1

WAS IST DIE DSGVO?

- Datenschutz-Grundverordnung.
- Vereinheitlichung des Dateschutzes innerhalb der EU.

Stichtag

25. Mai 2018

2

WER IST DAVON BETROFFEN?

Alle Organisationen & Unternehmen weltweit, die Daten natürlicher Personen (Bürger) der EU verabeiten oder speichern wollen, sind betroffen.

3

ZAHLEN UND FAKTEN

Bußgelder

bis zu **20** Million €

bis zu **4%** des Weltjahresumsatzes

Rechnungen

10 Jahre archivieren

IP-Adressen & pseudonyme Cookies

- Sind personenbezogene Daten.
- Müssen vertraulich behandelt werden.

Personenbezogene Daten sind durch technische und organisatorische Maßnahmen ("TOMs") vor Unbefugten zu schützen.

Datenschutzerklärung

- Muss leicht verständlich sein.
- Vollständig aufzuführen.

Checkliste Datenschutzprinzipien

✓ Rechtmäßigkeit

✓ Transparenz (s. Informationspflichten Art. 13 und 14 DSGVO)

- ✓ Gesetzliche Pflichten
- 🚩 Beispiel: Archivieren von Rechnungen.
- ✓ Verbot mit Erlaubnisvorbehalt (bei Verarbeitung personenbezogener Daten)
- ✓ Zweckbindung
  - Daten werden ausschließlich für den Zweck verwendet, für den sie erhoben worden sind.
- ✓ Datenminimierung
  - Datenerhebung auf Vorrat verboten. (Art. 5 Abs. 1 lit. c DSGVO)
- ✓ Integrität und Vertraulichkeit

Datenerhebung auf Vorrat

ist verboten

Privacy by Design

Datenschutzmaßnahmen müssen nach dem **Stand der Technik** bereits in die konzeptionelle Entwicklung von Produkten und Verfahren einbezogen werden.

Privacy by Default

Voreinstellungen bei Geräten oder bei Online-Plattformen muss standardmäßig die höchste Datenschutzstufe haben.

Beispiel: Newsletter Checkbox darf nicht automatisch angehakt sein.

Datenspeicherung

☑ **Nutzer der Seite muss eine Einwilligung ausdrücklich abgeben**

- Keine Nachteile bei Nichtabgabe.

- Einwilligung zeitlich protokollieren.
- Zweifel immer beim Datenverarbeiter.

Beispiel: Geschlossener Benutzerbereich auf einer Website oder Shop Registrierung.

Auftragsverarbeitungsvertrag

Grundlage für Verarbeitung von persönlichen Daten durch Dienstleister.

Daten sind nur entsprechend dem Auftrag und nach Weisung zu verarbeiten.

Beispiel: Web Hoster, Internetagentur, ERP oder CRM in der Cloud, Google, etc.

Checkliste Auftragsverarbeitungsvertrag

- ✓ Angaben zum Auftraggeber und Auftragnehmer
- ✓ Kategorien der verarbeiteten Daten

- ✓ Kategorien der Verarbeitung betroffenen Personen
- ✓ Zweck der Verarbeitung
- ✓ Vertragliche Verpflichtungen auf Befolgung von Weisungen, Genehmigung von Kontrollen, Beauftragung von Subunternehmern nur mit Zustimmung, Mitwirkung- und Information
- ✓ Vertragsdauer
- ✓ Technisch-organisatorische Schutzmaßnahmen und sonstige Garantien

Beispiel: Verschlüsselung von Entwicklungssystemen oder Vorschauumgebungen (Staging)

- ✓ Liste der Subunternehmer

Beispiel: Agentur nutzt Freelancer.

Datenverarbeitung

Checkliste

(Art. 6 DSGVO)

- ✓ Einwilligung der natürlichen Person
- ✓ Vertragserfüllung
- ✓ Gesetzliche Pflichten

- Schutz lebenswichtiger Interessen von Menschen
- Berechtigte Interessen

Checkliste Einhalten von Spezialregeln

Kinder und Minderjährige (Art. 8 DSGVO)

- Unerfahrenheit von Kindern berücksichtigen
- Altersgrenze für wirksame Einwilligungen Minderjähriger ab 16 Jahre
- Bis 16 Jahre - Zustimmung der Eltern erforderlich.

Besonders sensible Daten (Art. 9 DSGVO)

- Ausdrückliche Einwilligung der Betroffenen.
- Darunter fallen: Angaben zur Ethnie, Gesundheit, Sexualität, religiösen oder politischen Ansichten sowie Biometrie oder Genetik.

Spezialregeln für Beschäftigte (§26 BDSG-Neu)

- ✓ Beschäftigtendatenschutz
- ✓ Ungleichgewicht zu Lasten der Beschäftigten
- ✓ Ungleichgewicht muss beispielsweise bei der Beurteilung, ob die berechtigten Interessen der Arbeitgeber die von Arbeitnehmern überwiegen, berücksichtigt werden
- ✓ hohe Vorgaben für die Einwilligungen und heimliche Beobachtung von Arbeitnehmern

Videoüberwachung (§4 BDSG-Neu)

- ✓ bisherigen Regeln zur Videoüberwachung im öffentlichen Raum komplett übernommen

Zweckänderung (Art. 6 Abs. 4 DSGVO)

- ✓ Eine Zweckänderung ist erlaubt, wenn der neue Verarbeitungszweck mit dem alten vereinbar ist, Daten möglichst pseudonymisiert werden und die Betroffenen nicht zusätzlich belastet sind.

Checkliste Daten in Drittländer transferieren

Es wurde ein angemessenes Datenschutzniveau festgestellt (Art. 45 DSGVO).

