Datenschutz Grundverordnung (DSGVO)

Informationen

zum Inkrafttreten am 25. Mai 2018

Inhalt

- Einführung und Risiken
- Personenbezogene Daten und Betroffenenrechte
- Wie sind Daten zu schützen?
- Was müssen Sie tun?

Einführung und Risiken

DSGVO – in einem Satz

Jedes(r)

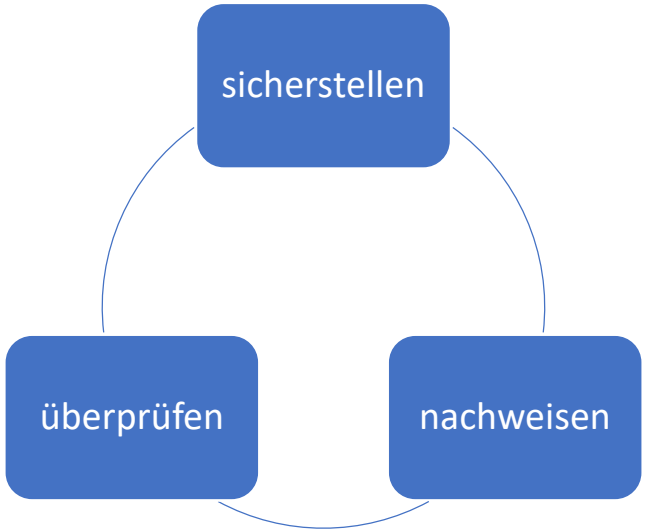
- Unternehmen
- Freiberufler
- Verein

muss alles tun, was

- dem Stand der Technik entspricht und
- im Verhältnis zu den finanziellen Mitteln steht

um Daten von lebenden, natürlichen Personen zu schützen.

Wer ist verantwortlich?



- Artikel 4 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; …

➢ Der „Boss“ ist und bleibt verantwortlich

Was ist wirklich neu?

- EU-Weit
  - Pflicht zur Bestellung eines Datenschutzbeauftragten
  - Konzernprivileg
  - One-Stop-Shop Prinzip: Betroffene wenden sich an Behörde Ihres Landes
- Personenbezogene Daten
  - Erweiterung der Definition
    - Genetisch, biometrisch
    - Direkt oder indirekt bestimmbar
  - Verschärfte Regelungen im Umgang mit Daten von Kindern und Jugendlichen

Was ist wirklich neu?

- Meldepflichten
  - Datenschutzbeauftragter (sofort nach Ernennung)
  - Verletzung des Schutzes (72h; evtl. auch Meldung an Betroffene)
- Kopplungsverbot
- Beweislastumkehr
- Höhe der Bußgelder
  - Alt: max. 300 000€
  - Neu: 20 Millionen € oder 4% des Jahresumsatzes (je nachdem was höher ist)
  - Verbandsklagen

Was wurde modifiziert?

- Verarbeitungsverzeichnis (alt : Verfahrensverzeichnis)
  - Muss Rechtsgrundlage enthalten
- Besondere Kategorien pb-Daten und der Umgang mit ihnen
  - Datenschutzfolgeabschätzung (alt : Vorabkontrolle)
  - Pflicht eines Datenschutzbeauftragten
- Trennungsgebot
- Auftragsverarbeitung (alt: Auftragsdatenverarbeitung)
  - Pflicht: Vertrag mit Partnern, die pb-Daten verarbeiten
- Umgang mit pb-Daten in nicht EU-Staaten verschärft

Besonderheiten für Klein- und Mittlere Unternehmen

- Verarbeitungsverzeichnis
  - ab 250 Mitarbeiter oder
  - ab 10 Personen, die regelmäßig mit der Verarbeitung von pb-Daten beschäftigt sind
- Datenschutzbeauftragter
  - reine Datenverarbeiter oder
  - ab 10 Personen, die regelmäßig mit der Verarbeitung von pb-Daten beschäftigt sind oder
  - Datenkategorien, die Datenschutzfolgeabschätzung erfordern
    - Ausnahme: Ärzte, Gesundheitsberufe, Anwälte
- Verhältnismäßigkeit der technischen und organisatorischen Maßnahmen

Definition „Verarbeitung“
- *erfassen*
- *bearbeiten*
- *nutzen*

Definition „regelmäßig“:
wenn mindestens eine der folgenden Eigenschaften erfüllt ist:
- *fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend*
- *immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend*
- *ständig oder regelmäßig stattfindend*

Risiken

- Abmahnverbände / Abmahnunternehmen
- Anzeige durch
  - Konkurrenten
  - Kunden
  - Lieferanten
  - Mitarbeiter

➢ Bußgelder

➢ Schadensersatz

➢ u.U. persönliche Haftung (Verantwortlicher, DSB, Mitarbeiter)

Personenbezogene Daten und Betroffenenrechte

Was sind personenbezogene Daten?

