Werbung und Marktkommunikation

Datenschutz: Checkliste für die Werbebranche

Wie fit ist Ihr Werbeunternehmen für das neue Datenschutzrecht?

Stand: August 2017

Mit der am 14.4.2016 vom Europäischen Parlament beschlossenen Datenschutz-Grundverordnung werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht.

Die Bestimmungen der DSGVO gelten ab 25.5.2018. Bis dahin müssen alle Datenanwendungen an die neue Rechtslage angepasst werden. Jedes Unternehmen, das in irgendeiner Weise personenbezogene Daten verarbeitet (z.B. eine Kundendatei führt, Rechnungen ausstellt, Lieferantendaten speichert), ist betroffen. Damit kommen wesentliche Neuerungen auf Unternehmen zu.

Die nachstehende Checkliste soll dabei helfen, die erforderlichen Schritte von der Analyse des Ist-Zustandes bis zur Umsetzung eines Maßnahmenplanes rechtzeitig zu setzen:

1. Vorbereitung

- Für die Anpassung an die DSGVO ist eine zuständige Person (intern/extern) zu nominieren
  (*Hinweis*: Jemand sollte sich im Betrieb unabhängig von der Verpflichtung einen Datenschutzbeauftragten zu benennen – siehe unten – um datenschutzrechtliche Fragen annehmen. Die Verantwortung bleibt datenschutzrechtlich bei demjenigen, der die Entscheidung trifft, Daten zu verarbeiten.)

- Zeit- und Budget-Planung
  (*Hinweis*: Davon ist abhängig, ob eine etwaig notwendige Umstellung im Betrieb ausgelagert werden muss/kann oder nicht.)

2. Status Quo-Erhebung (Ist-Zustandes) und Anpassungsbedarf (Soll-Zustand)

- Welche personenbezogene Daten werden verarbeitet?
  (*Hinweis*: Eine Bestandsaufnahme wird sinnvollerweise schriftlich vorgenommen. So können die Ergebnisse gleich für das Verarbeitungsverzeichnis – siehe unten – verwendet werden.)

- Welche Datenanwendungen bestehen?
  - Welche Standardanwendungen liegen derzeit vor?
    (*Hinweis*: Standardanwendungen gibt es ab 25. Mai 2018 in dieser Form nicht mehr. Sie müssen jedenfalls im Verarbeitungsverzeichnis protokolliert werden.)
  - Welche Datenanwendungen sind derzeit im DVR registriert?

(*Hinweis*: Das DVR ist mittlerweile bereits exportierbar, dh die gemeldeten Datenverarbeitungen können direkt im Verarbeitungsverzeichnis übernommen werden, siehe auch https://www.dsb.gv.at/dvr-online.)

- Erfolgt Profiling?
  (*Hinweis*: Bei gewissen Formen des Profilings kommen spezielle datenschutzrechtliche Regelungen zur Anwendung.)
- Was sind die Zwecke meiner Datenverarbeitungen?
- Was ist die Rechtsgrundlage der Datenverarbeitung?
  - Liegt eine Einwilligung vor?
    (*Hinweis*: Überprüfen Sie unbedingt bestehende Einwilligungen!)
- Welche sensiblen Daten werden verarbeitet?
- Werden Kindern Dienste der Informationsgesellschaft angeboten?
- Werden Auftragsverarbeiter (derzeit „Dienstleister") herangezogen?
  - Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
  - Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?
- Wie werden die Informationspflichten (nach der DSGVO) erfüllt?
- Wie werden die Betroffenenrechte (nach der DSGVO) erfüllt?
  - An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?
- Welche Datensicherheitsmaßnahmen sind vorhanden?
  (*Hinweis*: Geschäftsmodelle werden durch die DSGVO nicht „verhindert", aber es wird ein wesentlich größerer Wert auf Datensicherheitsmaßnahmen, auf den Schutz der Daten im Betrieb, gelegt werden (siehe hierzu auch www.it-safe.at).
- Wie ist privacy by design/privacy by default implementiert?
- Besteht für meine Datenverarbeitungen eine Dokumentationspflicht?
  - Wie wird die Dokumentationspflicht erfüllt?
- Welche Vorkehrungen gegen Datenschutzverletzungen existieren schon in meinem Unternehmen?
  (*Hinweis:* Es empfiehlt sich, „Mustervorgänge" bzw. Abläufe im Betrieb zu verankern, damit im Ernstfall auf diese „Automatismen" zurückgegriffen werden kann.)
- Ist für meine Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen?
  (*Hinweis*: Nach einer ersten Einschätzung der Artikel 29 Gruppe der EU-Datenschutzbehörden könnte diese bei Targeting-Geschäftsmodellen nötig werden)
- Ist eine vorherige Konsultation bei der Aufsichtsbehörde notwendig?
- Brauche ich einen Datenschutzbeauftragten?
  (*Hinweis*: Nach der Artikel 29 Gruppe ist das der Fall, wenn für eine große Zahl von Kunden Targeted Advertising angeboten wird.)
- Welcher Datenverkehr mit dem EU-Ausland besteht und auf welcher Rechtsgrundlage?
- Besonderheiten Arbeitnehmerdatenschutz
  - Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc.
  - Rechtzeitige Kommunikation mit dem Betriebsrat (wenn vorhanden)
- Wie weise ich nach, dass meine Datenverarbeitungen DSGVO-konform (siehe dazu „Pflichten des Verantwortlichen" und „Grundsätze und Rechtmäßigkeit der Verarbeitung") erfolgen? (z.B. Dokumentation der Einwilligungserklärungen, Verarbeitungsverzeichnis, Dokumentation der ergriffenen Sicherheitsmaßnahmen, Dokumentation der Risikoabschätzung, Protokollierung oder Dokumentation der Weisungen an dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen, Dokumentation der Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit, etc.)

3. Maßnahmenplan

- Zeitliche und budgetäre Planung (Priorisierung der Ziele)
- Maßnahmen festlegen
- Maßnahmen umsetzen

Weitere Dokumente:

- Sachlicher und räumlicher Anwendungsbereich
- Auskunftspflicht des Verantwortlichen
- Verantwortlicher und Auftragsverarbeiter (Überblick)
- Pflicht zur Berichtigung, Löschung ("Recht auf Vergessenwerden") und zur Einschränkung der Verarbeitung
- Datenschutzrechtliche Pflicht zur Datenübertragbarkeit
- Datenschutzrechtliche Pflicht zur Umsetzung eines Widerspruches
- Auswirkungen auf Websites und Webshops

Stand: 22.08.2017