Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

Nur noch 6 Monate bis zur Anwendung der Datenschutz-Grundverordnung!

Der Countdown läuft – ab dem 25. Mai 2018 muss jedes Unternehmen die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) und des neuen Bundesdatenschutzgesetzes (BDSG neu) umgesetzt und in den Unternehmensalltag integriert haben. Bei Nichtbeachtung oder Verstößen sieht die neue Rechtslage einen drastisch erhöhten Bußgeldrahmen von bis zu 20 Millionen Euro vor.

Diese Neuerungen nehmen wir zum Anlass, Ihnen als kleinem oder mittelständischem Unternehmen Hilfestellung zur Umsetzung des neuen Datenschutzrechts zu geben. Mit den folgenden Fragen möchten wir Ihnen helfen, die Bereiche in Ihrem Unternehmen zu identifizieren, in denen Sie schon gut vorbereitet sind und die Bereiche, in denen es bis zum 25. Mai 2018 noch Handlungsbedarf für Sie gibt. Die Fragen geben Ihnen zugleich Anhaltspunkte, worauf wir bei zukünftigen Prüfungen besonderen Wert legen werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit • Arndtstraße 1 • 27570 Bremerhaven

Tel.: 0421 – 361 – 20 10 oder 0471 – 596 – 20 10 •. Fax: 0421 – 496 – 18495 • e-mail-Adresse: office@datenschutz.bremen.de

Fragen zur Vorbereitung auf die DS-GVO

1. Datenschutz ist Chefsache

a. Haben Sie sich als Geschäftsleitung schon mit den neuen Anforderungen der DS-GVO und des BDSG (neu) befasst? Kennen Sie insbesondere die neuen Regelungen

- zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Artikel 5 Absatz 2 DS-GVO)?
- zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten (Artikel 12 - 14 DS-GVO)?
- zu den Rechten der Betroffenen auf Datenübertragbarkeit (Artikel 20 DS-GVO)?
- zur technischen und organisatorischen Sicherheit der Datenverarbeitung Artikel 32 DS-GVO?
- zur Datenschutz-Folgenabschätzung (Artikel 35 DS-GVO)?
- zur Meldung von Datenschutzverstößen (Artikel 33 DS-GVO)?

b. Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten bestellt (Artikel 37 DS-GVO, § 38 BDSG neu)?

c. Wurden Ihre Beschäftigen über die neuen Datenschutzregelungen informiert und/oder geschult?

2. Bestandsaufnahme

a. Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten[1] verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Artikel 30 DS-GVO)[2]? Denken Sie hierbei insbesondere an die

- Verarbeitung von Kundendaten
- Verarbeitung von Beschäftigtendaten
- Verarbeitung von Daten von Kindern
- Verarbeitung von Daten für Dritte als Auftragsverarbeiter

b. Wird dieses Verzeichnis regelmäßig aktualisiert? Wer ist hierfür in Ihrem Unternehmen zuständig?

3. Zulässigkeit der Verarbeitung

Auch nach neuem Recht benötigen Sie für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

a. Haben Sie für alle Verarbeitungen (siehe oben Nummer. 2) eine Rechtsgrundlage nach der neuen Rechtslage (Artikel 6 bis 11 DS-GVO sowie § 26 BDSG neu)?

b. Haben Sie dies dokumentiert?

c. Haben Sie Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten und so weiter an die Anforderungen von Artikel 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 zum Beispiel GmbHs oder AGs), siehe auch Artikel 4 Nummer 1 DS-GVO.

[2] siehe hierzu auch das Kurzpapier Nr. 1 der Aufsichtsbehörden – abzurufen unter https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_KPNr_1_Verzeichnis_Verarbeitungst%E4tigkeiten.pdf

4. Betroffenenrechte und Informationspflichten

a. Die 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 (Artikel 12 DS-GVO).
Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Artikel 13 und 14 DS-GVO genannten Punkte sicher?

Besonders wichtig sind in diesem Zusammenhang folgende Informationen:

- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
- Dauer der Speicherung, gegebenfalls Kriterien für die Festlegung der Speicherdauer
- Hinweis auf Betroffenenrechte
- Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Widerruf der Einwilligung
- Recht auf Beschwerde bei der Aufsichtsbehörde
- Herkunft der Daten

b. Wie stellen Sie die weiteren Betroffenenrechte sicher (Artikel 15-22 DS-GVO)? Denken Sie dabei insbesondere an folgende Rechte:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf fristgemäße Löschung der verarbeiteten Daten
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

5. Personenbezogene Daten von Kindern

a. Verarbeiten Sie auch personenbezogene Daten von Kindern in Bezug auf Dienste der Informationsgesellschaft[3]?

b. Wenn ja, haben Sie in diesen Fällen an die besonderen Anforderungen an die Einwilligung gedacht (Artikel 8 DS-GVO)?

6. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

a. Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Artikel 32 DS-GVO)? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung[4] dokumentiert?

b. Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? In welchen Fällen?

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

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

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

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

7. Verträge prüfen

a. Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, das heißt mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Artikel 26 – 28 DS-GVO) angepasst?
Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

b. Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland[5] möglich ist[6], entsprechende zusätzliche Garantien/Vereinbarungen[7]?

- EU-Standardvertragsklauseln
- Binding Corporate Rules
- Privacy Shield (nur für die USA)

8. Datenschutz-Folgenabschätzung[8]

a. Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Artikel 35 DS-GVO)? Dies gilt zum Beispiel bei einer umfangreichen Verarbeitung besonderer Kategorien[9] personenbezogener Daten.

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 (Artikel 33 DS-GVO)?

- 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 bestellt haben, denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde.

10. Dokumentation

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

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

---

[5] Drittland = ein Land außerhalb der EU beziehungsweise. des europäischen Wirtschaftsraums.

[6] Eine Übermittlung liegt zum Beispiel auch bei Supportzugriffen aus einem Drittland vor.

[7] siehe. hierzu auch das Kurzpapier Nr. 4 der Aufsichtsbehörden, abzurufen unter https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_KPNr_4_Drittl%E4nder.pdf

[8] siehe hierzu auch Kurzpapier Nr. 5 der Aufsichtsbehörden, abzurufen unter https://www.datenschutz.bremen.de/sixcms/media.php/13/DSK_KPNr_5_Datenschutz-Folgenabsch%E4tzung.pdf

[9] 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.