FIT für die DSGVO.

Ein Überblick für kleine und mittelständische Unternehmen, Vereine, Ärzte und Apotheker.

Anders als Sie es vielleicht vermuten werden, zählen auch kleine Unternehmen, Vereine, Ärzte und Apotheker zu datenverarbeitenden Unternehmen, denn sie verarbeiten in der Regel personenbezogene Daten. Damit unterliegen diese Unternehmen den Vorgaben des BDSG und der DSGVO. Damit tragen Sie als Geschäftsführer eine große persönliche Verantwortung für die Rechte der Betroffenen. Bei Verstößen gegen die DSGVO können die Betroffenen Schadensersatzansprüche geltend machen und die Aufsichtsbehörden können hohe Bußgelder verhängen. Das kann schnell existenzbedrohende Ausmaße erreichen. Bei Verstößen oder Datenpannen drohen auch Reputationsschäden, weil Kunden wegbleiben oder Mitarbeiter kündigen.

DSGVO kompakt. Diese Grundsätze müssen Sie kennen.

Seit 25 Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft. In der DSGVO werden in Deutschland im Grunde die Vorschriften des seit 1990 bestehenden Bundesdatenschutzgesetzes (BDSG) präzisiert. Viele Vorschriften der DSGVO sind also nicht neu. Neu ist jedoch, dass sich in den letzten Jahren auch in Deutschland der Umgang mit personenbezogenen Daten stark verändert hat. Mit der Digitalisierung ist die Masse an personenbezogenen Daten, die Unternehmen erfassen, stark gestiegen. Mit der DSGVO rücken die Prozesse, in denen diese Daten verarbeitet werden in den Vordergrund. Das Erfassen, Ablegen, Speichern und nicht zuletzt Löschen der personenbezogenen Daten ist zu dokumentieren. Ebenso sind die Personen, deren personenbezogenen Daten verarbeitet werden über diese Datenverarbeitung aufzuklären. Je nach Art und Umfang der Datenverarbeitung müssen diese Betroffenen in die Datenverarbeitung sogar einwilligen.

Aber nicht nur die Zulässigkeit einer Datenverarbeitung ist ein Eckpfeiler der DSGVO, sondern auch die Sicherheit der Daten.

Zulässigkeit Datenerhebung (Art. 6 DSGVO)

Die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn eine gesetzliche Vorschrift sie erlaubt oder der Betroffene in dies Datenverarbeitung eingewilligt hat. Verbot mit Erlaubnisvorbehalt.

Demnach ist nach DSGVO eine Datenverarbeitung erlaubt, wenn:

- die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist (Adresse des Kunden, Bankverbindung usw.)
- die Verarbeitung zur Erfüllung vorvertraglicher Maßnahmen erforderlich ist (z.B. Kontaktdaten wie E-Mailadresse zur Übermittlung eines Kostenvoranschlages usw.)
- die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen erforderlich ist und die Interessen des Betroffenen dieser Datenverarbeitung nicht entgegenstehen (Werbung, Kommunikation mit Kunden usw.). Interessenabwägung!

In allen anderen Fällen muss der Betroffene in die Datenverarbeitung einwilligen.

Die Anforderungen an die Datensicherheit werden konkret in Art. 32 DSGVO umfassend behandelt.

Als Geschäftsführer sind Sie dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten vor Missbrauch und Verlust geschützt sind. Angesichts täglicher Nachrichten über Hackerangriffe auf Unternehmen und Datenpannen durch unachtsame Mitarbeiter, stehen Unternehmen vor großen Herausforderungen bei der Umsetzung der geforderten technischen und organisatorischen Sicherheitsmaßnahmen.

Personenbezogene Daten

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben. Wobei ein beziehbares Datum z.B. eine Personalnummer, eine IP-Adresse oder eine E-Mailadresse sein kann.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert.

Rechte der Betroffenen. Das müssen Sie wissen.

Die Rechte der Betroffenen zu stärken, ist eine zentrale Motivation der DSGVO. Die Betroffenen sollen stets „Herr ihrer Daten“ sein. Dazu sind sie über den Zweck und den Umfang der Verarbeitung ihrer personenbezogenen Daten zu informieren und haben auch das Recht die Löschung der Daten zu fordern (Recht auf Vergessenwerden). Wenn Sie in Ihrem Unternehmen personenbezogene Daten ausschließlich beim Betroffenen selbst erheben, haben Sie schon eine wesentliche Voraussetzung für die Erfüllung Ihrer Transparenz- und Informationspflichten erfüllt. So weiß der Kunde in der Regel bei der Unterzeichnung eines schriftlichen Vertrages, welche Daten er eingetragen hat und für welchen Zweck diese bestimmt sind. Anders sieht es aus, wenn Sie z.B. eine Webseite im Internet betreiben, auf der Sie das Nutzungsverhalten der Besucher analysieren. In diesem Fall müssen Sie die Besucher der Seite über diese Datenverarbeitung informieren.

