Sehr geehrte Seminarbesucherin,
sehr geehrter Seminarbesucher,

Aufklärung über eine Datenerhebung
zur Durchführung der vorliegenden Veranstaltung haben wir personenbezogene Daten von Ihnen erhoben, und zwar

- Ihren Namen
- Ihr zugehöriges Unternehmen, d.h. dasjenige Unternehmen, welches Sie zu unserem heutigen Seminar angemeldet hat,
- ob die Seminargebühr für Sie bezahlt ist,
- die zur Zahlung gehörenden Bankdaten (Zahlungsdatum, Absenderkonto).

Sollten Sie mit uns im Zusammenhang mit Ihrer Anmeldung kommuniziert haben, haben wir die hierbei angefallenen Kommunikationsdaten ebenfalls erfasst, also die Telefonnummer Ihres Anrufs und/oder Ihre email-Adresse und ggf. den Namen Ihres Kollegen/Mitarbeiters, welcher für Sie anrief, ferner den Zeitpunkt des betreffenden Kontakts und dessen Inhalt.

Aufklärung über den Zweck der Datenerhebung und Datenverarbeitung
Ihre Daten werden verwendet, um das vorliegende Seminar durchführen zu können, insbesondere die Seminarteilnehmer und die Wirksamkeit ihrer Buchung durch Bezahlung feststellen zu können. Des weiteren dienen die Daten dem Ausstellen Ihrer jeweiligen Fortbildungsbescheinigung und, falls Sie noch nicht Mandant bei uns sind, der anschließenden Mandantenakquise, wenn wir Sie anrufen, auf das Seminar Bezug nehmen und fragen, ob Sie noch einen Anwalt brauchen. Sodann dienen die Daten buchhalterischen und steuerlichen Zwecken im Rahmen der gesetzlichen Vorschriften.

Aufklärung über das Berichtigungs- und Widerspruchsrecht
Sollten wir Ihre personenbezogenen Daten fehlerhaft erfasst, bspw. Ihren Namen falsch geschrieben haben, können Sie verlangen, daß wir das berichtigen. Sie können der Verwendung Ihrer Daten widersprechen und deren Löschung verlangen, soweit wir sie nicht zur Erfüllung einer rechtlichen Verpflichtung, zur Verwirklichung der Ziele dieser Datenverarbeitung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen.

Aufklärung über die Datensicherheit
Ihre oben benannten Daten werden bei uns an drei Stellen gespeichert:

- in der Buchhaltung
- in unserem physischen Seminarordner (dem Verzeichnis aller durchgeführten Seminare und der jeweiligen Teilnehmer)
- in einer Datei namens „Teilnehmerliste“ auf unserem Kanzleiserver.

Die bei uns hinterlegten Daten können ausschließlich von Kanzleiangehörigen eingesehen werden. Mit allen Kanzleiangehörigen einschließlich unserer Putzkräfte sowie mit unserem IT-Administrator, der über einen administrativen Fernzugang verfügt, bestehen Verschwiegenheitsvereinbarungen, die sicherstellen, daß Ihre Daten nicht nach außen gelangen. Unser Server, auf dem die Teilnehmerliste hinterlegt ist, ist durch eine Firewall gegen unbefugte Zugriffe von außen abgesichert. Ferner ist das betreffende Verzeichnis durch ein Passwort gesichert, so daß nur Frau Marx und RA Scheidacker persönlich darauf zugreifen können. Sollten Sie uns unverschlüsselt per email Daten übersandt haben, können wir jedoch nicht gewährleisten, daß diese bei Ihrem oder unserem Internetprovider nicht unbefugt erhoben, verwendet oder weitergegeben worden sind.

Aufklärung über Datenweitergabe
Die Weitergabe Ihrer Daten geschieht in vollem Umfang an unseren Steuerberater, welcher seinerseits Datensicherheitsgrundsätze beachtet und zur Verschwiegenheit verpflichtet ist, sowie über diesen an das Finanzamt. Des weiteren erhalten sämtliche Teilnehmer der vorliegenden Veranstaltung eine Teilnehmerliste mit einem reduzierten Datensatz, welcher nur den Namen des Teilnehmers und die zugehörige Firma enthält. Dies dient dazu, daß sich die Teilnehmer, die gemeinsam an dem Seminar teilgenommen haben, untereinander bei Bedarf kontaktieren können. Die Nicht-Weitergabe dieser Daten durch die Teilnehmer können wir nicht sicherstellen, da wir keine entsprechenden Datenschutzvereinbarungen mit ihnen abgeschlossen haben. Da aber der 25. Mai 2018 noch nicht erreicht ist, so daß die DSGVO noch nicht gilt, und da ein Schaden durch diese Datenweitergabe nicht zu befürchten ist, ist das unschädlich. Darüber hinaus werden Ihre Daten von uns nicht weitergegeben.

Aufklärung über Aufbewahrungsfristen und Löschung
Ihre Daten werden gelöscht, wenn die steuerlichen Aufbewahrungsfristen abgelaufen sind.

Benennung des Verantwortlichen und des Datenschutzbeauftragten
Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO ist vorliegend Rechtsanwalt Tobias Scheidacker, Mommsenstraße 5, 10629 Berlin, Tel. 030 - 88 48 90 22, email scheidacker@ikb-law.de. Datenschutzbeauftragter ist Rechtsanwalt Benjamin Stiegert, Mommsenstraße 5, 10629 Berlin, Tel. 030 - 88 48 90 22, email stiegert@ikb-law.de.

Datenschutz-Grundverordnung

Seminar am 28. Februar 2018

Referenten: Tobias Scheidacker
Benjamin Stiegert

Ort: private office berlin, Marburger Straße 2, 10789 Berlin

Inhaltsübersicht

Einführung
1. was gilt ab wann?
2. für wen gilt es und wofür?
3. warum ist die DSGVO für den privaten Sektor so relevant?
4. Unterscheidung zwischen Inhalten und Organisation

inhaltliche Vorgaben: zur Verarbeitung personenbezogener Daten
1. Grundsätze (Art. 5)
2. Rechtmäßigkeit (Art. 6)

Rechte der Betroffenen
1. Transparenz und Information (Art. 13)
2. Auskunft über Inhalt und Verwendung des Datenbestands (Art. 15)
3. Recht auf Berichtigung falscher Daten (Art. 16)
4. Recht auf Vergessenwerden (Art. 17)
5. Recht auf Datenübertragbarkeit (Art. 20)

organisatorische Vorgaben: strukturelle Anforderungen in Ihrem Unternehmen
1. Privacy by Design (Art. 25 Abs. 1)
2. Privacy by Default (Art. 25 Abs. 2)
3. Haftung bei Datenverarbeitung durch Dienstleister
4. Verarbeitungsverzeichnis (Art. 30)
5. Datensicherheit (Art. 32)
6. Meldepflicht bei Datenschutzverletzungen (Art. 33 und 34)
7. Datenschutz-Folgeabschätzung (Art. 35)
8. Datenschutzbeauftragter (Art. 37-39)

Konsequenzen bei Verletzung: Haftung, Schadensersatz, Geldbußen, Strafen
1. Haftung und Schadensersatz (Art. 82)
2. Geldbußen (Art. 83)
3. Strafvorschriften (Art. 84 und § 42 BDSG)

Fazit: was zu tun ist

Anlagen

Verordnungstext
- Datenschutz-Grundverordnung (vollständiger Verordnungstext im Amtsblatt der EU)

Checkliste, was bis zum 24.05.2018 noch zu tun ist
- Checkliste des BayLDA

Datenschutzkonferenz:
- Hinweise zum Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO
- Muster „Verzeichnis von Verarbeitungstätigkeiten (Verantwortlicher)
- Muster „Verzeichnis von Verarbeitungstätigkeiten (Auftragsverarbeiter)
- Kurzpapier Nr. 1 „Verzeichnis von Verarbeitungstätigkeiten - Art. 30 DSGVO“
- Kurzpapier Nr. 3 „Verarbeitung personenbezogener Daten für Werbung“
- Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DSGVO“

- Kurzpapier Nr. 6 „Auskunftsrecht der betroffenen Person, Art. 15 DSGVO“
- Kurzpapier Nr. 8 „Maßnahmenplan DSGVO für Unternehmen“
- Kurzpapier Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“
- Kurzpapier Nr. 11 „Recht auf Löschung / Recht auf Vergessenwerden“
- Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“
- Kurzpapier Nr. 14 „Beschäftigtendatenschutz“
- Kurzpapier Nr. 15 „Videoüberwachung nach der DSGVO“

Düsseldorfer Kreis:
- Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“
- Beschluß vom 22.10.2009: „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“
- Beschluß vom 27.01.2014: „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten“ nebst Anlage
- Beschluß vom 13./14.09.2016: „Fortgeltung bisher erteilter Einwilligungen unter der DSGVO“
- Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“
- Orientierungshilfe „datenschutzgerechtes Smart Metering“

