Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Nur noch kurze Zeit 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 mit Blick auf Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) einen drastisch erhöhten Bußgeldrahmen von bis zu 20 Millionen Euro vor.

Diese Neuerungen nehmen wir zum Anlass, Ihnen als KMU 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.

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 (Art. 5 Absatz 2 DS-GVO)?
- zu den Informationspflichten gegenüber den betroffenen Personen, deren Daten Sie verarbeiten (Art. 12 - 14 DS-GVO)?
- zu den Rechten der betroffenen Personen auf Datenübertragbarkeit (Art. 20 DS-GVO)?
- zur technischen und organisatorischen Sicherheit der Datenverarbeitung Art. 32 DS-GVO?
- zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)?
- zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO)?

b. Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten bestellt (Art. 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 verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)? 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?

Vertiefende Hinweise

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Davon zu unterscheiden sind die juristischen Personen (wie z.B. GmbHs oder AGs), siehe auch Art. 4 Nr. 1 DS-GVO. Informationen, die sich zwar auf eine juristische Person beziehen, jedoch automatisch auch Aussagen über die dahinterstehende Person treffen, sind ebenfalls als personenbezogene bzw. –beziehbare Daten zu behandeln (z.B. Einpersonengesellschaften, Einzelkaufleute).

Greifen Sie auf ein bereits bestehendes Verfahrensverzeichnis zurück und aktualisieren Sie dieses für die DS-GVO. Die Erstellung und Aktualisierung sollte durch die zuständigen Fachbereiche bzw. entsprechend fachlich zuständige Personen und – sofern vorhanden - unter Einbeziehung des betrieblichen Datenschutzbeauftragten erfolgen.

Weitere Informationen zum Verzeichnis von Verarbeitungstätigkeiten finden Sie in unserem Kurzpapier Nr. 1.[1]

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 Personen sein. Daneben kann es weitere Spezialregelungen in der DS-GVO (z.B. Art. 86 DS-GVO für amtliche Dokumente) als auch in anderen Spezialgesetzen (z.B. § 138 StGB) geben. Auch Kollektivvereinbarungen wie die Betriebsvereinbarung zum Datenschutz im Arbeitsverhältnis bleiben nach Art. 88 DS-GVO nach wie vor zulässig.

a. Haben Sie für alle Verarbeitungen (s.o. Nr. 2) eine Rechtsgrundlage nach der neuen Rechtslage (Art. 6 bis 11 DS-GVO sowie § 26 BDSG neu)?

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)?

Vertiefende Hinweise:

Zentrale Rechtsgrundlage der DS-GVO für eine Verarbeitung personenbezogener Daten ist Art. 6 Abs. 1 DSG-VO. Für eine rechtsgültige Einwilligung ergeben sich die vier wichtigsten Anforderungen aus Art. 7 DS-GVO; Art. 8 DS-GVO enthält besondere Anforderungen an die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft (s.u. Ziffer 5) und § 26 Abs. 2 S. 2 BDSG-neu an die Einwilligung bei der Verarbeitung personenbezogener Daten von Beschäftigten:

- Freiwilligkeit,
- Informiertheit,
- Ausdrücklichkeit und
- Widerrufbarkeit (für die Zukunft).

Die Verarbeitung von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, unterliegt nach wie vor besonderen Voraussetzungen. Die Verarbeitung dieser besonderen Kategorien personenbezogener Daten ist nur zulässig, wenn neben einem Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO zusätzlich ein Fall des Art. 9 Abs. 2 DS-GVO - gegebenenfalls in Verbindung mit dem einschlägigen nationalen Recht (etwa im Datenschutzgesetz Nordrhein-Westfalen oder im jeweiligen Fachrecht) – vorliegt.
Bereits im Zeitpunkt der Verarbeitung der Daten sollten Sie die Rechtsgrundlage der Verarbeitung dokumentiert haben. An die verschiedenen Rechtsgrundlagen sind unterschiedliche Rechte des von der Verarbeitung betroffenen Personen geknüpft, wie z.B. das Widerrufsrecht. Zudem muss das Unternehmen nach der DS-GVO die von der Datenverarbeitung betroffenen Personen über die Datenverarbeitung einschließlich der zugrunde liegenden Rechtsgrundlage informieren (siehe Ziff. 4). Außerdem können Sie bei der Geltendmachung von Auskunftsansprüchen von betroffenen Personen und Anfragen von Aufsichtsbehörden schneller reagieren (siehe Ziff. 4).

