Kurzinformation zur EU-Datenschutzgrundverordnung (EU-DSGVO)

Die nachfolgende Kurzinformation soll helfen, einige Fragen, die durch die neue EU-DSGVO aufkommen, zu beantworten und Ängste abzubauen. Sie erhebt keinen Anspruch auf juristische Korrektheit und Vollständigkeit, sondern versucht, die Anforderungen in einfachen Worten wiederzugeben.

Worum geht es?

Im Datenschutz geht es um personenbezogene Daten, das heißt, um Daten von natürlichen Personen. Firmenumsätze und Firmenadressen fallen z.B. gar nicht unter die EU-DSGVO. Auch bei personenbezogenen Daten muss man unterscheiden, ob es sehr sensible Daten sind (z.B. Gesundheitsdaten, Kontodaten von natürlichen Personen, Mitarbeiterbewertungen), oder ob es weniger sensible Daten wie z.B. Kontaktadressen sind. Weniger sensible Daten müssen zwar auch geschützt werden, aber die Anforderungen sind geringer und die Strafen würden bei einer Verletzung auch geringer ausfallen. Die EU-DSGVO achtet bei ihren Anforderungen immer auch auf die „Verhältnismäßigkeit“. Ein gutes Beispiel hierfür ist die Übergabe einer Visitenkarte. Die dürfen Sie auch weiterhin annehmen.

Neu sind die umfangreichen Informationspflichten!

Grundsätzlich sind „Betroffene“, also die Personen, von denen Sie Daten erheben, über eine Vielzahl von Punkten zu informieren. Artikel 13 der EU-DSGVO regelt das. Dazu gehören z.B. Kontaktdaten der Firma, die die Daten erhebt, Empfänger der Daten, umfangreiche Rechte der Betroffenen und Informationen dazu, warum die Daten erhoben werden und was mit den Daten gemacht wird.
Diese Informationen müssen **jedes Mal**, wenn Daten erhoben werden, gegeben werden. Personen, bei denen die Daten bereits vor in Kraft treten der EU-DSGVO erhoben wurden, müssen ebenfalls informiert werden. Aber auch hier gilt der Grundsatz der „Verhältnismäßigkeit“.
Kleinere Verkaufshäuser oder Werkstätten können solche Informationen aushängen, auf Internetseiten werden sie üblicherweise unten neben dem Impressum platziert. Bestehende Kunden erreicht man in der Regel über E-Mail (wenn auch nicht immer alle).

Zur Ausübung Ihres Geschäftes dürfen Sie die Daten immer verwenden!

Wenn Sie Ihrer Informationspflicht nachkommen, dürfen Sie die erhobenen Daten grundsätzlich zur Ausübung Ihres Geschäftes verwenden, also dazu, Produkte oder Dienstleistungen zu verkaufen. Hierzu benötigen Sie KEINE Einwilligung (Artikel 6 Abs. 1 b) EU-DSGVO). Sie dürfen allerdings auch nur diejenigen Daten speichern, die sie tatsächlich benötigen, um ihre Leistungen zu erbringen. Geht es zum Beispiel um die Auslieferung eines Produktes, benötigen Sie zwar Kontaktdaten, aber keine Geburtsdaten. Der Vertrieb hätte diese zwar manchmal gerne, beispielsweise um Geburtstagsgrüße zu versenden, das zählt aber nach EU-DSGVO nicht zum Geschäftszweck.

Sehr erfreulich dabei ist, dass Direktmarketing für eigene Produkte und Dienstleistungen gemäß Erwägungsgrund 47 zu Artikel 6 Abs. 1 f) der EU-DSGVO als ein berechtigtes Interesse eines Unternehmens betrachtet wird, solange nicht davon

auszugehen ist, dass der Betroffene dadurch nicht sehr stark in seinen Rechten verletzt wird. Auf Deutsch: Sie dürfen in aller Regel für Ihre eigenen Produkte und Dienstleistungen werben, ohne hierzu eine Einwilligung einzuholen. Allerdings müssen Sie in Ihrer Information darauf hinweisen und der Betroffene hat das Recht, zu widersprechen (Artikel 21 Abs. 2 EU-DSGVO). In einem solchen Fall müssen Sie den Widerspruch dokumentieren und sicherstellen, dass der Betroffene zukünftig keine Werbung mehr erhält.

Wann benötigen Sie eine Einwilligung?