Datenschutzgruppe
- Leitlinien in Bezug auf Datenschutzbeauftragte (WP 243)
- WP 243 Anhang - häufig gestellte Fragen
- Leitlinien zum Recht auf Datenübertragbarkeit (WP 242)
- WP 242 Anhang - häufig gestellte Fragen

weitere Unterlagen
- Berliner Datenschutzbeauftragter: „Merkblatt zu den Aufgaben von betrieblichen Datenschutzbeauftragten“

Einführung

Als Immobilienunternehmen verfügen Sie über eine Vielzahl von Daten, angefangen von den Personalien Ihrer Mieter über deren finanzielle Verhältnisse bis hin zu höchstpersönlichen Informationen über Gesundheit, Angewohnheiten, Beziehungen oder erbrechtliche Verhältnisse. Sie wissen, wer vom Amt lebt, wer Alkoholiker ist, bei wem die Polizei schon mal nach Drogen gesucht hat, wer selten zu Hause ist, wer regelmäßig zahlt, wer viel heizt und wer viel feiert. Auch über die Verhältnisse Ihrer Auftraggeber, der Eigentümer, wissen Sie in der Regel eine ganze Menge. Sie unterhalten geschäftliche Beziehungen zu Mitarbeitern und externen Dienstleistern, von denen Sie wiederum Daten über Ihre Mieter erhalten (z.B. Heizkostenableser) und Sie geben Ihrerseits Daten von Mietern oder Eigentümern an diese weiter. Kurz: Sie sind ein Datenpool, der Teilmengen in unterschiedlichste Richtungen verteilt oder das organisiert.

Damit sind Sie ein direkter Adressat der neuen DSGVO und vermutlich interessantes Ziel von Abmahnvereinen. Denn aufgrund Ihrer Betriebsgröße stehen die Chancen gut, daß Sie sich entweder nicht lückenlos und rechtzeitig auf die neue Rechtslage vorbereiten, oder daß Sie im Streitfall jedenfalls nicht mit einer internationalen Großkanzlei auf den Abmahner losgehen, sondern in der Defensive bleiben.

Umso besser ist es, daß Sie heute hier sind und sich informieren.

Mit dem nachfolgenden Skript erhalten Sie alle notwendigen Informationen, zunächst worum es bei der DSGVO im Kern geht (**Kapitel „Einführung"**), sodann welche inhaltlichen Vorgaben zu Datenerhebung und Verarbeitung künftig gelten (**Kapitel „inhaltliche Vorgaben“**), sodann welche Rechte die Personen haben, deren Daten Sie verarbeiten (**Kapitel „Rechte der Betroffenen“**) und schließlich, welche betriebsorganisatorischen Strukturen Sie einrichten müssen, um auch formal auf der sicheren Seite zu sein (**Kapitel „organisatorische Vorgaben“**).

1. was gilt ab wann?

Die DSGVO ist eine europäische Verordnung. Sie trat am 24.05.2016 in Kraft. Nach einer zweijährigen Übergangsfrist wird sie verbindliches nationales Recht, also ab dem 25. Mai 2018. Sie besteht aus 99 Artikeln. Diese werden in 173 sogenannten „Erwägungsgründen“ erläutert.

Überwiegend regelt die DSGVO die Materie selbst. In Teilen sieht sie jedoch vor, daß die Mitgliedstaaten eigenständige Regelungen treffen oder die vorhandenen ergänzen können (sog. „Öffnungsklauseln“). In Deutschland wird das durch eine Neufassung des Bundesdatenschutzgesetzes (BDSG) geschehen, welche zeitgleich am 25.05.2018 in Kraft tritt. Das macht es etwas kompliziert, weil sich das Gesamt der Vorschriften nicht aus einer einzigen Quelle erkennen läßt, sondern aus einer Wechselwirkung von mehreren.

2. für wen gilt es und wofür?

Die DSGVO betrifft **personenbezogene Daten natürlicher Personen, also nicht Daten von Unternehmen oder juristischen Personen**. Was personenbezogene Daten sind, bestimmt Art. 4 Ziffer 1 der Verordnung:

> *„personenbezogene Daten“* [sind] ***alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person*** *(im Folgenden „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 identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Adressat der Datenschutzvorschriften in der Verordnung ist zum einen die öffentliche Hand, zum anderen der Privatsektor nach folgender Maßgabe (Art. 2 DSGVO):

*(1) 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.*

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten … durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten …

Was ein **Dateisystem** ist, sagt uns **Erwägungsgrund 15**:

*Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen **technologieneutral** sein und nicht von den verwendeten Techniken abhängen. Der Schutz natürlicher Personen sollte für die automatisierte Verarbeitung personenbezogener Daten ebenso gelten wie für die manuelle Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. **Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, sollten nicht in den Anwendungsbereich dieser Verordnung fallen.***

„Nicht nach bestimmen Kriterien geordnet“ ist ein auslegungsfähiger Begriff. Zunächst fragt sich, ob er sich nur auf die Deckblätter bezieht oder auch auf Akten und Aktensammlungen. Allerdings sind Akten prinzipiell irgendwie „geordnet“, und sei es chronologisch (ansonsten wären es keine Akten). Auch Aktensammlungen sind zwingend irgendwie geordnet, andernfalls fände man keine Akte wieder, wenn man sie sucht, es wäre keine „Sammlung“. Das spricht m.E. dafür, daß sich das „nach bestimmten Kriterien geordnet“ nur auf die Deckblätter bezieht.

Das bedeutet: Ihre Mieterakten auf Papier unterfallen m.E. nicht dem Anwendungsbereich der DSGVO, sondern nur die Deckblätter, wenn Sie auf diesen personenbezogene Daten führen.

Um die bürokratischen Anforderungen für Nicht-Großkonzerne im Rahmen zu halten, enthält **Erwägungsgrund 13** zudem eine „**Klein- und Mittelstandsklausel**“:

*„Um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, enthält diese Verordnung eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die **weniger als 250 Mitarbeiter** beschäftigen. Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinstunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission maßgebend sein.“*

In diesem Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission heißt es:

> ***Artikel 2 Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen***
> *(1) Die Größenklasse der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.*
> *(2) Innerhalb der Kategorie der KMU wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.*
> *(3) Innerhalb der Kategorie der KMU wird ein Kleinstunternehmen als ein Unternehmen definiert, das weniger als 10 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 2 Mio. EUR nicht überschreitet.*

Wir finden das bei der Verpflichtung wieder, ein Verarbeitungsverzeichnis zu erstellen (Art. 30 DS-GVO), dazu weiter unten.

Mit Ausnahme dieser Regel zum Verarbeitungsverzeichnis und der für einen Datenschutzbeauftragten bei mindestens 10 Mitarbeitern (dazu unten Art. 37-39) **ist die Betriebsgröße für die Anwendung der DSGVO irrelevant. Sie gilt also auch bei einem Ein-Mann-Unternehmen!**

3. warum ist die DSGVO für den privaten Sektor so relevant?

Die Aufgabe, Datenschutzverstößen nachzugehen und gegebenenfalls einzuschreiten, liegt bei den Landesdatenschutzbehörden. Allerdings hat Deutschland (als einziges EU-Land) im Februar 2016 auch ein eigenes Verbandsklagerecht in Datenschutzsachen eingeführt. Das bedeutet, daß auch Verbände, zum Beispiele Verbraucherschutzverbände, Unternehmen wegen Datenschutzverletzungen abmahnen und verklagen dürfen.

Das Klagerecht für Verbände ist ein Bruch mit dem bisherigen System, weil plötzlich Private über öffentlich-rechtliche Normen entscheiden und abmahnen dürfen. Davon wird mit Sicherheit auch Gebrauch gemacht, so wie z.B. die Deutsche Umwelthilfe - ein privater Verein - Verstöße gegen Kennzeichnungspflichten in Wohnungsanzeigen, beim Gebrauchtwagenhändler oder bei Waschmaschinen prozessiert.

Darüber hinaus soll jede natürliche Person über ihre personenbezogenen Daten und deren Verwendung selbst bestimmen können. Sieht sie dieses informationelle Selbstbestimmungsrecht verletzt, kann sie das betreffende Unternehmen abmahnen. Allerdings war das auch schon bisherige Rechtslage, d.h. insoweit ändert sich nichts.

Die Wahrscheinlichkeit, von einem Verband abgemahnt zu werden, ist höher als eine Abmahnung durch die Datenschutzbehörden, weil dessen Fokus auf der Verfolgung von Verstößen liegt (und deren Finanzierung teilweise von der Einnahme entsprechender Abmahngebühren abhängt). Private Verbände haben allerdings nicht so weitgehende Rechte wie die Datenschutzbehörden. Letztere können Audits durchführen, also untersuchen, ob ein Unternehmen die Bestimmungen einhält. Dafür haben sie auch ein Begehungsrecht, dürfen also in die Firma kommen. Die Verbände hingegen können nur solche Datenschutzverletzungen abmahnen, die von außen für jeden sichtbar sind. Wird man durch einen Verband abgemahnt und es kommt zum Prozess, dann muss auch die Datenschutzbe-

hörde bei Kenntnisnahme ermitteln, sie hat dann einen Ermittlungszwang. Diese kann das Unternehmen begehen und interne Verstöße gegen die DSGVO abmahnen.

