Datenschutz nach DSGVO für KMU

DSB BADEN

IHRE DATENSCHUTZ-EXPERTEN AUS BADEN

DSB Baden GmbH

Referent – Datenschutzauditor (TÜV)



Thomas Schneider

DSB Baden GmbH
Geschäftsführender Gesellschafter

Datenschutzbeauftragter (TÜV)
Externer Datenschutzbeauftragter (TÜV)
Datenschutz-Auditor (TÜV)

Telefon 07802-989904-1
Email t.schneider@dsb-baden.de
Web www.dsb-baden.de

DSGVO - Grundlagen

Was ist Datenschutz?

Datenschutz:

Gesetzliche Regelungen für den „Umgang“ mit personenbezogenen Daten

personenbezogene Daten:

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen



DSGVO - Personenbezogene Daten



Aus dem privaten Umfeld:

- Name, Adresse, Geburtsdatum, Telefonnummer
- eMail-Adresse (privat) und eMails
- Einzelangaben (Geschlecht, Titel, Größe, Haarfarbe, …)
- Freunde, Hobbies, Interessen
- Familienverhältnisse, Eigentumsverhältnisse
- Urlaub-Fotos, SMS-Nachrichten, …

Aus dem geschäftlichen Umfeld

- Nutzerverhalten, Verbindungsdaten, IP-Adresse, Seitenverlauf, …
- Bild- und Videoaufzeichnungen (z.B. „Videoüberwachung“)
- Buchhaltungsdaten (z.B. Personenkonten, Rechnung), Personaldaten
- Bewerberunterlagen, Daten aus betrieblichem Eingliederungsmanagement
- Geschäftliche Kontaktdaten von Mitarbeitern und externen Ansprechpartnern
- Geschäftliches sowie privates eMail- und Telefonverhalten, …

Personenbezogen <> privat

DSGVO – warum eigentlich Datenschutz?

Datenschutz ist ein Grundrecht!

In der EU

- Art. 8 der EU-Grundrechtecharta: „Schutz personenbezogener Daten“

In Deutschland

- Recht auf informationelle Selbstbestimmung





Schutz der Persönlichkeitsrechte
= Datenschutz

Schutz der Daten
= Datensicherheit bzw. IT-Sicherheit

DSGVO – warum eigentlich Datenschutz?

Datenschutz ist ein Grundrecht!

Jeder Mensch

soll grundsätzlich selbst über die

Preisgabe und Verwendung

seiner persönlichen Daten bestimmen können.

DSGVO - Grundlagen

Was fordert die DSGVO von Unternehmen?

Einhaltung der Persönlichkeitsrechte, d.h.

Erst denken – dann handeln!

- Was will ich tun? (Zweck)
- Darf ich das überhaupt? (Rechtsgrundlage)
- Welche Risiken entstehen dadurch und wie kann ich diese eindämmen? (Angemessene „technische und organisatorische Maßnahmen" – (Integrität und Vertraulichkeit sichern)
- Welche Daten brauche ich dafür? (Datenminimierung)
- Wie lange benötige ich die Daten? (Speicherbegrenzung)
- Wie erfährt die betroffene Person, dass ich von ihr Daten habe und was ich damit tue, damit diese ihre Rechte (z.B. Auskunft, Widerspruch etc.) wahrnehmen kann und „Herr der Daten" bleibt? (Transparenz)
- …

Grundsätze für die Verarbeitung nach Art. 5 DSGVO

Einhaltung nachweisen → Rechenschaftspflicht!

DSGVO - Rechenschaftspflicht

Rechenschaftspflicht → Beweislast-Umkehr

(Art. 5 Abs. 2 DSGVO)