Direkte personenbezogene Daten	Indirekte personenbezogene Daten
Name, Vorname	IP-Adresse
Adresse	KFZ-Kennzeichen
Geburtsdatum	…
Telefonnummer(n)	
Staatsangehörigkeit	
Bankdaten	
Politische Orientierung	
Hautfarbe	
Gesundheitsdaten (z.B. Sehstärke, Krankheiten etc.)	
…	

Rot: Beispiele für besondere Datenkategorien

Wann dürfen Sie pb-Daten verarbeiten?

6 sog. „Rechtsgrundlagen“:

1. Mit Einwilligung der Person für einen oder mehrere bestimmte Zwecke
2. **Erforderlich für die Erfüllung des Auftrags**
3. Erforderlich für eine rechtliche Verpflichtung des Verantwortlichen
4. Erforderlich für lebenswichtige Interessen der Person
5. Für die Wahrnehmung der Aufgabe im öffentlichen Interesse
6. Es besteht ein berechtigtes Interesse des Verantwortlichen

Was sind die Betroffenen-Rechte?

- Recht auf Information, dass pb-Daten gespeichert und evtl. weitergegeben werden
  - bei der Erfassung, inkl. Erläuterung der Rechte
- Rechte:
  - Auskunftsrecht
  - Recht auf Berichtigung
  - Recht auf Sperrung
  - Recht auf Löschung
  - Recht auf Datenübertragung
  - Recht auf Widerspruch
  - Recht auf Beschwerde

➢Aus diesen Rechten ergeben sich Pflichten für Unternehmen / Vereine

➢Gilt für Kunden, Lieferanten, Mitarbeiter, Sonstige (z.B. Bewerber) …

Wie sind pb-Daten zu schützen?

Inhaltlich und technisch / organisatorisch

Wie sind die Daten inhaltlich zu schützen?

- Vertraulichkeit
  - keine unerlaubte oder unerwünschte Weitergabe der Daten
- Authentizität
  - Echtheit: es handelt sich auch um die Person
- Integrität
  - Korrektheit: die Daten stimmen
- Verfügbarkeit
  - Auf Daten kann zugegriffen werden und sie können rekonstruiert werden (Backup/Restore)

Empfehlenswert für alle Daten eines Unternehmens, nicht nur personenbezogene

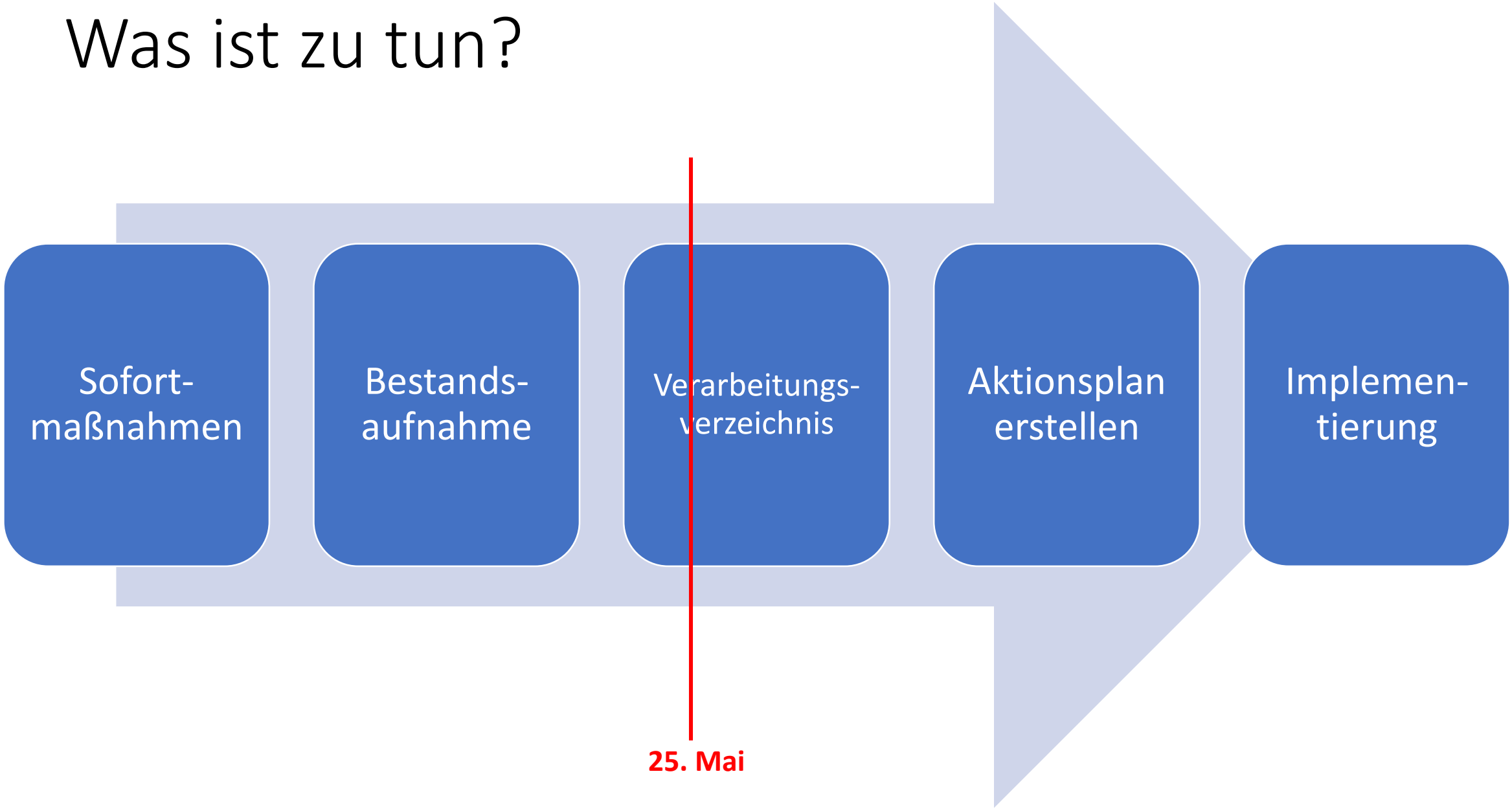
Wie sind die Daten technisch / organisatorisch zu schützen?

