EU-DATENSCHUTZGRUNDVERORDNUNG - DER COUNTDOWN LÄUFT

Checkliste für Eilige

Nur noch wenige Wochen, bis am 25. Mai 2018 die EU-Datenschutzgrundverordnung (DSGVO) in Kraft tritt. Bis dahin müssen Unternehmen, Selbständige und Vereine die neuen Datenschutzregeln umsetzen. Anderenfalls drohen kostenpflichtige Abmahnungen von Mitbewerbern und Abmahnvereinen und Bußgelder von den Datenschutzbehörden in Höhe von bis zu 4 Prozent des weltweiten Jahresumsatzes oder von bis zu 20 Millionen €. Betroffen sind alle, die personenbezogene Daten verarbeiten, wozu auch Telefonnummern und E-Mails gehören, so dass faktisch jedes Unternehmen, jeder Selbständige und jeder Verein betroffen ist.

Was ist konkret zu tun? Hier eine kurze Checkliste für Eilige - ohne Anspruch auf Vollständigkeit:

1. Datenschutzerklärung auf der eigenen Webseite ergänzen

Die betroffenen Personen, z.B. die Besucher einer Webseite, müssen umfangreicher als bisher darüber informiert werden, wer, wie, wann und wo ihre Daten speichert und welche Rechte sie diesbezüglich haben. Daher muss eine bestehende Datenschutzerklärung auf der Webseite entsprechend ergänzt bzw. neu gestaltet werden. Die erforderlichen Informationen müssen präzise, transparent, verständlich und leicht zugänglich sein. Wichtig: Viele der im Internet erhältlichen kostenlosen Generatoren zur Erstellung von Datenschutzerklärungen sind noch nicht auf dem neuesten Stand. Andererseits lässt die „Abmahn-Industrie“ bereits Crawler programmieren, die das Internet systematisch nach fehlerhaften Datenschutzerklärungen durchsuchen, um ab 25.05.2018 die ersten Abmahnwellen zu starten.

Eine rechtskonforme Datenschutzerklärung muss den Betroffenen folgende Informationen zur Verfügung stellen:

- Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls das nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

- Belehrung darüber, dass der Betroffene folgende Rechte bezüglich seiner Daten hat: Auskunftsrecht, Recht auf Berichtigung oder Löschung, Recht auf Einschränkung der Verarbeitung, Widerspruchsrecht gegen die Verarbeitung, Recht auf Datenübertragbarkeit
- falls die Datenverarbeitung auf einer Einwilligung des Betroffenen, zum Beispiel Kunden, beruht, muss ein gesonderter Hinweis darauf erfolgen, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt
- Aufklärung über das Beschwerderecht bei der Aufsichtsbehörde
- Information darüber, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und ob die betreffende Person verpflichtet ist, die Daten bereitzustellen und welche Folgen eine Weigerung hätte
- falls eine automatisierte Entscheidung im Einzelfall getroffen werden soll oder eine andere Profiling-Maßnahme stattfinden soll, muss der Betroffene über deren Tragweite, Logik und Algorithmus informiert werden
- wer einen Datenschutzbeauftragten hat, muss diesen mit seinen Kontaktdaten auf seiner Homepage benennen

2. Auftragsverarbeitungsverträge abschließen

Fast jedes Unternehmen hat einen externen IT-Dienstleister, dem Einblick in die eigene Datenhaltung mit personenbezogenen Daten gewährt wird und der daher "Auftragsverarbeiteter" im Sinne der Datenschutzgrundverordnung ist. Wer einen externen IT-Dienstleister/Auftragsverarbeiter einschalten möchte, muss vorher prüfen, ob dieser datenschutzkonform arbeitet. Mit dem externen IT-Dienstleister/Auftragsverarbeiter muss ein schriftlicher Vertrag abgeschlossen werden, mit dem sich der Auftraggeber umfassende Kontrollrechte einräumen lassen muss. Die GDD - Gesellschaft für Datenschutz und Datensicherheit e.V. stellt auf ihrer Webseite unter folgendem Link ein Muster für eine Auftragsverarbeitung zur Verfügung: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf.

3. Für IT-Sicherheit sorgen

Beispielsweise muss jeder, der auf seiner Webseite ein Kontaktformular anbietet, HTTPS als Transportverschlüsselung verwenden. Wer mobile Geräte, wie z.B. Smartphones, Tablets oder Notebooks, verwendet, auf denen personenbezogene Daten gespeichert sind, muss diese neben dem Kennwort zum Entsperren des Nutzer-Accounts auch mit einer Datenträgerverschlüsselung ausstatten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt hierfür z.B. das kostenfreie Produkt VeraCrypt, s. https://veracrypt.codeplex.com. Bei der Verwendung von Cloud-Diensten sollten personenbezogene Daten vor dem Versenden verschlüsselt werden, so dass der Cloud-Anbieter keine Zugriffsmöglichkeit auf diese Daten hat. Die regelmäßige Durchführung von Backups zur Abwehr von Schadsoftware ist Pflicht. Unter dem Link https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Ueberblick-IT-Grundschutz.pdf?__blob=publicationFile&v=4 stellt das BSI einen Überblick über die Anforderungen an einen IT-Grundschutz als Entscheidungshilfe zur Verfügung.

