DATENSCHUTZ - D01

Stand: August 2023

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

Umsetzung der DSGVO
- Praktisches Fallbeispiel -

Gesetzestexte sind – auch für Juristen – nicht immer leicht zu verstehen. Deshalb möchten wir Ihnen anhand eines praktischen Falls die Umsetzung der DSGVO näher bringen.

Unser Fallbeispiel:
Einzelunternehmerin Miranda Mustera, betreibt einen Einzelhandel mit Wohnaccessoires und Möbeln und bietet Stilberatungskursen an. Sie hat vier MitarbeiterInnen.

Was muss sie tun, um sich datenschutzkonform zu verhalten?

1. Vertrag mit ihren Kunden

Wenn Frau Mustera ihren Kunden etwas verkaufen 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 oder Teilnahme(interesse) an Kursen 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.

2. Einwilligung ihrer Kunden

Für personenbezogene Daten, die nicht für die Vertragserfüllung benötigt werden, muss Frau Mustera eine Einwilligung einholen. Diese sollte aus Nachweisgründen am besten schriftlich eingeholt werden. 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"). Zudem muss sie ihre Kunden darüber informieren, zu welchem Zweck sie diese Daten verarbeiten will.

➔**D02** „Einwilligung nach der DSGVO", Kennzahl 2356

Nutzt Frau Mustera die Daten zu Werbezwecken, also z.B. um über aktuelle Angebote per E-Mail zu informieren, müssen auch die Anforderungen des Gesetzes gegen unlauteren Wettbewerb (UWG) beachten werden.

➔**W08** „Telefon-, Telefax-, E-Mail- und Brief-Werbung", Kennzahl 65

3. Informationspflichten gegenüber ihren Kunden

Frau Mustera muss ihre Kunden über die Datenverarbeitung informieren.

➔**D05** „Informationspflichten nach der DSGVO", Kennzahl 2356

Zu den Informationspflichten gehören Informationen über:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters: *„Verantwortlicher" ist Frau Mustera als Einzelunternehmerin, sie muss ihre Namen und ihre Kontaktdaten angeben.*
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden): *Frau Mustera ist nicht gesetzlich verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Diese Pflicht greift erst ab 20 Beschäftigten ein.*

  ➔**D06** „Betrieblicher Datenschutzbeauftragter", Kennzahl 2356
- Zwecke der Verarbeitung: *(Lieferung der Möbel)* und Rechtsgrundlage *(Kaufvertrag, Art. 6 Abs. 1 b) DSGVO)*
- ggf. Empfänger oder Kategorien von Empfängern: nur bei Übermittlung anzugeben: „*Wir übermitteln Ihre Kundendaten an unsere Speditionsunternehmen*, *damit Sie Ihre Möbelbestellung erhalten.",*
- ggf. die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation
- Dauer der Datenspeicherung
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit,
- Recht auf Widerruf einer Einwilligung,

  ➔**D02** „Einwilligung nach der DSGVO", Kennzahl 2356

- 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.

Diese Informationspflichten müssen zum Zeitpunkt der Erhebung gegenüber dem (zukünftigen) Kunden erfüllt werden. Im Ladengeschäft kann sie die Informationen aushängen oder dem Kunden ein Informationsblatt aushändigen. In ihrem Onlineshop muss sie diese Informationen an zentraler Stelle platzieren.

➔**D07** „Die Datenschutzerklärung nach der DSGVO“, Kennzahl 2356
Falls die Daten nicht bei den Kunden direkt erhoben wurden, muss die Quelle angegeben werden: *Ihre Daten haben wir bei XYZ erworben.*

Für die Nutzer ihrer **Internetseite** muss Frau Mustera über diese Informationen hinaus angeben, inwiefern Daten verarbeitet werden. Sie muss u.a. angeben, ob und welche **Cookies** sie verwendet und ob sie sog. **Analyse- oder Tracking-Tools,** z.B. Google Analytics, nutzt. Nutzt sie hierfür einen externen Dienstleister, muss sie dazu eine **Vereinbarung über die Auftragsverarbeitung** abschließen.

