Handelsverband Bayern
HBE

PraxisWISSEN

Datenschutz-Grundverordnung: Quick-Check

Handelsverband Bayern e. V.
Brienner Straße 45
80333 München

Dr. Melanie Eykmann
Rechtsanwältin
(Syndikusrechtsanwältin)
Telefon 089 55118-124
Fax 089 55118-118
E-Mail eykmann@hv-bayern.de
Internet www.hv-bayern.de

Stand 01/2019

1. Vorbemerkung

Am 25. Mai 2018 ist die neue EU-Datenschutzgrundverordnung (DS-GVO) in Kraft getreten. Sie ist damit in allen Mitgliedsstaaten der EU unmittelbar anwendbares Recht. Seit diesem Zeitpunkt gilt parallel auch das neue Bundesdatenschutzgesetz (BDSG n. F.), in dem der deutsche Gesetzgeber die Vorgaben der DS-GVO, soweit zulässig, konkretisiert hat.

Hierdurch ergeben sich vielfältige neue Anforderungen in Bezug auf alle datenschutzrechtlichen Aspekte, insbesondere im Rahmen der Verarbeitung personenbezogener Daten. Betroffen sind nicht nur der Umgang mit Kunden- und Arbeitnehmerdaten, sondern z. B. auch die technischen Aspekte der Datensicherheit.

Um Ihnen den Einstieg in diese hochkomplexe Materie zu erleichtern, haben wir mit diesem Praxiswissen eine Art Checkliste für Ihren Einstieg in die neuen datenschutzrechtlichen Bestimmungen erarbeitet.

2. Verantwortung und Pflichten

In Unternehmen müssen zwingend die Verantwortlichkeiten für die Einhaltung der datenschutzrechtlichen Vorschriften geregelt werden. Der oder die Verantwortliche ist gegenüber den Auskunftsbehörden rechenschaftspflichtig und muss die Einhaltung des Datenschutzrechts nachweisen. Die Verantwortung für die Einhaltung des Datenschutzrechts liegt daher zunächst immer bei der Geschäftsführung. Allerdings kann - abhängig von der Unternehmensgröße - eine weitere Person benannt werden, die neben der Geschäftsführung für die Umsetzung der neuen Vorschriften zuständig ist. Es kann auch ein Team gebildet werden, das aus Beschäftigten aller betroffenen Bereiche (z. B. Personalabteilung, Marketing, IT) besteht oder alternativ eine externe Beratung in Anspruch genommen werden.

Die wichtigsten Pflichten des Verantwortlichen sind:

- Führung und laufende Aktualisierung eines Verzeichnisses von Verarbeitungstätigkeiten, Art. 30 DS-GVO
- Prüfung der Erforderlichkeit eines Datenschutzbeauftragten, Art. 37 ff. DS-GVO
- Ggf. Bestellung eines Datenschutzbeauftragten, Art. 37 ff. DS-GVO
- Abschluss von Verträgen mit Auftragsverarbeitern, Art. 28 DS-GVO
- Durchführung einer Datenschutzfolgenabschätzung in bestimmten Fällen, z. B. bei Einsatz einer Videoüberwachung, Art. 35 DS-GVO
- Meldepflicht für Datenschutzverstöße innerhalb von 72 Stunden an die Aufsichtsbehörde, Art. 33 DS-GVO
- Festlegung technischer und organisatorischer Maßnahmen, um im Hinblick auf die Sicherheit der Verarbeitung ein angemessenes Schutzniveau zu erreichen, Art. 32 DS-GVO

3. Informationspflichten und Betroffenenrechte

Die DS-GVO hat die Informationspflichten im Zusammenhang mit der Erhebung und Verarbeitung von Daten stark ausgeweitet. Dadurch sind viele Formulare und Datenschutzerklärungen sowie verwendete Muster auf die jeweilige Datenverarbeitung anzupassen. Wenn die Daten beim Betroffenen erhoben werden, müssen die Informationen zum Zeitpunkt der Datenerhebung zur Verfügung gestellt werden, Art. 13 DS-GVO. Wenn die Daten nicht direkt beim Betroffenen erhoben werden, ist dieser innerhalb einer angemessenen Frist spätestens innerhalb eines Monats nach der Datenerhebung zu informieren, Art. 14 DS-GVO.

