Michael Weber

„Die Datenschutzgrundverordnung
-
Sofortmaßnahmen für Unternehmen“

Quelle: shutterstock.com/Kb-photodesign; Ket4up

Die Datenschutzgrundverordnung

Geltung der DSGVO

- Ab 25.05.2018
- Europaweit
- Für alle öffentlichen Stellen, Unternehmen, Vereine, Verbände, Parteien, Genossenschaften, …

Konsequenzen von Datenschutzverstößen

- Bußgeld bis € 20 Mio. oder 4 % des weltweiten Umsatzes
- Abmahnung als Wettbewerbsverstoß
- Schadensersatz inklusive immaterieller Schaden (= Schmerzensgeld)

Sofortmaßnahmen

- Technischer und organisatorischer Datenschutz
- Verarbeitungsverzeichnis
- Datenschutzerklärung für Website
- Einwilligungen einholen und protokollieren
- Auftragsverarbeitungsverträge

Technische und Organisatorische Maßnahmen

TOMs

- Datenschutzbeauftragter
- Datensicherheit

TOM 1: Datenschutzbeauftragter

Bestellung eines Datenschutzbeauftragten

- Mindestens 10 Mitarbeiter sind mit elektronischer Datenverarbeitung betraut

oder

- Kerntätigkeit des Unternehmens
  - Erfordert regelmäßige oder systematische Überwachung
  - Ist umfangreiche Verarbeitung besonders sensibler Daten

TOM 1: Datenschutzbeauftragter

Bestellung eines Datenschutzbeauftragten

Sensibel sind Daten bzgl:

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit
- genetische und biometrische Daten
- Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person
- strafrechtliche Verurteilungen

TOM 1: Datenschutzbeauftragter

Anforderungen:

- Intern oder Extern
- Qualifikation und Fachwissen
- Erhält erforderliche Ressourcen
- Weisungsfrei

TOM 1: Datenschutzbeauftragter

Dem Landesdatenschutzbeauftragten zu melden

Wie? https://www.baden-wuerttemberg.datenschutz.de/

TOM 2: Datensicherheit

Zu Berücksichtigen:

- Stand der Technik
- Implementierungskosten
- Art, Umfang und Zweck der DV
- Datenschutzrisiko

TOM 2: Datensicherheit

Konkrete Maßnahmen

- Zutrittskontrolle (Schließanlage, Alarmanlage, etc.)
- Zugriffskontrolle (Rechtevergabe, Passwortregeln, Firewall, Pseudonomisierung und Verschlüsselung)
- Weitergabekontrolle (VPN, verschlüsselte Kommunikation)
- Eingabekontrolle (Protokollierung)
- Auftragskontrolle (Schriftliche Anweisungen)
- Verfügbarkeitskontrolle (Sicherheitskopien, Virenschutz)

Verarbeitungsverzeichnis

Verarbeitungsverzeichnis

Inhalt:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Abbildung des Prozesses
- Technische und organisatorische Maßnahmen

Verarbeitungsverzeichnis

Kontaktdaten

Name und Kotaktdaten des Verantwortliche sowie ggf. seines Vertreters:	**Mustermann GmbH, Max-Mustermann-Straße 123, 12345 Berlin, Deutschland**	**Name und Kotaktdaten des betrieblichen Datenschutzbeauftragter:**	**Max Mustermann, datenschutz@xyz.de**

Prozesse

Name der Datenverarbeitung	Zwecke der Datenverarbeitung	Verarbeitung besonderer Arten personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO	Betroffene / betroffene Personengruppen	Personenbezogene Daten / Datenkategorien	Empfänger / Empfängerkategorien	Drittstaatentransfer	Regelfristen für die Löschung	Allgemeine Beschreibung der technischen und organisatiorischen Maßnahmen
Newsletter	Versand von Newslettern	Nein	Newsletter-Abonnenten	E-Mail-Adresse, ggf. Name	Werbeagentur XY	Möglich	Grundsätzlich unbeschränkt. Gegebenenfalls unmittelbar nach Widerruf der Einwilligung oder nach Widerspruch.	TOM-Liste in Anlage
Recruiting/Bewerbungen	Auswertung von Bewerbungen für eine mögliche Einstellung in der Kanzlei.	Möglich	Bewerber	Personenbezogene Bewerberdaten wie Name, Anschrift, Alter, E-Mail, Adresse	Personalvermittlungsagentur als Dienstleister	Nein	Löschfrist: ohne Vorliegen einer Einwilligung sechs Monate. Bei Vorhandensein einer Einwilligung zwei Jahre. Nach Einstellung s. DV Personalführung	TOM-Liste in Anlage

