Datenschutz

Die DSGVO und was sie von uns will

BTK | BELTLE THEADO KANZLEI

Vorstellung

Selbständiger Rechtsanwalt seit dem Jahr 2010

Tätig im Bereich Urheber- und Medienrecht, gewerblicher Rechtsschutz und vor allem auch Datenschutz

Externer Datenschutzbeauftragter seit 2013

BTK | BELTLE THEADO KANZLEI

Übersicht

Die DSGVO gilt sein dem 25.05.2018

Was hat sich geändert?

Was muss ich beachten?

BTK | BELTLE THEADO KANZLEI

Hintergrund zur aktuellen Debatte

Ziel der DSGVO war/ist die weitgehende **Vereinheitlichung** des Datenschutzrechtes in den EU Mitgliedstaaten.

Die DSGVO ist **unmittelbar geltendes Recht**. Ergänzend gilt in Deutschland das Bundesdatenschutzgesetz (kurz: **BDSG**).

Hintergrund zur aktuellen Debatte

Die Ziele der DSGVO sind primär

- der **Schutz der Grundrechte und Grundfreiheiten** natürlicher Personen und insbesondere deren
  Recht auf Schutz personenbezogener Daten und

- der **freie Verkehr** personenbezogener Daten.

Hintergrund zur aktuellen Debatte

Diese Ziele sollen durch die in Art. 5 DSGVO festgelegten **Grundsätze der Verarbeitung** personenbezogener Daten erreicht werden, zu denen u.a. zählen:

Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit und Speicherbegrenzung (Löschung).

Hintergrund zur aktuellen Debatte

Besonderes Augenmerk legt die DSGVO auch auf die **Integrität und Vertraulichkeit** (Sicherheit) von IT-Systemen sowie auf die **Rechenschaftspflicht** der Personen, welche personenbezogene Daten verarbeiten (Verantwortlichkeit für die Einhaltung der rechtmäßigen Datenverarbeitung).

Vieles ändert sich – oder doch nicht?

Viele Grundsätze, die bereits im Datenschutz Gültigkeit hatten, sind auch mit Geltung der DSGVO vorgesehen und bleiben somit erhalten.

Hierzu zählen u. a. die Grundsätze des **Verbots mit Erlaubnisvorbehalt** (Datenverarbeitung ist nur zulässig, wenn entweder der Betroffene darin einwilligt oder das Gesetz sonst wie die Verarbeitung erlaubt).

Vieles ändert sich – oder doch nicht?

Im Folgenden sind einige der wichtigsten Punkte aufgezählt, die es zu beachten gilt:

1. Bestellung eines Datenschutzbeauftragten

Ein Betrieb muss immer dann einen Datenschutzbeauftragten bestellen, wenn in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Daneben gibt es auch andere Fälle, wann unabhängig von der Personenzahl ein DSB bestellt werden muss.

1. Bestellung eines Datenschutzbeauftragten

Wie bisher ist es nicht möglich, dass die Geschäftsführung die Funktion des Datenschutzbeauftragten übernimmt, da der Datenschutzbeauftragte eine gewisse **Unabhängigkeit** haben soll.

Der Datenschutzbeauftragte ist gemäß Art. 37 Abs. 8 DSGVO der jeweiligen zuständigen Aufsichtsbehörde zu **melden**.

2. Führen eines Verarbeitungsverzeichnisses

Das frühere öffentliche Verfahrensverzeichnis („Jedermanns-Verfahrensverzeichnis“) wurde abgeschafft.

Hingegen findet man das frühere Verfahrensverzeichnis in modifizierter Form und unter dem Begriff „Verarbeitungsverzeichnis“ bzw. „**Übersicht über die Verarbeitungstätigkeiten**“ wieder.

2. Führen eines Verarbeitungsverzeichnisses

In diesem Verarbeitungsverzeichnis müssen **sämtliche Prozesse**, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten bestehen, aufgeführt und genau beschrieben werden.

Unter Umständen kann auf die Führung eines solchen Verzeichnisses verzichtet werden.

3. Aufbau eines Datenschutzmanagementsystems

Neben dem angesprochenen Verzeichnis von Verarbeitungstätigkeiten findet sich in der DSGVO eine Vielzahl von Normen, die eine **Dokumentation** der getroffenen Datenschutzmaßnahmen (TOM) fordern.

Daneben schafft die DSGVO weitere Prozesse, die etabliert, und Aufgaben die wahrgenommen werden müssen.

4. Informationspflichten

Wenn personenbezogene Daten erhoben werden, muss die betroffene Person – sofern sie die Informationen nicht bereits kennt – über gewisse Umstände **informiert** werden.

Die Information muss „**im Zeitpunkt der Datenerhebung**“ erfolgen.

Die Information umfasst etwa:

4. Informationspflichten

- Name und Kontaktdaten des Verantwortlichen
- Zwecke, zu denen die Daten verarbeitet werden + Rechtsgrundlage
- Ggfs. Nennung der berechtigten Interessen
- Ggfs. Nennung von Empfängern bzw. Empfängerkategorien
- Ggfs. Übermittlungen in Drittländer
- Hinweise auf Betroffenenrechte, Beschwerderecht etc.
- Dauer der Speicherung bzw. Kriterien, wann gelöscht wird

5. Schutz besonderer Kategorien personenbezogener Daten

Besondere Anforderungen und Sicherheitsmaßnahmen sind zu treffen und zu belegen, wenn besondere Kategorien personenbezogener Daten verarbeitet werden.

Darunter fallen etwa **Daten der Gesundheit**, zur ethnischen Herkunft oder zur Religion.

