CHECKLISTE FÜR DIE DATENSCHUTZRECHTLICHEN BESTIMMUNGEN GEMÄSS DER DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Zum Stichtag 25. Mai 2018 ist die EU-weit geltende Datenschutzgrundverordnung (DSGVO) für alle verbindlich. Die Verfahren, Konzepte und Informationspflichten sowie die Online-Auftritte sind entsprechend anzupassen und um diese verbindlichen Aspekte zum Schutz personenbezogener Daten zu ergänzen. Andernfalls drohen Abmahnungen und hohe Bußgelder.
Mindestens ebenso wichtig: Website-Besucher und Kunden werden immer sensibler, wenn es um den Schutz ihrer Privatsphäre geht. Sie wollen erfahren, wann und wie Daten von ihnen erhoben werden und was damit geschieht.
Diese Checkliste erhebt keinen Anspruch auf Vollständigkeit, macht Sie jedoch mit der Materie vertraut und sensibilisiert Sie für die umzusetzenden Punkte.

Von der DSGVO sind grundsätzlich sämtliche Vorgänge betroffen, bei denen personenbezogene Daten erhoben, gespeichert und verarbeitet werden – egal, ob sie von eigenen Interessenten und Kunden stammen, von Arbeitnehmern oder ob sie von anderen Unternehmen zur Verarbeitung geliefert werden.

Die DSGVO betrifft aber nicht nur Unternehmen, die schwerpunktmäßig mit eigenen oder fremden Daten arbeiten. Auch von Betreibern von Websites, Online-Shops, Handelsbetrieben, Kreditinstituten und Behörden werden klare Verhältnisse verlangt. Sie müssen wissen und dokumentieren, ob, wie und mit welchen Genehmigungen sie Daten ihrer Interessenten, Kunden, Mitarbeiter und Auftragnehmer verarbeiten.

1. Verarbeiter und Auftragsverarbeiter im Sinne der DSGVO

Die Datenschutzgrundverordnung betrifft Sie als „Verarbeiter“, wenn nur eine der folgenden Aussagen zutrifft:

- Ich betreibe eine Website.
- Ich biete Dienstleistungen oder Waren in Deutschland oder in der EU an.
- Ich beschäftige Mitarbeiter in meinem Unternehmen.

Die Datenschutzverordnung betrifft Sie als „Auftragsverarbeiter“, wenn

- In Deutschland (oder der EU) Dienstleistungen angeboten werden, zu denen es gehört, dass der Auftraggeber personenbezogene Daten übermittelt.

So sind z.B. externe Lohnbüros, Business-Cloud-Anbieter, Aktenvernichtungsdienstleister oder Newsletter-Versanddienste typische Auftragsverarbeiter.

2. Verzeichnis der Verarbeitungstätigkeiten

Wenn die DSGVO Sie betrifft, besteht eine der wichtigsten Aufgaben darin, ein Verzeichnis darüber zu erstellen, wie, warum und von wem in Ihrem Betrieb personenbezogene Daten verarbeitet werden: das sog. „Verzeichnis von Verarbeitungstätigkeiten“ (Art. 30 DSGVO).
Man kann dieses Verzeichnis elektronisch oder auf Papier führen – Hauptsache, es ist vorhanden, wenn die Datenschutzbehörden es verlangen. Kunden oder anderen Dritten muss kein Einblick gewährt werden, wohl aber den Aufsichtsbehörden. Kann es nicht vorgelegt werden, droht ein Bußgeld.

Das Erstellen der Dokumentation ist keine einmalige, sondern eine fortlaufende Arbeit. Wenn sich die Prozesse ändern, muss das für Außenstehende nachvollziehbar sein: Falls eine neue Software zum Einsatz kommt oder Daten zusätzlich ausgewertet werden, muss dies durch datierte Versionen klar werden. Um das Verzeichnis der Verarbeitungstätigkeiten erstellen zu können, ist zunächst eine Bestandsaufnahme notwendig.