Der Betroffene hat das Recht auf:

- Transparenz und Modalität (Information in verständlicher Art und Weise)
- Information und Auskunft über Art und Umfang der Datenverarbeitung
- Berichtigung und Löschung der Daten
- Widerspruch gegen die Datenverarbeitung
- Beschwerderecht bei der Aufsichtsbehörde
- Recht auf Datenübertragbarkeit

Aus diesen Rechten leiten sich umfangreiche Dokumentationspflichten ab, die Sie in Ihrem Unternehmen erfüllen müssen. Wobei die Dokumentation hierbei kein Selbstzweck ist, sondern die Voraussetzung dafür, dass Sie den Betroffenen überhaupt Auskunft geben können und im Falle eines Berichtigungs- oder Löschanfrage die entsprechenden Daten tatsächlich berichtigen oder löschen können. Hierbei ist zu beachten, dass die Betroffenen diese Rechte einklagen können. So verstoßen Sie schon gegen die DSGVO, wenn Sie einem Auskunftsersuchen eines Betroffenen nicht binnen eines Monats nachkommen.

Sie müssen davon ausgehen, dass Ihre Kunden, Interessenten, Lieferanten und Beschäftigten in hohem Maße für den Datenschutz sensibilisiert sind. Die Datenschutzaufsichtsbehörden werden derzeit regelrecht überflutet mit Beschwerden und können diese kaum noch bearbeiten. Als Geschäftsführer müssen Sie demnach darauf vorbereitet sein, dass Betroffene auch bei Ihnen ihre Rechte einfordern. Dem können Sie nur gerecht werden, wenn Sie Ihre Datenverarbeitung ausreichend dokumentiert haben und Prozesse im Unternehmen etabliert haben, die z.B. ein Auskunftsersuchen oder

einen Löschantrag sachgerecht und zeitnah bearbeiten können.

Sie müssen aber auch im Falle einer Beschwerde gegenüber der Aufsichtsbehörde nachweisen können, dass Sie den Kunden informiert haben oder dass der Kunde in die entsprechende Datenverarbeitung eingewilligt hat. Dafür benötigen Sie entsprechende Formulare und Dokumentationen. Datenschutz ist demnach kein einmaliges Unterfangen, sondern ein Prozess.

DSGVO Diese Fragen stellen Ihnen die Datenschutzaufsichtsbehörden.

Mitte 2018 hat die Datenschutzaufsichtsbehörde von Niedersachsen den nachfolgen Fragenkatalog an Unternehmen verschickt. Für Sie als Geschäftsführer sollte das Motivation sein, sich auf solche Prüfungen vorzubereiten und aktiv zu werden.

1. Vorbereitung auf die DS-GVO

Wie haben Sie sich als Unternehmen auf die DS-GVO vorbereitet?

Schildern Sie (kurz) die Vorgehensweise, welche Bereiche involviert waren und welche Maßnahmen initiiert wurden. Sofern noch nicht alle Maßnahmen vollständig umgesetzt wurden, erläutern Sie bitte auch den Umsetzungsstatus.

2. Verzeichnis von Verarbeitungstätigkeiten

Wie haben Sie sichergestellt, dass alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen wurden? Wie stellen Sie dessen Aktualität sicher? Legen Sie bitte eine Übersicht Ihrer dokumentierten Verfahren sowie ein Beispielverfahren als Muster bei.

3. Zulässigkeit der Verarbeitung

Auf Basis welcher Rechtsgrundlagen verarbeiten Sie personenbezogene Daten? Sofern Sie auch auf Basis von Einwilligungen personenbezogene Daten verarbeiten, legen Sie bitte Ihre verwendeten Muster bei.

4. Betroffenenrechte

Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher? Skizzieren Sie Ihre diesbezüglichen Prozesse und gehen Sie insbesondere detailliert darauf ein, wie Sie Ihren Informationspflichten nachkommen. Vorhandene Musterinformationen fügen Sie bitte bei.

5. Technischer Datenschutz

a. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?

b. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen an den jeweiligen Stand der Technik angepasst werden?

c. Wie stellen Sie sicher, dass Sie für die von Ihnen aktuell oder zukünftig eingesetzten IT-Anwendungen ein dokumentiertes datenschutzkonformes Rollen und Berechtigungskonzept haben?

d. Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mitberücksichtigt werden (Privacy by Design und by Default)?

6. Auftragsverarbeitung

Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DS-GVO angepasst? Sofern Sie Musterverträge verwenden, fügen Sie diese bitte bei.

7. Datenschutzbeauftragter

Wie ist Ihr Datenschutzbeauftragter in Ihre Organisation eingebunden? Welche Fachkundenachweise hat er?

8. Meldepflichten

Wie stellen Sie sicher, dass Ihr Unternehmen Datenschutzverstöße fristgemäß an die Aufsichtsbehörde meldet? Skizzieren Sie Ihre diesbezüglichen Prozesse.

9. Dokumentation

Wie können Sie die Einhaltung aller vorstehend genannten Pflichten nachweisen?

Mit den nachfolgenden Fünf Schritten können Sie solche Anfragen der Aufsichtsbehörden beantworten und sicher sein, dass Ihr Unternehmen damit FIT für die DSGVO ist.

Datenschutz in der Praxis. In 6 Schritten DSGVO konform.

Als Geschäftsführer sind Sie gefordert die gesetzlichen Anforderungen der DSGVO in der betrieblichen Praxis vollumfänglich umzusetzen. Hierzu müssen Sie im Wesentlichen die nachfolgenden 6 Schritte ausführen.

