Tel. +49 (0) 7152 564 773
Fax. +49 (0) 7152 564 771
Mob. +49 (0) 176 327 441 72

Fabian Henkel

Diplom-Betriebswirt (FH) Markt-und Kommunikationsforschung
Zertifizierter Datenschutzbeauftragter

https://www.externer-datenschutzbeauftragter-stuttgart.de
info@externer-datenschutzbeauftragter-stuttgart.de

Unter welchen Voraussetzungen dürfen personenbezogene Daten verarbeitet werden? (Art. 6 Abs. 1 DSGVO)

Art. 6 Abs.1 DSGVO - RECHTSGRUNDLAGEN

RECHTSGRUNDLAGEN – wann dürfen personenbezogene Daten verarbeitet werden?

Grundsatz: Verbot mit Erlaubnisvorbehalt – was bedeutet das?

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn es eine Rechtsgrundlage erlaubt.

Welche Rechtsgrundlagen gibt es denn? → Siehe Artikel 6 Abs. 1 DSGVO

- Datenverarbeitung auf Grundlage einer **Einwilligung** (Art. 6 Abs. 1 Buchstabe a)
- Datenverarbeitung zur **Abwicklung von Verträgen oder vorvertraglichen Maßnahmen** (Art. 6 Abs.1 Buchstabe b)
- Datenverarbeitung aufgrund einer **rechtlichen Verpflichtung** (Art. 6 Abs.1 Buchstabe c)
- Datenverarbeitung zum **Schutze lebenswichtiger Interessen** (Art. 6 Abs.1 Buchstabe d)
- Datenverarbeitung im **öffentlichen Interesse oder Ausübung öffentlicher Gewalt** (Art. 6 Abs.1 Buchstabe e)
- Datenverarbeitung aufgrund **berechtigter Interessen** (Art. 6 Abs.1 Buchstabe f)
- Zur Durchführung und Anbahnung eines Arbeitsverhältnisses (Art. 88 DSGVO)

(→ Andere Gesetze können weitere Rechtsgrundlagen vorhalten)

Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO)

Art. 5 Abs. 1 DSGVO Grundsätze der EU DSGVO

Anforderungen an die Verarbeitung personenbezogener Daten

TRANSPARENZ	→ Informationspflicht ggü. Betroffenen
ZWECKBINDUNG	→ Daten nicht zweckentfremdet nutzen
DATENMINIMIERUNG	→ Nur die notwendigen Daten erheben
SPEICHERBEGRENZUNG	→ Pflicht zur Löschung nach Zweckerreichung
RICHTIGKEIT DER DATENVERARBEITUNG	→ Pflicht zur Korrektur unrichtiger Daten
INTEGRITÄT UND VERTRAULICHKEIT	→ Technische und Organisatorische Sicherheit

Art. 5 Abs. 1 DSGVO Grundsätze der EU DSGVO

GRUNDSATZ DER TRANSPARENZ (Informationspflicht nach Art. 13 / 24 / 21 DSGVO)

1. Wer ist verantwortlich für die Datenverarbeitung?
2. Wer ist (falls vorhanden bzw. erforderlich) der Datenschutzbeauftragte?
3. Zu welchem Zweck werden die Daten verarbeitet?
4. Welche Datenarten (z.B. Namen, Adressen) werden verarbeitet?
5. Nach welcher Rechtsgrundlage werden die Daten verarbeitet?
6. Welches Ereignis führ zur Löschung von Daten? Welche Löschfristen sind geplant?
7. Welche weiteren Empfänger (Firmen, Organisationen) der Daten sind involviert?
8. Welche Rechte haben die Betroffenen nach der DSGVO?

Wie umsetzen?

- Online (zum Beispiel in der Datenschutzerklärung oder als PDF)
- Aushang Informationsblatt
- Per E-Mail versenden
- In Papierform übergeben

(Muster zur Umsetzung der Informationspflicht kann bei www.externer-datenschutzbeauftragter-stuttgart.de heruntergeladen werden)

Probleme bei der Umsetzung der Anforderungen

DSB Datenschutz

GRUNDSATZ DER INTEGRITÄT UND VERTRAULICHKEIT (ZENTRALES THEMA)

Ziel: Sicherstellung, dass personenbezogene Daten technisch und organisatorisch sicher sind

ACHTUNG: Gesundheitsdaten gelten als besondere Kategorien personenbezogener Daten und erfordern ein hohes Schutzniveau.

Die Hauptproblemfelder bei der Organisation von Fahrten

Zentrale Datenspeicherung (Hauptspeicherort / Verwaltung) • **Sicherstellung Schutzniveau** • **Sicherstellung der rückstandslosen Löschung**	**Problem 1:** Beim Einsatz mehrerer (privater) PCs / Laptops sind in der Regel unterschiedliche sicherheitstechnische Maßnahmen vorhanden. Ein einheitliches Schutzniveau ist schwer umzusetzen. **Problem 2:** Die rückstandslose Datenlöschung kann schwerlich zentral organisiert und kontrolliert werden.
Nutzung von Privaten Geräten und E-Mail-Konten • **Daten auf privaten Geräten (Laptop, Smartphone, Tablet)** • **Nutzung privater E-Mail-Konten**	• Kein einheitlicher Schutzniveau • Keine Sicherstellung kompletter Datenlöschung • Nicht kontrollierbare Speicherorte • Apps können ggf. auf Daten zugreifen • Personen im privaten Umfeld könnten Daten sehen **Problem: Sicherstellung Transparenz / Integrität / Vertraulichkeit**
Übertragung von Daten • **Unverschlüsselter Versand von Daten** **→ insbesondere bei Gesundheitsdaten (sensibel)**	• Kein ausreichendes Schutzniveau • Daten können abgefangen und gelesen werden • „Fahrlässigkeit“ im Umgang mit sensiblen Daten