Als KMU ist es eher unwahrscheinlich, ins Visier der Datenschutzbehörden zu gelangen. Daher sollte der Fokus vor allem darauf liegen, eine Inanspruchnahme durch private Verbände zu verhindern, d.h. alle Regeln, die nach außen hin sichtbar sind, einwandfrei einzuhalten. Dazu gehören zum Beispiel das Double-Opt-in bei Newsletter-Anmeldungen, die richtige Datenschutzerklärung auf der Website oder das Widerrufsmanagement für Datenprozesse (das heißt: eine Aufklärung darüber, wie zum Beispiel Kunden die Erlaubnis, ihre Daten zu verarbeiten, widerrufen können).

Die Höhe der Strafen, die bei Verstößen gegen die DSGVO verhängt werden, können sich nach Art. 83 DSGVO auf maximal zwei bis vier Prozent des weltweiten Unternehmensumsatz beziehungsweise 10 bis 20 Millionen Euro belaufen, je nachdem, was höher ist. Solche Höchstwerte sind in der Praxis allerdings wenig realistisch und bei kleinen und mittleren Unternehmen ohnehin nicht verhältnismäßig. Schon nach dem alten Bundesdatenschutzgesetz konnten die Datenschutzbehörden Strafen bis zu 300.000 Euro aussprechen, aber Bußgelder waren selbst gegen große Unternehmen in der Vergangenheit selten mehr als vierstellig. Millionenbußgelder gab es in der Vergangenheit nur in absoluten Ausnahmefällen, zum Beispiel gegen Google. Bei der Bemessung ist zu berücksichtigen, welche Daten betroffen waren und ob es sich um den ersten oder einen wiederholten Verstoß handelt. Die Strafen werden in Zukunft vielleicht etwas höher ausfallen, aber Millionenbeträge werden nur fällig, wenn es beispielsweise um Millionen Nutzerdaten geht.

4. Unterscheidung zwischen Inhalten und Organisation

Um in Ihrem Unternehmen korrekt umgesetzt zu werden, müssen wir zwischen zwei Bereichen unterscheiden: 1) den inhaltlichen Datenschutzbestimmungen und zugehörigen Rechten der Betroffenen einerseits und 2) den organisatorischen Strukturen, um die Inhalte und die Rechte der Betroffenen umzusetzen, andererseits. An ersterem hat sich gegenüber dem BDSG a.F. gar nicht so viel geändert, letzteres ist hingegen aufwendig.

Demgemäß befassen wir uns in diesem Skript zunächst damit, welche inhaltlichen Vorgaben einzuhalten sind, also welche Daten betroffen sind und welcher Umgang mit ihnen vorgeschrieben wird. Sodann schauen wir uns die Betroffenenrechte an. Schließlich stellen wir dann zusammen, welche organisatorischen Vorgaben Ihr Unternehmen einhalten muß, um den strukturellen Anforderungen der DSGVO zu genügen.

inhaltliche Vorgaben:
zur Verarbeitung personenbezogener Daten

Wenn man das gesamte Regelwerk zu den Dateninhalten in kurzen Worten zusammenfassen müßte, so könnte man sagen, daß Sie alle Daten erheben, speichern und verarbeiten dürfen, die Sie für die jeweilige Geschäftsbeziehung oder zur rechtlichen Absicherung oder Rechtsdurchsetzung benötigen, so lange das der Fall ist. Das neue Datenschutzrecht verfolgt erklärtermaßen nicht das Ziel, die Wirtschaft zu behindern. Es soll lediglich eine gedankenlose, nicht erforderliche oder mißbräuchliche Erhebung, Verteilung und Verwendung von Daten beenden bzw. unterbinden.

Demgemäß ist es zwar wichtig, daß Sie die nachstehenden Vorschriften kennen. Sofern und solange bestimmte Daten von Ihnen jedoch für die zulässigen geschäftlichen Zwecke Ihres Unternehmens benötigt werden, werden Sie im Gesetz oder seinen Erläuterungen eine Erlaubnis dafür finden.

1. Grundsätze (Art. 5 DSGVO)

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);

- 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 gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („**Zweckbindung**“);

- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);

- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);

- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);

- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);

Die Einhaltung dieser Punkte muß nachgewiesen werden können („**Rechenschaftspflicht**“).

Das bedeutet nach Erwägungsgrund 39,

> *daß jede Verarbeitung personenbezogener Daten rechtmäßig und nach Treu und Glauben erfolgen sollte. Für natürliche Personen sollte **Transparenz** dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die **Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung** und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestäti-*

*gung und **Auskunft** darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden.*

Natürliche Personen sollten sodann über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten **informiert und darüber aufgeklärt** werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, 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 dürfen, 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, sollte der Verantwortliche **Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen**. Es sollten alle vertretbaren Schritte unternommen werden, 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.

2. Rechtmäßigkeit (Art. 6 DSGVO)

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

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

Art. 7 DSGVO. Bedingungen für die Einwilligung.

1. *Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.*
2. *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.*
3. *Die betroffene Person hat 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. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.*
4. *Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss 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.*

Erwägungsgrund 30

*Die Einwilligung sollte **durch eine eindeutige bestätigende Handlung erfolgen**, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezoge-*

nen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Wenn die Verarbeitung mehreren Zwecken dient, sollte für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden. Wird die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert, so muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen.

Erwägungsgrund 42
Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates sollte ***eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache*** *zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.*

Erwägungsgrund 43
Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung ***gilt nicht als freiwillig erteilt****, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder* ***wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.***

- 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;

  Erwägungsgrund 44
  Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.

- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- 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;
- 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.

Erwägungsgrund 47
Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. ***Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht,*** *z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt,* ***vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.*** *Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.*

Erwägungsgrund 48
Verantwortliche, die Teil einer ***Unternehmensgruppe*** *oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.*

Bei Weiterverarbeitung zu anderen als den ursprünglich eingewilligten Zwecken gilt:

Erwägungsgrund 50
Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte ***nur zulässig*** *sein,* ***wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist.*** *In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die*

betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen. Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

Die Verarbeitung bestimmter höchstpersönlicher oder solcher Daten, die unter Diskriminierungsverdacht stehen, ist nach **Art. 9** DSGVO untersagt:

"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."

Der Artikel enthält dann allerdings eine ganze Reihe von Ausnahmen, etwa wenn bestimmte Daten für die konkrete Rechtsbeziehung notwendig sind. So könnte sich im Rahmen eines barrierefreien Umbaus nach den Wünschen des Mieters die Notwendigkeit ergeben, bestimmte Gesundheitsdaten von Mieter zu erfassen und zu verarbeiten, um den barrierefreien Umbau sachgerecht konzipieren zu können. Es kann auch sein, daß Sie einen Israeli darüber informieren möchten, daß in dem Haus, in dem er sich bei Ihnen um eine Wohnung bewirbt, derzeit ausschließlich arabischen Bewohnern leben. Das bedeutet, daß es im Einzelfall notwendig sein kann, daß Ihnen diese Daten vorliegen und Sie sie verwenden. Bei solchen Sachgründen liegt keine Verletzung von Datenschutzvorschriften vor.

Rechte der Betroffenen

1. Transparenz und Information

Das Subjekt Ihrer Datenerhebung ist nach vorstehendem zwingend eine natürliche Person und die Daten, um die es geht, sind personenbezogene Daten zu ihr. Damit jeder einzelne Mensch in Erfahrung bringen kann, welche Daten über ihn bei wem im Umlauf sind und was damit geschieht, sieht die DSGVO in **Art. 13 Transparenz- und Informationspflichten** vor:

1. *Werden personenbezogene Daten **bei der betroffenen Person erhoben**, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:*

- *den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;*
- *gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;*
- *die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;*
- *wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;*
- *gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten*
- *…*

Erwägungsgrund 60
Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person ***über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet*** *wird. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Darüber hinaus sollte er die betroffene Person darauf hinweisen, dass Profiling stattfindet und welche Folgen dies hat. Werden die personenbezogenen Daten bei der betroffenen Person erhoben, so sollte dieser darüber hinaus mitgeteilt werden, ob sie verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Die betreffenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Werden die Bildsymbole in elektronischer Form dargestellt, so sollten sie maschinenlesbar sein.*

Erwägungsgrund 61
Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person ***zum Zeitpunkt der Erhebung*** *mitgeteilt werden oder, falls die Daten nicht von ihr, sondern aus einer anderen Quelle erlangt werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die personenbezogenen Daten rechtmäßig einem anderen Empfänger offengelegt werden dürfen, sollte die betroffene Person bei der erstmaligen Offenlegung der personenbezogenen Daten für diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck zu verarbeiten als den, für den die Daten erhoben wurden, so sollte er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und andere erforderliche Informationen zur Verfügung stellen. Konnte der betroffenen Person nicht mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.*

2. *Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:*

   - *die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;*
   - *das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;*
   - *wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu wider-*

rufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- *das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;*
- *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*
- *das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 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.*

3. *Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.*

4. *Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.*

Erwägungsgrund 62
Die Pflicht, Informationen zur Verfügung zu stellen, erübrigt sich jedoch, wenn die betroffene Person die Information bereits hat, wenn die Speicherung oder Offenlegung der personenbezogenen Daten ausdrücklich durch Rechtsvorschriften geregelt ist oder wenn sich die Unterrichtung der betroffenen Person als unmöglich erweist oder mit unverhältnismäßig hohem Aufwand verbunden ist. Letzteres könnte insbesondere bei Verarbeitungen für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken der Fall sein. Als Anhaltspunkte sollten dabei die Zahl der betroffenen Personen, das Alter der Daten oder etwaige geeignete Garantien in Betracht gezogen werden.