Schritt 1: Datenschutzbeauftragter

Die DSGVO schreibt vor, dass jedes Unternehmen bei dem mindestens 20 Personen im regelmäßigen Umgang mit personenbezogenen Daten stehen und diese verarbeiten, einen Datenschutzbeauftragten stellen müssen. Fällt Ihr Unternehmen unter diese Regelung, müssen Sie als Geschäftsführer entweder einen Mitarbeiter zum Datenschutzbeauftragten ausbilden oder einen externen Datenschutzbeauftragten mit der Aufgabe betrauen. Hierbei müssen Sie beachten, dass der Datenschutzbeauftragte eine entsprechende Fachkunde und Zuverlässigkeit nachweisen muss. Dazu sind entweder Ausbildungsnachweise oder anerkannte Zertifikate erforderlich. Zudem sollte sich der Datenschutzbeauftragte mit IT-Systemen und IT-Sicherheit auskennen. Der Datenschutzbeauftragte muss weisungsfrei agieren können und direkt an die Geschäftsleitung berichten. Als Geschäftsführer können Sie kein Datenschutzbeauftragter in Ihrem eigenen Unternehmen sein.

Mein Tipp

Gerade bei kleineren Unternehmen ist die Umsetzung der datenschutzrechtlichen Anforderungen nicht mit dauerhaft hohen Arbeitsaufwänden verbunden. Hier ist es oftmals sinnvoll einen externen Datenschutzbeauftragten zu bestellen und diesen in die relevanten Geschäftsprozess einzubinden. Das erspart Ausbildungs- und Fortbildungskosten.

Schritt 2. Verzeichnis der Verarbeitungstätigkeiten

Haben Sie geklärt, ob Sie einen Datenschutzbeauftragten benötigen, muss eine Bestandsaufnahme Ihrer Geschäftsprozesse erfolgen und festgestellt werden in welchen Prozessen personenbezogene Daten verarbeitet werden und zu welchen Datenkategorien dies Daten gehören. Regelmäßig werden personenbezogene Daten bei Lohnabrechnungen, in der Personalverwaltung, der Firmenwebseite, der Kundenverwaltung und der Buchhaltung verarbeitet. Die entsprechenden Datenkategorien sind Kundenstammdaten, Personaldaten, Rechnungsdaten usw.

Datensparsamkeit, Anonymisierung, Pseudonymisierung

Prüfen Sie bei Ihrer Bestandsaufnahme ob Sie diese Daten tatsächlich alle benötigen. (Datensparsamkeit). Ist die Löschung von Daten nicht möglich kann eine Anonymisierung (Löschung des Personenbezuges wie z.B. Name des Kunden) oder Pseudonymisierung (Ersetzen des Namens durch eine Nummer) die Risiken wesentlich reduzieren. Beachten Sie aber, dass bei einer Anonymisierung die Wiederherstellung des Personenbezuges ausgeschlossen sein muss und bei der Pseudonymisierung sichergestellt werden muss, dass z.B. die Datei mit den Nummern vor unerlaubten Zugriffen geschützt ist.

Verzeichnis der Verarbeitungstätigkeiten. Beispiel.

Die DSGVO fordert für solche Verarbeitungstätigkeiten ein sog. Verzeichnis der Verarbeitungstätigkeiten. Dieses Verzeichnis kann typischerweise wie folgt aufgebaut sein:

Verarbeitungstätigkeit	Buchhaltung	Personalverwaltung
Zwecke der Datenverarbeitung	Erfassung aller ein- und ausgehenden Zahlungen des Unternehmens. (siehe § 238 Abs. 1 HGB)	Führung von Personalakten und Lohnbuchhaltung.
Kategorien betroffener Personen	Kunden, Lieferanten, Dienstleister.	Beschäftigte
Kategorien personenbezogener Daten	Kundenstammdaten und Rechnungsdaten von Debitoren und Kreditoren.	Personaldaten
Besondere Arten personenbezogener Daten (Ja/Nein)	Nein	Ja (Krankmeldungen usw.)
Kategorien von internen und externen Empfängern *(einschließlich Drittland oder internationale Organisation)*	Beschäftigte, Kunden, Finanzbehörden und ggf. weitere Behörden.	Beschäftigte, Steuerberater, Finanzbehörden, Krankenkassen, Sozialversicherungsträger
Übermittlung in ein Drittland, Name des Drittlandes. Übermittlung an eine internationalen Organisation, Name der internationalen Organisation.	nicht vorgesehen	nicht vorgesehen
Dokumentierung geeigneter Garantien im Drittland, bzw. bei der internationalen Organisation.	nicht relevant	nicht relevant
Fristen für die Löschung der Daten	10 Jahre	10 Jahre, Akten unbefristet
allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Siehe gesonderte Beschreibung der technisch-organisatorischen Maßnahmen.	Siehe gesonderte Beschreibung der technisch-organisatorischen Maßnahmen.
ggf. Erlaubnisnorm	entfällt	Art. 6 Abs. 1 b) DSGVO i.V.m. § 26 Abs. 1 BDSG Art. 6 Abs. 1 c) DSGVO i.V.m. § 26 BDSG Art. 9 Abs. 2 h) i.V.m. § 22 Abs. 1 b) BDSG

Alle Verfahren, bei denen personenbezogene Daten verarbeitet werden, sind in ein solches Verzeichnis aufzunehmen.

