SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Fragenkatalog für KMU zur Datenschutz-Grundverordnung
Wie gut sind Sie aufgestellt?

Seit dem 25. Mai 2018 muss jedes Unternehmen die Vorgaben der Europäischen Datenschutz-Grundverordnung (DS-GVO) und der Neufassung des Bundesdatenschutzgesetzes (BDSG) umgesetzt haben. Bei Nichtbeachtung oder Verstößen sieht die neue Rechtslage neben behördlichen Anordnungen einen drastisch erhöhten Bußgeldrahmen vor. Zudem drohen Vertrauensverluste bei Geschäftspartnern.

Mit den folgenden Fragen möchten wir Ihnen als kleinem oder mittelständischem Unternehmen (KMU) helfen, die Bereiche in Ihrem Unternehmen zu identifizieren, in denen Sie schon gut aufgestellt sind und die Bereiche, in denen es noch Handlungsbedarf für Sie gibt. Die Fragen geben Ihnen zugleich Anhaltspunkte, worauf die Aufsichtsbehörde bei Prüfungen regelmäßig besonderen Wert legt.

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstr. 9, 39104 Magdeburg
Telefon: (0391) 81803-0
Telefax: (0391) 81803-33
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de

Fragen zur Umsetzung der DS-GVO

1. Datenschutz ist Chefsache

a. Als Geschäftsleitung müssen Sie sich mit den Anforderungen der DS-GVO und des BDSG befassen. Kennen Sie insbesondere die Regelungen
   - zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Art. 5 Abs. 2 DS-GVO)?
   - zu den Informationspflichten gegenüber den Betroffenen, deren personenbezogene Daten[1] Sie verarbeiten (Art. 12 bis 14 DS-GVO)[2]?
   - zum Recht der Betroffenen auf Datenübertragbarkeit (Art. 20 DS-GVO)[3]?
   - zur technischen und organisatorischen Sicherheit der Datenverarbeitung (Art. 32 DS-GVO)?
   - zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)[4]?
   - zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO)?

b. Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten benannt (Art. 37 DS-GVO, § 38 BDSG)[5]?

c. Wurden Ihre Beschäftigten über die neuen Datenschutzregelungen informiert und auf die Beachtung der datenschutzrechtlichen Anforderungen verpflichtet[6]?

2. Bestandsaufnahme

a. Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)[7]? Denken Sie hierbei insbesondere an die
   - Verarbeitung von Kundendaten
   - Verarbeitung von Beschäftigtendaten
   - Verarbeitung von Daten von Kindern
   - Verarbeitung von Daten für Dritte als Auftragsverarbeiter[8]

b. Wird dieses Verzeichnis aktualisiert, wenn sich die Datenverarbeitung bzw. die Voraussetzungen dafür verändern? Wer ist hierfür in Ihrem Unternehmen zuständig?

3. Zulässigkeit der Verarbeitung

Für jede Verarbeitung personenbezogener Daten benötigen Sie eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

a. Haben Sie für alle Verarbeitungen (s. o. Nr. 2) eine Rechtsgrundlage (Art. 6 bis 11 DS-GVO sowie §§ 22, 24, 26 bis 28 BDSG), z. B. einen Vertrag mit der betroffenen Person oder die Interessenabwägungsklausel (Art. 6 Abs. 1 Satz 1 lit. b bzw. f DS-GVO)?

b. Haben Sie dies dokumentiert?

c. Haben Sie Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten usw. an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

---

[1] Personenbezogene Daten = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (natürliche Person = Mensch, davon zu unterscheiden sind die juristischen Personen, wie z. B. GmbHs oder AGs), s. a. Art. 4 Nr. 1 DS-GVO.

[2] Siehe auch das Kurzpapier Nr. 10 der Aufsichtsbehörden, alle genannten Kurzpapiere sind abzurufen unter http://lsaurl.de/Kurzpapiere.

[3] Siehe auch die Leitlinien der Artikel-29-Datenschutzgruppe zum Recht auf Datenübertragbarkeit unter https://datenschutz.sachsen-anhalt.de/informationen/internationales/datenschutz-grundverordnung/leitlinien-der-artikel-29-datenschutzgruppe/.

[4] Siehe Kurzpapier Nr. 5.

[5] Siehe Kurzpapier Nr. 12.

[6] Siehe Kurzpapier Nr. 19.

[7] Siehe Kurzpapier Nr. 1.

[8] Siehe Kurzpapier Nr. 13.