Bei dieser Verarbeitung ist auf jeden Fall zuvor eine **Datenschutzfolgenabschätzung** (bisher: „Vorabkontrolle“) durchzuführen.

Gleiches gilt auch bei der **Einführung kritischer Verfahren** (z. B. großräumige Videoüberwachung, Scoring usw.)

6. Auftragsdatenverarbeitung

Verträge zur Auftragsverarbeitung (früher: Auftragsdatenverarbeitung) können nicht nur schriftlich, sondern auch **elektronisch** abgeschlossen werden.

Es gilt vor allem zu prüfen, inwieweit **Dritte** (Dienstleister) eingesetzt werden, um personenbezogene Daten zu verarbeiten.

Hier sind vor allem die Hoster der Internetauftritte zu berücksichtigen, IT-Dienstleister, Daten- und Aktenvernichter oder z. B. die Auslagerung von Diensten wie Seminaranmeldungen.

7. Das Recht auf Vergessenwerden

Das Recht auf Löschung wird in der DSGVO um das Recht auf Vergessenwerden erweitert, was insbesondere Bedeutung erlangt, wenn **personenbezogene Daten öffentlich** (z. B. auf der Website) gemacht wurden.

7. Das Recht auf Vergessenwerden

Zukünftig hat der Betrieb **unter Berücksichtigung der verfügbaren Technologie und der Kosten angemessene Maßnahmen** zu treffen, um darüber zu informieren, dass eine betroffene Person die Löschung aller Links zu diesen personenbezogenen Daten etc. verlangt hat.

8. Das Recht auf Datenübertragbarkeit

Den Kunden oder auch Beschäftigten müssen auf Wunsch deren Daten **elektronisch in einem einfachen maschinenlesbaren Format** zur Verfügung gestellt werden.

Damit soll der Wechsel eines Mitarbeiters oder Kunden vereinfacht werden und beim neuen Arbeitgeber oder Auftraggeber können die Stammdaten elektronisch eingespielt werden.

9. Bußgelder und Sanktionen

Die Geldbußen, welche für Datenschutzverstöße verhängt werden können, sind gestiegen.

Für Verstöße können nunmehr Bußgelder bis 10 Mio. Euro verhängt werden, bei schweren Verstößen bis zu 20 Mio. Euro.

Dies sind jedoch äußerste Grenzen.

Zudem können Datenschutzverstöße strafbar sein.

10. Sonstige Änderungen

Daneben finden sich an den unterschiedlichen Stellen in der DSGVO weitere Grundsätze wie z. B. **Privacy by design** und **Privacy by default**, was etwa bei der Programmierung oder Einführung einer neuen Verwaltungssoftware oder Homepage beachtet werden muss.

BTK | BELTLE THEADO KANZLEI

Checkliste

Ist mein Betrieb datenschutzkonform?

BTK | BELTLE THEADO KANZLEI

1. Beachtung des Datenschutzes

- Gibt es ein Bewusstsein, insbesondere innerhalb der Geschäftsführung, dass und welche Bedeutung der Datenschutz hat?
- Gibt es hierzu Dokumentationen? Namentlich:
  - Risikoeinschätzung und Beschreibung der Datenschutzziele
  - Eine Datenschutzrichtlinie
  - Regelungen zu Verantwortlichkeiten
- Muss ein Datenschutzbeauftragter bestellt werden (10 und mehr Personen, die automatisiert Daten verarbeiten)?
- Wenn ja, wer ist zum Datenschutzbeauftragten bestellt und verfügt die Person über hinreichende Fachkenntnis und Unabhängigkeit?

2. Übersicht über Verarbeitung

- Gibt es ein Verzeichnis der Verarbeitungstätigkeiten des Vereins?
  Muster und weitere Infos beispielhaft:
  https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
- Wird sichergestellt, dass Datenschutz bei Beginn oder Änderung eines jeden Prozesses Berücksichtigung findet?

BTK | BELTLE THEADO KANZLEI

3. Einbindung Externer

- Werden Externe zur Erledigung der Arbeiten (Auftragsverarbeiter) eingebunden?
- Wenn ja, gibt es eine Übersicht über die Auftragsverarbeiter?
- Sind Auftragsverarbeitungsvereinbarungen geschlossen worden und dokumentiert?
- Finden Datenübermittlungen in nicht-europäische Länder statt? Sind entsprechende Maßnahmen (Art. 44 DSGVO) gewährleistet?

4. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

- Sind Texte zur **datenschutzrechtlichen Information** der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 DSGVO angepasst?
- Ist gewährleistet, dass Anträge von betroffenen Personen auf **Auskunft** zu den eigenen Daten (Art. 15 DSGVO) zeitnah und vollständig erfüllt werden?

5. Verantwortlichkeit, Umgang mit Risiken

- Gibt es für jede Verarbeitungstätigkeit eine **Rechtsgrundlage**?
- Haben Sie geprüft, ob die **Einwilligungen**, auf die Sie eine Verarbeitung stützen, noch den Voraussetzungen der Art. 7 f. DSGVO entsprechen?
- Können Sie das Vorliegen der **Einwilligung nachweisen** (Auch z.B. für die Nutzung von Mitgliederfotos auf Homepage etc.)?
- Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DSGVO erfolgt, insbesondere mit Blick auf die Sicherheit der Verarbeitung (**Dokumentation technisch-organisatorischer Maßnahmen**)?

6. Datenschutzverletzungen

- Haben Sie sichergestellt, dass die **Meldung von Verletzungen** des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist? (Art. 33 DSGVO)
- Haben Sie einen Prozess aufgesetzt, wie mit potentiellen Verletzungen intern umzugehen ist?
- Haben Sie festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?

Thanks for watching the show!

BTK | BELTLE THEADO KANZLEI