für Verantwortliche lassen sich die wichtigsten umzusetzenden Compliance-Schritte wie folgt zusammenfassen:

1) Implementierung der Grundlagen eines **Datenschutz-Compliance-Programms** (siehe Kapitel 11) einschließlich der Bestellung eines **Datenschutzbeauftragten**, soweit dies im konkreten Fall zweckmäßig oder verpflichtend ist (siehe Kapitel 14),
2) Erstellung eines **Verzeichnisses der Verarbeitungstätigkeiten** (siehe Kapitel 12),
3) Prüfung der Rechtsgrundlage der jeweiligen Datenverarbeitung (siehe Kapitel 7), insbesondere der neuen Anforderungen an eine wirksame Einwilligung (siehe Kapitel 7.1),
4) Entwicklung DSGVO-konformer **Datenschutzerklärungen** (siehe Kapitel 8) und
5) Prüfung der Rechtsgrundlage für **internationale Datenübermittlungen** (siehe Kapitel 18).

Für Auftragsverarbeiter sind die wichtigsten Compliance-Schritte:
1) Bestellung eines **Datenschutzbeauftragten**, soweit dies im konkreten Fall verpflichtend oder zweckmäßig ist (siehe Kapitel 14),
2) Erstellung eines **Verzeichnisses von Verarbeitungstätigkeiten** (siehe Kapitel 12),
3) Implementierung **angemessener Sicherheitsmaßnahmen** (siehe Kapitel 15.1),
4) Sicherstellung, dass **Subauftragsverarbeiter** nur mit der vorherigen gesonderten oder allgemeinen, schriftlichen Genehmigung des Verantwortlichen herangezogen werden (Art 28 Abs 2) und
5) Sicherstellung, dass **internationale Datenübermittlungen** nur unter Einhaltung der Voraussetzungen der DSGVO erfolgen (siehe Kapitel 18).

Die oben genannten Maßnahmen werden keine vollständige Compliance mit der DSGVO garantieren, helfen jedoch, die personellen und finanziellen Ressourcen eines Verantwortlichen oder Auftragsverarbeiters auf zentrale Aspekte zu fokussieren.

Für größere Organisationseinheiten wird es zudem erforderlich sein, eine grundsätzliche Bewertung der regulatorischen Risiken nach der DSGVO vorzunehmen, um einen effizienten Ressourceneinsatz zu ermöglichen.

## 3. Grundlegende Begriffe der DSGVO

Die DSGVO findet ausschließlich auf **personenbezogene Daten** Anwendung (siehe Kapitel 4.1). Diese sind definiert als alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche** Person beziehen, welche wiederum als **betroffene Person** bezeichnet wird (Art 4 Nr 1).

Eine Teilmenge der personenbezogenen Daten sind **sensible Daten** (auch „besondere Kategorien personenbezogener Daten"). Hierbei handelt es sich nach Art 9 Abs 1 um personenbezogene Daten betreffend die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben oder die sexuelle Orientierung sowie Gesundheitsdaten iSd Art 4 Nr 15 und genetische Daten iSd Art 4 Nr 13. Darüber hinaus zählen auch biometrische Daten (zB Fingerabdrücke oder Gesichtsbilder), die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden (Art 9 Rz 6), zu den sensiblen Daten.

Normadressaten der DSGVO sind Verantwortliche und Auftragsverarbeiter (vgl Art 3 Rz 5). Die DSGVO definiert den Begriff des **Verantwortlichen** als natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art 4 Nr 7).

**Auftragsverarbeiter** ist demgegenüber eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet, dh selbst nicht über Zwecke und Mittel der Datenverarbeitung entscheidet (Art 4 Nr 8). Lagert beispielsweise ein Unternehmen den Betrieb seiner Kundendatenbank an einen IT-Dienstleister aus, so agiert das Unternehmen weiterhin als Verantwortlicher, während der IT-Dienstleister als Auftragsverarbeiter fungiert.