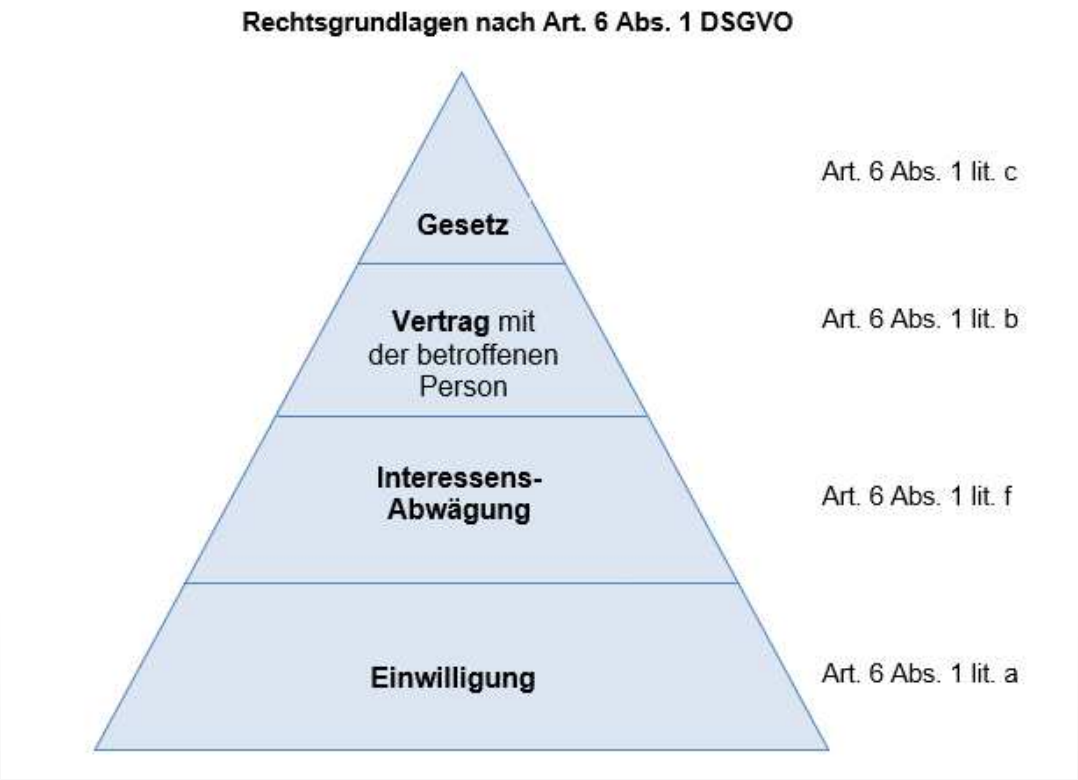
Nachweis für Einhaltung und Umsetzung aller gesetzlicher Vorgaben zum Datenschutz durch ein Datenschutz-Management-System (DSMS):



- Dokumentierte Zuordnung von Verantwortungen
- Implementieren von dokumentierten wirksamen Prozessen
- Schriftliche Regelungen (Richtlinien, Betriebsvereinbarungen etc.)
- Dokumentation von Vorgängen („Workflow“ und Entscheidungen, …)
- Bedarfsgerechte und wirksame Mitarbeiter-Sensibilisierung und –Unterweisung auf Basis eines Schulungskonzeptes
- Geeignete technische und organisatorische Maßnahmen (TOM) durch einen risiko-basierten Ansatz (u.a. auch durch Vorgabedokumente, Strategien etc.)
- Prüfungen der Einhaltung und Wirksamkeit aller Maßnahmen

Umsetzungsfehler in der Praxis

Rechtsgrundlage zur Verarbeitung





Falls keines der Kriterien erfüllt: Verarbeitung nicht zulässig!

Website

Klassische Mängel

- Unrechtmäßige Einbindung von
  - Plug-Ins
  - Google Maps
  - YouTube u.ä.
  - …
- Verwendung der Tracking-Cookies ohne Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO, z.B.
  - Werbetracker
- Bei Rechtsgrundlage Interessensabwägung nach Art. 6 Abs. 1 lit. f DSGVO fehlende Widerspruchsmöglichkeit (z.B. bei Google Analytics)
- DS-Erklärung nicht vorhanden oder nicht mit einem Klick erreichbar
- DS-Erklärung ohne konkrete Angaben (z.B. zu Kontaktmodul, eingesetzte Werkzeuge, Cookies), häufig nur generierter Text („Todsünde“: mit Quellenangabe!)
- Fehlerhafte Angabe der Rechtsgrundlagen
- Cookie-Banner mit „Einwilligung“, obwohl Rechtsgrundlage die Interessensabwägung ist.
- Unverschlüsselte Website-Kommunikation (http: anstelle https:)
- …

DSGVO – formale Vorgaben

Beispiel Hausbau

1. Bauwunsch festhalten (z.B. EFH-Plan)
2. Prüfung auf Zulässigkeit (Bebauungsplan)
3. Risikobewertung und Definieren der Maßnahmen, z.B. durch:
   - Statik
   - Bodengutachten
4. Besondere Gegebenheiten → spezielle Risikobetrachtung (Kindergarten an Straße, Treibsand, …)
5. Maßnahmen festlegen (z.B. weiße Wanne, Bodenaustausch, …)
6. Produktbestimmung
7. Partnerauswahl
8. Auftragserteilung
9. Umsetzung nach Plan (mit Kennzeichnung „roter Punkt“, Grundbucheintrag) und Abnahme