Darüber hinaus haben betroffene Person folgende Rechte:

- Recht auf Auskunft, Art. 15 DS-GVO
- Recht auf Berichtigung, Art. 16 DS-GVO
- Recht auf Löschung, Art. 17 DS-GVO
- Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO
- Recht auf Datenübertragbarkeit, Art. 20 DS-GVO
- Widerspruchsrecht, Art. 21 DS-GVO

4. Rechtsgrundlagen für die Datenverarbeitung

Für jede Verarbeitung personenbezogener Daten muss eine Rechtsgrundlage bestehen, die die Datenverarbeitung erlaubt. Ansonsten ist die Verarbeitung rechtswidrig. Die wichtigsten Rechtsgrundlagen für eine Datenverarbeitung sind folgende:

- Die Verarbeitung ist für die Vertragsdurchführung mit der betroffenen Person erforderlich (z. B. Abwicklung des Kaufvertrags, Art. 6 Abs. 1 b) DS-GVO
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt (z. B. steuerliche Aufbewahrungspflichten), Art. 6 Abs. 1 c) DS-GVO
- Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich um ein Kind handelt, Art. 6 Abs. 1 f) DS-GVO
- Die betroffene Person hat eingewilligt, Art. 6 Abs. 1 a), Art. 7 f. DS-GVO
- Eine Rechtsgrundlage für die Datenverarbeitung kann sich im Bereich des Beschäftigtendatenschutzes auch aus einer Kollektivvereinbarung (z. B. Betriebsvereinbarung) ergeben, Art. 88 DS-GVO, § 26 BDSG n. F.

Eine Weiterverarbeitung zu einem anderen Zweck als dem Zweck der ursprünglichen Datenerhebung (nachträgliche Zweckänderung) ist nur unter den engen Voraussetzungen des Art. 6 Abs. 4 DS-GVO zulässig.

5. Wichtige Schritte zur Umsetzung

Die wichtigsten Schritte zur Umsetzung der DS-GVO sind aufzulisten wie folgt:

a) Datenschutz ist Chefsache – die Geschäftsführung sollte sich mit dem Thema „Umsetzung der DS-GVO“ befassen. Abhängig von der Unternehmensgröße sollte eine Person benannt werden, die neben der Geschäftsführung für die Umsetzung der neuen Vorschriften zuständig ist. Es kann ein Team gebildet werden, das aus Beschäftigten aller betroffenen Bereiche (z. B. Personalabteilung, Marketing, IT) besteht. Alternativ kann eine externe Beratung in Anspruch genommen werden.

b) Identifizieren Sie alle Verfahren und Prozesse, bei denen personenbezogene Daten verarbeitet werden. Relevant sind dabei folgende Fragen:

   - Wie heißt das Verfahren?
   - Wer ist im Unternehmen verantwortlich für einen Geschäftsprozess/eine Verarbeitungstätigkeit?
   - Welcher Zweck wird mit der Verarbeitung verfolgt?
   - Welche Arten von Daten werden erhoben (z. B. Name, Adresse etc.)?
   - Wie heißt der Kreis der Betroffenen (z. B. Kunden?)
   - Woher kommen die Daten?
   - Werden die Daten weitergegeben? Wenn ja, an wen?
   - Welche technisch-organisatorischen Maßnahmen zur Sicherheit der Verarbeitung werden eingesetzt (z. B. Passwörter, Berechtigungen, Verschlüsselung

etc.)? Welche IT kommt zum Einsatz?
- Wann werden die Daten gelöscht?
- Welche Dienstleister sind beteiligt?

c) Die Antworten auf diese Fragen bilden die Grundlage für ein Verzeichnis von Verarbeitungstätigkeiten.

d) Prüfen Sie, ob für jede Verarbeitung eine Rechtsgrundlage besteht. Wenn die Datenverarbeitung auf der Einwilligung basiert, muss das Einwilligungsformular den Anforderungen der DS-GVO entsprechen (Informationspflichten und Hinweis auf jederzeitige Widerrufsmöglichkeit der Einwilligung beachten).

e) Informationspflichten – bei allen Verarbeitungen muss zum richtigen Zeitpunkt über alle in Art. 13 und 14 DS-GVO genannten Punkte informiert werden.

f) Betroffenenrechte – Erstellen Sie einen Prozess, der es Ihnen ermöglicht, insbesondere Auskunftsbegehren, z. B. von Kunden oder abgelehnten Bewerbern, vollständig zu beantworten. Erstellen Sie Löschkonzepte und setzen Sie dies in der Praxis um.

g) Prüfen Sie, ob Sie einen Datenschutzbeauftragten benötigen und wenn ja, ob Sie einen internen oder externen Datenschutzbeauftragten benennen wollen.
Achtung: Der Datenschutzbeauftragte ist nicht mehr für die operative Umsetzung, sondern für die Kontrolle und Beratung des Verantwortlichen zuständig.