➔**D12** „Auftragsverarbeitung nach der DSGVO“, Kennzahl 2356

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 das sog. EU-U.S. Data Privacy Framework 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 des Data Privacy Framework erfüllen.

4. Hinzuziehung externer Dienstleister

In der Regel kooperieren Unternehmen mit externen Dienstleistern. Folgende Fälle sind dabei zu beachten:

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 Webdesign-Agentur gestaltet wird. Hat die Webdesign-Agentur Zugriff auf die personenbezogenen Daten, die ihre Interessenten/Kunden dort angeben? Falls ja, muss sie auch hier eine **Vereinbarung über die Auftragsverarbeitung schließen.**

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. Sie muss ihre Kunden darauf aufmerksam machen, dass sie im Falle ausstehender Zahlungen ein Inkassounternehmen mit der Wahrnehmung ihrer Interessen beauftragt: *Wir weisen Sie darauf hin, dass wir im Falle der Nichtzahlung Ihre Kundendaten an ein Inkassounternehmen zur Verfolgung unserer Ansprüche weitergeben.*

e) Frau Mustera nutzt einen **elektronischen Bezahldienst,** mit dem sie einen Auftragsdatenverarbeitungsvertrag schließen muss.

5. Daten von 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 im Normalfall im Rahmen der Vertragsabwicklung an. Dann ist der Vertrag die Rechtsgrundlage für die Datenverarbeitung.

6. Mitarbeiterdaten

Bei der Verarbeitung von Mitarbeiterdaten ist § 26 BDSG zu beachten.

➔ **D10** „Beschäftigtendatenschutz nach der DSGVO“, Kennzahl 2356

Sie muss ihre **Mitarbeiter auf die Vertraulichkeit von Daten verpflichten** und sie auf den Datenschutz hinweisen bzw. angemessen **schulen** und dies dokumentieren. Die Geheimhaltungsverpflichtung ist Bestandteil oder Zusatz zum Arbeitsvertrag.

7. Verzeichnis von Verarbeitungstätigkeiten

Miranda Mustera muss 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

Bezüglich der Löschfristen muss Frau Mustera ein **Löschkonzept** entwickeln. Grundsätzlich müssen Daten bzw. Dokumente mit personenbezogenen Daten gelöscht bzw. vernichtet werden, wenn sie nicht mehr benötigt werden. Gesetzlich gibt es teilweise Aufbewahrungsfristen, so z.B. im Steuer- und Handelsrecht, wonach Geschäftsbriefe 6 Jahre, steuerrelevante Unterlagen 10 Jahre aufzubewahren sind. Aufbewahrungsfristen gibt es auch im arbeitsrechtlichen Bereich (so z.B. mind. 2 Jahre für die Aufzeichnungen von Arbeitszeiten bei Minijobbern).

Praxistipp: Daran schließt sich die Frage an, wie datenschutzkonform Unterlagen vernichtet werden können und müssen (z. B. Datenträger zerstören, Papierunterlagen mit personenbezogenen Daten schreddern).

8. Technisch-organisatorische Maßnahmen

Technische und organisatorische Maßnahmen (TOM) sollen personenbezogene Daten, die von Frau Mustera erhoben, verarbeitet und gespeichert werden, auf bestmögliche Weise schützen. Darunter fallen sämtliche Maßnahmen die die Sicherheit von den eingesetzten IT-Systemen, bis hin zur Gebäudesicherheit, gewährleisten. Nachstehende Punkte geben einen groben Anhaltspunkt für solche Maßnahmen:

a) Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

aa) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren: *Kunden haben keinen Zutritt zu Büroräumen*

bb) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können: *EDV-System wird nach Arbeitsende so gesperrt, dass z.B. Reinigungskraft keinen Zugriff hat.*

cc) 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.

dd) Trennungskontrolle

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

b) Integrität (Art. 32 Abs. 1 lit. b DSGVO)

aa) 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.

bb) 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.

cc) 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.

dd) Auftragskontrolle

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

c) Verfügbarkeitskontrolle

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

d) 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.