Eine explizite Einwilligung in die Verarbeitung von Daten benötigen sie z.B. immer dann, wenn es nicht um den Abschluss eines Geschäftes geht, wenn Sie für mehr als Ihre eigenen Produkte werben möchten oder wenn Sie Daten von betroffenen Personen für eigene Werbezwecke öffentlich machen möchten. Dazu gehört beispielsweise auch die Veröffentlichung von persönlichen Fotos zu Veranstaltungen, die Sie organisiert haben oder auf denen Sie sich präsentieren.
Die EU-DSGVO fordert zwar nicht explizit eine schriftliche Einwilligung, allerdings müssen Sie nachweisen, dass der Betroffene seine Einwilligung gegeben hat. Und das geht am Besten schriftlich. Bei Mitarbeitern kann man aber auch dann von einer Einwilligung ausgehen, wenn ein ökonomischer Vorteil mit der Datenerhebung verbunden ist. Das ist zum Beispiel der Fall, wenn Mitarbeiter in den Pausen private E-Mails austauschen oder privat im Internet surfen dürfen. Die Daten werden in den Systemen aus Sicherheitsgründen protokolliert, da man nicht zwischen privater und geschäftlicher Nutzung unterscheiden kann. Ein Erwägungsgrund zu § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG neu) besagt, dass hierfür keine explizite Einwilligung erforderlich ist, weil der Mitarbeiter dadurch Vorteile hat.

Egal, ob eine Einwilligung schriftlich gegeben wurde oder aufgrund eines zu erwartenden Vorteils angenommen werden kann, muss der Betroffene darüber informiert werden, was mit seinen Daten gemacht wird (vgl. „Informationspflichten“). Ganz wichtig ist auch, dass der Betroffene darüber informiert wird, dass er im Falle einer Einwilligung jederzeit das Recht hat, diese zu widerrufen (Artikel 7 EU-DSGVO).

Benötige ich einen Datenschutzbeauftragten?

Wie auch bei dem Mitarbeiterdatenschutz ist dieser Punkt für Deutschland im BDSG neu geregelt. Die EU-DSGVO hat für bestimmte Themen sogenannte Öffnungsklauseln vorgesehen, die in den nationalen Gesetzen geregelt werden dürfen. Für Unternehmen in Deutschland bedeutet das, sie benötigen immer dann einen Datenschutzbeauftragten, wenn mindestens 20 Personen Zugriff auf personenbezogene Daten haben, die im Unternehmen verarbeitet werden (§ 38 Abs. 1 BDSG neu). Üblicherweise haben mindestens folgende Abteilungen/ Aufgabenbereiche Zugriff auf personenbezogene Daten: Personalwesen, IT, Vertrieb, Marketing, Management. Sehr häufig zählen auch Auszubildende zu diesem Personenkreis, da sie in verschiedenen Aufgabenbereichen arbeiten.

Grundsätzlich ist die Geschäftsführung für die Einhaltung der gesetzlichen Vorschriften zum Datenschutz verantwortlich. Das gilt auch dann, wenn ein Datenschutzbeauftragter bestellt werden muss.

Was muss alles dokumentiert werden?

Die EU-DSGVO stellt sehr hohe Anforderungen an die Dokumentation. Sie müssen dokumentieren, welche Daten Sie zu welchem Zweck verarbeiten, wann und von wem Sie eine Einwilligung eingeholt haben und wie Sie die Betroffenen informiert haben.

Zentrales Element der Dokumentation sind Ihre Prozesse, in denen personenbezogene Daten verarbeitet werden. Dabei sollte man nicht zu detailliert werden. Typischerweise gibt es im Mittelstand 10 bis 20 Prozesse, in denen personenbezogene Daten verarbeitet werden (z.B. Gehaltsabrechnung, Bewerbungsverfahren, Monitoring der IT, Gewinnspielaktionen, Kfz-Reparatur, ...).

Pro Prozess ist genau zu dokumentieren, wer welche Daten zu welchem Zweck erhält. Insbesondere Empfänger, die nicht zum Unternehmen gehören (z.B. Lieferanten, IT-Dienstleister, ...), sind hier aufzuführen. Auch die IT-Systeme, in denen die Daten verarbeitet werden, sind zu dokumentieren. Und die Maßnahmen, die zum Schutz der Daten (Papierdokumente oder Daten in IT-Systemen) durchgeführt wurden. Die EU-DSGVO spricht hier vom sogenannten „Verzeichnis von Verarbeitungstätigkeiten“ (Artikel 30 EU-DSGVO).

Neu in der EU-DSGVO ist, dass Prozesse mit hohen Risiken bezüglich personenbezogener Daten einer sogenannten Datenschutz-Folgenabschätzung unterzogen werden müssen. Das sind Prozesse, in denen besonders sensible Daten (z.B. Gesundheitsdaten, Vorstrafen, ...) verarbeitet werden. Auch alle Prozesse, in denen neue Technologien verwendet werden, zählen dazu, zum Beispiel Internet-Technologien, die in Gebrauchsgegenständen wie KfZ, Kühlschränken usw. eingesetzt werden. Hier sind die Risiken in Bezug auf mögliche Datenschutzverletzungen zu prüfen. Falls keine ausreichenden Maßnahmen zur Eindämmung der Risiken durchgeführt werden, müssen diese Verarbeitungstätigkeiten der Aufsichtsbehörde gemeldet werden, die die Tätigkeiten im schlimmsten Fall untersagen darf.