i) Prüfen Sie, ob Verarbeitungen voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten betroffener Person verbunden sind. Dann ist eine Datenschutzfolgenabschätzung durchzuführen (z. B. bei der Videoüberwachung).

j) Sind bei einer Videoüberwachung die Kennzeichnung und die erforderlichen Informationen zum frühestmöglichen Zeitpunkt angebracht?

k) Prüfen Sie, ob Daten bei Dienstleistern verarbeitet werden. Es kann sich um eine Auftragsdatenverarbeitung handeln. Prüfen Sie, ob die Verträge zur Auftragsdatenverarbeitung aktuell sind und den Anforderungen der DS-GVO genügen und ob Anweisungen gegenüber Auftragsverarbeitern dokumentiert werden.

l) Prüfen Sie, ob technisch-organisatorische Maßnahmen getroffen und ausreichend sind, um ein angemessenes Schutzniveau zu gewährleisten.

m) Stellen Sie sicher, dass Sie einen Datenschutzverstoß innerhalb von 72 Stunden der Aufsichtsbehörde melden können.

n) Informieren Sie alle mit Datenverarbeitungsvorgängen befasste Mitarbeiter über die jeweilige Änderung bei den von ihnen durchzuführenden Tätigkeiten.

o) Nur wenn Sie alle Schritte zur Einhaltung der DS-GVO dokumentieren, können Sie dies gegenüber der Aufsichtsbehörde nachweisen.

6. Checkliste

Sofern Sie im Quick-Check nachfolgende Aufgaben bereits umgesetzt haben, befinden Sie sich auf einem guten Weg. Anderenfalls sollten folgende Punkte umgehend umgesetzt werden:

- Überarbeitung der Datenschutzerklärung auf der Website
- Einwilligungserklärung für Fotos auf der Website
- Erstellung von Verarbeitungsverzeichnissen
- Vertragsschluss mit Auftragsverarbeitern
- Bestellung eines Datenschutzbeauftragten (falls erforderlich)
- Überprüfung des Umgangs mit Kundendaten
- Umsetzung der wichtigsten Regelungen im Beschäftigtendatenschutz
  - Informationserteilung zur Datenverarbeitung im Beschäftigungsverhältnis
  - Unterzeichnung der Verpflichtungserklärung auf den Datenschutz von Beschäftigten

Für sämtliche hier angesprochenen Punkte stellt der HBE Muster bzw. sonstige Hilfestellungen zur Verfügung. Diese können über unsere Homepage oder bei Ihrer zuständigen Bezirksgeschäftsstelle abgefragt werden können.

7. Übersicht Praxiswissen

Zu allen weiteren angesprochenen Punkten stellen wir Ihnen ebenfalls gesonderte Praxiswissen zur Verfügung, denen Sie weitergehende detaillierte Informationen entnehmen können. Zur besseren Übersichtlichkeit listen wir Ihnen diese nochmals wie folgt auf:

1. Videoüberwachung, Art. 6 Abs. 1 f) DS-GVO, § 4 BDSG n. F.
2. Weiterverarbeitung der Daten zu einem anderen Zweck, Art. 6 Abs. 4 DS-GVO
3. Einwilligung, Art. 7 DS-GVO
4. Informationspflichten, Art. 13 DS-GVO
5. Informationspflichten, Art. 14 DS-GVO
6. Recht auf Auskunft, Art. 15 DS-GVO
7. Recht auf Berichtigung, Art. 16 DS-GVO
8 Recht auf Löschung, Art. 17 DS-GVO
9. Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO
10. Recht auf Datenübertragbarkeit, Art. 20 DS-GVO
11. Recht auf Widerspruch, Art. 21 DS-GVO
13. Auftragsdatenverarbeitung, Art. 28 DS-GVO
13. Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO
14. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DS-GVO
15. Datenschutzfolgenabschätzung, Art. 35 DS-GVO
16. Datenschutzbeauftragter – Benennung und Stellung, Art. 37 DS-GVO
17. Datenschutzbeauftragter – Aufgaben, Art. 39 DS-GVO
18. Wichtige Änderungen beim Arbeitnehmerdatenschutz, Art. 88 DS-GVO, § 26 BDSG n. F.

Für weitere Informationen stehen wir Ihnen gern zur Verfügung. Ihre Ansprechpartner in den HBE-Geschäftsstellen finden Sie unter www.hv-bayern.de