Wichtig

Werden Daten an Dritte übermittelt, muss dies dokumentiert werden. Dritte können z.B. Dienstleister, Steuerberater aber auch Behörden wie z.B. Finanzämter sein. Bei einer Datenübermittlung in Drittländer wie z.B. Nutzung von Cloudspeichern wie DropBox in den USA ,müssen besondere Anforderungen erfüllt werden.

Bei der Erstellung des Verzeichnisses sollten Sie unbedingt Ihre IT-Systeme umfassend dokumentieren. Nur so können Sie im Nachgang prüfen ob die Anforderungen an die Sicherheit der Daten erfüllt werden. Wenn Sie einen Dienstleister mit der Betreuung Ihrer IT-Systeme beauftragt haben, müssen Sie diesen in die Dokumentation einbinden. Sie sollten an dieser Stelle auch eine Übersicht der Dienstleister erstellen, die Sie selbst mit der Verarbeitung personenbezogener Daten beauftragt haben oder die im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten haben. Das können z.B. IT-Dienstleister, Servicekräfte, Putzdienste oder Papierentsorger sein.

Schritt 3. Formulare und Datenschutzprozesse, Betroffenenrechte

Sie haben Ihre Prozesse erhoben, Ihre IT-Systeme dokumentiert und das Verzeichnis der Verarbeitungstätigkeiten erstellt. Ferner haben Sie dokumentiert, welche Dienstleister Sie einsetzen. Nun gilt es die Formulare zu erstellen, die Sie für die Erfüllung Ihrer datenschutzrechtlichen Pflichten benötigen. Im gleichen Schritt sind Prozesse zu etablieren, die sicherstellen, dass die datenschutzrechtlichen Anforderungen in Ihrem Unternehmen auch umgesetzt werden.

Informationspflichten

Erheben Sie personenbezogene Daten, müssen Sie den Betroffenen in verständlicher Form informieren in welcher Weise und zu welchem Zweck seine personenbezogenen Daten verarbeitet werden. Bei einer Direkterhebung kann dies durch ein Informationsblatt erfolgen, das dem Kunden bei einer Vertragsunterzeichnung oder einer Angebotserstellung ausgehändigt wird. Dieses Formular muss mindestens Informationen zu den nachfolgenden Punkten beinhalten:

- Verarbeitungsrahmen
- Rechtsgrundlage der Datenverarbeitung
- Aufbewahrungsdauer
- Löschung
- Kategorien personenbezogener Daten
- Weitergabe und Auslandsbezug
- Betroffenenrechte
- Beschwerderecht

Beachten Sie auch, dass Sie nicht nur die Daten von Kunden sondern auch die Daten der Beschäftigten und ggf. weiterer Personen wie z.B. Dienstleister Putzhilfen usw. verarbeiten. Auch diese Personen müssen Sie informieren.

Betreiben Sie eine Firmenwebseite oder haben Sie einen geschäftlichen Auftritt bei Facebook oder anderen sozialen Netzwerken, sind besondere Informationspflichten zu erfüllen. Näheres hierzu finden Sie auf den folgenden Seiten.

Auskunftsrecht

Jeder Betroffene hat das Recht Auskunft über die bei Ihnen verarbeiteten personenbezogenen Daten zu erhalten. Diesem Auskunftsersuchen müssen Sie innerhalb eines angemessenen Zeitraumes – in der Regel ein Monat – nachkommen. Hierzu sollten Sie wissen wo diese Daten verarbeitet werden (Verfahrensverzeichnis) und Ihre Mitarbeiter müssen wissen, wie Sie einem solchen Auskunftsersuchen nachkommen. Hierzu benötigen Sie ein Formular zur Beantwortung des Auskunftsersuchens und Ihre Mitarbeiter müssen sensibilisiert werden. Denn Sie wissen nicht immer an welcher Stelle das Auskunftsersuchen ankommt. Das kann ein Anruf, eine E-Mail oder auch ein persönlich vorgetragenes Anliegen sein.

Sie müssen demnach sicherstellen, dass alle Mitarbeiter ein solches Ersuchen annehmen

und an die entsprechende Stelle weiterleiten. Der Prozess sollte wie folgt aussehen:

- Annahme des Auskunftsersuchens
- Zweifelsfreie Feststellung der Identität des Betroffenen
- Weiterleitung der Anfrage an verantwortliche Stelle (z.B. Datenschutzbeauftragter)
- Ermittlung der Daten
- Bereitstellung der Informationen mittels Formular
- Dokumentation des Vorgangs

Vorsicht

Sensibilisieren Sie die Mitarbeiter dahingehend, dass keine Auskünfte zu personenbezogenen Daten am Telefon oder per E-Mail gegeben werden, wenn die Identität des Betroffenen nicht zweifelsfrei geklärt wurde. Hier empfiehlt sich grundsätzlich eine postalische Zustellung des Auskunftsersuchens zu verlangen. Bei E-Mail können Sie nämlich nicht sicher sein, dass der Absender nicht gefälscht wurde. Zudem müssen Sie E-Mails verschlüsseln, wenn Sie personenbezogene Daten übermitteln.

Den gleichen Prozess können Sie im Grunde auch für die Bearbeitung eines Antrages auf Berichtigung oder Löschung der Daten nutzen. Wichtig ist, dass Sie eine zentrale Stelle im Unternehmen etablieren, die solche Ersuchen der Betroffenen sachgerecht und zeitnah bearbeiten. Schließlich drohen hier hohe Bußgelder.

