Industrie- und Handelskammer zu Düsseldorf
Postfachadresse: Postfach 10 10 17 · 40001 Düsseldorf
Hausadresse: Ernst-Schneider-Platz 1 · 40212 Düsseldorf
Telefon 02 11 35 57-0

Datenschutz für Existenzgründer

Sie wollen ein Unternehmen gründen, das Kontakt zu Endkunden hat? Dann sollten Sie bezüglich des Datenschutzes folgendes beachten:

1. **Rechtsgrundlage für Ihre Datenverarbeitung**

a) Vertrag

Wenn Sie Kunden etwas verkaufen wollen oder Ihnen eine Dienstleistung erbringen wollen, handelt es sich um die Anbahnung bzw. Erfüllung eines Vertragsverhältnisses. Hierzu benötigen Sie entsprechende Angaben ihrer Kunden (z. B. Name, Anschrift, Telefonnummer, vielleicht auch darüberhinausgehende Angaben wie das Geburtsdatum, Kontodaten, Fotos). Für die Grunddaten zur Abwicklung des Vertrags benötigen Sie keine gesonderte Einwilligung ihrer Kunden, für darüber hinausgehende Daten ja. Falls der Vertrag erfüllt ist und es keine gesetzlichen Gründe für seine Aufbewahrung mehr gibt (z. B. steuerliche oder handelsrechtliche Gründe), müssen die Daten gelöscht werden.

b) Einwilligung

In der Einwilligungserklärung müssen Sie auf die jederzeitige Widerrufbarkeit dieser Einwilligung hinweisen. Sie sollten hier nach obligatorischen und freiwilligen Daten trennen. Sie können eine elektronische Einwilligung einholen, dürfen aber keine voreingestellte Einwilligung in Form eines Häkchens benutzen („double-opt-in“). Zudem müssen Sie ihre Kunden darüber informieren, zu welchem Zweck Sie diese Daten verarbeiten wollen. Sie müssen die Einwilligungen dokumentieren.

c) Sie müssen Informationspflichten erfüllen:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters,
- Kontaktdaten des Datenschutzbeauftragten,
- Zwecke der Verarbeitung und Rechtsgrundlage,
- wenn die Verarbeitung auf Art. 6 Abs. 1 f beruht: berechtigtes Interesse des Verantwortlichen,
- ggf. Empfänger oder Kategorien von Empfängern,
- Absicht der Übermittlung in ein Drittland/internationale Organisation sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission,
- Dauer der Datenspeicherung,
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit,
- Recht auf Widerruf einer Einwilligung (bei Verarbeitung mit Art. 6 Abs. 1 a o. Art. 9 Abs. 2 a),
- Bestehen eines Beschwerderechts gegenüber einer Aufsichtsbehörde,
- Information, ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte,
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Art. 22).

Diese Informationspflichten müssen zum Zeitpunkt der Erhebung gegenüber dem – zukünftigen – Kunden erfüllt werden.

Falls die Daten nicht bei der betroffenen Person erhoben wurden, muss die Quelle angegeben werden.

Für die Nutzer Ihrer Internetseite müssen Sie bekannt geben, ob und welche Cookies Sie verwenden und ob Sie die Nutzer der Seiten tracken. Nutzen Sie hierfür einen Dienstleister, müssen Sie dazu eine Vereinbarung über die Auftragsverarbeitung schließen. Hat der Dienstleister seinen Sitz in einem Drittland, z. B. den USA, müssen Sie prüfen, ob die Weitergabe der Daten über EU-Standardvertragsklauseln oder über Privacy Shield abgesichert ist. Dabei handelt es sich um eine Vereinbarung zwischen der EU und den USA zur Angemessenheit des Datenschutzniveaus bei denjenigen Unternehmen, die die Anforderungen von Privacy Shield erfüllen.

2. Dienstleister

a) Wo verarbeiten Sie diese Daten? Auf Ihrem eigenen Server oder bei einem Dritten? Bei letzterem müssen Sie eine schriftliche (oder elektronische) Vereinbarung über die Auftragsverarbeitung schließen, denn der IT-Dienstleister darf die Daten nur nach Ihrer Weisung verarbeiten. Liegen die Daten auf Ihrem eigenen Server, nutzen Sie aber eine Cloud-Anwendung, müssen Sie klären, ob die Daten in Deutschland, in Europa oder in den USA gespeichert sind. Im letzteren Fall handelt es sich um einen Datentransfer in Drittländer, so dass Sie hierfür eine besondere Grundlage benötigen, wenn die Daten in die USA übermittelt werden.

b) Haben Sie einen Internetauftritt, der von einer Webdesignagentur gestaltet wird? Hat die Webdesignagentur Zugriff auf die personenbezogenen Daten, die Ihre Interessenten/Kunden dort angeben? Dann müssen Sie auch hier eine Vereinbarung über die Auftragsverarbeitung schließen. Zudem sind Sie nach dem Telemediengesetz verpflichtet, ein sogenanntes Impressum zu haben, d. h. Sie müssen hier angeben: Name, Anschrift, Rechtsform, E-Mail-Adresse, Umsatzsteuer-Identnummer usw. [Bei mehr als 10 Beschäftigten müssen Sie zusätzlich angeben, inwieweit Sie bereit oder verpflichtet sind, an einem Verfahren vor einer Verbraucherschlichtungsstelle teilzunehmen (§§ 36, 37 Verbraucherstreitbeilegungsgesetz).] Bei Online-Verträgen müssen Sie Ihrer Informationspflicht nach Art. 14 der sog ODR-Verordnung nachkommen.

c) Wollen Sie Ihre Buchführung, insbesondere auch die Gehaltsabrechnung Ihrer Mitarbeiter, über einen Steuerberater abwickeln, müssen Sie hierzu einen entsprechenden Dienstvertrag schließen.

d) Wollen Sie ein Inkassounternehmen einschalten, um säumige Kunden zur Zahlung auffordern zu lassen, benötigen Sie hierfür ebenfalls einen Dienstvertrag.

e) Falls Sie einen elektronischen Bezahldienst nutzen, müssen Sie mit ihm einen Dienstleistungsvertrag schließen.