Für jeden Arbeitsprozess sollten folgende Punkte festgehalten werden:

- Wer ist verantwortlich? (Name und Kontaktdaten)
- Welche Art von Daten wird gespeichert und verarbeitet? (z.B. E-Mail-Adressen, Kontodaten, Arbeitszeiten, Standortdaten)
- Welchen Zweck hat die Datenverarbeitung? (z.B. Lohnabrechnung, E-Mail-Marketing, Beschwerde-Management)
- Wessen personenbezogene Daten sind das? (z.B. Mitarbeiter, Interessenten, Kunden, Patienten, Lieferanten, Auftragnehmer)
- Besteht ein „hohes Risiko für die Rechte und Freiheiten“ betroffener Personen? (z.B. ist das bei Identitäts- oder Zahlungsdaten der Fall, da sie für Identitätsdiebstahl oder Betrug missbraucht werden können)
- Was ist die Rechtsgrundlage für die Verarbeitung? (z.B. gesetzliche Pflicht bei Lohnabrechnung, Einwilligung der Betroffenen bei E-Mail-Marketing)
- Welche Personen oder Stellen haben Zugriff oder verarbeiten die Daten intern? (Personen, Abteilungen)
- Welche Auftragsverarbeiter verarbeiten die Daten extern? (z.B. Cloud-Dienstleister, Werbeagenturen und deren Unterauftragnehmer)
- Wann werden nicht mehr benötigte Daten gelöscht?
- Was für Maßnahmen stellen den Datenschutz sicher? (z.B. IT-Sicherheitsmaßnahmen, abgestufte Zugriffsberechtigungen, Zugangskontrollen, Mitarbeiterschulungen)

Je größer ein Unternehmen oder eine Organisation ist, desto ausführlicher und detaillierter wird das Verzeichnis ausfallen. Grundsätzlich ist es ab 250 Beschäftigten in jedem Fall Pflicht. Betriebe und Organisationen mit weniger Mitarbeitern benötigen das Verzeichnis zwar nur, wenn

- „nicht nur gelegentlich“ Daten verarbeitet werden (damit sind bereits alle Arbeitgeber oder Unternehmen mit laufendem Bestelleingang zum Verzeichnis verpflichtet),
- die Datenverarbeitung mit einem Risiko „für die Rechte und Freiheiten der betroffenen Personen“ verbunden ist (damit sind wohl alle Unternehmen mit Bestellvorgängen von Verbrauchern zum Verzeichnis verpflichtet, weil sie Zahlungsdaten speichern),
- „besondere Datenkategorien“ verarbeitet werden (z.B. Angaben zur ethnischen Herkunft, Religionszugehörigkeit oder Gesundheitsdaten – auch deshalb muss jeder Arbeitgeber ein Verzeichnis führen, weil Krankheitstage und Konfessionszugehörigkeit gespeichert werden).

Letztlich wird nur eine Minderheit kleiner Betriebe ohne ein Verzeichnis auskommen. Das Bayerische Landesamt für Datenschutzaufsicht empfiehlt zwei Erweiterungen zum Verzeichnis:

1. Eine konkrete Beschreibung des Umgangs mit den personenbezogenen Daten; also z.B. was und wie erhoben, gespeichert, abgefragt oder sonst wie verarbeitet wird.
2. Eine Liste darüber, welche Belege als rechtliche Basis dienen; also z.B. Arbeitsvertrag, Betriebsvereinbarung, Einwilligungen.

3. Auftragsverarbeitungsvereinbarung (Auftragsdatenverarbeitung)

Dienstleistungen werden „Auftragsdatenverarbeitung“ oder „Auftragsverarbeitung“ genannt, wenn folgenden Merkmale zutreffen:

1. Ein Unternehmen beauftragt ein anderes Unternehmen mit einer Dienstleistung, die mit personenbezogenen Daten zu tun hat, die der Auftraggeber bereitstellt oder übermittelt.
2. Es besteht keine direkte Vertragsbeziehung zwischen dem Auftragnehmer und den Personen, zu denen die Daten gehören.
3. Der Auftragnehmer arbeitet weisungsgebunden, entscheidet also nicht selbst darüber, was er mit den Daten anstellt.

