Allgemeine Hinweise zur DSGVO

Durch die neue Datenschutzgrundverordnung soll der Schutz der Daten natürlicher Personen erheblich verbessert werden. Es gelten nun strengere Anforderungen für die Erhebung, Speicherung und Verwendung von Daten. Die Datensicherheit im Unternehmen muss neu überdacht und ggf. ein Datenschutzbeauftragter bestellt werden. Außerdem stehen der betroffenen Person erheblich mehr Rechte zur Verfügung. Zu beachten ist insbesondere das Recht auf Vergessenwerden. Die Informationspflicht, die Sie mit Bereithalten der Datenschutzerklärung erfüllen, besteht, sobald Sie Daten erheben. Grundsätzlich gilt für Altdaten, dass rechtswirksame Einwilligungen wohl weiterhin gültig sein sollen, sofern die Einwilligung der Art nach den Bedingungen der DSGVO entsprach.

Eine staatliche Aufsichtsbehörde wird die neuen Vorschriften im Datenschutzrecht kontrollieren und bei Verstößen kann sie empfindliche Bußgelder verhängen. Vorgesehen sind unangekündigte Kontrollen direkt im Unternehmen. Es ist daher ratsam insbesondere in der Anfangszeit ein besonderes Augenmerk auf den Datenschutz zu legen. Wie bei jeder neuen gesetzlichen Regelung bestehen noch viele Unsicherheiten hinsichtlich der Umsetzung. Praxisbeispiele und Urteile existieren noch nicht, so dass wir nur eine Einschätzung anhand des Gesetzes abgeben können. Aus anwaltlicher Vorsicht wird daher meist die strengste Auslegung zugrunde gelegt.

Im Folgenden haben wir einige Punkte zusammen gefasst, die Sie in Ihrem Unternehmen überprüfen und ggf. umsetzen sollten, und diese mit Beispielen versehen. Bei speziellen Datenverarbeitungsvorgängen (z.B. Auftragsdatenverarbeitung, Scoring) sind weitere Punkte zu beachten, die in diesen allgemeinen Hinweisen aufgrund des Umfangs jedoch nicht enthalten sind. Unsere Datenschutzerklärung ist für die Verwendung im Rahmen eines Internetauftritts ggfs. mit Online-Shop erstellt worden. Wenn Sie eine weitergehende Datennutzung vornehmen, muss diese entsprechend ergänzt werden.

Hierzu wenden Sie sich bitte direkt an uns.

- Einhaltung der Datenschutzgrundsätze, Art. 5 Abs. 1 DSGVO: Nennung der rechtlichen Grundlage; angemessene Berücksichtigung der Interessen des Betroffenen; Informationsstrukturen und –leitlinien; Zweck der konkreten Datenverarbeitung; Sperr- und Löschkonzept; Prüfkonzept hinsichtlich Aktualität personenbezogener Daten; Festlegung und Überprüfung von Speicherfristen; Sicherheitskonzept

- Datensicherheit
  Um diese sicherzustellen, können die folgenden Beispiele für die Umsetzung verwendet werden: Konzepte zum Zugriff, Verschlüsslungen und Antivirenkonzepte; Dokumentationen über Zutritte, Zugänge, durchgeführte Rücksicherungstests und Sicherheitskonfigurationen; Notfallhandbücher; Netzwerkpläne und Übersichten über Hard- und Software; Wartungs- und Austauschpläne

- Rechenschaftspflicht
  Zu Beweiszwecken sollten die Informationen in Textform festgehalten werden. Die Art der durchzuführenden Maßnahmen zur Einhaltung dieser Pflicht sind nicht detailliert festgelegt worden. Allerdings wurden in einer Stellungnahme folgende Beispiele genannt:
    - die Festlegung interner Verfahren vor Beginn neuer Verarbeitungen personenbezogener Daten (interne Prüfung, Beurteilung usw.)
    - die Aufstellung schriftlicher und verbindlicher Datenschutzstrategien
    - die Bestellung eines Datenschutzbeauftragten und anderer für den Datenschutz zuständiger Personen
    - angemessene Mitarbeiterschulungs- und -fortbildungsangebote im Bereich Datenschutz

