Industrie- und Handelskammer Dresden

Merkblatt

Datenschutzgrundverordnung: Änderungen für kleine Unternehmen

Ansprechpartner: Referat Recht

Dr. Arne Schümann
Telefon: 0351 2802-194
Fax: 0351 2802-7194
Schuemann.Arne@dresden.ihk.de

Stand: 2017

Hinweis:

Vorbemerkungen:

Die EU-Datenschutz-Grundverordnung (DSGVO) erhöht zwar die Anforderungen an den Datenschutz, vieles ist aber bisher schon geltende Rechtslage in Deutschland nach dem Bundesdatenschutzgesetz (BDSG). Nachfolgend soll an einem praktischen Beispiel des Muster-Unternehmens „Homedreams“, Inh.: Miranda Mustera, Geschäftszweig: Einzelhandel mit selbst genähten Wohnaccessoires, Angebot von Selbstnähkursen und Einrichtungsberatung; MitarbeiterInnen: 4 [ab 10 Beschäftigte: Bestellung eines betrieblichen Datenschutzbeauftragten] dargestellt werden, welche Anforderungen sich (neu) aus der DSGVO ergeben.

1. Rechtsgrundlage für die Datenverarbeitung

a) Vertrag

Wenn Frau Mustera ihren Kunden etwas verkaufen will oder eine Dienstleistung erbringen will, handelt es sich um die Anbahnung bzw. Erfüllung eines Vertragsverhältnisses. Hierzu benötigt sie entsprechende Angaben ihrer Kunden (z. B. Name, Anschrift, Telefonnummer). Darüber hinausgehende Angaben wie E-Mail-Adresse, Geburtsdatum (für Glückwunschbriefe), Kaufinteressen, Teilnahme(interesse) an Kursen, Kontodaten und Fotos von TeilnehmernInnen) sind hingegen nicht erforderlich für die Erfüllung des Vertrags.
Für die Grunddaten zur Abwicklung des Vertrags benötigt Frau Mustera keine gesonderte Einwilligung ihrer Kunden, für darüber hinausgehende Daten aber schon. 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

Neu: In der Einwilligungserklärung muss sie auf die jederzeitige Widerrufbarkeit dieser Einwilligung hinweisen. Sie sollte hier nach obligatorischen und freiwilligen Daten trennen. Frau Mustera kann eine elektronische Einwilligung einholen, darf aber keine voreingestellte Einwilligung in Form eines Häkchens verwenden („double-opt-in“) **(neu)**. Zudem muss sie ihre Kunden darüber informieren, zu welchem Zweck sie diese Daten verarbeiten will.
Sie muss prüfen, ob die bisherigen Einwilligungen, die sie eingeholt hat, den – neuen – Anforderungen entsprechen. Falls nicht, wenn also der Hinweis auf den jederzeitigen Widerruf oder die Angabe des Zwecks fehlt, müssen die Einwilligungen neu eingeholt werden.

Sie muss die Einwilligungen dokumentieren.

c) Sie muss Informationspflichten erfüllen (teilweise neu):

- 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 muss Frau Mustera bekannt geben, ob und welche Cookies sie verwendet und ob sie die Nutzer der Seiten trackt. Nutzt sie hierfür einen Dienstleister, muss sie dazu eine Vereinbarung über die Auftragsverarbeitung schließen. Hat der Dienstleister seinen Sitz in einem Drittland, z. B. den USA, muss 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 verarbeitet Frau Mustera diese Daten? Auf ihrem eigenen Server oder bei einem Dritten? Bei letzterem muss 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, nutzt sie aber eine Cloud-Anwendung, muss 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) Frau Mustera hat einen Internetauftritt, der von einer Webdesignagentur gestaltet wird. Hat die Webdesignagentur Zugriff auf die personenbezogenen Daten, die ihre Interessenten/Kunden dort angeben? Falls ja, muss sie auch hier eine Vereinbarung über die Auftragsverarbeitung schließen. Zudem ist sie nach dem Telemediengesetz verpflichtet, ein sogenanntes Impressum mit folgenden Angaben zu haben: Name, Anschrift, Rechtsform, E-Mail-Adresse, Umsatzsteuer-Identnummer usw. [Bei mehr als 10 Beschäftigten muss Frau Mustera zusätzlich angeben, inwieweit sie bereit oder verpflichtet ist, an einem Verfahren vor einer Verbraucherschlichtungsstelle teilzunehmen (§§ 36, 37 Verbraucherstreitbeilegungsgesetz).] Bei Online-Verträgen muss sie ihrer Informationspflicht nach Art. 14 der sog. ODR-Verordnung nachkommen.