Vom Auftraggeber werden personenbezogene Daten (z.B. E-Mail-Adressen von Kunden, Lohndaten von Arbeitnehmern, Besuchsverläufe und IP-Adressen von Website-Besuchern) an das beauftragte Unternehmen weitergegeben, von diesem verarbeitet oder gespeichert.
Diese Daten unterliegen allerdings einem besonderen Schutz. Wer Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt, benötigt dafür eine korrekte Vereinbarung zur Auftragsverarbeitung.

Darin muss u.a. Folgendes geregelt sein:

- der Gegenstand, die Dauer sowie Art und Zweck der Datenverarbeitung (z.B. Web Analytics, Usability-Optimierung, Speicherung von Personaldaten)
- die Art der personenbezogenen Daten (Namen, Postanschriften, IP-Adressen, biometrische Daten, Vertragsdaten, Zahlungsangaben)
- die „Kategorien von Personen“ (Kunden, Arbeitnehmer, Website-Besucher)
- die Pflichten und Rechte, welche der Auftraggeber hat (z.B. dass er für die Wahrung der Datenschutzrechte der betroffenen Personen verantwortlich bleibt und dass er über Änderungen an der Datenverarbeitung entscheidet.

Die Vereinbarung zur Auftragsvereinbarung muss eine ganze Reihe von Verpflichtungen für den Auftragnehmer enthalten, damit sie den Anforderungen der DSGVO entspricht. Vertragsklauseln alleine reichen jedoch nicht, um der DSGVO als Auftraggeber gerecht zu werden. Man muss auch hinschauen: Aufträge zur Auftragsverarbeitung dürfen nur dann vergeben werden, wenn der Auftragnehmer „geeignete technische und organisatorische Maßnahmen“ zur Einhaltung der Datenschutzbestimmungen gewährleisten kann. Wenn absehbar war, dass der Auftragnehmer den vorgeschriebenen Datenschutz nicht einhalten konnte, droht bei Datenschutzverstößen auch dem Auftraggeber die Haftung; und zwar selbst dann, wenn der Vertrag alle Anforderungen erfüllt.

4. Datenschutzbeauftragter

Die neue Rechtslage in Art. 37 DSGVO legt die Pflicht zur Berufung eines Datenschutzbeauftragten etwas anders fest als der § 38 BDSG-neu) im Bundesdatenschutzgesetz.

Praktisch bedeutet das:

- Man braucht einen Datenschutzbeauftragten, wenn
    - mindestens 10 Personen ständig mit automatisierter Verarbeitung personenbezogener Daten befasst sind oder
    - wenn personenbezogene Daten geschäftsmäßig verarbeitet werden oder
    - sofern die Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen aufwirft.

- Man benötigen außerdem einen Datenschutzbeauftragten, wenn
  - Daten aus der laufenden Überwachung von Personen verarbeitet werden oder
  - die Daten sehr sensibel sind (d.h., wenn die Kerntätigkeit in der Verarbeitung von Daten besteht, die eine umfangreiche, regelmäßige und systematische Überwachung der Betroffenen erfordert) oder
  - wenn „besondere Kategorien" personenbezogener Daten verarbeitet werden (wie Daten zur rassischen und ethnischen Herkunft, zur politischen Meinung, religiösen oder weltanschaulichen Überzeugung, zur Gewerkschaftszugehörigkeit, wenn es sich um Daten zum Sexualleben, genetische, biometrische und Gesundheitsdaten handelt.

Der Datenschutzbeauftragte ist mit weit reichenden Befugnissen ausgestattet und ist bei der Wahrnehmung seiner Tätigkeit nicht weisungsgebunden. Es ist seine Aufgabe, die Einhaltung der Datenschutzbestimmungen zu „überwachen"; bisher reicht das bloße „Hinwirken". Mit Appellen und Belehrungen ohne Kontrolle ist es jetzt nicht mehr getan.
In die Zuständigkeit des Datenschutzbeauftragten fällt i.d.R. auch, nach Art. 35 DSGVO für eine Datenschutz-Folgenabschätzung zu sorgen. Das ist eine spezielle Risikoanalyse für Unternehmen und Organisationen mit erhöhtem Datenschutzrisiko, weshalb solche Betriebe ohnehin einen Datenschutzbeauftragten ernennen müssen.
Ob als Datenschutzbeauftragter ein Arbeitnehmer oder ein externer Berater benannt wird, liegt im Ermessen des Unternehmers. Er muss aber die notwendige Sachkenntnis besitzen. Wenn es einen Datenschutzbeauftragten gibt, müssen seine Kontaktdaten veröffentlicht werden (z.B. in der Datenschutzerklärung und/oder dem Impressum sowie im Verzeichnis der Verarbeitungstätigkeiten).