Das **Verarbeiten** personenbezogener Daten ist denkbar weit definiert und umfasst jegliche Handhabung personenbezogener Daten, beginnend mit ihrer Erhebung, über das Ordnen, Verändern, Auswerten, Abfragen, Übermitteln und Gespeichert-Halten bis hin zum Löschen oder Vernichten (Art 4 Nr 2).

Der Begriff **Übermitteln** wird in der DSGVO häufig gebraucht, jedoch nicht definiert. Es kann hierunter die Offenlegung gegenüber einem anderen Verantwortlichen oder einem Auftragsverarbeiter bzw Subauftragsverarbeiter verstanden werden (siehe Art 44 Rz 2).

Der Begriff **Aufsichtsbehörde** bezeichnet die Datenschutzbehörde in jedem Mitgliedstaat.

## 4. Der Geltungsbereich der DSGVO

Im Folgenden wird beschrieben, für welche Tätigkeiten die DSGVO gilt (Kapitel 4.1), für wen die DSGVO gilt (Kapitel 4.2) und wo sie gilt (Kapitel 4.3).

### 4.1. Der sachliche Anwendungsbereich – Welche Datenverarbeitungen sind erfasst?

Grundsätzlich gilt die DSGVO für jegliche Verarbeitung personenbezogener Daten. Wie oben in Kapitel 3 ausgeführt, sind personenbezogene Daten alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen. Ob eine natürliche Person identifizierbar ist, muss **objektiv** beurteilt werden, sodass nicht nur auf die rechtlichen und tatsächlichen Möglichkeiten des Verantwortlichen, sondern auch auf die rechtlich zulässigen Möglichkeiten Dritter abzustellen ist (Art 4 Rz 4).

Beziehen sich die Daten auf **juristische Personen**, sind sie nur dann personenbezogen iSd DSGVO, wenn der Firmenwortlaut der juristischen Person den Namen einer natürlichen Personen enthält (Art 4 Rz 1). Daten, welche sich auf **verstorbene Personen** beziehen, sind ebenso wenig personenbezogen iSd DSGVO (Art 4 Rz 2).

Die DSGVO gilt grundsätzlich nur für **elektronisch verarbeitete Daten**. Für manuell (in der Regel auf Papier) verarbeitete Daten gilt die DSGVO nur, wenn die Daten in einem Dateisystem gespeichert sind oder dort gespeichert werden sollen (Art 2 Abs 1). Ein Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind (Art 4 Nr 6), wie zB eine nach Namen geordnete Personalaktenverwaltung. Einzelne Papierakten unterliegen jedoch nicht der DSGVO (Art 2 Rz 6).

Als Rechtsakt der Union findet die DSGVO außerhalb des Anwendungsbereichs des Unionsrechts (zB im Bereich der nationalen Sicherheit) keine Anwendung (Art 2 Abs 2 lit a). Weiters gilt die DSGVO nicht für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik (GASP; Art 2 Abs 2 lit d) sowie für die Bereiche der Strafrechtspflege, des Strafvollzugs und der öffentlichen Sicherheit (Art 2 Abs 2 lit d; hier ist die DSRL-PJeinschlägig, welche insbesondere in den §§ 36–61 DSG umgesetzt wurde).

Schließlich gilt die DSGVO nicht bei der Verarbeitung von personenbezogenen Daten durch natürliche Personen zur Ausübung ausschließ-

lich persönlicher oder familiärer Tätigkeiten („**Household Exemption**"; Art 2 Abs 2 lit c). Hierzu zählt insbesondere die zu privaten Zwecken erfolgende Nutzung sozialer Netzwerke (Art 2 Rz 10).

### 4.2. Der persönliche Anwendungsbereich – Für wen gilt die DSGVO?

Normadressaten der DSGVO sind sowohl Verantwortliche als auch Auftragsverarbeiter (siehe Kapitel 3 zur Definition dieser Begriffe).