Werden Daten nicht bei der betreffenden Person erhoben, sondern bspw. bei Dritten über sie, gelten sinngemäß ähnliche Informationspflichten nach Art. 14 DSGVO.

2. Auskunft über Inhalt und Verwendung des Datenbestands

Art. 15 sieht sodann **Auskunftsrechte** vor. 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:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- 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;
- 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;
- 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;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 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.

Die betroffene Person hat Anspruch auf eine (kostenlose) Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Für alle weiteren Kopien, die die betroffene Person beantragt, kann ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangt werden. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt. Das Recht auf Erhalt einer Kopie darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

> ***Erwägungsgrund 63***
> *Eine betroffene Person sollte ein **Auskunftsrecht** hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.*

> ***Erwägungsgrund 64***
> *Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die **Identität einer Auskunft suchenden betroffenen Person zu überprüfen**, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.*

3. Recht auf Berichtigung falscher Daten

Nach Art. 16 DSGVO hat die betroffene Person 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 das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

> ***Erwägungsgrund 65***
> *Eine betroffene Person sollte ein Recht auf Berichtigung der sie betreffenden personenbezogenen Daten besitzen sowie ein „Recht auf Vergessenwerden", wenn die Speicherung ihrer Daten gegen diese Verordnung oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt. Insbesondere sollten betroffene Personen Anspruch darauf haben, dass ihre personenbezoge-*

nen Daten gelöscht und nicht mehr verarbeitet werden, wenn die personenbezogenen Daten hinsichtlich der Zwecke, für die sie erhoben bzw. anderweitig verarbeitet wurden, nicht mehr benötigt werden, wenn die betroffenen Personen ihre Einwilligung in die Verarbeitung widerrufen oder Widerspruch gegen die Verarbeitung der sie betreffenden personenbezogenen Daten eingelegt haben oder wenn die Verarbeitung ihrer personenbezogenen Daten aus anderen Gründen gegen diese Verordnung verstößt. Dieses Recht ist insbesondere wichtig in Fällen, in denen die betroffene Person ihre Einwilligung noch im Kindesalter gegeben hat und insofern die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang absehen konnte und die personenbezogenen Daten – insbesondere die im Internet gespeicherten – später löschen möchte. Die betroffene Person sollte dieses Recht auch dann ausüben können, wenn sie kein Kind mehr ist. Die weitere Speicherung der personenbezogenen Daten sollte jedoch rechtmäßig sein, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

4. Recht auf Vergessenwerden

Die betroffene Person hat nach Art. 17 DSGVO das Recht, zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er nach vorstehendem zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, 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.

Vorstehendes gilt nicht, soweit die Verarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89
- Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- **zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.**

> ***Erwägungsgrund 66***
> *Um dem „Recht auf Vergessenwerden" im Netz mehr Geltung zu verschaffen, sollte das Recht auf Löschung ausgeweitet werden, indem ein Verantwortlicher, der die personenbezogenen Daten öffentlich gemacht hat, verpflichtet wird, den Verantwortlichen, die diese personenbezogenen Daten verarbeiten, mitzuteilen, alle Links zu diesen personenbezogenen Daten oder Kopien oder Replikationen der personenbezogenen Daten zu löschen. Dabei sollte der Verantwortliche, unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen – auch technischer Art – treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren.*

5. Recht auf Datenübertragbarkeit

Die betroffene Person hat nach Art. 20 DSGVO des weiteren das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

- die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Buchstabe b beruht und
- die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Bei der Ausübung ihres Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.

> ***Erwägungsgrund 68***
> *Um im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten zu haben, sollte die betroffene Person außerdem berechtigt sein, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat,* ***in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format*** *zu erhalten und sie einem anderen Verantwortlichen zu übermitteln. Die Verantwortlichen sollten dazu aufgefordert werden, interoperable Formate zu entwickeln, die die Datenübertragbarkeit ermöglichen. Dieses Recht sollte dann gelten, wenn die betroffene Person die personenbezogenen Daten mit ihrer Einwilligung zur Verfügung gestellt hat oder die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist. Es sollte nicht gelten, wenn die Verarbeitung auf einer anderen Rechtsgrundlage als ihrer Einwilligung oder eines Vertrags erfolgt. Dieses Recht sollte naturgemäß nicht gegen Verantwortliche ausgeübt werden, die personenbezogenen Daten in Erfüllung ihrer öffentlichen Aufgaben verarbeiten. Es sollte daher nicht gelten, wenn die Verarbeitung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer ihm übertragenen Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung einer ihm übertragenen öffentlichen Gewalt erfolgt, erforderlich ist. Das Recht der betroffenen Person, sie betreffende personenbezogene Daten zu übermitteln oder zu empfangen, sollte für den Verantwortlichen nicht die Pflicht begründen, technisch kompatible Datenverarbeitungssysteme zu übernehmen oder beizubehalten. Ist im Fall eines bestimmten Satzes personenbezogener Daten mehr als eine betroffene Person tangiert, so sollte das Recht auf Empfang der Daten die Grundrechte und Grundfreiheiten anderer betroffener Personen nach dieser Verordnung unberührt lassen. Dieses Recht sollte zudem das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten und die Beschränkungen dieses Rechts gemäß dieser Verordnung nicht berühren und insbesondere nicht bedeuten, dass die Daten, die sich auf die betroffene Per-*

son beziehen und von ihr zur Erfüllung eines Vertrags zur Verfügung gestellt worden sind, gelöscht werden, soweit und solange diese personenbezogenen Daten für die Erfüllung des Vertrags notwendig sind. Soweit technisch machbar, sollte die betroffene Person das Recht haben, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden.

organisatorische Vorgaben: strukturelle Anforderungen in Ihrem Unternehmen

Um die korrekte Verwendung von Daten in Ihrem Unternehmen sicherzustellen, sieht die DSGVO diverse organisatorische Strukturen vor, welche Sie einführen und fortlaufend aktuell halten müssen. Hierzu gehören

- technische Mindestvorgaben für Datenerfassungs- und -verarbeitungssysteme,
- Vorgaben bei Verarbeitung der Daten durch Dienstleister,
- Mindestvorgaben für die Sicherheit von Daten,
- die Anlage eines sog. Verarbeitungsverzeichnisses,
- eine Meldepflicht bei Datenschutzverletzungem,
- eine Datenschutz-Folgeabschätzung und
- das Vorhandensein eines Datenschutzbeauftragten, der sich um die Einhaltung aller Regeln kümmert.

Grundlegende Vorschrift zu all dem ist **Art. 24 Abs. 1 DSGVO**. Er lautet:

> *„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. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“*

> ***Erwägungsgrund 74***
> *Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.*

Im einzelnen:

1. Privacy by Design (Art. 25 Abs. 1 DSGVO)

Die Vorschrift trägt den Titel „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“. Privacy by Design meint den Datenschutz durch die Gestaltung der Technik:

> *„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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung ***geeignete technische und organisatorische Maßnahmen*** *– wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung 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."*

Erwägungsgrund 78
Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den ***Grundsätzen des Datenschutzes durch Technik*** *(data protection by design)* ***und durch datenschutzfreundliche Voreinstellungen*** *(data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.*

Beispiel: Verwendung von Verschlüsselungstechniken

2. Privacy by Default (Art. 25 Abs. 2 DSGVO)

Demgegenüber mein Privacy by Default den Datenschutz durch Voreinstellungen im Rahmen der Verwendung der geeigneten Technik:

„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass ***durch Voreinstellung*** *grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden."*

Beispiel: Das Eingabefeld auf einer Webseite sieht nur dort zwingende Eintragungen vor, wo Mindestangaben abgefragt werden, die für die jeweilige Aktion tatsächlich zwingend benötigt werden. Darüber hinaus gehende Daten können ebenfalls abgefragt werden, sind aber keine zwingende Voreinstellung.

3. Haftung bei Datenverarbeitung durch Dienstleister

In einer Hausverwaltung kommt es ständig vor, daß Daten an Dienstleister weitergegeben werden, um dort verarbeitet zu werden: dem Heizkostenableser, einem Buchhaltungsbüro, dem Steuerberater, dem Anwalt, Ein- und Auszugsinformationen an Versorger und andere Dienstleister, Bürgen, Banken, Handwerkern bei Mängeln und anderem, dem Abfallentsorger bei personenzahlabhängigen Gebühren, Architekten bei Modernisierungen, dem Schornsteinfeger für Emissionsmessungen oder einfach nur dem Hausmeister.
Soweit diese Dritten Daten für Sie verarbeiten, bezeichnet man sie künftig als „Auftragsverarbeiter". Damit Sie für deren Datenschutzverletzungen in Haftung genommen werden können, sieht **Art. 28 DSGVO** entsprechende strukturelle Verpflichtungen vor.