5. Datenschutzerklärung

Die DSGVO legt fest, dass Betroffene in verständlicher und detaillierter Form über das Speichern und Verarbeiten ihrer personenbezogenen Daten informiert werden müssen.
Websites, auf denen gar keine Daten erhoben werden, gibt es nur selten – als Voraussetzung reicht bereits die Möglichkeit für ein Newsletter-Abo oder das Erheben und Auswerten einer Besucherstatistik. Das bedeutet: Selbst wenn man eine Datenschutzerklärung auf der Website hat, muss sie wahrscheinlich angepasst werden. Wenn es noch keine Datenschutzerklärung gibt, wird es Zeit dafür.

Eine Datenschutzerklärung sollte folgende Elemente enthalten:

- Kontaktdaten des Verantwortlichen (Website-Betreiber und ggf. der Datenschutzbeauftragte) müssen genannt werden.
- Zweck und Rechtsgrundlage der Datenverarbeitung müssen genannt werden; und zwar für jede Anwendung bzw. jede Konstellation, zu der personenbezogene Daten erhoben werden. (z.B. „Für Bestellungen werden Zahlungs- und Adressdaten gespeichert, Adressdaten auch an den Paketdienst übermittelt, der Käufer stimmt dem ausdrücklich zu.").
  Rechtsgrundlage kann eine gesetzliche Regelung sein, welche die Datenerhebung ermöglicht oder eine Einwilligung des Nutzers.
- Häufig wird als Rechtsgrundlage das „berechtigte Interesse" an der Verarbeitung nach Art. 6 DSGVO in Frage kommen. In diesem Fall muss dieses Interesse konkret benannt werden (z.B. „berechtigte wirtschaftliche Interessen": Interessentendaten, die per Online-Formular erhoben werden, müssen an eine Unternehmensabteilung weitergeleitet werden, um die Anfragen überhaupt beantworten zu können).
- Dritte, an die Daten übermittelt werden, müssen genannt werden. Dazu gehören u.a. auch die Betreiber sozialer Netzwerke, wenn deren Buttons eingebunden sind und diese Nutzerdaten speichern.

- Es muss ein Hinweis erfolgen, falls Daten in Nicht-EU-Staaten übermittelt werden (z.B. wenn die Betreiber der sozialen Netzwerke ihre Server in den USA haben). Die Übermittlung von personenbezogenen Daten in EU-Drittstaaten ist gemäß DSGVO ohnehin sehr problematisch.
- Die Dauer der Datenspeicherung bzw. der vorgesehene Zeitpunkt der Datenlöschung muss genannt werden.
- Die Besucher und Nutzer müssen informiert werden, welche Rechte sie in Bezug auf ihre gespeicherte Daten haben (Recht auf Auskunft, Löschung, Berichtigung und Ergänzung, Widerspruch gegen die Verarbeitung, Widerruf einer erteilten Einwilligung, Beschwerde bei Datenschutzbehörden, Datenübertragbarkeit). Es muss klar darauf hinwiesen werden, dass diese Rechte bestehen und wie diese ausgeübt werden können.
- Falls eine „automatisierten Entscheidungsfindung" verwendet wird, muss dies genannt werden. Damit sind z.B. automatisierte Scores gemeint, welche die Bonität bei Finanzierungen ermitteln und entsprechend unterschiedliche Konditionen für unterschiedliche Interessenten ausgeben. Solche Algorithmen sind gemäß Art. 22 DSGVO ohnehin problematisch, wenn ihr Einsatz nicht erforderlich ist oder der Nutzer nicht ausdrücklich zustimmt.