- die Einführung und Überwachung von Kontrollverfahren

- informierte Einwilligungserklärung
  Die Einwilligung sollte folgende Punkte beinhalten: genaue Bezeichnung der erhobenen Daten; Zweck der Verarbeitung; Möglichkeit des Widerspruchs; Weitergabe an Dritte; Verwendung der Daten. Sie muss ausdrücklich durch die betroffene Person erfolgen und darf nicht nur Teil der AGB sein. Empfehlungen für die technische Umsetzung:
  - auf der Startseite umfassende und deutlich sichtbare Hinweise über die Verwendung von Cookies (z.B. Eingangsbildschirm, Banner, Dialog-Fenster), den Zweck der Verwendung sowie die Speicherfrist und die Möglichkeit, Cookies abzulehnen
  - Einwilligung vor dem Setzen oder Lesen von Cookies durch ausdrückliche Handlung oder eine andere aktive Verhaltensweise (z.B. Anklicken einer Schaltfläche oder eines Links und Markieren eines Feldes)
  - wenn möglich, sollte bei jeder Datenerhebung eine anklickbare Schaltfläche vorhanden sein, mit der der Kunde in die Datenerhebung einwilligt und gleichzeitig bestätigt, dass er die Datenschutzerklärung zur Kenntnis genommen hat. Diese sollte verlinkt werden. Außerdem darf es sich dabei nicht um ein Pflichtfeld handeln und es sollte auf die Freiwilligkeit der Einwilligung, den Zweck der Verwendung und die Widerrufsmöglichkeit hingewiesen werden.

- Datenverarbeitung zur Wahrung berechtigter Interessen, Art. 6 Abs. 1 f DSGVO
  Das berechtigte Interesse ist dem Betroffenen mitzuteilen. Es muss rechtmäßig und hinreichend bestimmt sein und tatsächlich (d.h. nicht spekulativ) bestehen. Ein berechtigtes Interesse kann nicht nur rechtlicher, sondern auch ideeller oder wirtschaftlicher Natur sein. Beispielhaft könnten folgende Interessen als berechtigt gelten:
  - Erhebung personenbezogener Daten der Gegenseite durch einen Rechtsanwalt im Rahmen eines Mandatsverhältnisses zur Durchsetzung von Rechtsansprüchen des Mandanten
  - Die Speicherung und Übermittelung personenbezogener Kundendaten im Rahmen eines von der Versicherungswirtschaft eigerichteten Risikoanalysesystems
  - Speicherung von Käuferdaten durch Autohersteller zur Kontaktaufnahme im Falle möglicher Rückrufaktionen
  - Übermittlung von Kunden- und/der Schuldnerdaten an die SCHUFA
  - Unterhaltung eines Arztbewertungsportals
  - Einsatz sog. Dash-Cams zu Beweissicherungsinteressen
  - Direktmarketing
  - Adresshandel
  - Betrugs- und Kriminalitätsbekämpfung
  - Datenaustausch innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung von Kunden- und/oder Beschäftigtendaten
  - Effektives Forderungsmanagement durch Inkassounternehmen
  - Wahrnehmung des Rechts auf Meinungs- und Informationsfreiheit, auch in den Medien und in der Kunst
  - unerbetene Mitteilungen zu nichtgewerblichen Zwecken, darunter im Rahmen von politischen Kampagnen oder des Sammelns von Zuwendung für gemeinnützige Zwecke
  - Überwachung von Arbeitnehmern aus Sicherheits- oder Verwaltungsgründen
  - persönliche Sicherheit, IT- und Netzsicherheit
  - Verarbeitung für historische, wissenschaftliche oder statistische Zwecke

- Informationspflichten, Art. 13 DSGVO: Name und Kontaktdaten, ggf. auch des Datenschutzbeauftragten; Zwecke und Rechtsgrundlagen der Verarbeitung; berechtigte Interessen; Empfänger; ggf. Übermittlung in Drittländer;
  voraussichtlich (diese Angaben befinden sich trotzdem in unserer Datenschutzerklärung) nur auf Nachfrage: Dauer der Speicherung; Betroffenenrechte

- Zusätzliche Informationspflichten bei Dritterhebung (also nicht bei der betroffenen Person selbst), Art. 14 DSGVO: Datenkategorien; Herkunft der Daten
  Datenkategorien sind nicht vorgeschrieben, empfohlen wird folgende Schutzklasseneinstufung, die dem des Standard-Datenschutzmodell (SDM) entspricht:
  - Kategorie 1: Daten, die frei zugänglich sind. Hierzu gehören im Einzelfall u.a. Adress- und Kommunikations- und sonstige Stammdaten und solche Daten die der Betroffene selbst veröffentlicht hat (z.B. über soziale Medien)
  - Kategorie 2: Daten, deren unsachgemäße Handhabung zwar keine besonderen Beeinträchtigungen des Betroffenen erwarten lässt und die aus „beschränkt öffentlichen Quellen“ stammen. Hierzu zählen im Einzelfall u.a. Adress-, Kommunikations- und Forderungsdaten
  - Kategorie 3: Daten, deren Verarbeitung grundsätzlich eine Beeinträchtigung des Betroffenen bedingt und/oder Daten, gegen deren Verwendung der Schuldner explizite Einwände erhoben hat. Hierzu zählen u.a. sensible Schuldnerdaten, Bonitätsdaten, Daten über Beziehungen des Betroffenen zu Dritten
  - Kategorie 4 – besondere Kategorie personenbezogener Daten: Daten, die in den Art. 9 und 10 DSGVO genannt sind, Daten betr. Kinder gem. Art. 8 sowie weitere Daten, deren Bekanntwerden ein vergleichbares Schadenspotential mit sich bringt