[1] Die vollständige Sammlung der Kurzpapiere zur DS-GVO der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) finden Sie auf der Homepage der LDI NRW im Bereich „EU-Datenschutzreform“ oder unter https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html.

4. Rechte der betroffenen Personen und Informationspflichten

a. Die betroffenen Personen 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 Personen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher?

b. Wie stellen Sie die weiteren Rechte der betroffenen Personen sicher (Art. 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 (Sperrung)
- Recht auf Datenübertragbarkeit

Vertiefende Hinweise:

a) Informationspflichten: Art. 13 DS-GVO regelt Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person, z.B. dem Kunden eines Onlinehandels, der erstmalig eine Bestellung aufgibt. Art. 14 DS-GVO legt die Informationspflichten fest, wenn die personenbezogenen Daten nicht bei der betroffenen Person selbst, sondern z.B. über Dritte wie z.B. Adresshändler erhoben werden. Denkbar sind häufig auch Mischformen. Um das Beispiel des Kunden eines Onlinehandels weiter aufzugreifen, sind Fallgestaltungen denkbar, in welchen ein Teil der Daten zunächst im Rahmen des Bestellvorgangs vom Kunden selbst eingegeben werden, dann aber noch weitere Daten hinzukommen, wie z.B. eine Bonitätsprüfung oder eine Adressverifikation bei einer Wirtschaftsauskunftei.

Besonders wichtig sind in diesem Zusammenhang unter anderem folgende Informationen:

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

Weitere Informationen zu diesem Thema finden Sie in unserem Kurzpapier Nr. 10, zur Verarbeitung von personenbezogenen Daten für Werbung in unserem Kurzpapier Nr. 3. Weitere allgemeine Hinweise zum betrieblichen Datenschutzbeauftragten enthält das Kurzpapier Nr. 12.

b) Rechte der betroffenen Personen: Besondere Beachtung sollten Sie der Implementierung von Geschäftsprozessen zur Wahrung von Rechten der betroffenen Personen schenken. Diese sind unter der Geltung der DS-GVO weitreichender als dies bislang unter Geltung des alten Bundesdatenschutzgesetzes der Fall war. So muss im Rahmen einer Auskunft nach Art. 15 DS-GVO z.B. nunmehr auch auf das Recht zur Berichtigung, Sperrung (Einschränkung der Verarbeitung) und Löschung von Daten (Art. 16 ff. DS-GVO) ebenso hingewiesen werden wie auf das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde.

Weitere Informationen zum Auskunftsrecht sowie zum Recht auf Löschung finden Sie in unseren Kurzpapieren Nr. 6 und Nr. 11.

5. Personenbezogene Daten von Kindern

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

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

Vertiefende Hinweise:

Unter Dienste der Informationsgesellschaft sind in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistungen, z.B. der Online-Verkauf von Waren, Video auf Abruf, Download eines Klingeltons, Beitritt zu sozialen Netzwerken zu verstehen.

Für die Verarbeitung personenbezogener Daten von Kindern muss eine Altersverifizierung durchgeführt werden: Zur Verarbeitung personenbezogener Daten unter 16 Jähriger sind die Eltern bzw. die Träger der elterlichen Verantwortung hinzuzuziehen.
Die nach Art. 6 Abs. 1 lit. f DS-GVO durchzuführende Interessenabwägung ist bei der Verarbeitung personenbezogener Daten von Kindern besonders sorgfältig durchzuführen (vgl. auch EG 38).
Sind Kinder betroffen, muss die Information zur Datenverarbeitung besonders einfach und kindgerecht sein (Art. 12 Abs. 1 DS-GVO, EG 58).

6. Sicherheit der Verarbeitung und Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

b. Setzen Sie
   i. Pseudonymisierungs-
   ii. Anonymisierungs-
   iii. 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 (Art. 25 DS-GVO, Stichwort „eingebauter Datenschutz“)?

Vertiefende Hinweise:

Unter einer Schutzbedarfsklassifizierung ist die Bewertung des konkreten Schutzbedarfs der verarbeiteten Daten zu verstehen.