Vorsicht.

Sie müssen die gesetzl. Aufbewahrungsfristen beachten. Bei Geschäftsdaten sind das in der Regel 10 Jahre. Sie müssen für alle personenbezogenen Daten ermitteln, wie lange diese aufbewahrt werden dürfen und dann auch dafür sorgen, dass die Daten nach diesen Fristen gelöscht werden. Dem Betroffenen müssen Sie dies entsprechend mitteilen.

Verpflichtung der Beschäftigten

Alle Beschäftigte, die Zugang zu personenbezogenen Daten haben, müssen darauf verpflichtet werden diese nach den geltenden Datenschutzvorschriften zu verarbeiten. Diese Verpflichtung muss schriftlich erfolgen. Verwahren Sie diese Verpflichtungen am besten in der Personalakte. Musterformulare können Sie bei Ihren Aufsichtsbehörden erhalten.

Mein Tipp

Denken Sie daran, dass nicht nur Ihre Mitarbeiter Zugang zu personenbezogenen Daten haben. Auch Putzkräfte von Dienstleistern oder Berater, die nur zeitweise in den Räumen anwesend sind, können Zugang zu personenbezogenen Daten bekommen. Sie sollten sich von solchen Personen eine „Verschwiegenheitserklärung“ unterzeichnen lassen.

Datenpanne

Auch wenn Sie alle Maßnahmen zur Sicherheit der Verarbeitung umgesetzt haben, sind Datenpannen nicht auszuschließen. Sie müssen darauf vorbereitet sein. Laut DSGVO müssen Sie eine Datenpanne der Aufsichtsbehörde innerhalb von 72 Stunden melden, wenn zu befürchten ist, dass die Rechte der Betroffenen in erheblichen Maßen verletzt werden. Damit Sie fristgerecht reagieren können, sollten Sie ein Meldeformular und einen Meldeprozess im Unternehmen haben.

Einwilligung

In der Regel werden Sie personenbezogene Daten im Rahmen der Erfüllung eines vertraglichen Zweckes verarbeiten. Dies bezieht sich sowohl auf Ihre Kunden als auch auf Ihre Beschäftigten. Für diese Verarbeitungszwecke benötigen Sie keine Einwilligungen der Betroffenen. Aber rund um Kunden und Beschäftigte gibt es Datenverarbeitungen, die nicht unmittelbar zur Erfüllung des Geschäftszweckes erforderlich sind. Hierzu gehören Werbung, Veröffentlichung von Fotos aber auch die Kommunikation über Telefon oder E-Mail.

Hier greifen neben dem Datenschutzrecht weitere Gesetze wie z.B. das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG), das Gesetz gegen unlauteren Wettbewerb (UHG) oder das Kunst- und Urhebergesetz (KUG). Für Sie als Geschäftsführer ist es nicht erforderlich, eine Abgrenzung dieser Gesetze zu finden. Sie müssen aber zumindest die nachfolgenden grundsätzlichen Anforderungen beachten:

Verfahren	Einwilligung erforderlich Ja/Nein (Beschreibung)
Veröffentlichung von personenbeziehbaren Daten des Kunden auf Firmenwebseite/Facebook oder Medien (Fotos des Hauses mit Ortsangaben, Einzelpersonen, KFZ mit Kennzeichen usw.)	Ja (schriftlich)
Veröffentlichung von Fotos des Kunden oder Mitarbeiters auf Firmenwebseite/Facebook oder Medien bei Veranstaltungen (Tag der offenen Tür, Betriebsfeier usw.)	Nein (konkludent. Es genügt eine allgemeine Information, dass fotografiert wird und Veröffentlichungen stattfinden. Eventuell auf der Einladung oder bei einer Begrüßungsansprache.)
Veröffentlichung von Mitarbeiterfotos auf der Firmenwebseite oder Facebook	Ja (schriftlich)
Kommunikation mit Kunden oder werbliche Ansprache per Fax, E-Mail, WhatsApp, Telefon	Ja (schriftlich)
Übermittlung von personenbezogenen Daten in Drittländer (Nutzung von Cloudspeichern wie DropBox, OneDrive usw.)	Ja (schriftlich)
Verarbeitung personenbezogener Daten (Cookies usw.) auf der Firmenwebseite	Ja (Opt In / Anklicken einer Information)
Versand von Newslettern	Ja (Double Opt In /Anklicken einer Information plus Bestätigung per E-Mail)
Nutzung von Kontaktdaten bei Gewinnspielen zur Kontaktaufnahme oder Werbung	Ja (schriftlich)
Übermittlung eines Angebotes per E-Mail	Ja (schriftlich bei Erhebung der Kommunikationsdaten. Wenn Kontakt nur telefonisch, ist keine Einwilligung erforderlich.)

Diese Liste ist nicht abschließend, sondern bezieht sich auf typische Verfahren im Unternehmensumfeld. Im Zweifel müssen Sie die oben genannten Gesetze prüfen und feststellen, ob Sie die Daten ohne Einwilligung des Betroffenen für die jeweiligen Zwecke verarbeiten dürfen.

Vorsicht!