3. Lieferanten

Haben Sie Lieferanten, von denen Sie ebenfalls Daten, wie Name, Anschrift, Telefonnummer, Produktangebot, Ansprechpartner, URL der Homepage und E-Mail-Adressen gespeichert haben, so fallen auch diese Angaben unter das Vertragsverhältnis bzw. Sie benötigen für bestimmte Angaben ebenfalls die Einwilligung der Person zur Speicherung ihrer Daten.

4. Mitarbeiter

Sie müssen Ihre Mitarbeiter darüber informieren, welche Daten und zu welchem Zweck sie diese verarbeiten. Sollten Sie Ihren Mitarbeitern die private Nutzung von E-Mails und des Internets in der Arbeitszeit gestatten, sollten Sie dazu klären, welchen Umfang diese Nutzung umfassen darf und dass die Nutzung bestimmte Inhalte nicht betreffen darf. Die Gestattung können Sie mit einer Einwilligung verbinden, dass die Mitarbeiter Ihre Kontrollen gestatten, damit weder Inhalt noch Umfang der Nutzung gegen Gesetze und die arbeitsrechtlichen Pflichten verstoßen. Diese Einwilligung muss in Schriftform erfolgen.

5. datenschutzrechtliche Anforderungen

Sie müssen Ihre Verfahren in einem sogenannten Verzeichnis für die Verarbeitungstätigkeiten mit folgenden Angaben dokumentieren:

- Name und Kontaktdaten des Verantwortlichen, des Vertreters, ggfs. des gemeinsam Verantwortlichen sowie des etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Rechtsgrundlage
- Kategorie der betroffenen Personen und personenbezogenen Daten
- Kategorie von Empfängern der Daten
- Übermittlung in Drittstaaten
- Löschfristen
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherung

Falls Sie Mitarbeiter haben, müssen Sie sie auf die Vertraulichkeit von Daten verpflichten (auf das Berufsgeheimnis müssen Sie verpflichten, soweit solche Daten verarbeitet werden) und sie auf den Datenschutz hinweisen bzw. sie angemessen schulen und dies dokumentieren. Sie sollten überlegen, wie Sie mit einem Auskunftsersuchen umgehen, wenn jemand erfahren möchte, welche Daten Sie über ihn gespeichert haben. Sie sollten zusätzlich schauen, ob Sie einen Prozess aufsetzen, falls es zu Datenverstößen kommt und Sie dies innerhalb von 72 Stunden der Aufsicht melden müssen. Die betroffene Person müssen Sie unverzüglich über den Datenverstoß informieren.

Sie müssen ein Löschkonzept vorsehen (geregelt für: 6 Jahre Geschäftsbriefe, 10 Jahre steuerrelevante Unterlagen, 6 Monate Bewerbungsunterlagen). Alle anderen Daten bzw. Dokumente mit personenbezogenen Daten müssen gelöscht bzw. vernichtet werden, wenn sie nicht mehr benötigt werden. Daran schließt sich die Frage an, wie datenschutzkonform Unterlagen vernichtet werden können und müssen (Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten schreddern).

6. technisch-organisatorische Maßnahmen

Sie betreffen die Frage, wie sicher Ihre Informationssicherheit (IT, Sicherheit im Büro/Geschäft) ist; auch dies muss dokumentiert werden. Sie müssen insbesondere mit Ihrem Steuerberater klären, wie die sensiblen Daten ihrer Mitarbeiter (Gesundheitsdaten, Religionszugehörigkeit) gut geschützt sind. Hierzu müssen bestimmte Maßnahmen ergriffen werden (Risikobewertung/Datenschutz-Folgenabschätzung). Eine Übermittlung per E-Mail ohne weitere Sicherheitsmaßnahmen ist datenschutzrechtlich nicht zulässig. Nachstehende Punkte geben einen groben Anhaltspunkt für solche Maßnahmen:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

2.2 Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

2.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

2.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

3.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Haben Sie Ihre Daten so gesichert, dass Sie sie bei einem eventuellen Verlust wiederherstellen können?

Bei der Einholung der Einwilligung Ihrer Kunden müssen Sie nicht nur die datenschutzrechtlichen Anforderungen erfüllen, sondern auch bei einer Einwilligung zur Werbung das Gesetz gegen unlauteren Wettbewerb (UWG) beachten.

Weitere Informationen finden Sie unter

www.gdd.de – Gesellschaft für Datenschutz und Datensicherheit mit Mustern z. B. zu einem Vertrag über die Auftragsverarbeitung

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html - Kurzpapier der Datenschutzaufsichtsbehörden zu bestimmten Aspekten der DSGVO

Stand: Februar 2019