Art. 28 DSGVO. Auftragsverarbeiter.

1. ***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 dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.***
2. *Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.*
3. ***Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags** oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter*
   a) *die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;*
   b) *gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;*
   c) *alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;*
   d) *die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;*
   e) *angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;*
   f) *unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;*
   g) *nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,*
   h) *dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.*

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

4. *Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.*
5. ***Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.***
6. *Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.*
7. *Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.*
8. *Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.*
9. ***Der Vertrag** oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 **ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.***
10. *Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.*

Das bedeutet:

- Sie bleiben für die Datenverarbeitung durch Ihre Dienstleister verantwortlich.
- Der Auftrag an Ihren Dienstleister muß bestimmte Mindest-Pflichtinhalte aufweisen.
- Die Schutzmaßnahmen müssen angemessen sein.
- Die Schutzmaßnahmen müssen nachgewiesen werden können. Eine Datenschutz-Zertifizierung Ihres Dienstleisters ist dabei ein Positivkriterium.
- Der Auftrag muß schriftlich sein. Wenn er in einem elektronischen Format erteilt wird, muß dieses der Schriftform entsprechen (vermutlich ist damit eine qualifizierte Signatur gemeint).

> ***Erwägungsgrund 81***
> *Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, **nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen.** Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und*

> *die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind.* ***Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden.*** *Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.*

Zugleich sind Sie selbst ebenfalls Auftragsverarbeiter, und zwar für Ihren Auftraggeber, den Eigentümer. Eine Definition finden wir in Art. 4 Abs. 7 und 8 DSGVO. **„Verantwortlicher“** ist hiernach

> *die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.*

„Auftragsverarbeiter“ ist

> *eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;*

Sie müssen also als Auftragsverarbeiter auch einen entsprechenden Vertrag mit Ihrem auftragegebenden Eigentümer schließen. Das liegt zwar primär in dessen Interesse, um seine eigene Haftung für Datenschutzfehler in Ihrem Hause abzusichern. Als sein Dienstleister für unter anderem die rechtlichen Angelegenheiten im Zusammenhang mit der Verwaltung seiner Immobilien haben Sie aber mglw. eine entsprechende Hinweispflicht. Zumindest ist es ein Ausweis der hohen fachlichen Qualität Ihrer Arbeit, wenn Sie ihn entsprechend hinweisen und ein Vertragsformular anbieten, das die datenschutzrechtlichen Aspekte mit berücksichtigt.

4. Verarbeitungsverzeichnis (Art. 30 DSGVO)

Die hier geregelten Pflichten gelten nach Absatz 5 der Vorschrift nicht 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 Artikel 9 Absatz 1** bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Bevor wir beurteilen können, ob Sie als kleines oder mittleres Unternehmen ein Verarbeitungsverzeichnis führen müssen, steht also die Bewertung, ob

- Ihre Verarbeitung der Daten Risiken für die Rechte der betroffenen Person birgt oder
- die Verarbeitung nicht nur gelegentlich erfolgt oder
- Sie Daten nach Art. 9 Abs. 1 DSGVO, also betreffend die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen

Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person verarbeiten.

Leider sagt uns kein Erwägungsgrund, wann „Risiken“ in diesem Sinne vorliegen oder was „nur gelegentlich“ ist.

Allerdings betreffen die meisten der von Ihnen geführten Daten nicht Personen, sondern Objekte bzw. Wohnungen. Die Entscheidung, eine Mieterhöhung durchzuführen, hängt nicht von personenbezogenen Daten des Mieters ab, sondern von der Wohnungsgröße, ihrer Lage, der aktuellen Miete pro qm und anderen objektiven, nur auf die Immobilie bezogenen Faktoren. Eine Betriebskostenabrechnung verarbeitet zwar Verbrauchsdaten des Mieters. Ob diese personenbezogen sind, kann man aber trefflich streiten. Aus Sicht der Verwaltung sind Verbrauchsdaten wohnungsbezogen. Das gilt offenkundig, wenn in der Wohnung mehrere Personen leben und man den Wasser- oder Gasverbrauch nicht zwischen ihnen exakt aufteilen kann.

Personenbezogen sind die Daten, mit denen Sie arbeiten, allerdings in Bezug auf den Namen des Mieters, seine Anschrift und betreffend Geldbewegungen. So findet eine monatliche Buchhaltung statt, welche Bankdaten - vielleicht, aber nicht notwendigerweise, vollständig automatisiert - mit Mietkontodaten abgleicht und letztere aktualisiert. **Das ist regelmäßig, also nicht nur gelegentlich.** Insbesondere wenn es zu Zahlungsrückständen kommt, werden die Daten dann auch weiter verwendet.

Des weiteren speichern Sie Daten über die „rassische und ethische Herkunft“ Ihrer Mieter und in Einzelfällen auch Gesundheitsdaten, so wenn Depressionen eine Zwangsräumung verhindern oder der Mieter einen barrierefreien Umbau wünscht.

Obwohl die DSGVO gerade Unternehmen Ihrer Größe also vor überdimensioniertem Bürokratismus schützen will, ist die Ausnahmeeinschränkung so gefasst, daß sie wohl greift, d.h. daß Sie sich **nicht auf den KMU-Status berufen können**. So leid es mir tut, **Sie müssen wohl auch ein Verarbeitungsverzeichnis nach Art. 30 DSGVO führen**.

Art. 30 DSGVO. Verzeichnis von Verarbeitungstätigkeiten.

1. *Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält **sämtliche folgenden 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 Artikel 49 Absatz 1 Unterabsatz 2 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 Artikel 32 Absatz 1.*
2. *Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:*

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) 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 Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

3. Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

4. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Erwägungsgrund 82

Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

Was ist eine „**Verarbeitungstätigkeit**“? Kurz gesagt: jeder Vorgang, in dem Sie Daten verarbeiten. Wie kleinteilig das sein muß, geht aus der DSGVO nicht hervor. So ist unklar, ob es ausreicht, wenn Sie die „Mietsonderverwaltung“ als Verarbeitungstätigkeit bezeichnen, ob Sie die „Anlage einer Mieterakte“ als einen Schritt hieraus herausgreifen müssen oder ob das noch weiter in seine einzelnen Verarbeitungsschritte aufzugliedern ist. Ich fürchte, letzteres. Denn die konkrete Datenverarbeitung ist das Eintragen der Personalien, Finanzdaten, Arbeitgeber etc. des ausgewählten Mietinteressenten in die Stammdaten der neuen Mieterakte bei Vertragsabschluss, ist das Anlegen eines Mietkautionskontos, ist der Abgleich mit den Bankdaten bei Prüfung, ob die Kaution hinterlegt wurde, und so weiter. **Wenn man es genau nimmt, dann bedeutet das, daß sich Ihr Verwaltungsaufwand durch das Führen des Verarbeitungsverzeichnisses verdoppelt, weil Sie jede einzelne Datenverarbeitung darin verzeichnen müssen.**

Datenverarbeitungsvorgänge fallen zum Beispiel an im Rahmen von

- Anbahnung von Verträgen (Mietverträge, Arbeitsverträge, Ausbildungsverträge, Kaufverträge, Handwerkerverträge, Maklerverträge, Dienstleistungsverträge etc.)
- Abschluß von Verträgen (wie vor)
- Durchführung von Verträgen (Buchhaltung, Mängel, Nebenkostenerfassung und -abrechnung)
- Beendigung von Verträgen (wie vor)
- Rechtsdurchsetzungen und Abwehr von Ansprüchen

Bitte berücksichtigen Sie dabei, daß es um **personenbezogene Daten** geht. Ein Verarbeitungsverzeichnis von Firmen, mit denen Sie zusammenarbeiten, in Bezug auf deren Firmendaten unterfällt nicht dem Anwendungsbereich der DSGVO, ist also nicht notwendig.

Eine Mustervorlage für ein Verarbeitungsverzeichnis gibt uns die DSGVO leider nicht. Aus dem Verordnungstext ergeben sich die Dokumentationsanforderungen. Man kann das entweder in Tabellenform führen, oder man legt für jeden einzelnen Datenverarbeitungsschritt ein eigenes Dokumentationsblatt an, das Verzeichnis ist dann die Sammlung dieser Blätter. Ich bin gespannt, wie Sie das in der Praxis umsetzen.

