DATENSCHUTZ UND IT-SICHERHEIT ALS IMAGEFAKTOR UND MARKETINGINSTRUMENT FÜR DEN DEUTSCHEN MITTELSTAND

Kirsten Bock @privacyDE

DATENSCHUTZ?

- Geltungsbeginn der DSGVO im Mai 2018
- Was ist Datenschutz?
- Und was hat Datenschutz mit Digitalisierung zu tun?
- Bürokratie oder Mehrwert: Warum ist Datenschutz gut für mein Unternehmen?
- Welchen Wert haben Investitionen in den Datenschutz?

DATENSCHUTZ UND DATENSCHUTZRECHT

- Das Datenschutzproblem adressiert das Machungleichgewicht, dass bei der Verarbeitung von personenbezogenen Daten zwischen der Daten verarbeitenden Organisation und dem Individuum entsteht.

- Das Datenschutzrecht antwortet auf dieses Problem, indem es die Verarbeitung personenbezogener Daten unter Bedingungen stellt.
  - Datenschutz-Grundverordnung (DSGVO), Art. 1 DSGVO
  - Ausgleich und Fairness, Art. 5 DSGVO

Das Schutzgut des Datenschutzrechts

(1) Diese Verordnung enthält **Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten** und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten **natürlicher Personen** und insbesondere deren Recht auf Schutz personenbezogener Daten.

ART. 1 ABS. 1, 2 DSGVO

AUSGLEICH UND FAIRNESS

- Das Datenschutzrecht schützt nicht die Daten, sondern natürliche Personen.
- Dafür wird die Verarbeitung personenbezogener Daten unter **Bedingungen** gestellt
- Die Bedingungen sind in der DSGVO und ergänzend im BDSG und evt. im sektorspezifischen Recht geregelt
- Verantwortlichkeit liegt bei der verarbeitenden Organisation, Art. 5 Abs. 2 DSGVO
- Für Organsiationen bedeutet dies in erster Linie
  - **Kontrolle** über die eigene Datenverarbeitung zu erlangen und auszuüben,
  - Bedingungen einzuhalten und
  - Dies nachweisen zu können.

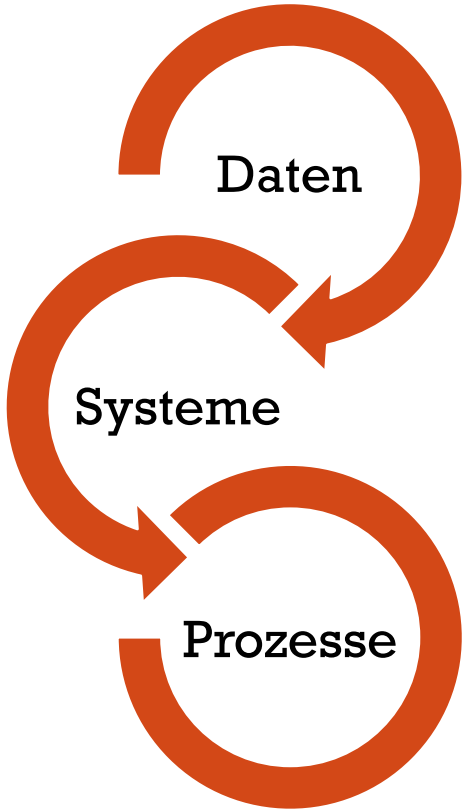
BEDINGUNGEN

- Rechtsgrundlage der Verarbeitung: Art. 6 Abs. 1 DSGVO
  a) Einwilligung
  b) Vertrag
  c) Rechtpflicht
  d) Lebenswichtige Interessen
  e) Öffentliches Interesse
  f) Berechtigte Interesse
- Prinzipien der Verarbeitung einhalten, Art. 5 DSGVO
- Sicherheit der Verarbeitung gewährleisten, Art. 32 DSGVO
- Informationspflichten erfüllen, Art. 12-14 DSGVO
- Betroffenenrechte beachten, Art. 15 DSGVO

PERSONENBEZOGENES DATUM

- Art. 4 Nr. 1 DSGVO
  - **alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen** (im Folgenden "betroffene Person") ;
  - als identifizierbar wird eine natürliche Person angesehen, die **direkt oder indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

VERARBEITUNG, ART. 4 ABS. 2 DSGVO



„Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

DATENSCHUTZ = IT-SICHERHEIT?