- Betroffenenrechte, Art. 15-22 DSGVO: Auskunft, Recht auf Berichtigung, Recht auf Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit, Einwilligungswiderruf, Beschwerderecht

- datenschutzfreundliche Voreinstellung, Art. 25 DSGVO: Bei der Verarbeitung von Daten sollten die Voreinstellungen möglichst datenschutzfreundlich sein, so dass der Nutzer selbst die datenschutzunfreundlichere Möglichkeit auswählen kann

- Gemeinsame Verantwortlichkeit oder Auftragsdatenverarbeitung, Art. 26 ff. DSGVO: Details der Auslagerung von Datenverarbeitungsvorgängen müssen in einem begleitenden Auftragsdatenverarbeitungsvertrag festgehalten werden; zentrale Verfahren müssen schriftlich dokumentiert werden
  - Wir weisen bei der Nutzung von Google Analytics darauf hin, dass die Datenschutzbehörden für den zulässigen Einsatz von Google Analytics den Abschluss einer Auftragsdatenverarbeitungs-Vereinbarung verlangen. Eine entsprechende Vorlage finden Sie unter http://www.google.com/analytics/terms/de.pdf. Dies gilt auch für alle anderen Analyse- und Tracking-Tools und könnte auch für jede Plattform gelten, auf der Sie tätig sind (z.B. eBay, Amazon). Bei der Verwendung des Analyse-Tools Google Analytics raten wir Ihnen außerdem unter dem Gesichtspunkt des Grundsatzes der Datensparsamkeit dazu, die Verwendung von IP-Masking zu aktivieren.
  - Unsicherheiten bestehen bei der Nutzung von Verkaufsplattformen. Das Kurzpapier der Datenschutzkonferenz spricht von einer gemeinsamen Verantwortung von Plattformbetreiber und Nutzer. Nicht klar ist, ob davon auch Verkaufsplattformen umfasst sind. Sollte diese Ansicht sich durchsetzen, würden Sie als Verkäufer auf Plattformen wie eBay oder Amazon gemeinsam mit dem Betreiber für die Datenerhebung verantwortlich sein und gesamtschuldnerisch haften. Es sollte daher eine entsprechende Vereinbarung mit der Plattform getroffen werden. Besteht eine

gemeinsame Verantwortlichkeit, ohne dass eine Vereinbarung nach Art. 26 DSGVO getroffen wurde, können Geldbußen nach Art. 83 Abs. 4 lit. a verhängt werden

- Verzeichnis von Verarbeitungstätigkeiten, Art 30 DSGVO: eine Ausnahme von dieser Pflicht besteht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, es bestehen Risiken für den Betroffenen, die Verarbeitung erfolgt nicht nur gelegentlich oder es werden Daten der Kategorie 4 verarbeitet
    - mögliche Risiken: Diskriminierung, Identitätsdiebstahl oder –betrug, finanzieller Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Datenschutz, unbefugte Aufhebung der Pseudonymisierung, erhebliche wirtschaftliche oder gesellschaftliche Nachteile oder sonstige physische, materielle oder immaterielle Schäden beim Betroffenen
      → da diese Risiken recht unspezifisch sind, können wir Ihnen aus anwaltlicher Vorsicht nur zum Führen eines solchen Verzeichnisses raten; es kann auch elektronisch geführt werden und ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen
    - erforderliche Angaben: den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten; die Zwecke der Verarbeitung; eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten; die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen; ggfls. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien; wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien; wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1

- bei bestimmten Datenverlustszenarien sind die Datenschutzaufsichtsbehörde und die Betroffenen zu informieren, § 31 DSGVO

- Datenschutz-Folgenabschätzung, Art. 35 DSGVO: nur bei hohem Risiko für Rechte und Freiheiten natürlicher Personen → wird bestimmt durch Art, Umfang, Umständen und Zwecken der Verarbeitung (z.B. neue oder neuartige Technologien, umfangreiche Verarbeitungsvorgänge), insbesondere in folgenden Fällen erforderlich:
    - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durch automatisierte Verarbeitung einschließlich Profiling, die wiederum als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
    - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 (rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO
    - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

- strengere Anforderungen an sog. Scoring, § 31 Abs. 1 BDSG-Neu

- Datenschutzbeauftragter, § 38 BDSG-Neu: Unternehmen müssen einen externen oder internen Datenschutzbeauftragten bestellen, wenn der Fokus der Tätigkeit auf der Datenverarbeitung liegt, sie der Pflicht einer Datenschutz-Folgeabschätzung unterliegen oder mindestens zehn Mitarbeiter regelmäßig am PC arbeiten und mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind; Schulungspflicht der Beschäftigten gem. Art. 37 DSGVO; Datenschutzbeauftragter kann auch ein fachkundiger Mitarbeiter sein; Inhaber, Geschäftsführer und Personen, bei denen ein Interessenkonflikt droht (z.B. Leiter der IT-Abteilung) sind ausgeschlossen