Dr. Martin Bahr

Check-up-Liste für die Umsetzung der DSGVO in Ihrem Unternehmen – Teil 3

In den beiden letzten Teilen haben wir die praktischen Auswirkungen der Datenschutzgrundverordnung (DSGVO) auf den Online-Bereich dargestellt. Da die Reform in Kürze, nämlich am 25. Mai 2018, wirksam wird, wollen wir Ihnen eine praktische Check-up-Liste für die Umsetzung an die Hand geben. Diese Liste kann und will keine umfassende Datenschutzprüfung Ihres Unternehmens ersetzen. Gerade viele kleine Unternehmen wissen jedoch angesichts des Umfangs und der Komplexität des Themas überhaupt nicht, wo sie anfangen sollen. Genau an dieser Stelle setzt die vorliegende Liste an und bietet Ihnen die Möglichkeit, einen Einstieg in das schwierige Thema zu finden. Nicht mehr – aber auch nicht weniger. Wenn Sie die Check-up-Liste durchgegangen sind, werden Sie sehen, wo bei Ihnen der Schuh drückt und wo Sie noch nacharbeiten müssen, um auf die neuen gesetzlichen Regelungen vorbereitet zu sein.

1. Frage: Ist in Ihrem Unternehmen bereits ein Datenschutzbeauftragter bestellt?

a. Antwort „Ja“

Sehr gut, damit ist der wichtigste Schritt bereits getan. Bitte beachten Sie in jedem Fall auch noch:

» Die Ernennung als Datenschutzbeauftragter sollte schriftlich erfolgen, eine bloß mündliche Erklärung reicht nicht aus, da Sie ansonsten die Ernennung nicht hinreichend sicher nachweisen können.
» Sie müssen Ihren Datenschutzbeauftragten der zuständigen Datenschutz-Aufsichtsbehörde mitteilen (Art. 37 Abs. 7 DSGVO).
» Verfügt Ihr Datenschutzbeauftragter über ausreichende Sachkenntnis und ist ausreichend unabhängig (Art. 37, 38 DSGVO)?
» Verfügt Ihr Datenschutzbeauftragter über eine Haftpflichtversicherung in ausreichender Höhe?

b. Antwort „Nein“

Sind Sie sicher, dass Sie keinen Datenschutzbeauftragten bestellen müssen?

Ein Datenschutzbeauftragter muss nämlich u. a. in folgenden Fällen bestellt werden:

» Wenn in der Regel mindestens zehn Personen in Ihrem Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG neu).
» Wenn die Kerntätigkeit Ihres Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht (Art. 38 DGSVO).

2. Frage: Verfügt Ihr Unternehmen über ein sogenanntes Ver- zeichnis von Verarbeitungstätigkeiten?

Ein solches Verzeichnis ist eine schriftliche Aufstellung aller Datenverarbeitungsvorgänge in Ihrem Unternehmen. Haben Sie bereits nach altem Recht ein Verfahrensverzeichnis erstellt, können Sie dieses als Grundlage für die Dokumentation verwenden.

a. Antwort „Ja“

Sehr gut. Überprüfen Sie sicherheitshalber noch einmal den Mindestinhalt des Verzeichnisses, den das Gesetz vorschreibt (Art. 30 DSGVO).

DER AUTOR

Die **Kanzlei Dr. Bahr** *(http://www.Dr-Bahr.com)* ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

Ist alles in Ihrer Dokumentation enthalten?

Achten Sie auch darauf, das Verzeichnis stets aktuell zu halten, d. h. bei Änderungen Ihrer Datenverarbeitungsvorgänge ein Update vorzunehmen.

b. Antwort „Nein“

Achtung, es besteht vermutlich dringender Handlungsbedarf! Denn in etwa 99,9 % aller Fälle sind auch Sie verpflichtet, ein solches Verzeichnis zu erstellen.

Art. 30 DSGVO verlangt ein solches Verzeichnis zwar grundsätzlich erst aber einer Mitarbeiteranzahl von 250 Personen. Der Teufel steckt hier aber im Detail!

Eine Verpflichtung besteht nämlich – unabhängig von der Mitarbeiteranzahl – auch dann, wenn die „Datenverarbeitung nicht nur gelegentlich“ erfolgt. Dies bedeutet für die Praxis somit, dass faktisch alle Unternehmen ein Verzeichnis erstellen müssen, denn (fast) alle Firmen werden auf die eine oder andere Art und Weise regelmäßig personenbezogene Daten verarbeiten.