Nachstehend ein Beispiel für den Fall, daß Sie von einem Mietinteressenten anläßlich der Erstellung eines Mietvertragsentwurfs die **Kontodaten** abfragen:

verlangte Mindestinhalte	Beispiel
Art. 30 Abs. 1a) DSGVO: den **Namen und die Kontaktdaten** des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	Verantwortlicher: Fa. Verwaltung von Immobilien GmbH vertreten durch den Geschäftsführer <Name> <Firmenadresse> <Telefonnummer> <email> <Webseite> Datenschutzbeauftragter: <Name> <Geschäftsdresse> <Telefonnummer> <email>
Art. 30 Abs. 1b) DSGVO: die **Zwecke der Verarbeitung**	- Eintragen der Bankdaten in den Mietvertrag zwecks Lastschrifteinzug - ggf. spätere Kontopfändungen u.ä. im Rahmen von Zwangsvollstreckungen
Art. 30 Abs. 1c(DSGVO: eine **Beschreibung der Kategorien** betroffener Personen und der Kategorien personenbezogener Daten *hier muß aufgelistet werden: welche Personengruppen betroffen sind und pro Personengruppe welche personenbezogenen Daten erhoben werden*	betroffene Personenkategorie: Mieter betroffene Datenkategorie: Bankdaten
Art. 30 Abs. 1d) DSGVO: die **Kategorien von Empfängern**, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen *hier muß aufgelistet werden: wer enthält personenbezogenen Daten, welche pbD von wem erhält er*	Kategorie von Empfängern der Daten: - Vermieter/Eigentümer der Mietsache - dessen Bank - Mitarbeiter des Unternehmens des Verantwortlichen - Dienstleister des Unternehmens des Verantwortlichen wie bspw. Anwälte, Steuerberater und deren Mitarbeiter - im Falle des Objektverkaufs: Käufer der Mietsache, Makler - im Falle prozessualer Auseinandersetzungen: Gerichte und deren Mitarbeiter, Gerichtsvollzieher
Art. 30 Abs. 1e) DSGVO: 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 Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien	keine
Art. 30 Abs. 1f) DSGVO: wenn möglich, die **vorgesehenen Fristen für die Löschung** der verschiedenen Datenkategorien	nach Mietvertragsende, Ausgleich sämtlicher wechselseitigen Ansprüche und Ablauf der steuerlichen Aufbewahrungsfristen

verlangte Mindestinhalte	Beispiel
Art. 30 Abs. 1g) DSGVO: wenn möglich, eine allgemeine **Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1 hier muß aufgelistet werden: welche toM werden getroffen, um die Datensicherheit sicher zu stellen? Zutritt, Zugang, Zugriff, Eingabekontrolle, Weitergabekontrolle, Verfügbarkeitkontrolle, Auftragskontrolle, Trennungsgebot	die Bankdaten des Mieters werden im Unternehmen des Verantwortlichen an zwei Stellen gespeichert: in der Mietvertragsurkunde, welche sich in der Mieterakte befindet, und in den Stammdaten der Mieterakte (Software Domus), auf welche durch alle weiteren Module (z.B. Buchhaltung) zurückgegriffen wird. Die Daten liegen nicht im Internet in einer Cloud o.ä., sondern auf dem Server in den Räumen der Verwaltung. Gegen unbefugte Zugriffe von außerhalb ist der Verwaltungsserver durch eine Firewall geschützt. Zutritt zu den Verwaltungsräumen haben die Mitarbeiter der Verwaltung, Mieter, Eigentümer, Dienstleister und Kunden. Zugang zum Serverraum haben ausschließlich die Mitarbeiter der Verwaltung sowie ggf. Servicetechniker. Zugriff auf die Daten haben ausschließlich diejenigen Mitarbeiter des Verwaltungsunternehmens, welche die Verwaltungssoftware anwenden. Die Eingabe von Daten geschieht durch den für das Objekt zuständigen Sachbearbeiter. Eine Weitergabe der Bankdaten geschieht nur im Einzelfall, anlaßbezogen und aufgrund bewußter Entscheidung. Bei Weitergabe werden die Empfänger verpflichtet, den Datensatz nur im Rahmen der zugewiesenen Aufgabe zu verwenden und anschließend zu löschen, soweit nicht eigene Verpflichtungen (wie zB. steuerliche Aufbewahrungsfristen) entgegenstehen.

Welche technischen und organistatorischen Maßnahmen zu treffen sind, können Sie aus vorstehendem schon erahnen. Tatsächlich wird die Datensicherheit in einem eigenen Artikel geregelt:

5. Datensicherheit (Art. 32 DSGVO)

Art. 32 DSGVO. Sicherheit der Verarbeitung.

1. *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****; diese Maßnahmen schließen unter anderem Folgendes ein:*

a) *die Pseudonymisierung und* ***Verschlüsselung*** *personenbezogener Daten;*

b) *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*

c) *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*

d) *ein* ***Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung*** *der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

2. *Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.*

3. *Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.*
4. *Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.*

Es gilt hier wieder der oben bereits zitierte Erwägungsgrund 78. Er wird ergänzt durch

> ***Erwägungsgrund 79***
> *Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer **klaren Zuteilung der Verantwortlichkeiten** durch diese Verordnung, einschließlich der Fälle, in denen ein Verantwortlicher die Verarbeitungszwecke und -mittel gemeinsam mit anderen Verantwortlichen festlegt oder ein Verarbeitungsvorgang im Auftrag eines Verantwortlichen durchgeführt wird.*

> ***Erwägungsgrund 83***
> *Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der **Bewertung der Datensicherheitsrisiken** sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.*

6. Meldepflicht bei Datenschutzverletzungen (Art. 33 und 34 DSGVO)

Wenn in Ihr Büro eingebrochen und der Computer gestohlen wurde, haben Sie in der Vergangenheit Kontakt mit Ihrer Versicherung aufgenommen und dann versucht, wieder betriebsfähig zu werden. Künftig müssen Sie parallel dazu unverzüglich und relativ detailliert die Datenschutzverletzung aufarbeiten und melden:

> ***Art. 33 DSGVO. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde.***
> 1. *Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.*
> 2. *Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.*
> 3. *Die Meldung gemäß Absatz 1 enthält **zumindest folgende Informationen**:*
> a) *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;*
> b) *den **Namen und die Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen;*

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

4. *Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.*
5. *Der Verantwortliche **dokumentiert Verletzungen** des Schutzes personenbezogener Daten **einschließlich aller** im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden **Fakten**, von deren **Auswirkungen** und der ergriffenen **Abhilfemaßnahmen**. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.*

Erwägungsgrund 85
*Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten **unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann** im Einklang mit dem Grundsatz der Rechenschaftspflicht **nachweisen, dass** die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen **führt**. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.*

Erwägungsgrund 87
*Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. **Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde** im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen **führen**.*

Erwägungsgrund 88
*Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. **Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen**, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde.*

Das gilt natürlich auch in anderen Fällen, in denen Daten abhanden kommen, etwa wenn

- Mieterakten in Ihrem Auto liegen und das gestohlen wird,
- Ihnen Ihr Laptop abhanden kommt

- oder mglw. Ihr Smartphone, mit dem ein Zugriff auf Mieterdaten möglich ist; hier reicht schon, daß Sie auf Ihrem Telefon einen synchronisierten Kalender haben, in dem Daten enthalten sind, die eine Personenidentifikation mit Name/Adresse erlauben.
- Sie selbst Opfer einer Datenschutzverletzung werden und die gestohlenen Daten Zugriff auf weitere Daten in Ihrem Unternehmen erlauben.

Ob und was zu veranlassen ist, entscheidet die Datenschutzbehörde nach Ihrer Meldung.

Neben der Pflicht einer Meldung an die Aufsichtsbehörde müssen Sie darüber hinaus die betroffenen Personen informieren, ***wenn sie*** *durch die Datenschutzverletzung* ***voraussichtlich einem hohen Risiko ausgesetzt ist***. Die Vorschrift adressiert primär Fälle wie das Abhandenkommen von Kreditkartendaten, ebay- oder PayPal-Zugangsdaten etc., also Situationen, in denen durch Identitätsdiebstahl im Internet finanzielle Schäden angerichtet werden können und der Verursacher mglw. nicht greifbar zu machen ist.

Gleichwohl kann es auch in Ihrer Praxis vorkommen, daß Datenverluste hohe Risiken für einzelne Personen bewirken, zum Beispiel wenn Mieter oder Wohnungseigentümer einer Auskunftssperre beim Einwohnermeldeamt unterliegen, um aus gesetzlich geschützten Gründen ihren Aufenthaltsort geheim zu halten. Wenn deren Adressdaten nach außen dringen und Sie den Kreis der potentiellen Empfänger nicht identifizieren oder beschränken können, dürfte ein Fall des Art. 34 DSGVO vorliegen:

> ***Art. 34 DSGVO. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person.***
>
> 1. *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 die betroffene Person unverzüglich von der Verletzung.*
> 2. *Die in Absatz 1 genannte* ***Benachrichtigung*** *der betroffenen Person beschreibt* ***in klarer und einfacher Sprache*** *die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen.*
> 3. *Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist* ***nicht erforderlich, wenn*** *eine der folgenden Bedingungen erfüllt ist:*
>   a) *der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,*
>   b) *der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,*
>   c) *dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.*
> 4. *Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.*
>
> ***Erwägungsgrund 86***
>
> *Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung*

sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

Unklar ist, ob Sie sich anläßlich einer Datenschutzverletzung die Kenntnisse erst verschaffen müssen, die Ihnen die Beurteilung erlauben, ob ein solches Risiko besteht. So dürfte wohl keiner Verwaltung standardmäßig zu allen Mietern bekannt sein, wer einer EMA-Meldesperre unterliegt und wer nicht. Im Einzelfall, bei entsprechenden Recherchen, erfährt man davon gelegentlich, aber normalerweise nicht. Damit ist die von der DSGVO verlangte Risikobeurteilung nicht ohne weiteres möglich.