4. Betroffenenrechte und Informationspflichten

a. Alle Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DS-GVO). Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher[9]? Denken Sie dabei, wenn vorhanden, auch an Datenverarbeitungen auf Ihrer Internetseite. Besonders wichtig sind in diesem Zusammenhang folgende Informationen:
   - Kontaktdaten des Verantwortlichen und seines Datenschutzbeauftragten (falls vorhanden)
   - Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
   - Herkunft und Empfänger der Daten
   - Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer
   - Hinweis auf Betroffenenrechte, darunter auch das Recht auf Beschwerde bei der Aufsichtsbehörde und ggf. das Recht auf Widerruf der Einwilligung

b. Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15 bis 22 DS-GVO)? Denken Sie dabei insbesondere an folgende Rechte:
   - Recht auf Auskunft[10]
   - Recht auf Berichtigung
   - Recht auf Widerspruch
   - Recht auf fristgemäße Löschung der Daten[11]
   - Recht auf Einschränkung der Verarbeitung
   - Recht auf Datenübertragbarkeit

5. Personenbezogene Daten von Kindern

a. Haben Sie, sofern Sie die Verarbeitung personenbezogener Daten von Kindern (alle Minderjährigen nach deutschem Recht) auf die Interessenabwägung stützen, deren Interessen besonders gewichtet (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO)?

b. Verarbeiten Sie auch personenbezogene Daten von Kindern, die das 16. Lebensjahr noch nicht vollendet haben, in Bezug auf Dienste der Informationsgesellschaft[12]? Wenn ja, haben Sie in diesen Fällen an die besonderen Anforderungen an die Einwilligung gedacht (Art. 8 DS-GVO)?

6. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

a. Welche technischen und organisatorischen Maßnahmen, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DS-GVO), setzen Sie oder Ihre Dienstleister ein[13]? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung[14] dokumentiert?

b. Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? Letztere sind z. B. bei Verwendung von Online-Formularen verpflichtend.

c. Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?

d. Wie stellen Sie sicher, dass bei der Neuentwicklung oder Änderung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Art. 25 DS-GVO)?

---

[9] Siehe Kurzpapier Nr. 10.

[10] Siehe Kurzpapier Nr. 6.

[11] Siehe Kurzpapier Nr. 11.

[12] Dienste der Informationsgesellschaft = jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, z. B. Online-Verkauf von Waren, Video auf Abruf, Download eines Klingeltons, Beitritt zu sozialen Netzwerken.

[13] Hilfestellung hierzu bietet eine Checkliste des Landesbeauftragten für den Datenschutz, abrufbar unter http://lsaurl.de/checktom.

[14] Schutzbedarfsklassifizierung = Bewertung des konkreten Schutzbedarfs der verarbeiteten Daten.

7. Verträge prüfen

a. Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d. h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten (z. B. wenn Sie die Finanzbuchhaltung, die Wartung der EDV oder die Datenträgerentsorgung ausgelagert haben)[15], an die neuen Regelungen (Art. 26 bis 28 DS-GVO) angepasst?[16]

   Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

b. Führt Ihr Unternehmen Verarbeitungen durch, bei denen eine Übermittlung personenbezogener Daten in ein Drittland[17] möglich ist? Dies kommt auch in Betracht bei der Nutzung von außereuropäischen Speichermöglichkeiten in einer Cloud.

   Bestehen für diese Verarbeitungen entsprechende zusätzliche Garantien/Vereinbarungen[18]? Z. B. EU-Standardvertragsklauseln, Einzelverträge, zertifizierte Verfahren, Binding Corporate Rules.

8. Datenschutz-Folgenabschätzung[19]

a. Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten[20] der Betroffenen durch (Art. 35 DS-GVO)? Dies gilt z. B. bei einer umfangreichen Verarbeitung besonderer Kategorien[21] personenbezogener Daten. Eine Liste von Datenverarbeitungen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, hat die Aufsichtsbehörde gemäß Art. 35 Abs. 4 DS-GVO veröffentlicht[22].

b. Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?

c. Wer ist für diesen Prozess zuständig?

9. Meldepflichten

a. Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)[23]?
   - Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72 Stunden beachtet?
   - Wer ist in Ihrem Unternehmen für die Meldung zuständig?

b. Falls Sie einen Datenschutzbeauftragten benannt haben[24], denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde[25].

10. Dokumentation

a. Können Sie die Einhaltung aller genannten Pflichten/Anforderungen (schriftlich) nachweisen?

b. Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

---

[15] Siehe Kurzpapier Nr. 13.

[16] Formulierungshilfen für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO finden Sie unter http://lsaurl.de/MusterAV.

[17] Drittland = ein Land außerhalb der EU bzw. des europäischen Wirtschaftsraums. Eine Übermittlung liegt z. B. auch bei Supportzugriffen aus einem Drittland vor.

[18] Siehe Kurzpapier Nr. 4.

[19] Siehe Kurzpapier Nr. 5.

[20] Siehe Kurzpapier Nr. 18.

[21] Besondere Kategorien personenbezogener Daten = Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Siehe auch das Kurzpapier Nr. 17.

[22] So genannte Muss-Liste, siehe http://lsaurl.de/DSFAListe. Bitte beachten Sie, dass diese Liste nicht abschließend ist.

[23] Ein Online-Formular für Meldungen an den Landesbeauftragten für den Datenschutz Sachsen-Anhalt finden Sie unter http://lsaurl.de/DSVerletzung.

[24] Siehe Kurzpapier Nr. 12.

[25] Ein Online-Formular für die Meldung an den Landesbeauftragten für den Datenschutz Sachsen-Anhalt finden Sie unter https://datenschutz.sachsen-anhalt.de/nc/service/online-formulare-des-landesbeauftragten/datenschutzbeauftragten-melden/.