3. Frage: Erbringen Dritte irgendwelche Dienstleistungen für Sie, die in Zusammenhang mit personenbezogenen Daten stehen?

a. Antwort „Ja“

Wenn Dritte Ihre personenbezogenen Daten verwalten, müssen Sie mit diesen eine sogenannte Vereinbarung zur Auftragsdatenverarbeitung (ADV) abschließen. In der Praxis ist in einer Vielzahl von Fällen eine Auftragsdatenverwaltung gegeben, ohne dass dies den Betroffenen überhaupt bewusst ist: in den Fällen der externen Lohn- und Gehaltsabrechnung oder bei der Pflege und Aktualisierung von Datenbeständen durch Dritte, u. a. auch beim Cloud Computing.

Haben Sie z. B. ein Google-Analytics-Konto? Dann müssen Sie auch hier eine ADV-Vereinbarung abschließen. Wenn Sie feststellen, dass Sie eine ADV-Vereinbarung benötigen, besteht dringender Handlungsbedarf!

b. Antwort „Nein“

Sind Sie ganz sicher, dass Dritte keine personenbezogenen Daten von Ihnen erhalten? Hierzu gehören beispielsweise auch Analyse-Dienste wie Google Analytics oder Post-Unternehmen wie DHL oder Hermes. Wenn tatsächlich Dritte keine Daten von Ihnen erhalten, benötigen Sie keinerlei Vereinbarungen zur Auftragsdatenverarbeitung.

4. Frage: Haben Sie Ihre Datenschutzerklärungen den neuen Informationspflichten nach der DSGVO angepasst?

Art. 13 und 14 DSGVO verpflichten Sie als Unternehmer zukünftig zu umfangreichen Informationspflichten (u. a. Zweck der Datenverarbeitung, Rechtsgrundlage, Empfänger/Empfängerkategorien, Zeitdauer der Speicherung, Aufklärung über Rechte, Bestehen eines Beschwerderechts usw.). Wir hatten in unseren beiden bisherigen Artikeln bereits darüber berichtet.

a. Antwort „Ja“

Sehr gut. Überprüfen Sie sicherheitshalber noch einmal den genauen Inhalt der Informationspflichten, die das Gesetz vorschreibt (Art. 13 und 14 DSGVO). Sind tatsächlich sämtliche Punkte in Ihrer Datenschutzerklärung enthalten? Achten Sie auch darauf, die Informationspflichten stets aktuell zu halten, d. h. bei Änderungen Ihrer Datenverarbeitungsvorgänge ein Update vorzunehmen.

b. Antwort „Nein“

Es besteht dringender Handlungsbedarf: Sie müssen zwingend die neuen Informationspflichten umsetzen! Wenn Sie diesen Pflichten nicht nachkommen, handelt es sich hierbei um eine Datenschutzverletzung, die u. a. von der Aufsichtsbehörde mit einer Geldbuße geahndet werden kann.

5. Frage: Haben Sie Ihre Werbe-Einwilligungen (E-Mail, Telefon u. a.) an die neuen Vorgaben nach der DSGVO angepasst?

a. Antwort „Ja“

Sehr gut. Sie müssen zu diesem Punkt nichts weiter unternehmen. Achten Sie noch darauf, die Einwilligungserklärungen stets aktuell zu halten, d. h. bei Änderungen Ihrer Datenverarbeitungsvorgänge ein Update vorzunehmen.

b. Antwort „Nein“

Es besteht dringender Handlungsbedarf: Sie müssen zwingend Ihre Werbe-Einwilligungen anpassen! Wenn Sie diesen Pflichten nicht nachkommen, handelt es sich hierbei um eine Datenschutzverletzung, die u. a. von der Aufsichtsbehörde mit einer Geldbuße geahndet werden kann.

6. Frage: Haben Sie ein Verfahren installiert, um Betroffenen rechtzeitig und umfassend die gewünschte Auskunft zukommen zu lassen?