Hier gibt es m.E. drei mögliche Lösungen:

a) Sie müssen nur berücksichtigen, was Sie wissen. Die theoretische, Ihnen aber nicht näher bekannte Möglichkeit, daß Mieter EMA-Sperren unterliegen, ist keine Kenntnis, so daß keine Informationspflicht besteht.
b) Sie informieren die Datenschutzbehörde darüber, daß Sie hier keine Kenntnis über besondere Risiken haben, aber auch nicht wissen, welche Mieter EMA-Auskunftssperren unterliegen, und überlassen die Entscheidung weiteren Vorgehens denen.
c) Sie informieren vorsorglich alle Mieter über den Datendiebstahl, so daß diejenigen, für die es eine besondere Gefahr bedeutet, auf jeden Fall einbezogen sind.

Keine dieser Lösungen ist aus heutiger Sicht die richtige. Variante a) berücksichtigt den Wortlaut der Vorschrift, Variante b) den der Erwägung 86 und Variante c) ist m.E. völlig unverhältnismäßig, schützt aber die Rechte der Betroffenen am besten und darum geht es ja bei diesen Vorschriften. In der Praxis würde ich vermutlich zu einem Vorgehen gemäß Variante b) raten.

7. Datenschutz-Folgeabschätzung (Art. 35 DSGVO)

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. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. Das ist insbesondere dann der Fall, wenn eine **umfangreiche Verarbeitung besonderer Kategorien** von personenbezogenen Daten **gemäß Artikel 9 Absatz 1** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder eine **systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche** stattfindet.

So richtig greifbar ist diese Vorschrift nicht, weil sie eine Vielzahl unbestimmter Begriffe verwendet. Beispielsweise ist unklar, was eine „umfangreiche“ Verarbeitung oder Überwachung ist. Die Erläuterungen im zugehörigen Erwägungsgrund 91 geben keinen richtigen Aufschluss:

Erwägungsgrund 91
*Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, **große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene** zu verarbeiten, eine **große Zahl von Personen betreffen** könnten **und** – beispielsweise aufgrund ihrer Sensibilität – wahr-*

*scheinlich ein **hohes Risiko** mit sich bringen **und** bei denen entsprechend dem jeweils aktuellen Stand der Technik **in großem Umfang eine neue Technologie eingesetzt** wird, **sowie für andere Verarbeitungsvorgänge**, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, **wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten**, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln **verarbeitet werden**. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die **weiträumige Überwachung öffentlich zugänglicher Bereiche**, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte **nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt**. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.*

Nach Art. 35 Abs. 4 DSGVO werden die Aufsichtsbehörden eine Liste derjenigen Vorgänge erstellen, die unter diese Norm fallen werden. Derzeit kursieren Vermutungen, daß Mieterselbstauskünfte, Bonitäts-Scorings oder die Verwendung von Datenstandorten außerhalb der EU (Dropbox, Google-Drive u.ä.) darunter fallen könnten. Selbst große Immobilien-Verwaltungsunternehmen operieren jedoch idR. regional. Datenmengen und Verarbeitungsstrukturen wie bei Visa oder Amazon fallen hier nicht an.

Von daher vermute ich, daß eine Datenschutz-Folgeabschätzung für KMU-Verwaltungen nicht erforderlich werden wird.

Andernfalls gälte Art. 35 Abs. 7 DSGVO:

"Die Folgenabschätzung enthält zumindest Folgendes:

*a) eine **systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke** der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*

*b) eine **Bewertung der Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck;*

*c) eine **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*

*d) die zur Bewältigung der Risiken **geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren**, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird."*

Haben Sie Zweifel über a) die Verpflichtung zur Erstellung einer Datenschutz-Folgeabschätzung für Ihren Betrieb oder b) die darin abzuschätzenden Vorgänge, können Sie die Datenschutzbehörde um eine konkrete Auskunft bitten. Bleibt diese aus, dürfte es nicht fahrlässig sein, wenn Sie Ihre Betriebsgröße und -vorgänge als nicht umfangreich oder besonders risikoreich iSd. Art. 35 DSGVO einschätzen.

8. Datenschutzbeauftragter (Art. 37-39 DSGVO)

Nach Art. 37 DSGVO müssen Sie einen Datenschutzbeauftragten benennen, wenn Ihre Kerntätigkeit

> *"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"*

Das ist nach § 38 BDSG n.F. der Fall,

> *"soweit sie in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen."*

Der Hausmeister wird bei diesen zehn Personen nicht mit zählen, der Angestellte in der Buchhaltung oder der Objektsachbearbeiter aber schon.

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben. Er kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

> ***Erwägungsgrund 97***
> *In Fällen, in denen die Verarbeitung durch eine Behörde – mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht,* ***sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden.*** *Im privaten Sektor bezieht sich die* ***Kerntätigkeit*** *eines Verantwortlichen auf seine* ***Haupttätigkeiten*** *und* ***nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit****. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.*

Der Erwägungsgrund wirft die interessante Frage auf, was Ihre Haupttätigkeit ist. Gehört die Erfassung und Verarbeitung von Daten im Kern dazu, oder besteht Immobilienverwaltung primär aus etwas anderem? Bei einem Handwerker, der zwar seine Kundendaten erfasst, dessen Tätigkeit im Kern aber etwas anderes beinhaltet, ist das einfach zu beantworten, bei einem Architekten oder Psychologen ebenfalls. Eine Hausverwaltung beinhaltet zu einem ganz wesentlichen Teil aber Buchhaltung. Buchhaltung ist die Erfassung und der Abgleich von personenbezogenen Daten. Ich kann daher nicht ausschließen, daß Sie - ab der genannten Betriebsgröße - verpflichtet sind, einen Datenschutzbeauftragten zu bestimmen.

Der Datenschutzbeauftragten hat folgende Aufgaben (Art. 39 DSGVO):

- **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 Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35
- **Zusammenarbeit mit der Aufsichtsbehörde**;
- Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Konsequenzen bei Verletzung: Haftung, Schadensersatz, Geldbußen, Strafen

1. Haftung und Schadensersatz (Art. 82 DSGVO)

Kapitel 8 der DSGVO trägt den Titel „Rechtsbehelfe, Haftung und Sanktionen“. Davon soll vorliegend nicht alles ausführlich behandelt werden. Nach den Vorschriften

Art. 77 - Recht auf Beschwerde bei einer Aufsichtsbehörde
Art. 78 - Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde
Art. 79 Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche und Auftragsverarbeiter
Art. 80 Vertretung von betroffenen Personen
und
Art. 81 Aussetzung des Verfahrens

regelt Art. 82 die „**Haftung und Recht auf Schadenersatz**“. Die Vorschrift lautet:

1. *Jede Person, der wegen eines Verstoßes gegen diese Verordnung **ein materieller oder immaterieller Schaden** entstanden ist, hat **Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter**.*
2. ***Jeder an einer Verarbeitung beteiligte Verantwortliche haftet** für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.*
3. *Der Verantwortliche oder der Auftragsverarbeiter wird **von der Haftung** gemäß Absatz 2 **befreit, wenn er nachweist, dass er in keinerlei Hinsicht** für den Umstand, durch den der Schaden eingetreten ist, **verantwortlich ist**.*

4. *Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, **so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden**, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.*
5. *Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.*
6. *Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.*

Immaterieller Schadenersatz wird nach deutschem Recht kaum zugestanden. Wir kennen das im wesentlichen bei Körperverletzungen oder auch Verletzungen des Persönlichkeitsrechts (z.B. durch fehlerhafte oder zu aufdringliche Presseberichterstattung) als Schmerzensgeld. Die Beträge sind meist niedrig. Das könnte sich ändern, wenn man den Erläuterungen zu dieser Vorschrift folgt:

> ***Erwägungsgrund 146***
> *Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. **Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.** Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. **Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.** Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.*

Bei den materiellen Schäden hat der Verordnungsgeber wohl wieder an Kreditkarten- oder Identitätsmißbrauch gedacht. Hier geht es um genau bezifferbare Summen. Schwieriger wird es schon, wenn aufgrund unberechtigter Datenerhebung ein Mietinteressent keine Wohnung von Ihnen erhält, sondern Sie einen anderen Bewerber vorziehen. Beinhaltet Ihr Bewerbungsbogen unzulässige Fragen, ist das mit kausal für Ihre Entscheidung und muß der abgelehnte Interessent deswegen im Hotel unterkommen? Was ist hier verletzungskausal und wie hoch ist der kausalitätsbedingte Schaden? Kommt ein immaterieller Schaden hinzu? Wenn ja in welcher Höhe?

2. Geldbußen (Art. 83 DSGVO)

Neben der privatrechtlichen Haftung gegenüber verletzten Betroffenen sieht die Verordnung auch eine öffentlich-rechtliche Inanspruchnahme durch die Aufsichtsbehörden vor. Art. 83 lautet:

Art. 83 DSGVO. Allgemeine Bedingungen für die Verhängung von Geldbußen.