- Datenschutzrecht schützt Personen

- IT-Sicherheit schützt Organisationen

DATENSCHUTZRECHT UND DATENSICHERHEIT UNTERSCHEIDEN

Datensicherheit:
Schutz von Hardware, Software und Daten einer Organisation vor Verlust, Zerstörung, Fremdzugriff

Technische und organisatorische Maßnahmen, Technik-gestaltung

Datenschutz:
Schutz natürlicher Personen vor Beeinträchtigungen durch Verarbeitung personenbezogenen Daten

IMAGEFAKTOR DATENSCHUTZ

- Wettbewerbsvorteile nutzen
  - Viele Unternehmen haben noch immer viel Aufholbedarf
  - Datenschutz als USP
- Compliance als Vertrauensanker B2B und B2C
- Risikomanagement erfolgreich nachweisen
- IT-Kontrolle = Kostenkontrolle

VERANTWORTLICHE

Definition Art. 4 Nr. 7 DSGVO

„*Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die* ***allein*** *oder* ***gemeinsam*** *mit anderen* ***über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet****[…]“*

AUFTRAGSVERARBEITER

Definition Art. 4 Nr. 8 DSGVO

„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

INSTRUMENTE DER DSGVO

- (Datenschutz-Folgenabschätzung (DSFA), Art. 35 DSGVO)
- Selbstverpflichtung auf Verhaltensregeln (CoC), Art. 4 DSGVO
- Freiwillige Zertifizierung durch unabhängige Zertifizierungsstelle, Art. 42 DSGVO

DATENSCHUTZFOLGENABSCHÄTZUNG

Art. 35 DSGVO

- Verpflichtend für bestimmte risikoträchtige Verfahren, s. schwarze Liste der Aufsichtsbehörden
- Durchzuführen vor Verarbeitungsbeginn
- Die Einhaltung von CoCs kann bei einer DSFA positiv berücksichtigt werden, Art. 35 Abs. 8 DSGVO

VERHALTENSREGELN (COC)

Art. 40 DSGVO

- Selbstregulierung für bestimmte Kategorien von Verantwortlichen und Verarbeitern
- Durch Verbände und andere Vereinigungen, die Kategorien von Verantwortliche oder Auftragsverarbeiter vertreten
- Zur Präzisierung der DSGVO
  - Beispiele in Art. 40 Abs. 2 lit. a) – k)

- https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en_0.pdf

ANWENDUNGSBEREICHE

Compliance-Nachweis

- Verantwortliche, Art. 24 Abs. 3 DSGVO
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 3 DSGVO
- Auftragsverarbeiter, Art. 28 Abs. 5 DSGVO
- Sicherheit der Verarbeitung, Art. 32 Abs. 3 DSGVO
- Datenübermittlung vorbehaltlich geeigneter Garantien, Art. 46 Abs. 2 lit. f DSGVO

ZERTIFIZIERUNG

Art. 42, 43 DSGVO

- Ist der freiwillige Nachweis, dass ein Zertifizierungsverfahren erfolgreich durchlaufen und mit einem Datenschutzsiegel oder -prüfzeichen abgeschlossen wurde, das dazu dient, nachzuweisen, dass bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern die Vorgaben der DSGVO eingehalten werden.

ZERTIFIZIERUNG: WAS, WER, WIE

- **Was:** Verarbeitung personenbezogener Daten durch einen Verantwortlichen oder Verarbeiter
- **Wer:** unabhängige, akkreditierte Zertifizierungsstellen oder zuständige Aufsichtsbehörde nach von der Aufsicht genehmigten Kriterien
  - Nationale Verfahren
  - EU-weites Siegelverfahren
- **Wie:** erfolgreicher Abschluss eines Zertifizierungsverfahrens
  - Evaluation der Einhaltung von Zertifizierungskriterien
  - Für max. 3 Jahre gültig

VORTEILE EINER ZERTIFIZIERUNG

- Erfüllung der Pflichten des Verantwortlichen, Art. 24 Abs. 3
- Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f)

ZERTIFIZIERUNG

Ablauf

- Welche Verarbeitung soll zertifiziert werden?
- Prüfung der Dokumentation auf Aktualität und Vollständigkeit
- Auswahl des passenden Siegelverfahrens
- Abschluss eines Zertifizierungsvertrages
- Evaluation durch akkreditierte Zertifizierungsstelle
- Bei Erfolg Erteilung des Zertifikats
- Re-Zertifizierung

AUSWAHL EINES GEEIGNETEN VERFAHRENS

- Nur akkreditierte Zertifizierungsstellen, in Deutschland durch die DAkkS
- Durch eine Aufsichtsbehörde genehmigte Kriterien
- National oder EU-weit
- Generell oder spezifisches Verfahren (zB Cloud-Zertifizierung)
- Erfasst das Verfahren den Verarbeitungsgegenstand (ToE)?
- Wird Dokumentation über das Zertifizierungsverfahren erstellt und zur Verfügung gestellt?

DATENSCHUTZKONFERENZ

Kurzpapier Nr. 9

Zertifizierung nach Art. 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

- https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf

WEITERE INFORMATIONEN

- European Data Protection Board

https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Fragen?

KONTAKT

Kirsten Bock

@privacyDE