Hier lauern erhebliche Risiken. Viele Betroffenen reagieren sehr sensibel darauf, wenn ihre Daten veröffentlicht oder zu Werbezwecken missbraucht werden. Sie können sich viel Ärger ersparen, wenn Sie sich bei einem Vertragsabschluss grundsätzlich Einwilligungen von Ihren Kunden oder Beschäftigten zu den oben genannten Verfahren einholen. Dann sind Sie auf der sicheren Seite.

Schritt 4. Firmenwebseite, Facebook & Co

Eine Firmenwebseite im Internet und bei Facebook gehört zu einem modernen Unternehmen dazu. Solche Auftritte unterliegen strengen datenschutzrechtlichen Anforderungen aber auch weiteren einschlägigen Gesetzen (TKG, TMG, UHG, KUG usw.). Hier drohen Abmahnungen und Bußgelder in erheblicher Höhe. Das Geschäftsmodell etlicher Kanzleien basiert alleine darauf Abmahnungen zu versenden.

Regelmäßig benötigen Sie sowohl für Ihre Firmenwebseite als auch bei Facebook eine Datenschutzerklärung und ein Impressum. Die Datenschutzerklärung muss die Besucher Ihrer Seite über die Verarbeitung ihrer personenbezogenen Daten informieren und leicht erreichbar sein. Eine Datenschutzerklärung muss zumindest folgende Fragen beantworten:

- Wer ist verantwortlich für die Datenerfassung auf dieser Website?
- Wer ist der Datenschutzbeauftragte?
- Wie werden die Daten erfasst?
- Wofür werden die Daten genutzt?
- Welche Recht hat der Betroffene bezüglich seiner Daten?
- Welche Analyse Tools und sonstige Tools von Drittanbietern werden eingesetzt?
- Wo kann sich der Betroffene beschweren

Vorsicht

Zurzeit testen Abmahnanwälte inwieweit Unternehmen mit unvollständigen oder nicht vorhandenen Datenschutzerklärungen abgemahnt werden können. Die erste Abmahnung in Höhe von mehreren Tausend Euro wurde im September 2018 von einem Landgericht bestätigt. Es ist zu befürchten, dass dies erst der Anfang einer Abmahnwelle ist.

Solche Abmahnungen und Bußgelder können Sie vermeiden, wenn Sie nachfolgende Regeln befolgen:

Verfahren	Regel	Umgesetzt Ja/Nein
Firmenwebseite	Impressum und Datenschutzerklärung vorhanden und aktuell. Datenschutzerklärung enthält Informationen zu allen Tools wie z.B. Google Analytics, Facebook Like Button, Google AD Words, Google Fonts, Google Maps usw.	
Firmenwebseite	Cookie Hinweis mit Link auf Datenschutzerklärung und OK Button.	
Facebook Firmenseite	Impressum vorhanden und Link auf Datenschutzerklärung der Firmenwebseite vorhanden.	
Firmenwebseite Dienstleister	Mit allen Dienstleistern rund um die Firmenwebseite (Hoster, Grafikbüro usw.) wurden Verträge zur Auftragsverarbeitung geschlossen. Ebenso mit Google (Google Analytics), Dienstleister für Newsletter usw.	
Newsletter	Es besteht ein Double Opt In Verfahren bei der Anmeldung. Der Besucher wird auf die Datenschutzerklärung hingewiesen. Optimal Bestätigung (Opt In) der Kenntnisnahme.	
Kontaktformular	Die Webseite ist mittels SSL/TLS verschlüsselt (https). Es werden ausschließlich Kontaktdaten (E-Mailadresse) erhoben. Der Besucher wird auf die Datenschutzerklärung hingewiesen. Optimal Bestätigung (Opt In) der Kenntnisnahme.	
Firmenwebseite	Datensparsamkeit. Es werden nur Daten erhoben, die zur Erfüllung des jeweiligen Zweckes erforderlich sind. Z.B. kein Geburtsdatum beim Kontaktformular usw.	
WhatsApp	Einwilligung aller Personen in Ihrem Adressbuch in die Nutzung liegt vor (Da WhatsApp diese Daten bei der Nutzung nach USA übermittelt ist eine Einwilligung erforderlich).	
Fotos, Bilder	Einwilligung der Betroffenen in die Nutzung liegt vor. Sie haben die Rechte an allen Bildern (KUG). Keine Kopien von Bildern aus dem Internet.	

Schritt 5. Auftragsverarbeitung

Als Geschäftsführer sind Sie auch dafür verantwortlich, dass personenbezogene Daten bei Ihren Dienstleistern oder Auftragsverarbeitern ordnungsgemäß verarbeitet und vor Missbrauch geschützt werden. Bei Verstößen oder Datenpannen haften Sie genauso wie der Dienstleister. Sie müssen den Dienstleister gem. DSGVO vertraglich verpflichten die Anforderungen der DSGVO umzusetzen. Hierzu nutzen Sie am besten Standardverträge, wie Sie von den Aufsichtsbehörden bereitgestellt werden. Wichtig ist in diesem Zusammenhang, dass Sie sich vor der Auftragsvergabe versichern, dass der Dienstleister die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen umgesetzt hat. Das können Sie z.B. damit dokumentieren, dass der Dienstleister Ihnen eine entsprechende Checkliste ausfüllt und diese dem Vertrag als Anlage beigefügt wird.

