Praktische Umsetzung der DS-GVO

So bereiten Sie Ihr Unternehmen auf die neuen Herausforderungen vor

Andreas Stürzl
16.05.2018

Ihr Datenschutzberater

Andreas Stürzl

- zertifizierter Datenschutzauditor (TÜV)
- zertifizierter IT-Prozessmanager (FH)
- geprüfter EDV Sachverständiger (VSD)

→ Firma Interaktiv EDV in Stephanskirchen bei Rosenheim

→ Seit 15 Jahren als Datenschutzberater tätig

Sie als Verantwortliche vertreten …

- Vereine und Verbände
- Selbständige/freie Berufe
- Unternehmen bis 10 Personen
- Unternehmen ab 10 Personen

- Sie sind Datenschutzbeauftragter?
- Sie haben einen Datenschutzbeauftragten?

Ist Datenschutz attraktiv?

Die Zeitschrift Absatzwirtschaft schreibt:

„Nutzen Sie die DSGVO, um Ihre Kunden endlich glücklich zu stimmen“

Quelle: Björn Bauer in „http://www.absatzwirtschaft.de/nutzen-sie-die-dsgvo-um-ihre-kunden-endlich-gluecklich-zu-stimmen-124999/“, abgerufen am 21.03.2018

Das große Missverständnis

- In öffentlich-rechtlichen Medien heißt es:

- Sendung SUPER.MARKT vom 14.05.2018
- Quelle: Rundfunk Berlin-Brandenburg

Art. 6 DSGVO: Rechtmäßigkeit der Verarbeitung

- Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist (…)

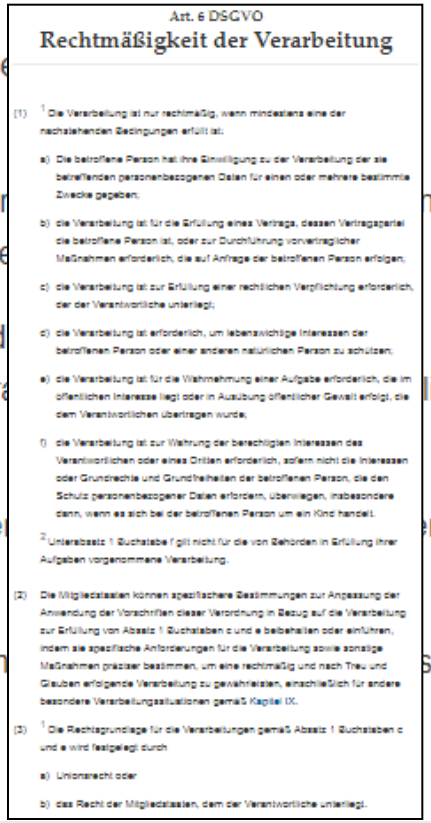
(1) [1] Die Verarbeitung ist nur rechtmäßig, wenn mindestens e
Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Ver
personenbezogenen Daten für einen oder mehrere be

b) die Verarbeitung ist für die Erfüllung eines Vertrags, d
betroffene Person ist, oder zur Durchführung vorvertra
die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Ve
Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige In
oder einer anderen natürlichen Person zu schützen;



Art. 6 DSGVO

Rechtmäßigkeit der Verarbeitung

(1) [1] Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

[2] Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) [1] Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

[2] Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. [3] Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. [4] Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

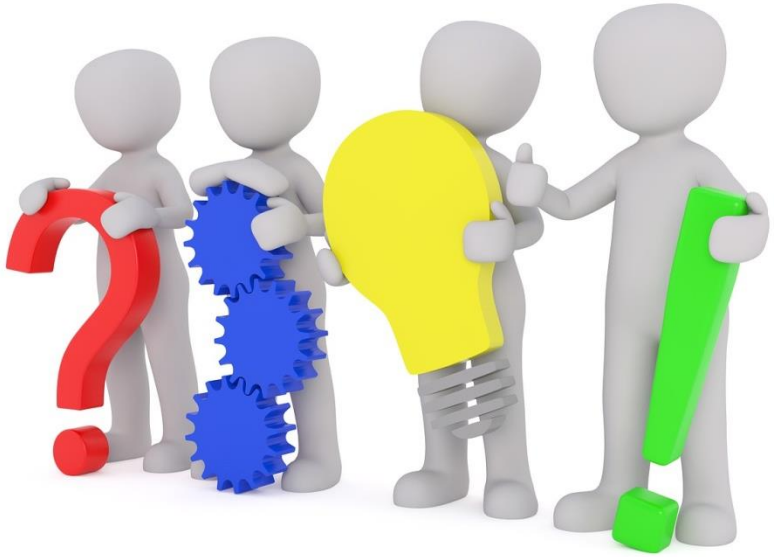
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

was Sie wissen sollten
und
was Sie tun sollten

Für wen?