Wie gehe ich mit den Datenschutz-Verträgen um, die mir Partner zusenden?

Um es gleich vorwegzunehmen, es handelt sich nicht um Verträge, sondern um Vereinbarungen zum Datenschutz, die als Anlagen zu bestehenden Dienstleistungsverträgen geführt werden. Sie müssen sich also nur dann damit beschäftigen, wenn Sie tatsächlich eine Vertragsbeziehung zu diesem Partner haben.

Wenn ein Partner Zugriff auf Ihre personenbezogenen Daten hat oder Sie Zugriff auf personenbezogene Daten des Partners haben, dann ist man nach EU-DSGVO dazu verpflichtet, mit dem Partner eine sogenannte Vereinbarung zur Auftragsverarbeitung abzuschließen (Artikel 28 EU-DSGVO). Wenn diese nicht abgeschlossen wird und es zu einer Datenschutzverletzung kommt, **haften beide Parteien**.
Große und etablierte Partner haben solche Vereinbarungen gemeinsam mit Juristen erstellen lassen. Diese sind in der Regel ausreichend für die Belange des Artikel 28 EU-DSGVO. Auch werden Vorlagen renommierter Datenschutz-Institutionen (z.B. bitkom, Gesellschaft für Datenschutz und Datensicherheit, ...) im Internet angeboten, die ebenfalls genutzt werden können.

Grundsätzlich muss in den Vorlagen beschrieben werden, welcher Art die Partnerschaft ist und was der Partner mit den Daten des Auftraggebers machen darf. Der Auftraggeber wird nach EU-DSGVO als „verantwortliche Stelle“ bezeichnet, der Auftragnehmer ist der „Auftragsverarbeiter“. Der Auftraggeber hat unter anderem das Recht, den „Auftragnehmer zu überprüfen und der Auftragnehmer muss den Auftraggeber unterstützen, wenn z.B. Betroffene Auskunft haben möchten, in welchen Systemen ihre Daten verarbeitet werden.

Wen die juristische Prüfung eines Vertrags für Sie zu umfangreich und kostenintensiv ist, prüfen Sie zumindest die Frage nach der Haftung. Gerne wird in solchen Vereinbarungen zum Datenschutz auf die Haftungsregelungen der EU-DSGVO hingewiesen. Sie sollten hier einen Verweis auf Ihre eigenen Haftungsregelungen einbringen, so, wie sie auch in den Allgemeinen Geschäftsbedingungen beschrieben sind.

Welche Strafen können auf mich zukommen?

Die hohen Strafen der EU-DSGVO veranlassen viele Unternehmen, sich intensiv mit der EU-DSGVO auseinanderzusetzen. Immerhin maximal 20 Millionen Euro oder bis zu 4 % des Konzern-Jahresumsatzes! Das treibt echte Stilblüten: Manch ein Unternehmen stellt seine kompletten Marketing-Vorhaben ein, andere Unternehmen trauen sich nicht einmal mehr, Preislisten an die Kunden rauszuschicken. Das sind ja Kundenadressen, und die Preisübersicht könnte ja als „Werbung“ durchgehen.

Was im Endeffekt tatsächlich von den angedrohten Strafen bei den Unternehmen ankommt, wird sich erst noch zeigen. Aber vorweg einige Überlegungen dazu:

- Die EU-DSGVO soll insbesondere die großen Internet-Betreiber (Google, Amazon, Facebook, ...) und diejenigen Unternehmen, die systematisch Daten sammeln und aus verschiedenen Quellen zusammenführen, für Datenschutz sensibilisieren.
- Einzelne Europäische Länder haben bereits angekündigt, dass sie sich zunächst mit Kontrollen stark zurückhalten werden. Dazu zählen unter anderem Deutschland und Österreich.
- Auch die EU-DSGVO spricht, wie das alte Bundesdatenschutzgesetz, von einer „Verhältnismäßigkeit“ der Maßnahmen. Es liegt nicht in der Absicht der Datenschützer, Ihren Geschäftsbetrieb nachhaltig zu stören.
- Die hohen Strafen drohen vor allem für absichtliche und vorsätzliche Verstöße und in Fällen, in denen Rechte einzelner Personen nachhaltig verletzt wurden.

Es gilt also, zu prüfen, wie stark Sie mit Ihrem Geschäftsmodell Rechte einzelner Betroffener verletzen können. Achten Sie den Wunsch Ihrer Kunden und Mitarbeiter, wenn Sie der Verwendung von Daten, die nichts mit einem Vertrag zu tun haben, widersprechen oder eine Einwilligung widerrufen. Informieren Sie über die Verwendung und Speicherung Ihrer Daten überall dort, wo es mit vertretbarem Aufwand möglich ist (z.B. in Verkaufsräumen, im Internet und über Newsletter). Wenn Sie dann noch einzelne Prozesse dokumentieren, haben Sie schon viel für Ihre Datenschutz-Organisation getan.