Typische Dienstleister mit denen Sie solche Verträge zur Auftragsdatenverarbeitung (ADV) abschließen müssen sind IT-Dienstleister mit Zugriff auf personenbezogene Daten (Wartung, Backup, Hosting, Installation, Netzwerk usw.) oder Entsorgungsunternehmen. Steuerberater oder Wirtschaftsprüfer sind keine Auftragsverarbeiter. Es sind demnach keine ADV-Verträge abzuschließen.

Schritt 6. Datensicherheit, technischer Datenschutz

Die Sicherstellung aller nach Art. 32 DSGVO bzw. ggf. § 22 BDSG notwendigen techn. und organisatorischen Maßnahmen nach dem aktuellen Stand der Technik ist gerade in der heutigen Zeit von wesentlicher Bedeutung für die Sicherheit der Daten. Hierzu zählen zumindest nachfolgende Maßnahmen:

- Festlegung von Sicherheitsmaßnahmen zur Wahrung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten nach gängigen Standards (BSI Grundschutz, ISO 27001). Hierzu zählen:
  - Einsatz von Firewalls an den Netzwerkgrenzen (Internet, Firmennetze, Dienstleisternetze)
  - Einsatz von Antivirensoftware
  - Einsatz von Spam-und Internet-Filtern
  - regelmäßiges Patchen aller IT-Systeme und Anwendungen
  - Absicherung von mobilen Systemen (Notebooks, Tablets, Smartphones)
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Sicherheitsmaßnahmen.
  - Löschkonzepte.
  - Verschlüsselung und Sicherheitskonzepte.
  - Verpflichtung zur Pseudonymisierung bzw. Anonymisierung.
  - Wiederherstellbarkeit der Daten im Notfall.
  - Regelmäßige Schulung und Sensibilisierung der Beschäftigten.

Wichtig.

In Art. 32 DSGVO werden Sicherheitsmaßnahmen nach dem „aktuellen Stand der Technik“ gefordert. Das bedingt eine regelmäßige Kontrolle der eingesetzten Verfahren dahingehend, ob sie noch dem aktuellen Stand der Technik entsprechen. Ist dies nicht der Fall müssen die Verfahren durch aktuelle ersetzt werden.

Als Geschäftsführer sollten Sie dafür sorgen, dass Sicherheitsmaßnahmen nach den Vorgaben des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) in Ihrem Unternehmen etabliert werden. Das BSI stellt hierfür sehr gute Verfahren und Methoden zur Verfügung. Diese Verfahren sind immer risikoorientiert und unter Kosten/Nutzen Gesichtspunkten umzusetzen und müssen dokumentiert werden.

Verschlüsselung

Eine zentrale Anforderung der DSGVO zur Datensicherheit ist die Verschlüsselung. Das bedeutet, dass bei bestimmten Verfahren eine Verschlüsselung zwingend umzusetzen ist.

So müssen z.B. personenbezogene Daten auf Internetseiten mittels TLS/SSL verschlüsselt werden. Auch E-Mals mit personenbezogenen Daten müssen verschlüsselt werden. Da personenbezogene Daten ihren Personenbezug verlieren, wenn sie verschlüsselt sind, sollten sie aus Haftungsgründen grundsätzlich verschlüsselt gespeichert werden. Denn verschlüsselte Daten können nicht missbraucht werden. Dies selbst dann nicht, wenn sie verlorengehen oder gestohlen werden. Es ist demnach empfehlenswert die Festplatten der PC's, Notebooks und Serversysteme zu verschlüsseln. Hierzu gibt es einfache und kostengünstige Lösungen wie z.B. Veracrypt oder Bitlocker. Denken Sie auch daran, dass mobile Datenträger sehr leicht verlorengehen oder gestohlen werden können. Sorgen Sie dafür, dass solche Datenträger immer verschlüsselt werden.

Smartphones und Tablets

Auf Smartphones werden regelmäßig eine Vielzahl personenbezogener Daten der Nutzer gespeichert. Im geschäftlichen Einsatz werden auch personenbezogene Daten der Kunden oder Beschäftigten auf den Smartphones oder Tablets gespeichert. Seien es E-Mails, Kontaktdaten oder Daten, die über Fernzugriffe in das Unternehmensnetz verarbeitet werden. Die Risiken eines Datenverlustes oder Missbrauchs sind gerade bei Smartphones und Tablets erheblich. Sie sollten als Geschäftsführer die betriebliche Nutzung von Smartphones nur zulassen, wenn sichergestellt ist, dass die Geräte in ein zentrales „mobile Device Management" (MDM) eingebunden sind. Mit solchen Systemen können die Geräte aus der Ferne gesteuert werden und wichtige Sicherheitsrichtlinien können unternehmensweit durchgesetzt werden. Hierbei sind folgende Mindestanforderungen umzusetzen:

- Sicherung der Geräte mit einem mindestens 4-stelligen Passwort
- Verschlüsselung aller Daten
- Verhinderung des Rooten oder Jailbreaks (Deaktivieren zentraler Sicherheitseinstellungen)
- Fernlöschung der Geräte
- Regelmäßige Updates der Systeme und Apps

DSGVO. Das sind die größten Risiken.

Als Geschäftsführer stehen Sie vor der Herausforderung eine Vielzahl von Anforderungen im Unternehmen umsetzen zu lassen. Gerade deshalb ist es wichtig risikoorientiert vorzugehen und nicht mit Kanonen auf Spatzen zu schießen. Die Anforderungen der DSGVO sind immer in Abhängigkeit zu der Sensibilität der Daten und den Risiken für die Betroffenen umzusetzen.