c) Frau Mustera lässt ihre Buchführung, insbesondere auch die Gehaltsabrechnung ihrer Mitarbeiter, über einen Steuerberater abwickeln. Hierfür muss sie einen entsprechenden Dienstvertrag schließen.

d) Miranda Mustera schaltet ein Inkassounternehmen ein, um säumige Kunden zur Zahlung auffordern zu lassen. Hierfür benötigt sie ebenfalls einen Dienstvertrag. Sie muss ihre Kunden zudem darauf aufmerksam machen, dass sie im Falle ausstehender Zahlungen ein Inkassounternehmen mit der Wahrnehmung ihrer Interessen beauftragt.

e) Frau Mustera nutzt einen elektronischen Bezahldienst, mit dem sie auch einen Dienstvertrag schließen muss.

3. Lieferanten

Miranda Mustera hat Lieferanten, von denen sie ebenfalls Daten, wie Name, Anschrift, Telefonnummer, Produktangebot, Ansprechpartner, URL der Homepage und E-Mail-Adressen gespeichert hat. Diese Angaben fallen entweder unter das Vertragsverhältnis oder sie benötigt für bestimmte Angaben ebenfalls die Einwilligung der Person zur Speicherung ihrer Daten unter Angabe des Zweckes der Speicherung.

4. Mitarbeiter

Wenn Frau Mustera ihren Mitarbeitern die private Nutzung von E-Mails und des Internets in der Arbeitszeit gestattet, sollte sie vereinbaren, welchen Umfang diese Nutzung umfassen darf und dass die Nutzung bestimmte Inhalte nicht betreffen darf. Die Gestattung kann Frau Mustera 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

Miranda Mustera muss ihre Verfahren in einem sogenannten Verzeichnis für die Verarbeitungstätigkeiten **(neu)** 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

Sie muss ihre Mitarbeiter auf die Vertraulichkeit von Daten verpflichten und sie auf den Datenschutz hinweisen bzw. angemessen schulen und dies dokumentieren. Sie sollte überlegen, wie sie mit einem Auskunftsersuchen umgeht, wenn jemand erfahren möchte, welche Daten sie über ihn gespeichert hat. Sie sollte zusätzlich prüfen, ob sie einen Prozess aufsetzt, falls es zu Datenverstößen kommt und sie dies der Aufsicht binnen 72 Stunden **(neu)** melden muss. Die betroffene Person muss unverzüglich über den Datenverstoß informiert werden.

Frau Mustera muss 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 die Informationssicherheit ist (IT, Sicherheit im Büro/Ge-schäft); auch dies muss dokumentiert werden. Miranda Mustera muss insbesondere mit ihrem Steuerberater klären, wie die sensiblen Daten ihrer Mitarbeiter (Gesundheitsdaten, Religionszugehörigkeit) gut geschützt sind. Hierzu müssen bestimmte Maßnahmen ergriffen werden (**neu:** 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.

Frau Mustera muss ihre Daten so sichern, dass sie sie bei einem eventuellen Verlust wiederherstellen kann.

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

Weitere Informationen unter

https://www.lfd.niedersachsen.de/startseite/dsgvo/fragen_zur_vorbereitung_auf_dsgvo/ - ein spezieller Fragebogen der Landesbeauftragten für den Datenschutz Niedersachsen

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