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- …

❖Transport und Speicherung von pb-Daten muss verschlüsselt erfolgen

Was müssen Sie tun?

Was ist zu tun?



1. Sofortmaßnahmen (vor 25. Mai erledigt)

Alles nach außen sichtbare!

- Homepage DSGVO konform
  - Impressum, Datenschutzerklärung, Disclaimer
  - Kontaktformular -> SSL (besser gesamte Webseite)
  - Registrierung -> Double OptIn
  - Facebook like und share -> nicht originale Funktionen nutzen!
  - Google Analytics (o.Ä.) -> Anonymisierung
- Facebook Impressum
- Entscheidung / Meldung Datenschutzbeauftragter
- Mitarbeiter informieren und sensibilisieren
- Informationspflicht -> Einwilligungserklärungen für Laufkundschaft
- Kein WhatsApp (zumindest intern, wenn von Kunden dann ohne pb-Daten)

2. Bestandsaufnahme (vor 25. Mai beginnen)

- Welche Hardware oder IT Systeme nutzen Sie und wie sind sie geschützt?
  - In welchen Gebäuden mit welchem Zugang
  - PCs, Laptops, Tablets, Smartphones, lokaler Server, hosted Server
  - Internet-Zugang, Internet Provider
- Mit welchen Softwares werden pb-Daten verarbeitet?
  - Kunden, Lieferanten, Mitarbeiter, Sonstige?
  - Wo sind die „Master-Daten“?
  - Erfassung, Bearbeitung, Nutzung (*Bilder von Mitarbeitern*)
- An wen werden pb-Daten weitergegeben und wie?
  - Z.B. Lohnbuchhaltung, (Achtung: Reinigungsfirma)
  - Weitergabe geschützt? (verschlüsselt oder mit Passwort?)

3. Verarbeitungsverzeichnis erstellen (vor 25. Mai beginnen)

- Beginn Datenschutzhandbuch mit generellen Technischen und Organisatorischen Maßnahmen (TOM)
  - als Referenz in den einzelnen Verarbeitungstätigkeiten
  - Schwachstellen identifizieren und dokumentieren für spätere Implementierung
- Vorlage nutzen
- Änderungshistorie
- Hauptblatt für Organisation
- Gruppieren der Bestandsaufnahme in Verarbeitungstätigkeiten
- Für jede Verarbeitungstätigkeit eine Anlage im Verarbeitungsverzeichnis
  - Zweck der Verarbeitung, Rechtsgrundlage der Verarbeitung, Datenfelder, Spezielle TOMs
- Selbst Auftragsverarbeiter: spezielles Verarbeitungsverzeichnis