6. Einwilligung der Betroffenen

Nicht in jedem Fall muss laut DSGVO eine ausdrückliche Einwilligung zum Speichern der Daten vorliegen, denn die Speicherung kann entweder auf einem berechtigten Interesse oder einer gesetzlichen Vorschrift beruhen. Allerdings sollte Klarheit herrschen, für welche Datenbestände welche Rechtsgrundlage existiert und was rechtlich problematisch sein könnte. Und dort, wo eine Einwilligung des Betroffenen nötig ist, muss später nachweisbar sein, dass sie tatsächlich erteilt wurde.

Eine Einwilligung kommt nur dann wirksam zustande, wenn der Betreffende über den Zweck der Datenverarbeitung informiert wird und sich dafür oder dagegen entscheiden kann. Ein Vertragsabschluss darf z.B. nicht daran gekoppelt sein, dass man weitere, dafür nicht notwendige personenbezogene Daten von sich preisgibt (Kopplungsverbot). Außerdem muss die Einwilligung ausdrücklich den Hinweis enthalten, dass der Betreffende seine Einwilligung später widerrufen kann.
Vor diesem Hintergrund müssen alle Abfragen, Kontakt-, Anmelde- und Bestellformulare und Abo-Funktionen, die eine Einwilligung zur Datenspeicherung beinhalten, überprüft und DSGVO-konform angepasst werden.
Allerdings muss der Betroffene nicht immer einwilligen. Wichtige Ausnahmen sind u.a. die Vertragserfüllung sowie die Wahrung berechtigter (wirtschaftlicher) Interessen. Personenbezogene Daten, die dafür notwendig sind, dürfen ohne Einwilligung gespeichert und verarbeitet werden.

Berechtigte Interessen seitens des Verarbeiters können sein:

1. Kunden- und Bestellverwaltung: Wenn ein Kunde eine Ware bestellt bzw. kauft, muss er personenbezogene Daten (z.B. Name, Adresse, E-Mail-Adresse, Geburtsdatum (Volljährigkeit), Konto- oder Kreditkartennummer) von sich preisgeben. Diese Daten sind für die Vertragserfüllung erforderlich, denn ohne sie kann weder die Ware versendet noch die Rechnung gestellt werden. Bei Ratenzahlungen dürfen auch Daten der SCHUFA verarbeitet werden.
2. Direktwerbung: Man möchte Käufer im Online-Shop auf weitere Angebote hinweisen, die zu bereits erfolgten Bestellungen passen (z.B. Kunden, die Katzenfutter gekauft haben, darf man auf die neuen Kratzbäume aufmerksam machen und dazu deren Namen und E-Mail-Adressen verarbeiten). Allerdings muss der Adressat die Möglichkeit haben, solcher Direktwerbung jederzeit zu widersprechen (Opt-out). Nicht zulässig ist es, personenbezogene Daten an Dritte zu übergeben, die in keinem Zusammenhang mit dem ursprünglichen Vertrag stehen (z.B. an Adresshändler oder andere Shop-Betreiber).

3. Kontaktangaben von Arbeitnehmern: Wenn die Namen und geschäftlichen Kontaktdaten von Mitarbeitern des Vertriebs oder der Presseabteilung im Internet veröffentlicht sind, entspricht das einem berechtigen Interesse des Unternehmens. Damit muss ein Mitarbeiter rechnen, zu dessen Kernaufgaben die Kontaktpflege nach außen gehört.

Es liegt auf der Hand, dass in der Praxis viele Grenz- und Zweifelsfälle existieren. Dann hilft nur eine Abwägung der beiderseitigen Interessen und Rechte. Es wird einige Zeit dauern, bis die Gerichte eine klare Linie entwickelt haben, wo genau die Grenze der „berechtigten Interessen" von Unternehmen in der Praxis verläuft.