DR. WEBER & DR. BENEKE

Rechtsanwälte Rastatt

Dr. jur. Martin Weber
Dr. jur. Berhhard Beneke
Michael Weber

Datenschutzerklärung für Website

Datenschutzerklärung

Inhalt:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Zweck der Verarbeitung
- **Empfänger oder Kategorien von Empfängern**
- **Speicherdauer**
- **Recht auf Auskunft, Berichtigung, Löschung, Widerruf der Einwilligung**
- **Beschwerderecht bei der Aufsichtsbehörde**
- **Nutzungseinschränkungen wegen fehlender Datenangabe**

Datenschutzerklärung

Insbesondere Erläuterungen zu:

- Kontaktformular
- Newsletter
- Plug-Ins
- Cookies

Einwilligungen protokollieren

Erlaubte Datenverarbeitung

- Erforderlich
  - zur Durchführung eines Vertrages
  - zur Erfüllung einer rechtlichen Verpflichtung
  - zur Wahrung berechtigter Interessen

oder

- Einwilligung des Betroffenen

Einwilligung

- Freiwillig
- Informiert
- Unmissverständlich
- Nicht mehr erlaubt: opt out, z.B. vorangekreuzte Kästchen

Einwilligung

Zum Newsletter anmelden: abc@xyz.de

Ich stimme der Nutzung der angegebenen E-Mail-Adresse zum Versand des Werbenewsletters der Firma YYY zu. Die Einwilligung in den Versand ist jederzeit widerruflich (per E-Mail an cba@yyy.de oder an die im Impressum angegebenen Kontaktdaten) und erfolgt entsprechend der Datenschutzerklärung des Anbieters.

Einwilligung

- Nachweispflicht

⇒ Dokumentation

- Jederzeit widerruflich

Auftragsverarbeitungsverträge

Auftragsverarbeitung

Verarbeitung von Daten für ein anderes Unternehmen.

Beispiele:

- Externes Rechenzentrum
- Newsletterversand durch Werbeagentur
- Auswertung von Kundenverhalten
- Externe Buchhaltung

Auftragsverarbeitung

Pflichten des Auftraggebers

- Sorgfältige Auswahl (ggfs. anhand Zertifizierung)
- Schriftlicher Vertrag
- Information der Betroffenen bei Datenerhebung
- Weisungen an Auftragnehmer dokumentieren

Auftragsverarbeitung

Pflichten des Auftragnehmers

- Eigenes Verarbeitungsverzeichnis
- Technische und organisatorische Maßnahmen (TOMs)
- Weisungen des Auftraggebers befolgen

Auftragsverarbeitung

- Für Datenschutzverstöße haften Auftraggeber und Auftragnehmer gemeinsam

- Ausnahme nur: Beteiligter ist in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich

Auftragsverarbeitung im Ausland

Zulässig, wenn

- EU-Kommission feststellt, dass angemessenes Datenschutzniveau besteht
  - z.B. Schweiz, Andorra, Kanada
  - USA bei Unternehmen, die bei Privacy Shield registriert sind
- Standarddatenschutzklauseln

Beispiel für ein neues Projekt

-

Newsletter

Newsletter

- Unternehmen möchte Newsletter an Interessenten versenden.
- Die Anmeldung erfolgt über die Website.
- Der Versand wird von einer Werbeagentur durchgeführt.

Newsletter

Schritt 1: Vor der Einführung

- Aufnahme in die Datenschutzerklärung der Website
- Aufnahme ins Verfahrensverzeichnis

Newsletter

Schritt 2: Datenerhebung

- freiwillige, informierte und unmissverständliche Einwilligung
- Double-opt-in-Verfahren
- Dokumentation
- Jederzeit widerruflich

Newsletter

Schritt 3: Weitergabe an die Werbeagentur

- Auftragsverarbeitung
- Nur garantiert datenschutztreue Auftragnehmer
- Schriftlicher Vertrag
- Dokumentierte Weisungen

Danke für Ihre Aufmerksamkeit!