Art. 15 DSGVO verpflichtet Sie, in Ihrem Unternehmen Sorge dafür zu tragen, dass Personen, die von Ihnen wissen wollen, welche Daten über sie bei Ihnen gespeichert sind, zeitnah eine Antwort von Ihnen erhalten.

a. Antwort „Ja“

Sehr gut. Sie müssen zu diesem Punkt nichts weiter unternehmen. Achten Sie noch darauf, das Verfahren zur Auskunftserteilung stets aktuell zu halten, d. h. bei Änderungen Ihrer Datenverarbeitungsvorgänge ein Update vorzunehmen.

b. Antwort „Nein“

Es besteht dringender Handlungsbedarf: Sie müssen zwingend ein Verfahren zur Auskunftserteilung festlegen! Wenn Sie dieser Pflicht nicht nachkommen, handelt es sich hierbei um eine Datenschutzverletzung, die u. a. von der Aufsichtsbehörde mit einer Geldbuße geahndet werden kann.

7. Frage: Haben Sie ein Datenschutz-Management-System eingeführt?

Das neue Gesetz verwendet zwar den Begriff „Datenschutz-Management-System“ nicht, inhaltlich ist jedoch genau das damit gemeint: Sie als Unternehmer sind zukünftig verpflichtet nachzuweisen, dass die Verarbeitung der personenbezogenen Daten in Ihrem Hause rechtlich einwandfrei geschieht, d. h. es trifft Sie eine umfassende Rechenschaftspflicht.

a. Antwort „Ja“

Sehr gut. Überprüfen Sie sicherheitshalber noch einmal, ob Ihr Datenschutz-Management-System tatsächlich alle Eventualitäten und Umstände berücksichtigt. Haben Sie insbesondere die unterschiedlichen Fachabteilungen Ihres Unternehmens zurate gezogen und sich dort über alle denkbaren Konstellationen informieren lassen?

Achten Sie auch darauf, das Datenschutz-Management-System stets aktuell zu halten, d. h. bei Änderungen Ihrer Datenverarbeitungsvorgänge ein Update vorzunehmen.

b. Antwort „Nein“

Es besteht dringender Handlungsbedarf: Sie müssen zwingend ein Datenschutz-Management-System einrichten! Wie in den beiden bisherigen Artikeln erläutert, trifft Sie die volle Nachweispflicht.

Wenn Sie dieser nicht nachkommen, handelt es sich hierbei um eine Datenschutzverletzung, die u. a. von der Aufsichtsbehörde mit einer Geldbuße geahndet werden kann.

8. Frage: Haben Sie Ihre Datensicherheit an den aktuellen Status quo angepasst?

Gemeint ist: Haben Sie alle technischen Sicherheitsmaßnahmen (z. B. Firewall, Passwörter, Verschlüsselung) an die derzeit geltenden technischen Standards angepasst?

a. Antwort „Ja“

Sehr gut. Überprüfen Sie zukünftig in regelmäßigen, wiederkehrenden Abständen, ob Ihre Datensicherheit noch dem aktuellen Status quo entspricht. Ziehen Sie hier insbesondere externes Technik-Know-how zurate.

b. Antwort „Nein“

Es besteht dringender Handlungsbedarf: Sie müssen zwingend die Datensicherheit an den aktuellen Status quo anpassen! Wenn Sie dieser Pflicht nicht nachkommen, handelt es sich hierbei um eine Datenschutzverletzung, die u. a. von der Aufsichtsbehörde mit einer Geldbuße geahndet werden kann. ¶

DIE CHECK-UP-LISTE IM ÜBERBLICK:

1. Frage: Ist in Ihrem Unternehmen bereits ein Datenschutzbeauftragter bestellt?
2. Frage: Verfügt Ihr Unternehmen über ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten?
3. Frage: Erbringen Dritte irgendwelche Dienstleistungen für Sie, die in Zusammenhang mit personenbezogenen Daten stehen?
4. Frage: Haben Sie Ihre Datenschutzerklärungen den neuen Informationspflichten nach der DSGVO angepasst?
5. Frage: Haben Sie Ihre Werbe-Einwilligungen (E-Mail, Telefon u. a.) an die neuen Vorgaben nach der DSGVO angepasst?
6. Frage: Haben Sie ein Verfahren installiert, um Betroffenen rechtzeitig und umfassend die gewünschte Auskunft zukommen zu lassen?
7. Frage: Haben Sie ein Datenschutz-Management-System eingeführt?
8. Frage: Haben Sie Ihre Datensicherheit an den aktuellen Status quo angepasst?

Einen ausführlicheren interaktiven Check-up – natürlich kostenlos und anonym – bietet der Autor auf der Webseite **www.DSGVO-Checkup.de** an.