7. Datenschutzfreundliche Grundeinstellungen

Die DSGVO fordert, dass die Voreinstellungen bei Online-Diensten, bei Software und anderen technischen Angeboten grundsätzlich möglichst datenschutzfreundlich gewählt werden (privacy by default). Bereits die technische Gestaltung soll möglichst datenschutzorientiert erfolgen (privacy by design). Das ergibt sich aus dem Grundsatz der Datenminimierung in Art. 5 DSGVO und aus der Verpflichtung zur Gewährleistung eines angemessenen Schutzniveaus nach Art. 32 DSGVO.
Die Technologie muss also mehr gewährleisten als den Schutz der persönlichen Nutzerdaten gegen Hacker. Sie muss vielmehr so gestaltet sein, dass der Nutzer nur die für den Zweck des Programms oder Dienstes wirklich notwendigen personenbezogenen Daten angeben muss und darüber hinaus selbst entscheiden kann, ob er weitere Daten von sich preisgeben will.

Anwendungsbeispiele aus der Praxis:

- Eingabe- und Bestellmasken sollten nicht mehr personenbezogene Pflichtangaben enthalten als notwendig. Wenn Interessenten sich per E-Mail ein kostenloses Whitepaper zuschicken lassen können, kann das Bestellformular zwar die Eingabe der Postadresse ermöglichen, der Abschluss der Bestellung sollte aber nicht davon abhängen.
- Wenn Kunden sich untereinander in einem Online-Forum austauschen können, sollte die Software nicht ohne triftigen Grund die Angabe der Klarnamen erzwingen.
- Eine Kundendatenbank sollte so eingerichtet sein, dass sie nur denjenigen Mitarbeitern Zugriff auf personenbezogene Daten gewährt, die diese für ihre Aufgaben tatsächlich benötigen.

8. Datensicherheit und IT-Sicherheit

Art. 32 DSGVO verlangt bei der Datenverarbeitung „geeignete technische und organisatorische Maßnahmen", um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Zu geeigneten technischen und organisatorischen Maßnahmen zählen u.a.:

- gängige Verschlüsselungstechnologien (z.B. SSL für Websites, PGP oder S/MIME für E-Mail, Datensicherungskonzepte mit Verschlüsselung).
- allgemeine IT-Sicherheitsmaßnehmen (z.B. Passwortgeschützte Hard- und Software, permanente Software-Updates, Einsatz von Firewalls, Virenschutz oder Intrusion Detection).
- Organisatorische Konzepte (z.B. Auslagerung sensibler Daten in sichere Rechenzentren, Zugangsschutz für Server-Räume und Aktenarchive, abgestufte Zugriffsberechtigungen für personenbezogene Daten).
- Schulungen und Verpflichtungen für Arbeitnehmer.

Die DSGVO erwähnt explizit, dass eine Datenschutz-Zertifizierung als Nachweis für die Erfüllung dieser Vorschrift wichtig sein kann. Es ist noch nicht definiert, was als Zertifizierung im Sinne der DSGVO gilt bzw. ob das z.B. mit ISO-27001-Konformität erreicht ist.

9. Maßnahmen bei Datenpannen

Verletzungen des Schutzes personenbezogener Daten (z.B. Datenpannen und -verluste), müssen laut Art. 33 DSGVO innerhalb von 72 Stunden an die Aufsichtsbehörden gemeldet werden, wenn das möglich ist.

Diese Meldung muss

- die voraussichtlichen Folgen der Datenschutzverletzung umfassen
- die ergriffenen Maßnahmen darlegen.

Geplant ist, dass solche Meldungen auch online bei der Aufsichtsbehörde abgegeben werden können. Damit diese Pflicht im Fall eines Hacks oder einer Rechner-Havarie umgesetzt werden kann, sollte es klare interne Anweisungen und einen Reaktionsplan für solche Situationen geben – das gilt auch für kleinere Unternehmen.

10. Rechte der betroffenen Person

Art. 15-23 DSGVO verlangen, dass ein Verarbeiter in der Lage sein muss, den umfangreichen Rechten einer betroffenen Person hinsichtlich ihrer personenbezogenen Daten zu entsprechen, wenn sie es verlangt und kein berechtigtes Interesse entgegensteht.