Beispiele für Verarbeitungstätigkeiten

- Internet
- E-Mail oder Groupware
- Kunden-Auftragsbearbeitung
- Rechnungswesen
- Bestellwesen
- IT (bei größeren Unternehmen)
- Mitarbeiter Zeiterfassung
- Lohnbuchhaltung
- …

Technische und Organisatorische Maßnahmen (TOM)

- Dokumentationspflichten implementieren
  - Datenschutzbeauftragter ja/nein
  - Weitergabe von Daten
  - Verletzungen
  - Betroffenen-Information
  - Eingabe, Änderung, Löschung – wer und wann?
- Informationspflicht und Betroffenenrechte prüfen und implementieren
  - Website (Datenschutzerklärung, Impressum)
  - Laufkundschaft, Lieferanten, Mitarbeiter -> Vorlage
  - Einwilligungserklärungen
- Prozesse anpassen und dokumentieren
  - Betroffenenrechte -> Auskunft, Berichtigung, Löschung
  - Datenschutz (inhaltlich und technisch)
- Prozesse zur Meldepflicht implementieren
- IT Sicherheitsmaßnahmen auf allen Komponenten -> angemessenes Schutzniveau
  - Verschlüsselung von Transport und Speicherung der pb-Daten
    - Kontaktformular
    - Bestellprozess online
    - Laptops/PC Festplatten
    - E-Mails mit pb-Daten: mindestens Passwort auf Dokument
  - Passwörter und Regeln, Bildschirmschoner mit PW
  - Update/Patches
  - Antivirus
  - Backup/Restore
  - Gäste-WLAN
- Verhaltensregeln für Mitarbeiter
  - Schulung
  - Verschwiegenheitserklärung
- Verträge mit Auftragsverarbeiter

4. Aktionsplan erstellen und
5. Implementieren

- Datenschutzbeauftragter melden
- Auftragsverarbeitungs-Verträge abschließen
  - Vor 25. Mai: bei den großen Partnern
- Offene TOMs (Schwachstellen)
- Prozesse anpassen oder implementieren für die regelmäßige Wiederholbarkeit, dokumentieren
- Verarbeitungsverzeichnis updaten
- Regelmäßig (1 mal pro Jahr) überprüfen

Meine Leistungen

Leistung	Preis (netto)
Webseitenanalyse, Impressum, Datenschutzerklärung, Disclaimer	200€
Facebook Impressum	25€
Datenschutzerklärung Vor-Ort Kunden, Mitarbeiter, Lieferanten	50€
Verschwiegenheitserklärung Mitarbeiter	25€
Einwilligungserklärung Mitarbeiter zur Bilderveröffentlichung	25€
DSGVO-Projekt bis 5 Verarbeitungstätigkeiten	600€
DSGVO-Projekt bis 10 Verarbeitungstätigkeiten	1200€
DSGVO-Projekt bis 15 Verarbeitungstätigkeiten	1800€
DSGVO-Projekt bis 20 Verarbeitungstätigkeiten	2400€
Datenschutzbeauftragter B2B (ausschließlich Geschäftskunden)	300€ / Monat
Datenschutzbeauftragter B2C (Endkunden) ohne webshop	400€ / Monat
Datenschutzbeauftragter B2C mit webshop	500€ / Monat

Projekt und DSB beinhaltet nicht Datenschutzhandbuch und Implementierung von TOM-Empfehlungen

udo.schairer@schairer-its.com 07176/452116 www.schairer-its.com

Backup

Datenschutzbeauftragter DSB

- Datenschutz ist Managementverantwortung
  -> Verantwortlicher bleibt verantwortlich
- DSB berichtet an die höchste Managementstelle
- Aufgaben
  - Unterrichtung (Schulung) und Beratung des Management, Mitarbeiter, Auftragsverarbeiter
  - Überwachung der Einhaltung (Audit)
  - Anlaufstelle der Behörden
  - Anlaufstelle für Betroffene (Kontakt in Datenschutzerklärung, eigenes Kontaktformular)
- Muss der Behörde gemeldet werden
- Interner oder externer DSB möglich
- DSB benötigt entsprechende Qualifikation (technisch, Gesetze, persönlich)

Alles bleibt anders

- DSGVO basiert zum Großteil auf deutschem Datenschutz (99 Artikel)
  - BDSG-Neu als deutscher Zusatz (88 Paragraphen)
  - 177 Erwägungsgründe
- Inhalte beziehen sich auf Daten natürlicher Personen
  - Stärkt die Rechte im Umgang mit deren personenbezogenen Daten
  - Erhöht Druck auf Unternehmen sich um Datenschutz zu kümmern
    -> Großkonzerne aber auch kleine und mittlere Unternehmen