7. Verträge prüfen

a. Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d.h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 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 ohne angemessenes Datenschutzniveau möglich ist, zusätzliche Garantien, z.B.
   - Standarddatenschutzklauseln der EU-Kommission (EU-Standardvertragsklauseln)
   - Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules/BCR)?

Vertiefende Hinweise:

Bisher richten sich die Inhalte von Verträgen mit Auftragsverarbeitern nach § 11 Absatz 2 Bundesdatenschutzgesetz. Viele Elemente daraus wurden in die Regelungen der DS-GVO übernommen.

Ein Drittland ist ein Land außerhalb der EU bzw. des europäischen Wirtschaftsraums (EWR). Eine Übermittlung in ein Drittland liegt z.B. auch bei Supportzugriffen aus diesem vor. Die EU-Kommission kann in einem Beschluss die Angemessenheit des Datenschutzniveaus in einem Drittland im Vergleich zum Datenschutzniveau in der EU feststellen. Dies ist beispielsweise der Fall für die Schweiz und den USA (Privacy Shield). Dann müssen keine zusätzlichen Garantien/Vereinbarungen getroffen werden. Ohne zusätzliche Garantien/Vereinbarungen kommen für Übermittlungen in Drittländer eventuell Ausnahmetatbestände in Betracht.

Weitere Informationen zu Datenübermittlungen in Drittländer finden Sie in unserem Kurzpapier Nr. 4.

8. Datenschutz-Folgenabschätzung

a. Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten betroffener Personen durch (Art. 35 DS-GVO)? Dies gilt z.B. bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (zum Begriff der besonderen Kategorien personenbezogener Daten s.o. Ziffer 3, vertiefende Hinweise).

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?

Vertiefende Hinweise:

Falls Sie bereits heute für bestimmte Verarbeitungsprozesse mit personenbezogenen Daten so genannte Vorabkontrollen durchgeführt haben bzw. durchführen: Insbesondere diese Abläufe sollten Sie auf die Notwendigkeit einer Datenschutz-Folgeabschätzung hin überprüfen. Die Wahrscheinlichkeit ist hoch, dass Sie für diese Abläufe eine Datenschutz-Folgeabschätzung durchführen müssen. Dafür können Sie ggfs. auf die vorangegangene Prüfung aufsetzen. Prüfen Sie die Aktualität dieser Unterlagen!

Weitere Informationen zur Datenschutz-Folgenabschätzung finden Sie in unserem Kurzpapier Nr. 5.

9. Meldepflichten

a. Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 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 der entsprechenden Kontaktdaten an die Aufsichtsbehörde ab dem 25.05.2018.

Vertiefende Hinweise:

Meldepflicht bei Datenschutzverstößen: Art. 33 DS-GVO sieht eine Meldepflicht von Datenschutzverstößen gegenüber der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden innerhalb Ihres Unternehmens vor. In Anbetracht dieser kurzen Reaktionszeit empfiehlt es sich, bereits im Vorfeld zuständige Personen in Ihrem Unternehmen zu identifizieren und – z.B. durch eine entsprechende Einweisung – sicher zu stellen, dass den Anforderungen der Norm (insbesondere nach Art. 33 DS-GVO Absätzen 3 und 5) Rechnung getragen wird.

Meldung des Datenschutzbeauftragten: Nach Art. 37 Abs. 7 DS-GVO sind die Kontaktdaten des betrieblichen Datenschutzbeauftragten zu veröffentlichen und der (zuständigen) Aufsichtsbehörde mitzuteilen. Die LDI NRW wird hierzu ein einheitliches Meldeformular für Unternehmen mit Sitz in NRW zur Verfügung stellen.
Weitere Informationen finden Sie unter
https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Mitteilungspflicht-der-Kontaktdaten-von-Datenschutzbeauftragten-nach-DS-GVO/Mitteilungspflicht-der-Kontaktdaten-von-Datenschutzbeauftragten-nach-DS-GVO.html

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?

Vertiefende Hinweise:
Der Verantwortliche ist für die Einhaltung der Vorgaben aus der DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“, Art. 5 Abs. 2 DS-GVO).

Zudem setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert („Nachweispflicht“, Art. 24 Abs. 1 DS-GVO).

Um dieser Rechenschafts- oder Nachweispflicht nachzukommen, wird dringend empfohlen, wesentliche Aktivitäten und weitere Arbeitsergebnisse, welche der Umsetzung der Vorgaben der DS-GVO dienen, festzuhalten.