Zu diesen Rechten gehören u.a.:

- Auskunftsrecht
  - über die Verarbeitungszwecke
  - über die Kategorien
  - über die Empfänger, denen die Daten offengelegt wurden oder werden
  - über die Dauer der Datenspeicherung sowie die Kriterien für diese Fristfestlegung
- Recht auf Berichtigung
- Recht auf Löschung
  - sofern die Zwecke für die Datenerhebung oder -verarbeitung nicht mehr notwendig sind
  - sofern die vorliegende Einwilligung widerrufen wird und keine anderweitige Rechtsgrundlage für die Verarbeitung vorliegt
  - sofern die personenbezogenen Daten unrechtmäßig verarbeitet wurden
- Recht auf Einschränkung der Verarbeitung
  - wenn die Richtigkeit der Daten bestritten wird (für die Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der Daten zu überprüfen)
  - wenn die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der Daten ablehnt
  - wenn die Daten für die Verarbeitung nicht länger benötigt werden, sie aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vorgehalten werden sollen
  - wenn Widerspruch gegen die Verarbeitung eingelegt wurde, aber noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen
- Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung
- Recht auf Datenübertragbarkeit

- Widerspruchsrecht
    - Die betroffene Person hat das Recht, jederzeit gegen die Verarbeitung ihrer Daten Widerspruch einzulegen. Sofern keine zwingenden schutzwürdigen Gründe vorliegen, die die Interessen, Rechte und Freiheiten der Person überwiegen, oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient, dürfen die Daten nicht mehr verarbeitet werden.
    - Die betroffene Person hat das Recht, jederzeit gegen die Verarbeitung ihrer Daten zum Zweck der Direktwerbung Widerspruch einzulegen.
    - Die betroffene Person muss unmittelbar, in verständlicher und abgetrennter Form ausdrücklich auf die Widerspruchsrechte hingewiesen werden.
- Automatisierte Entscheidungen im Einzelfall

Natürlich greifen bestimmt Rechtsansprüche nicht, wenn ein Kunde, der noch nicht bezahlt hat, die Löschung seiner Daten aus Ihrer Buchhaltung verlangt. Aber man sollte in der Lage sein, die Daten eines Nutzers zu löschen, der unter vollem Namen auf Ihrer Website Kommentare hinterlassen oder nur den Newsletter abonniert hat und es sich dann anders überlegt.
Im Idealfall gibt es für alle personenbezogenen Daten ein Löschkonzept, das dokumentiert, ob bzw. wann die jeweiligen Datensätze gelöscht werden können und sicherstellt, dass dies dann tatsächlich passiert. Das Löschkonzept ist Bestandteil oder Anlage zum Verzeichnis der Verarbeitungstätigkeiten.

11. Verpflichtung auf das Datengeheimnis

Das Bundesdatenschutzgesetz schrieb vor, dass Arbeitnehmer, die mit personenbezogenen Daten zu tun hatten, vom Arbeitgeber auf das Datengeheimnis verpflichtet werden mussten. Das konnte im Rahmen des Arbeitsvertrags oder durch eine gesonderte Erklärung erfolgen. In der DSGVO ist diese Forderung nicht mehr explizit enthalten, wohl aber implizit. Eine arbeitsrechtliche Verpflichtung der Mitarbeiter auf die Einhaltung datenschutzrechtlicher Bestimmungen im Sinne der DSGVO ist also weiterhin sinnvoll.
Falls die Formulierung der bisherigen Verpflichtungserklärung ausdrücklich auf § 5 BDSG Bezug nimmt, ist diese zu aktualisieren.

Für Unternehmen, Selbstständige und Behörden, die den Datenschutz ernst nehmen und sich bereits um datenschutzkonforme Strukturen und Abläufe bemüht haben, wird die Umsetzung der Bestimmungen in der DSGVO kaum vor unüberwindbare Probleme stellen.
Einerseits ist die rechtskonforme Umsetzung des Regelwerks sicher mit zusätzlichem administrativem Aufwand verbunden. Andererseits bietet die DSGVO die vielleicht einmalige Chance, die betrieblichen Prozesse aufzulisten, zu überprüfen und sie dann im Zuge einer Neuorganisation so anzupassen, dass diese dem geltenden EU-Recht entsprechen.