1. *Jede Aufsichtsbehörde stellt sicher, dass die **Verhängung von Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 **in jedem Einzelfall wirksam, verhältnismäßig und abschreckend** ist.*
2. *Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:*
   a) ***Art, Schwere und Dauer des Verstoßes** unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;*
   b) ***Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes**;*
   c) *jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter **getroffenen Maßnahmen zur Minderung des** den betroffenen Personen entstandenen **Schadens**;*
   d) *Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 **getroffenen technischen und organisatorischen Maßnahmen**;*
   e) *etwaige einschlägige **frühere Verstöße** des Verantwortlichen oder des Auftragsverarbeiters;*
   f) ***Umfang der Zusammenarbeit mit der Aufsichtsbehörde**, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;*
   g) ***Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind;*
   h) *Art und Weise, **wie der Verstoß der Aufsichtsbehörde bekannt wurde**, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;*
   i) *Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;*
   j) *Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und*
   k) ***jegliche anderen erschwerenden oder mildernden Umstände** im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.*
3. *Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.*
4. *Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 **Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs** verhängt, je nachdem, welcher der Beträge höher ist:*
   a) *die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;*
   b) *die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;*
   c) *die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.*
5. *Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 **Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs** verhängt, je nachdem, welcher der Beträge höher ist:*
   a) *die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*
   b) *die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;*
   c) *die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;*

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

6. *Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels* ***Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs*** *verhängt, je nachdem, welcher der Beträge höher ist.*
7. *Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.*
8. *Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.*
9. *Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.*

Erwägungsgrund 150

Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen. In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind. Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen" im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.

3. Strafvorschriften (Art. 84 DSGVO und § 42 BDSG n.F.)

Neben Haftung und Bußgeldandrohung sieht die DSGVO schließlich vor, daß die einzelnen Mitgliedstaaten weitere Sanktionen vorsehen können. Der deutsche Gesetzgeber hat davon insoweit Gebrauch gemacht, als daß das neue BDSG sogar Strafvorschriften enthält:

§ 42 BDSG (neu). Strafvorschriften.

1. *Mit* ***Freiheitsstrafe bis zu drei Jahren*** *oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,*
   1. einem Dritten übermittelt oder
   2. auf andere Art und Weise zugänglich macht
   und hierbei ***gewerbsmäßig*** *handelt.*

2. *Mit **Freiheitsstrafe bis zu zwei Jahren** oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,*
   1. ohne hierzu berechtigt zu sein, verarbeitet oder
   2. durch unrichtige Angaben erschleicht
   *und hierbei **gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen**.*
3. *Die Tat wird **nur auf Antrag verfolgt**. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.*
4. *…*

Fazit: was zu tun ist

Zunächst brauchen Sie einen Überblick über die in Ihrem Unternehmen anfallenden Datenerhebungs- und Datenverarbeitungsvorgänge. Ermitteln Sie, in welchen Situationen welche Daten anfallen, wie diese bei Ihnen gespeichert werden, an wen sie in welcher Situation weitergegeben werden und wann sie gelöscht werden. Erstellen Sie sodann gemäß Art. 30 DSGVO entsprechende **Verarbeitungsverzeichnisse**.

Datenzentralisierung zu Auskunftszwecken: um Auskunftsansprüche von Betroffenen (z.B. Mietern, Sondereigentümern) unverzüglich erfüllen zu können, ist es notwendig, Zugriff auf alle zu einer bestimmten natürlichen Person bei Ihnen hinterlegten personenbezogenen Daten zu haben und diese zur Verfügung stellen zu können. Ermitteln Sie deshalb, ob in Ihrem Unternehmen solche personenbezogenen Daten an verschiedenen Stellen hinterlegt sind, und führen Sie diese verschiedenen Datensätze in einem Datensatz zusammen. Sorgen Sie dafür, daß es so bleibt. Hinterlegen Sie diesen Datensätzen gemäß Art. 15 DSGVO Informationen über a) die Zwecke der Datenverarbeitung, b) die jeweilige Rechtsgrundlage, c) die Liste der Empfänger oder Kategorien der Empfänger und d) etwaige weitere Informationen, die Art. 15 DSGVO vorschreibt.

Ermitteln Sie, wem Sie Daten zu Verarbeitungszwecken weitergeben. Prüfen Sie und belegen Sie Ihre Prüfung, ob diese Dienstleister ihrerseits Datenschutzgrundsätze einhalten. Schließen Sie mit diesen Empfängern (außer Anwälten, die ohnehin einer Berufsverschwiegenheit unterliegen) **Datenverarbeitungsverträge** gemäß Art. 28 DSGVO.

Sorgen Sie dafür, daß Sie gemäß Art. 13 DSGVO Betroffene im Zuge der Datenerhebung über selbige, die Datenverarbeitung und ihre Zwecke informieren. In der Regel wird das bei Ihnen im Zusammenhang mit Mietvertragsabschlüssen stattfinden. **Überarbeiten Sie hierfür sämtliche Formulare, die Daten erfassen**, bspw. Selbstauskünfte von Mietinteressenten oder Bürgen, Lastschriftermächtigungen etc., und fügen Sie diesen Formularen entsprechende Informationen bei.

Das gleiche gilt in Bezug auf interne Daten, z.B. **Mitarbeiterverträge**. Verpflichten Sie außerdem Ihre Mitarbeiter, die Datenschutzgrundsätze Ihres Unternehmens zu beachten.

Sofern über Ihre Webseite Daten erfasst werden - bspw. wenn Sie einen Newsletter zur Verfügung stellen und man sich dafür anmelden kann, oder wenn man sich online auf eine Wohnung bei Ihnen bewerben kann - **überarbeiten Sie ihre Webseite:** sorgen Sie dafür, daß die Webseite die notwendigen Informationen enthält, technisch die Privacy-Grundsätze des Art. 25 DSGVO wahrt und Ihr Datenschutzbeauftragter auf ihr zu finden ist.

Entwickeln Sie **interne Richtlinien und Routinen** und schreiben Sie sie möglichst auf. Schulen Sie Ihre Mitarbeiter und entwickeln Sie standardisierte Abläufe. Wie reagieren Mitarbeiter, wenn Betroffene (Mieter, Sondereigentümer, Untermieter, Familienangehörige, Hausmeister, Eigentümer) fragen, welche Daten von Ihnen gespeichert wurden? Wie werden Betroffene über die Verarbeitung ihrer Daten informiert? Was ist der Prozess, wenn ein Betroffener darauf besteht, dass seine Daten gelöscht werden? Wer ist dafür verantwortlich? Was ist der Prozess, falls es zu einem Datenleck kommt und personenbezogene Daten in falsche Hände geraten? Wie gewährleisten Sie, daß Sie binnen 72 Stunden die zuständige Landesdatenschutzbehörde informieren können? Wie wird ermittelt, ob Daten noch benötigt werden, und wie wird sichergestellt, daß nicht mehr benötigte Daten gelöscht werden? Definieren Sie, für welche Daten unter welchen Voraussetzungen das der Fall ist. Wie werden Mitarbeiter geschult, damit sie diese Prozesse kennen und ausführen können?

Dokumentieren Sie, welche **Datensicherheitsvorkehrungen** Sie treffen, und passen Sie diese ggf. dem Stand der Technik an. Prüfen Sie, ob Daten unnötigerweise extern lagern (Dropbox, iCloud, Google-Drive, emails bei Ihrem Internetprovider), ob Sie Daten außerhalb Ihres Hauses verarbeiten (z.B. über eine webbasierte Textverarbeitungssoftware), ob Sie Daten über externe Dienstleister versenden, bei denen Sie nicht positiv wissen, daß Sie Ihre Datenschutzgrundsätze beachten (z.B. WhatsApp oder andere Messenger-Programme, auch auf Computern) oder ob Sie Dienstleistern externen Zugriff auf Ihre Daten geben (z.B. Fernwartungs- und Fernadministrations-Zugänge Ihrer IT-Leute). Ändern Sie das, wenn es nicht zwingend notwendig ist, oder schließen Sie mit diesen Dritten entsprechende Datenschutzvereinbarungen.

Wenn Ihre Betriebsgröße es erfordert (dann zwingend) oder wenn Sie wollen, daß sich jemand permanent um all diese Dinge kümmert (dann sinnvoll), bestellen Sie einen **Datenschutzbeauftragten**, melden Sie ihn bis zum 25.05.2018 der Aufsichtsbehörde und sorgen Sie dafür, daß er hinreichend in der Materie geschult ist. Geben Sie ihm die Freiheiten, die er benötigt, um Ihr Unternehmen so anzupassen, daß es die Vorschriften wahrt.

Dokumentieren Sie sämtliche Datenschutz-Anstrengungen: zu welchem Seminar ist der Datenschutzbeauftragte gegangen? Welche Firewall wurde wann von wem installiert und was schützt sie? Welche Datenverarbeitungsverträge wurden mit Dienstleistern geschlossen? Denn selbst bei eingetretenen Verstößen besteht bei guter Dokumentation die Chance, ohne Bußgeld davonzukommen. Dafür muss man aber die Unterlagen auf Anfrage umgehend vorlegen können.