Diebstahl und Missbrauch

Kriminelle nutzen die zu befürchtenden hohen Bußgelder oder Reputationsschäden dazu aus, die betroffenen Unternehmen mit den gestohlenen Daten zu erpressen. Der Erpresser kann auch ein unzufriedener Mitarbeiter sein. Der beste Schutz ist zunächst, nur die Daten zu speichern, die Sie für Ihre Geschäftszwecke benötigen. Alles andere sollten Sie löschen oder anonymisieren. Dann müssen Sie dafür sorgen, dass jeder nur Zugriff auf die Daten erhält, die er zur Erledigung seiner Aufgaben benötigt (Minimalprinzip). Sorgen Sie dafür, dass die wesentlichsten Sicherheitsmaßnahmen umgesetzt und dass sensible Daten stets verschlüsselt werden. Wenn Sie Ihre Mitarbeiter dann noch regelmäßig sensibilisieren und schulen, haben Sie diese Sicherheitsrisiken im Griff.

Beschwerden von Kunden

Kunden beschweren sich in der Regel dann bei Aufsichtsbehörden, wenn sie mit den Leistungen eines Unternehmens unzufrieden sind. Ursache kann sein, dass ihr Anliegen nicht bearbeitet wurde, dass Mitarbeiter unsensibel auf Beschwerden reagiert haben oder berechtigte Auskunftsersuchen aus Unwissenheit ignoriert wurden. Als Geschäftsführer müssen Sie daher wirksame Prozesse etablieren, die sicherstellen, dass die Anliegen Ihrer Kunden sachgerecht bearbeitet werden. Das gilt auch für alle Anliegen rund um den Datenschutz.

Sie müssen den Datenschutz als einer Ihrer zentralen Geschäftszwecke im Unternehmen etablieren und aktiv bei Ihren Kunden mit Ihren Datenschutzmaßnahmen werben. Dann haben Sie auch dieses Risiko im Griff. Vielleicht sogar mehr Kunden.

Abmahnungen

Verstöße gegen datenschutzrechtliche Vorgaben sind nach dem letzten Urteil eines Landesgerichtes abmahnfähig. Gleiches gilt bei Verstößen gegen das UWG. Wenn Sie Firmenwebseiten betreiben oder auf Facebook präsent sind, stehen Sie in der Öffentlichkeit und sind damit auch ein leichtes Opfer für Abmahnanwälte. Das kann leicht sehr teuer werden. Nicht zu vergessen, dass auch die Aufsichtsbehörden Webseiten regelmäßig prüfen und Bußgelder verhängen, wenn diese nicht den datenschutzrechtlichen Vorgaben entsprechen. Sie sollten Ihre Internet- und auch Ihre Facebook Seite von Fachleuten prüfen lassen. Nur so können Sie das Risiko, Opfer von Abmahnungen oder anderer Rechtsstreitigkeiten zu werden vermeiden.

Fazit. Das müssen Sie als Geschäftsführer beachten.

Die DSGVO ist in Kraft und als Geschäftsführer müssen Sie die Anforderungen in Ihrem Unternehmen umsetzen. Weglaufen oder Wegducken ist also keine Handlungsoption. Sie müssen sich den Fragen der Datenschutzaufsichtsbehörden stellen. Schließlich drohen erhebliche Bußgelder, Schadensersatzforderungen oder Kosten durch Abmahnungen. Sie müssen eine Bestandsaufnahme in Ihrem Unternehmen durchführen, Lücken identifizieren und diese mit sachgerechten und risikoorientierten Maßnahmen schließen. Das können Sie insbesondere bei den Prozessen noch mit eigenem Sachverstand erledigen, bei den Formularen sollten Sie jedoch auf rechtlich geprüfte Mustervorlagen zurückgreifen. Bei weiteren Themen wie Internet, Facebook und IT-Sicherheit, sollten Sie sich Unterstützung seitens erfahrener Datenschützer holen. Dieser initiale Aufwand bringt Ihnen Rechtssicherheit und schützt Sie vor den wesentlichen Risiken. Sind alle Prozesse etabliert und die Maßnahmen umgesetzt, können Sie alles Weitere mit Unterstützung seitens externer Datenschutzbeauftragten oder durch eigene qualifizierte Mitarbeiter umsetzen bzw. auf dem aktuellen Stand halten. Sowohl die technischen und organisatorischen Sicherheitsmaßnahmen, als auch die datenschutzrechtlichen Anforderungen müssen regelmäßig auf Sachgerechtigkeit und Wirksamkeit geprüft werden. Denn schließlich haften Sie persönlich für Datenschutzverstöße in Ihrem Unternehmen.

Datenschutz ist ein Prozess und kein einmaliger Aufwand.

Mit diesem Leitsatz und unserer regelmäßigen Unterstützung werden Sie alle Herausforderungen der DSGVO zweifelsohne meistern.

Nutzen Sie unsere Angebote und Newsdienste.

Ihr Autor: Andreas Hessel

Datenschutzbeauftragter, Informationssicherheitsbeauftragter
Geschäftsführer Datenschutz und Informationssicherheit (https://ds-ism.de)

Mitglied bei: