Eine Datenschutzerklärung soll dazu dienen, die Besucher einer Internetseite über die auf der Seite stattfindende Verarbeitung ihrer personenbezogenen Daten zu informieren. Das Fehlen der Datenschutzerklärung oder deren Unvollständigkeit kann Geldbußen und Abmahnungen nach sich ziehen. Da die Europäische Datenschutz-Grundverordnung (DS-GVO) auch erhöhte Informationspflichten mit sich bringt, haben wir für Sie einen Leitfaden erstellt, mit deren Hilfe Sie nachprüfen können, ob Sie in Ihrer Datenschutzerklärung alle geforderten Angaben veröffentlicht haben.

Der Leitfaden ist in zwei Abschnitte unterteilt: im ersten Abschnitt ist die Veröffentlichung der Pflichtangaben und im zweiten der individuellen Angaben zu finden.

I. Wichtige zu veröffentlichende Angaben (Pflichtangaben)

1. Informationen über den Verantwortlichen

Ein Verantwortlicher ist jede natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (vollständige Definition des Begriffs ist dem Artikel 4 Nr. 7 DS-GVO zu entnehmen). Beim Betreiben einer Homepage ist der Verantwortliche das Unternehmen selbst, sodass die Kontaktdaten des Unternehmens veröffentlicht werden müssen. Hierzu gehören neben der Anschrift des (Haupt-)Sitzes, Angaben wie die E-Mail Adresse und gegebenenfalls die Telefonnummer oder eine Faxnummer.

2. Zwecke der Verarbeitung

Weiterhin müssen Sie angeben, zu welchen Zwecken die Verarbeitung personenbezogener Daten auf Ihrer Homepage erfolgt. Wenn Sie auf Ihrer Homepage ein Kontaktformular nutzen, könnte ein möglicher Zweck der Verarbeitung personenbezogener Daten die Kontaktaufnahme sein. Ist die Verarbeitung personenbezogener Daten für mehrere Zwecke vorgesehen, sind die Seitenbesucher vor der Verarbeitung in der Datenschutzerklärung darauf hinzuweisen und alle Zwecke anzugeben.

3. Rechtsgrundlage der Verarbeitung

Eine Verarbeitung der personenbezogenen Daten bedarf stets einer Rechtsgrundlage. Als solhe kommen in Betracht eine Einwilligung oder ein gesetzlicher Erlaubnistatbestand (zum Beispiel Vertrag).
Beispiel: Einwilligung (Double-Opt-In-Verfahren)des Seitenbesuchers in den Bezug eines E-Mail-Newsletters
Der Verantwortliche darf die Anmeldedaten zum Versand des Newsletters Verwenden. Die Einwilligung muss als Rechtsgrundlage in der Datenschutzerklärung angegeben werden.
Beim Kauf von Waren oder Dienstleistungen über die Homepage erlaubt die gesetzliche Rechtsgrundlage „Vertrag“ die Verarbeitung von personenbezogenen Daten des Käufers, sofern diese Daten zum Abschluss und Abwicklung eines Kaufvertrages benötigt werden. Diese Verarbeitung ist somit durch das Gesetz legitimiert. Auch hier müssen Sie die Rechtsgrundlage (Vertrag) in der Datenschutzerklärung benennen.

4. Speicherdauer oder deren Kriterien

Die Besucher Ihrer Seite sind auch über die Speicherdauer oder über die Kriterien für die Festlegung der Speicherdauer zu informieren. Sofern Sie keinen genauen Zeitrahmen benennen können, müssen Sie Kriterien veröffentlichen, anhand derer die Seitenbesucher selbst ausrechnen können, wann ihre Daten gelöscht werden. So könnte bei der Newsletter Anmeldung das Kriterium der Speicherdauer „innerhalb von 24 Stunden nach erfolgter Abmeldung von Newsletter“ lauten.

5. Betroffenenrechte
Die Seitenbesucher sind auch auf ihre persönlichen Rechte nach DS-GVO, die Betroffenenrechte, hinzuweisen. Diese beinhalten: Recht auf Auskunft, Berichtigung, Löschung, Vergessenwerden oder Einschränkung der Verarbeitung, ferner das Recht ggf. auf Datenportabilität und auf Widerspruch bei erteilten Einwilligungen.
Praxistipp
Auf ein Widerspruchsrecht muss hervorgehoben (zum Beispiel durch Fettdruck) und in einer von anderen Informationen getrennten Form hingewiesen werden

6. Beschwerderecht
Ein weiteres Recht des Seitenbesuchers ist das Beschwerderecht bei der Datenschutzaufsichtsbehörde, sofern dieser der Ansicht ist, die Verarbeitung seiner personenbezogenen Daten sei rechtswidrig erfolgt. Auf dieses Recht müssen Sie ebenfalls hinweisen und die Aufsichtsbehörde benennen.

Bei den allen oben genannten Angaben handelt es sich um die Pflichtangaben. Deren Fehlen oder die Unvollständigkeit können zu einem Bußgeld oder einer Abmahnung führen. Prüfen Sie daher sehr sorgfältig, ob Sie alle geforderten Angaben veröffentlich haben.

II. Die individuell zu veröffentlichenden Angaben

Neben den Pflichtangaben können je nachdem, ob Sie folgende Dienste nutzen, weitere Veröffentlichungen notwendig sein.

1. Kontaktdaten des Datenschutzbeauftragten
Sofern Sie einen Datenschutzbeauftragten bestellt haben, müssen Sie dessen Kontaktdaten in der Datenschutzerklärung veröffentlichen. Dies gilt unabhängig davon, ob es sich hierbei um einen internen oder externen Datenschutzbeauftragten handelt. Erforderlich sind folgende Angaben: Name des Datenschutzbeauftragten (ausreichend ist eine Veröffentlichung der Funktionsbezeichnung ohne Bekanntgabe des Namens, dies ist strittig unter den Aufsichtsbehörden – Praxistipp: Abklärung mit der zuständigen Datenschutzaufsichtsbehörde), Anschrift, Telefonnummer und seine E-Mail-Adresse (ausreichend ist eine Funktions-E-Mail-Adresse wie datenschutzbeauftragter@mustermann.ag.de; dies ist strittig unter den Aufsichtsbehörden - Praxistipp: Abklärung mit der zuständigen Datenschutzaufsichtsbehörde).

2. Zweck der Verarbeitung: berechtigtes Interesse
Gründet die Verarbeitung der personenbezogenen Daten (wie zum Beispiel möglicherweise bei Werbeaktionen) auf der Rechtsgrundlage überwiegendes berechtigtes Interesse des Daten verarbeitenden Unternehmens (siehe hierzu Pflichtangaben nach Punkt 3), so sind Gründe, die der Interessenabwägung zu Grunde liegen, ebenfalls anzugeben.

3. Empfänger oder Kategorien von Empfängern personenbezogener Daten
Sofern personenbezogene Daten an Dritte weitergegeben werden, sind diese in der Datenschutzerklärung zu benennen. Sie können entweder die Empfänger selbst benennen, wie zum Beispiel Ihre Tochtergesellschaft, oder Sie können die Kategorien von Empfängern angeben, wie zum Beispiel Gruppen wie Hoster, Lettershops oder Dienstleister.

4. Übermittlung ins Nicht-EU- Ausland (sog. Drittland)
Die Übermittlung von personenbezogenen Daten ins Nicht-EU-Ausland (in das sog. Drittland) muss dem Seitenbesucher ebenfalls bekanntgemacht werden. Ergänzend zur Rechtsgrundlage ist hier anzugeben, welche Garantie (zum Beispiel Standardvertragsklauseln, EU-US-Privacy-Shield) ein angemessenes Datenschutzniveau gewährleistet und so die Weitergabe der Daten ins Drittland legitimiert; ferner, über wen ein Betroffener eine Kopie dieser Garantie beziehen kann.

5. Verpflichtung zur Bereitstellung personenbezogener Daten
Sofern personenbezogene Daten erforderlich sind, um zum Beispiel beim Kauf über die Homepage die Vertragsabwicklung zu gewährleisten, sind die Seitenbesucher auf diese Verpflichtung zur Bereitstellung hinzuweisen und die Folgen der Nichtbereitstellung anzugeben. Die Folge der Nichtbereitstellung könnte sein, dass zum Beispiel der Kaufvertrag ohne die personenbezogenen Daten nicht abgewickelt werden kann, das sich auch im Gesetz wiederfindet.

6. Automatisierte Entscheidungsfindung und Profiling
Sofern automatisierte Entscheidungsfindung oder Profiling eingesetzt werden, sind die besondere Tragweite des Einsatzes und die angestrebten Auswirkungen sowie die verwendete Logik oder Algorithmus anzugeben.

Hinweis: Bei den oben genannten Angaben handelt es sich um die individuellen Angaben. Deren Fehlen oder die Unvollständigkeit kann ebenfalls zu einem Bußgeld oder einer Abmahnung führen. Prüfen Sie daher sorgfältig, ob Sie unter die Verpflichtung zur Veröffentlichung der individuellen Angaben fallen.

Quelle: IHK München und Oberbayern

Stand: Mai 2018

Ansprechpartner:

Eva Schönmetzler
Stettenstraße 1 + 3 | 86150 Augsburg
Tel 0821 3162-207 | Fax 0821 3162-174
eva.schoenmetzler@schwaben.ihk.de