4. Verzeichnis von Verarbeitungstätigkeiten erstellen

Jeder, der personenbezogene Daten verarbeitet oder speichert, muss ein Verzeichnis von Verarbeitungstätigkeiten erstellen, in dem Folgendes dokumentiert werden muss.

- Name und die Kontaktdaten des Verantwortlichen, ggfs. auch Vertreter und Datenschutzbeauftragte
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
- wenn möglich, vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM)

Das Bayerisches Landesamt für Datenschutzaufsicht stellt auf seiner Webseite Musterverzeichnisse für Verarbeitungstätigkeiten für verschiedene Branchen zur Verfügung: https://www.lda.bayern.de/de/kleine-unternehmen.html.

Natürlich muss bei der Erstellung des Verfahrensverzeichnisses auch geprüft werden, ob die dokumentierte Datenverarbeitung rechtmäßig erfolgt. Das Verzeichnis muss stets aktuell sein und ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

5. Datenschutzbeauftragten benennen

Wer in seinem Unternehmen oder Verein mindestens 10 Personen damit beschäftigt, personenbezogene Daten automatisiert zu verarbeiten, muss einen internen oder externen Datenschutzbeauftragten benennen. Das Gleiche gilt für Unternehmen oder Vereine, die im Rahmen einer Kerntätigkeit besonders sensible Daten verarbeiten, zum Beispiel Gesundheitsdaten. Die Benennung sollte aus Beweisgründen schriftlich erfolgen. Die Kontaktdaten des Datenschutzbeauftragten müssen der Aufsichtsbehörde mitgeteilt werden.

6. Betriebsvereinbarung anpassen oder ergänzen

Wer einen Betriebsrat hat, sollte prüfen, ob die bestehenden Betriebsvereinbarungen (auch) Datenverarbeitungsvorgänge regeln, zum Beispiel Vereinbarungen betreffend bring your own device (BYOD) enthalten. Wenn dies der Fall ist, müsste geprüft werden, ob die bestehenden Regelungen den Vorgaben der EU-Datenschutzgrundverordnung entsprechen. Möglicherweise ist es sinnvoll, eine Rahmen-Betriebsvereinbarung abzuschließen, zum Beispiel hinsichtlich der allgemeinen Informationspflichten des Arbeitgebers. Das ist wichtig, weil anderenfalls auch Beweisverwertungsverbote drohen: Datenerhebungen, die nicht im Einklang mit der EU-Datenschutzgrundverordnung stehen, können in Kündigungsschutzverfahren möglicherweise nicht zur Rechtfertigung von Kündigungen angeführt werden.

7. Datenschutz-Folgeabschätzung vornehmen

Für besonders risikobehaftete Datenverarbeitungen muss mittels einer Risikoanalyse festgestellt werden, ob eine sogenannte Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist, z.B. in folgenden Fällen:

- bei systematischer und umfassender Bewertung persönlicher Aspekte von Personen auf Grundlage automatisierter Datenverarbeitung, einschließlich Profiling
- bei umfangreicher Verarbeitung sensitiver Daten, zum Beispiel politischer Meinungen, religiöser oder weltanschaulicher Überzeugungen und Daten über Straftaten
- bei systematischer weiträumiger Überwachung öffentlich zugänglicher Bereiche

Auf Aufforderung einer Aufsichtsbehörde müssen Datenverantwortliche nachweisen können, dass sie alle Datenschutzregeln einhalten.

8. Fazit

Obwohl einige Einzelfragen in Bezug auf die Umsetzung der EU-Datenschutzgrundverordnung immer noch nicht abschließend geklärt sind, sollte jedes Unternehmen, jeder Selbständige und jeder Verein, der personenbezogene

Daten verarbeitet, dafür Sorge tragen, dass er alle Anforderung der DSGVO bis zum 25. Mai 2018 erfüllt.

Literaturtipp: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine - Das Sofortmaßnahmen-Paket, herausgegeben vom Bayerischen Landesamt für Datenschutzaufsicht, C. H. Beck Verlag, 5,50 €

VON THÜNGEN-REICHENBACH
RECHTSANWÄLTIN | FACHANWÄLTIN

Rechtsanwältin Gabriele Freifrau von Thüngen-Reichenbach ist Fachanwältin für gewerblichen Rechtschutz, für Urheber- und Medienrecht und für IT-Recht in Coburg und hat sich auf die Beratung von Unternehmen und Selbständigen spezialisiert. Sie berät und unterstützt ihre Mandanten bei der Vertragsgestaltung, der rechtskonformen Gestaltung ihrer Webseiten, der Entwicklung und Umsetzung umfassender Schutzrechts-Strategien für geistiges Eigentum (Marken und Designs), und der Umsetzung gesetzlicher Regelungen, z.B. Datenschutz und Wettbewerbsrecht, insbesondere in der digitalen Welt.

www.von-thuengen.de

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung.

Gabriele Freifrau von Thüngen-Reichenbach
Rechtsanwältin
Fachanwältin für gewerblichen Rechtsschutz
Fachanwältin für Urheber- und Medienrecht
Fachanwältin für Informationstechnologierecht

Hinterer Glockenberg 12
96450 Coburg
Tel. +49 (0) 9561 35 47 811
gvt@von-thuengen.de
www.von-thuengen.de