- Kunden und Mitarbeiter
- Eigener Anspruch (was mache ich?)
- Mitbewerber und Abmahner
- Staat



EU-DSGVO - gesetzlicher Rahmen

- EU-Datenschutz-Grundverordnung
- Bundesdatenschutzgesetz wird durch neues Gesetz abgelöst
- E-Privacy-Richtlinie → EU-Privacy-Verordnung
- Cookie-Richtlinie

- **➔ Veränderungen, auf die Verantwortliche angemessen reagieren müssen**

Grundlagen DSGVO

- Betrifft: alle Unternehmen und Einrichtungen
- Verarbeitung von personenbezogenen Daten natürlicher Personen
- Informationen, die
  - eine Person unmittelbar identifizieren
  - es erlauben könnten, die Identität einer Person festzustellen

Anforderung an das Unternehmen

- Rechtmäßigkeit und Einwilligung
  - Rechtsvorschrift, Vertrag oder Einwilligung
- Rechte betroffener Personen
  - Information, Berichtigung, Löschung, Widerspruch
- Rechenschaftspflicht für die Einhaltung
  - erweiterte Dokumentations- und Nachweispflichten
  - Verfahrensverzeichnis
- Technik und Voreinstellungen
- Auftragsverarbeitung
- Und anderes mehr

Die wichtigsten Änderungen

- Meldepflicht des Datenschutzbeauftragten
- Meldepflicht bei Datenpannen: Betroffene und Aufsichtsbehörden innerhalb von 72 Stunden???
- Bußgeld in Höhe von bis zu 20 Millionen EUR oder 4 % des jährlichen weltweiten Umsatzes???
- Haftung → kaufmännische Sorgfaltspflicht

Der Datenschutzbeauftragte (DSB)

- Anforderungen an Fachkunde
  - Recht, Technik und Organisation
- Zuverlässigkeit: keine Interessenkollisionen

- Aufgaben
  - Schulung und Verpflichtung der Mitarbeiter
  - Beratung
  - Kontrolle
  - Bearbeitung von Anfragen und Beschwerden

was Sie wissen sollten
und
was Sie tun sollten

WER macht die Arbeit?

- Brauche ich einen Datenschutzbeauftragten?
- Ja/Nein: wer? intern/extern?
- Wer unterstützt Ihn?

➔ Berater benennen und Unterstützer festlegen

➔ Unterstützer Grundkenntnisse erwerben lassen (Tagesschulung)

Welche Arbeit?

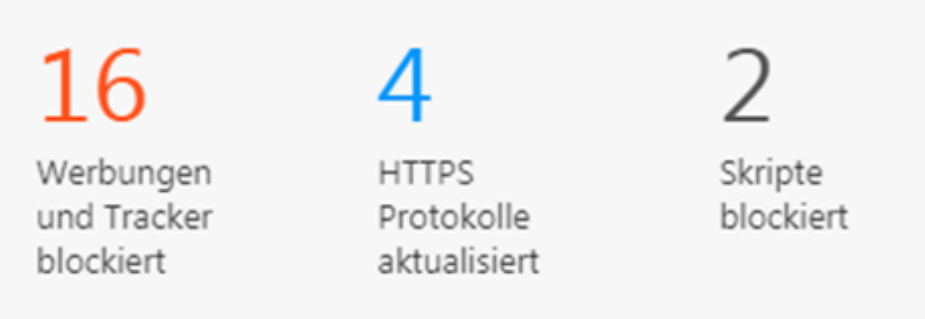
- Vertraulichkeitsverpflichtung der Beschäftigten
  - Datengeheimnis
  - Telekommunikationsgeheimnis
  - Geschäfts- und Betriebsgeheimnisse

- Schulung der Mitarbeiter und Geschäftsleitung
  - Präsenzschulung
  - Training-Tool (online)

Wo brennt es?

Internetauftritt

- Was macht denn eigentlich meine Internetseite?
  - Tracking,
  - Cookies, …
- Cookie-Richtlinie
- Datenschutzerklärung
- Auftragsverarbeitung
- Newsletter



Was fällt sonst noch an?

- technisch-organisatorische Maßnahmen
- Auftragsverarbeitung
  - Hauptvertrag, Anlage, TOM
- Dokumentation von Verarbeitungstätigkeiten

Verarbeitungstätigkeit

- Verantwortlicher
- welche Daten
- von welchen Personen
- Empfänger
- Zugriffsberechtigte
- Rechtsgrundlage
- Fristen für die Löschung

Bezeichnung der Verarbeitungstätigkeit	Anlage
Datum der Anlegung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse	
Bezeichnung der Verarbeitungstätigkeit	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ Sonstige:
Beschreibung der Datenkategorien	☐ ☐ ☐ Sonstige:

Fazit

- Handeln Sie jetzt
- Holen Sie sich Unterstützung von Experten
- Nutzen Sie Hilfsmittel

Was können wir für Sie tun

- Bestellung als externer Datenschutzbeauftragter
- Datenschutzberatung und Service
- Seminare und Vorträge

- Wir beraten und unterstützen Sie bei der Planung, Konzeption, Einführung und Optimierung eines Datenschutzmanagementsystems

Ihre Fragen?

Interaktiv EDV

Andreas Stürzl und Sabine Licht GbR

Telefon: 08036 - 90 80 520

E-Mail: info@interaktiv-edv.de

Internet: www.interaktiv-edv.de