Nach der DS-RL war die Rolle des Auftragsverarbeiters im Vergleich zum Verantwortlichen attraktiv, da diesen nur untergeordnete regulatorische Pflichten trafen. Der wirtschaftliche Nachteil der Rolle des Auftragsverarbeiters bestand und besteht freilich darin, die personenbezogenen Daten nicht für eigene Zwecke verwenden zu dürfen. Wer personenbezogene Daten zu eigenen Zwecken verwenden und so aus ihnen einen wirtschaftlichen Wert schöpfen wollte (Stichwort „**Dateneigentum**"), musste hingegen die Rolle des Verantwortlichen für sich beanspruchen, was mit erheblichen zusätzlichen Pflichten verbunden war.

Diese Gleichung ändert die DSGVO insofern, als Auftragsverarbeiter – ebenso wie Verantwortliche – nunmehr primäre Normadressaten sind, erheblichen regulatorischen Pflichten unterworfen werden (siehe einleitend Kapitel 2 oben) und insbesondere denselben Geldbußen ausgesetzt sind (siehe Kapitel 20). Durch diese tendenzielle Annäherung der Verantwortlichkeit von Verantwortlichen und Auftragsverarbeitern treten daher die wirtschaftlichen Vorteile der Verantwortlichenstellung in den Vordergrund. Viele Unternehmen, die sich vor In-Kraft-Treten der DSGVO ausschließlich auf eine Auftragsverarbeiterstellung beschränkt haben, versuchen daher zunehmend, eine Stellung als Verantwortlicher zu erlangen. Dies bedeutet jedoch nicht nur, dass regulatorische Pflichten hinsichtlich der Rechtsgrundlage der Datenverarbeitung, wie insbesondere der Einwilligung der Betroffenen (siehe Kapitel 7) und der Transparenz (siehe Kapitel 8) einzuhalten sind, sondern auch, dass bestehende Verträge mit Kunden, Abnehmern und allenfalls Betroffenen zu überarbeiten waren, um diese neue regulatorische Realität zu reflektieren.

### 4.3. Der räumliche Anwendungsbereich – Wo gilt die DSGVO?

Die DSGVO findet jedenfalls auf Verantwortliche und Auftragsverarbeiter Anwendung, welche ihren **Sitz in der EU bzw dem EWR** (vgl

Art 3 Rz 7) haben. Auftragsverarbeiter mit Sitz in der EU bzw dem EWR unterliegen sogar dann der DSGVO, wenn sie für Verantwortliche tätig sind, die nicht der DSGVO unterliegen (Art 3 Rz 5).

Weiters gilt die DSGVO auch dann, wenn der Verantwortliche bzw Auftragsverarbeiter seinen Sitz zwar nicht in der EU bzw dem EWR hat, jedoch eine Niederlassung (zB eine Tochtergesellschaft) in der EU oder dem EWR hat und die Datenverarbeitung **im Rahmen der Tätigkeiten dieser Niederlassung** erfolgt. Ein solcher Fall liegt zB vor, wenn die US-Konzernmutter die personenbezogenen Daten der Kunden einer österreichischen Tochtergesellschaft verarbeitet, um die Verkaufsaktivitäten der Tochtergesellschaft zu unterstützen (vgl Art 3 Rz 3).

Um sicherzustellen, dass Wirtschaftsakteure ohne Niederlassung in der EU bzw dem EWR, welche auf dem europäischen Markt tätig werden, denselben Wettbewerbsbedingungen wie europäische Unternehmen unterliegen, gilt die DSGVO auch für Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der Union, wenn diese ihre **Waren oder Dienstleistungen entgeltlich oder unentgeltlich in der EU bzw dem EWR anbieten** (Art 3 Abs 2 lit b).

Weiters findet die DSGVO auch auf Verantwortliche und Auftragsverarbeiter ohne Niederlassung in der Union Anwendung, die das Verhalten betroffener Personen in der Union **beobachten** (Art 3 Abs 2 lit b). Dies gilt insbesondere für sog Online-Advertising-Networks, welche das Surf-Verhalten von Internetnutzern protokollieren, um personenbezogene Online-Werbung ausliefern zu können.

## 5. Das Verhältnis zu nationalen Datenschutzgesetzen

Grundsätzlich gilt, dass die DSGVO wie jede EU-Verordnung unmittelbar anwendbar ist und daher nicht durch nationales Recht umgesetzt werden darf. Das DSG 2000 besteht daher seit dem 25. Mai 2018 nicht mehr in seiner damaligen Form.

Außerhalb des Anwendungsbereichs der DSGVO (siehe Kapitel 4) bleibt es dem nationalen Gesetzgeber jedoch überlassen, Regelungen zu treffen. Bei der Frage des Datenschutzes für juristische Personen, zum Beispiel, stellt der ohnedies bereits lange gegebene und in Umsetzung der Geschäftsgeheimnis-RL (2016/943/EU) noch präzisierte Schutz von Geschäftsgeheimnissen (§§ 123 f StGB, §§ 11 f und insbesondere §§ 26a – 26j UWG) bereits ein hinreichendes Regelungsinstrument dar, sodass es eines nationalen Sonderwegs mit zweifelhafter systematischer Einordnung

des auch datenschutzrechtlichen Schutzes juristischer Personen nicht bedarf; trotzdem schützt § 1 DSG weiterhin auch juristische Personen.

Hiervon unabhängig gibt es zahlreiche Regelungsfragen im Anwendungsbereich der DSGVO, für welche die DSGVO keine oder keine abschließende Antwort vorsieht, sondern durch **Öffnungsklauseln** bewusst und kompromisshaft eine legislative Zuständigkeit der Mitgliedstaaten begründet und damit Unterschiede innerhalb der Mitgliedsstaaten zulässt. Dies ist insbesondere bei folgenden Regelungsfragen der Fall (vgl Art 92 Rz 4):

- Ab welchem Alter kann ein Minderjähriger wirksam in die Verarbeitung seiner personenbezogenen Daten einwilligen? (Art 8 Abs 1 UAbs 2)
- Wann ist eine wirksame Einwilligung in die Verarbeitung sensibler Daten ausgeschlossen? (Art 9 Abs 2 lit a)
- Unterliegt die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten zusätzlichen Beschränkungen? (Art 9 Abs 5)
- Dürfen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten überhaupt verarbeitet werden?
- Sind automatisierte Entscheidungen und Profiling, welche für den Abschluss oder die Erfüllung eines Vertrages mit der betroffenen Person nicht erforderlich sind, auch ohne Einwilligung der betroffenen Person zulässig? (Art 22 Abs 2 lit b)
- Unterliegen die Betroffenenrechte zusätzlichen Beschränkungen? (Art 23)
- Müssen nur bestimmte oder alle Verantwortlichen und Auftragsverarbeiter einen Datenschutzbeauftragten bestellen? (Art 37 Abs 4)
- Können gegen Behörden und öffentliche Stellen Geldbußen verhängt werden? (Art 83 Abs 7)
- Können Datenschutzorganisationen im Namen der Betroffenen Schadenersatz begehren? (Art 80 Abs 1)
- Können Datenschutzorganisationen auch ohne Auftrag eines Betroffenen gegen einen Verantwortlichen oder Auftragsverarbeiter mit Klage vorgehen? (Art 80 Abs 2)
- Unter welchen Voraussetzungen ist eine Sekundärnutzung wissenschaftlicher Daten zulässig? (Art. 89 Abs 1)

Österreich hat von einigen, dieser Öffnungsklauseln gebraucht gemacht: So liegt in Österreich etwa das Einwilligungsalter bei 14 Jahren (§ 4 Abs 4 DSG). Nicht umgesetzt wurde allerdings zB die Möglichkeit,

Datenschutzorganisationen das Recht zu geben, ohne Auftrag eines Betroffenen gegen einen Verantwortlichen oder Auftragsverarbeiter mit Klage vorzugehen.

Darüber hinaus räumt die DSGVO den Mitgliedstaaten eine nahezu unbeschränkte Regelungskompetenz für den **Beschäftigungskontext** ein (Art 88) und überlässt es weiters den Mitgliedstaaten weitgehend, die Verarbeitung personenbezogener Daten zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken zu regeln (Art 85; vgl § 9 DSG) sowie einen Ausgleich zwischen einem Recht auf Zugang zu amtlichen Dokumenten und dem Datenschutz zu finden (Art 86).

Im Ergebnis ist es daher notwendig, die DSGVO stets mit dem jeweils anwendbaren nationalen „DSGVO-Umsetzungsgesetz" in Zusammenschau zu lesen, weshalb die DSGVO auch als „**hinkende Verordnung**" bezeichnet wird (zum Begriff vgl *Constantinesco*, Das Recht der Europäischen Gemeinschaften, Band I: Das institutionelle Recht (1977) 562). Das sich stellende Problem ist, dass die DSGVO **keinerlei Kollisionsrecht** enthält und damit die Frage offen lässt, wann das Recht welches Mitgliedstaates anzuwenden ist.

Hierbei handelt es sich uE um eine planwidrige Lücke, welche in **Analogie zur Zuständigkeitsordnung** der DSGVO (siehe hierzu Kapitel 19) zu schließen ist. Besteht daher für einen Verantwortlichen oder Auftragsverarbeiter eine federführende Zuständigkeit einer bestimmten Aufsichtsbehörde nach Art 56, so ist grundsätzlich nur das DSGVO-Umsetzungsgesetz dieses Mitgliedstaates anwendbar (siehe ausführlich Art 92 Rz 5).

## 6. Die Grundsätze der Datenverarbeitung

Die DSGVO normiert folgende Grundsätze, welche bei jeder Verarbeitung personenbezogener Daten einzuhalten sind (Art 5 Abs 1):

- **Rechtmäßigkeit** (Art 5 Abs 1 lit a): Personenbezogene Daten müssen auf rechtmäßige Weise verarbeitet werden, was bedeutet, dass eine Rechtsgrundlage für die Verarbeitung vorhanden sein muss (siehe Kapitel 7).
- **Treu und Glauben** (Art 5 Abs 1 lit a): Die Verarbeitung personenbezogener Daten darf nur nach Treu und Glauben erfolgen, was insbesondere bei der Durchführung von Interessensabwägungen zu berücksichtigen ist (vgl zB Art 6 Abs 1 lit f).
- **Transparenz** (Art 5 Abs 1 lit a): Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet

werden. Dieser Grundsatz wird durch die in der DSGVO normierten Informationspflichten konkretisiert (siehe Kapitel 8).

- **Zweckbindung** (Art 5 Abs 1 lit b): Erstens dürfen personenbezogene Daten nur erhoben werden, wenn spätestens zum Zeitpunkt der Erhebung ein eindeutiger und legitimer Zweck festgelegt wurde (Grundsatz der **Zweckfestlegung**). Dies kann insbesondere durch eine Dokumentation der Verarbeitungszwecke im Verzeichnis der Verarbeitungstätigkeiten (siehe Kapitel 12) erfolgen. Im Übrigen ergibt sich aus der Anforderung der Legitimität der Verarbeitungszwecke, dass sonstige Rechtsvorschriften (zB das Konsumentenschutzrecht oder § 174 TKG 2021) bei einer datenschutzrechtlichen Prüfung mittelbar ebenso zu berücksichtigen sind. Das zweite Element des Zweckbindungsgrundsatzes besteht darin, dass die erhobenen Daten – vorbehaltlich der Einwilligung der betroffenen Person (Art 6 Rz 37) – nur zu Zwecken weiterverarbeitet werden dürfen, welche mit den ursprünglich festgelegten Zwecken vereinbar sind (**Zweckbindung ieS**). Ob eine Vereinbarkeit der Zwecke gegeben ist, muss anhand einer Reihe von Kriterien geprüft werden, welche in Art 6 Abs 4 normiert sind. Ist der neue Zweck mit dem alten (ursprünglichen) Zweck vereinbar, so ist die Verarbeitung zulässig, ohne dass eine andere Rechtsgrundlage (zB eine neuerliche Einwilligung) erforderlich wäre (vgl Art 6 Rz 39). Allerdings ist die betroffene Person über den neuen Verarbeitungszweck zu informieren (Art 13 Abs 3 und Art 14 Abs 4).
- **Datenminimierung** (Art 5 Abs 1 lit c): Art und Umfang der verarbeiteten Daten müssen den Verarbeitungszwecken angemessen sein sowie auf das für die Zwecke notwendige Maß beschränkt sein. Hierbei handelt es sich um die datenschutzrechtliche Ausprägung des allgemeinen Verhältnismäßigkeitsgrundsatzes. Ein unzulässiger Datenerhebungsexzess liegt beispielsweise vor, wenn zu dem Zweck, das von jedem Mitarbeiter verbrauchte Datenvolumen zu dokumentieren, nicht nur die Größe der heruntergeladenen Dateien, sondern auch der Dateiname und die Uhrzeit jedes Downloads protokolliert wird.
- **Richtigkeit** (Art 5 Abs 1 lit d): Personenbezogene Daten müssen sachlich richtig und, wenn dies für den Verarbeitungszweck erforderlich ist, auf dem neuersten Stand sein.
- **Speicherbegrenzung** (Art 5 Abs 1 lit e): Personenbezogene Daten dürfen nur solange gespeichert werden, wie dies für die festgelegten Verarbeitungszwecke erforderlich ist. Nach Ablauf dieser Frist sind

die Daten entweder zu löschen oder zu anonymisieren. Mit dem Grundsatz der Speicherbegrenzung wäre es zB nicht vereinbar, die Dokumentation zu einem Vertragsverhältnis zum Zweck der Abwehr allfälliger Ansprüche des Kunden gespeichert zu halten, wenn alle denkbaren Ansprüche bereits verjährt sind.

– **Integrität und Vertraulichkeit** (Art 5 Abs 1 lit f): Entgegen seinem Namen erfordert dieser Grundsatz nicht nur angemessene Maßnahmen zum Schutz der Integrität und Vertraulichkeit der Daten, sondern auch zum Schutz ihrer Verfügbarkeit sowie der Rechtmäßigkeit ihrer Verarbeitung. Eine treffendere Bezeichnung des Grundsatzes des Art 5 Abs 1 lit f wäre daher „Sicherheit und Rechtmäßigkeit" (vgl Art 5 Rz 21).

Diese Grundsätze der Datenverarbeitung werden durch den Grundsatz der **Rechenschaftspflicht** („Accountability") ergänzt, wonach der Verantwortliche erstens Compliance-Maßnahmen zu implementieren hat, welche die Einhaltung der oben genannten Grundsätze sicherstellen, und zweitens die Einhaltung dieser Grundsätze nachweisen können muss (Art 5 Abs 2). Beim zweiten Element der Rechenschaftspflicht handelt es sich um keine (mit der Unschuldsvermutung ohnedies nicht vereinbare) Beweislastregelung, sondern eine materielle Nachweispflicht, deren Verletzung nach der DSGVO jedoch nicht mit einer Geldbuße bedroht ist, sondern von der zuständigen Aufsichtsbehörde lediglich zwangsweise durchgesetzt werden kann (Art 5 Rz 23).

## 7. Erforderlichkeit einer Rechtsgrundlage für jede Datenverarbeitung

Nach der Regelungssystematik der DSGVO ist jegliche Verarbeitung personenbezogener Daten verboten, es sei denn, einer der in Art 6, 9 und 10 abschließend geregelten Ausnahmetatbestände bietet eine entsprechende Rechtsgrundlage für die Datenverarbeitung. Bei der Prüfung der Zulässigkeit einer Datenverarbeitung muss daher eine konkrete Rechtsgrundlage für die Datenverarbeitung bejaht werden, widrigenfalls es bei der Unzulässigkeit der Verarbeitung bleibt.

Um eine potentiell anwendbare Rechtsgrundlage zu identifizieren, muss zunächst eine Differenzierung anhand der Art der personenbezogenen Daten erfolgen.

Handelt es sich um personenbezogene **Daten über strafrechtliche Verurteilungen und Straftaten** oder damit zusammenhängende Siche-