- ✓ Angemessenheitsbeschlüsse
- ✓ US-Unternehmen, die nach dem Privacy-Shield-Abkommen zertifiziert sind

Wurde kein angemessenes Datenschutzniveau festgestellt, müssen geeignete Garantien vorgelegt werden (Art. 46 DSGVO).

- ✓ Unternehmensinterne Selbstverpflichtungen
- ✓ Standarddatenschutzklauseln der Kommission/Aufsichtsbehörde
- ✓ Genehmigte Zertifizierungsverfahren

Es wurden Ausnahmen für bestimmte Fälle getroffen (Art. 49 DSGVO)

- ✓ Einwilligung der Nutzer
- ✓ Weitergabe von Daten ist zur Vertragserfüllung erforderlich
- ✓ Verfolgung von Rechtsansprüchen

Berechtigte Interessen

- Nutzer haben Interesse am Datenschutz.
- Webseitenbetreibter
  haben wirtschaftliche Interessen.
- gegenüberstehende Interessen abwiegen.

Online Marketing

- Analyse, Optimierung und wirtschaftliche Vorteile sind berechtigte Interessen, auf die man sich beim Einsatz der Tools berufen kann.
- Profiling ist ein gesetzlich verankerter Risikoindikator.

Beispiel: Bewegungsprofile von Kunden im Shop.

Meldepflichten bei Datenpannen

- Meldung an die Datenschutzbehörde. (Art 33 DSGVO)
- Liegt eine meldepflichtige Datenpanne vor?
- Meldung an Betroffene. (Art 34 DSGVO)

Beispiel: Kundendaten die im Rahmen eines Shop Hacks kompromittiert wurden.

- Inhalt der Meldung: Alle vorhandenen Informationen + Name, Firma, Adresse, zuständige Personen und deren Kontaktdaten.
- **72h Zeit**
- Meldung per E-Mail

Checkliste Rechte der Nutzer

- ✓ Auskunftsrecht (Art. 15 DSGVO)
  - Anliegen: Welche Daten werden über mich gespeichert?
  - Antwort muss umfassend sein (nicht nur Online Shop, sondern auch ERP, Newsletter, etc.)
  - Achtung: Validierung der Berechtigung erforderlich.
- ✓ Berichtigungsrecht (Art. 16 DSGVO)
  - Anliegen: Ich möchte meine Daten korrigieren lassen.
- ✓ Recht auf Löschung und Einschränkung der Verarbeitung von Daten (Art. 17 DSGVO)
- ✓ Recht auf Vergessen werden (Art. 17 DSGVO)
- ✓ Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
  - Export von Daten z.B. als CSV Datei frühzeitig vorsehen.
- ✓ Widerspruchsrecht (Art. 21 DSGVO)
- ✓ Recht auf Beschwerde bei Aufsichtsbehörden

Updates

! Seit 2015 Gesetz

- Updates müssen **sofort** gemacht werden
- Sowohl Soft- als auch Hardware
- Technik aktuell halten

Dokumentations- & Nachweispflichten

Es müssen Nachweise über Datenverarbeitungsprozesse geführt werden.

Zwecke, Art und Umfang und risikomindernde Maßnahmen wie „Privacy by Design“ sind zu dokumentieren und Zulässigkeit zu prüfen

Tipp: Datenverarbeitungsverzeichnis erstellen und umfassend dokumenteieren.

Checkliste Wann haftet der Geschäftsführer?

- ✓ Bei selbstbegangenen Datenschutzverstöße
- ✓ Er haftet als sog. „Garant“ dafür, dass die Unternehmensangehörigen sich an das Datenschutzrecht halten
- ✓ Datenschutz-Compliance im Unternehmen einführen um Haftung zu entgehen
  - Zuständige Mitarbeiter müssen sorgfältig ausgesucht, instruiert und regelmäßig überwacht werden.
- ✓ Vollständige Delegation der Haftung auf einen Mitarbeiter ist nicht möglich
- ✓ Haftung kann nicht vollständig auf den Datenschutzbeauftragten übertragen werden

Tipp: Eigene Versicherung gegen Verlust, die Veränderung oder Blockade elektronischer Daten. (auch von den Dienstleistern einfordern)

Checkliste Umstellung DSVGO

- ✓ Alle Datenverarbeitungsprozesse auf deren Zulässigkeit prüfen
- ✓ Verfahrensverzeichnis mit der Übersicht aller Datenverarbeitungsprozesse erstellen.
- ✓ Prüfen ob die Anforderungen an die technisch-organisatorische Sicherheit der Daten betroffener Personen erfüllt werden und gegebenenfalls eine Datenfolgeabschätzung durchzuführen ist
- ✓ Prüfen, ob ein Datenschutzbeauftragter benannt werden muss?
  - Ab Betrieben mit 10 Personen (§38 BDSG-Neu)
- ✓ Prüfen ob Datenübermittlungsprozesse zulässig sind und notwendige Auftragsverarbeitungsverträge vorliegen
- ✓ Prüfen, ob ein Beschwerdemanagement für die Fälle

der Geltendmachung von Betroffenenrechten eingerichtet ist

- ✓ Datenschutzerklärung aktualisieren
- ✓ Mitarbeiter sensibilisieren, auf Vertraulichkeit verpflichten, zur Befolgung der Prinzipien von Privacy by Design und Privacy by Default anhalten sowie dazu, alle datenschutzrechtlich relevanten Vorgänge dokumentieren
- ✓ Regelmäßig überwachen, ob die Datenschutzprozesse weiterhin den gesetzlichen Anforderungen entsprechen

Diese Infografik stellt keine Rechtsberatung dar.

Copyright ® web-vision GmbH