Beispiel Verarbeitung

1. Geplante VT beschreiben Art. 30 DSGVO
2. Prüfung auf Zulässigkeit (Rechtsgrundlage) Art. 6 Abs. 1
3. Risikobewertung durch Schwellenwertanalyse Art. 35 DSGVO
4. Besondere Gegebenheiten → spezielle Risikobetrachtung: DSFA (Datenschutz-Folgenabschätzung) Art: 35, 36 DSGVO
5. Maßnahmen (TOM) festlegen Art. 32 DSGVO
6. Produktauswahl „privacy by design“ Art. 25 Abs. 1 DSGVO
7. Partnerauswahl „AV-Vereinbarung“ Art. 28 DSGVO
8. Kauf bzw. (interne) Beauftragung
9. Umsetzung nach „privacy by default“ Art. 25 Abs. 2 DSGVO und Informationspflichten Art. 13, 14 DSGVO

DSGVO – Checkliste (Auszug)

Projektplan-Auszug zur Umsetzung

- VVT - Verzeichnis der Verarbeitungstätigkeiten
- AV - Auftragsverarbeitung mit Dienstleistern
- Schulungs- und Sensibilisierungskonzept und -Maßnahmen
- Produktauswahl: Privacy by default und Design nach Art. 25 DSGVO
- Einwilligungen nach Art. 7 DSGVO
- …
- TOM nach „Stand der Technik“ gemäß Art. 32 DSGVO
- Regelungen zur datenschutzkonformen Umsetzung, z.B. für
  - Passwörter, Email- und Internet, Telefonie, Mobile Geräte etc.
- Betroffenenrechte umsetzen durch Prozesse etc., u.a.
  - Information, Auskunft, Sperrung, Löschung
- Datenpanne innerhalb 72 Stunden melden
- Videoüberwachung
- Website, Web-Präsenzen
- …

DSGVO

Klassische Aussage: „Wir wollen nur das Nötigste!“

- Jeder Verstoß kann mit einer Geldbuße von bis zu 10 Mio. bzw. 20 Mio. Euro geahndet werden
- Das Unternehmen ist für die Umsetzung aller Vorgaben verantwortlich und muss alle nachweisen können
- Es geht nicht nur um die formale Umsetzung, sondern die tatsächliche Einhaltung aller DSGVO-Vorgaben (d.h. lebende Prozesse etc.)

Résumé:

Die DSGVO ist komplett umzusetzen. Nur bei der Ausgestaltung der einzelnen Punkte („Tiefe“) gibt es einen Interpretations-Spielraum.

DSGVO – Umsetzung

Herangehensweise für klassische Unternehmen

Datenschutz-Ist-Analyse

Ermittlung des Ist-Zustandes, Bewertung, Handlungsbedarf und Priorisierung

DSGVO-Projekt

Umsetzung der Vorgaben, Einrichten des DSMS

DSB oder Berater

Betrieb, Verifizierung, Überwachung, Beratung etc.
Bereitstellung der Werkzeuge

DSGVO – Umsetzung

Herangehensweise für Kleinst-Unternehmen

Werkzeuge

Erwerb der Werkzeug-Nutzung der DSB Baden Cloud

DSGVO-Projekt

Unterstützung X Tage durch DSB Baden GmbH, u.a. für

- Einweisung / Schulung DS-Manager / Team
- Kleine IST-Analyse
- Anpassung schriftlicher Dokumente (Richtlinien, Prozesse etc.)
- Umsetzung Informationspflichten
- Datenschutzkonforme Internet-Präsenz (Website etc.)
- …

Berater-Vereinbarung

Audits, Unterweisungen, Neuigkeiten, Beratung, Auslegungen, …

Fragen?

DSB Baden GmbH

Ansprechpartner in Datenschutz-Angelegenheiten



Thomas Schneider

Datenschutzbeauftragter (TÜV)
Externer Datenschutzbeauftragter (TÜV)
Datenschutz-Auditor (TÜV)

Telefon 07802-989904-1
Email t.schneider@dsb-baden.de



Dennis Bauske

Datenschutzbeauftragter (TÜV)

Telefon 07802-989904-2
Email d.bauske@dsb-baden.de