Probleme bei der Umsetzung der Anforderungen

Einsatz eines DSGVO-konformen Cloud-Speichers

Cloud-Speicher waren lange im Verruf, haben sich aber etabliert und bieten viele Vorteile.

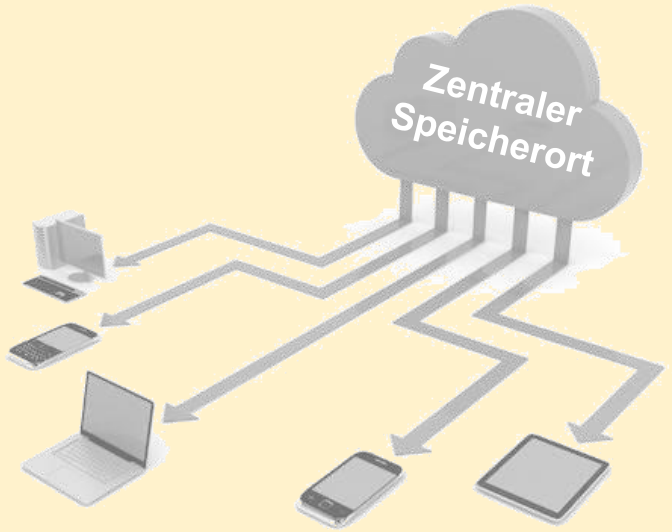
Vorteile:
- Die Daten liegen zentral auf einem sicheren Server
- Die Daten können zentral verwaltet und gelöscht werden
- Die Daten sind vor Verlust (z.B. durch Defekt) geschützt
- Es ist nachvollziehbar, welcher Nutzer wann Daten eingegeben oder gelöscht hat

Außerdem:
- Es kann festgelegt werden, welcher Nutzer Daten bearbeiten oder nur sehen darf
  → Berechtigungskonzept

Dabei Beachten:
- Sichere Passwörter verwenden!! Mind. 8 Zeichen (besser 12) mit Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen!!
  → Unsicheres Passwort ist meistens die Schwachstelle
- Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO mit Anbieter abschließen

Beispiele:
Teamdrive https://teamdrive.com
DriveonWeb https://www.driveonweb.de
IDGARD https://www.idgard.de

Der Cloud-Speicher als Datenzentrale:



Probleme bei der Umsetzung der Anforderungen

Einsatz eines DSGVO-konformen Cloud-Speichers

So ließe sich ein Cloud-Speicher einsetzen
(Hier können auch für den Erhalt von Benachrichtigungen private E-Mail-Konten eingesetzt werden)

Kalenderfunktion des Cloud-Speichers nutzen

- Viele Cloud-Speicher bieten neben der reinen Dateiverwaltung auch eine Kalenderfunktion, in die Tagesfahrten eingetragen werden könnten.
- Kalender lassen sich für einzelne Fahrer oder alle Fahrer freigeben und können über jedes Gerät online eingesehen werden.
- Bei Änderungen erhält der Fahrer eine E-Mail-Benachrichtigung und kann diese im Kalender einsehen.

✓ Daten bleiben im Cloud-Speicher. Integrität der Daten kann gewahrt bleiben.

Dateifreigabe gewähren

- Werden die Fahrten beispielsweise in einer Tabelle geführt, kann auch auf diese Datei eine Freigabe gewährt werden.
- Die Datei kann dann online eingesehen werden, im Prinzip analog zu einer Kalender Anwendung.
- Der Fahrer erhält eine E-Mail-Benachrichtigung bei Änderungen und kann die Datei jederzeit online einsehen.

✓ Daten bleiben im Cloud-Speicher. Integrität der Daten kann gewahrt bleiben.

Montag, 18.März	
08:00	Abholung Frau Maier, Aalenerstraße Ziel: Praxis Dr. Brecher
08:30	Abholung Frau Guttbier, Stuttgarterstraße Ziel: Praxis Dr. Einrenk

Probleme bei der Umsetzung der Anforderungen

Alternative (weniger empfehlenswert) Versand von E-Mails mit Verschlüsselung

Sensible Daten sollten nur per Ende-zu-Ende Verschlüsselung übertragen werden. Free-Mail-Anbieter leisten dies in aller Regel nicht. Zudem besteht das Problem der Unkontrollierbarkeit bei der Verwendung privater E-Mail-Adressen.

Beim Versand sensibler Informationen <u>als E-Mail-Anlage</u> zu beachten:

- Entweder werden die Daten vor dem Versand gezipt (zum Beispiel mit 7-ZIP) mit einem **Passwort verschlüsselt**. Hier ist ein sicheres Passwort zu wählen.
- Das Passwort darf nicht mit der gleichen E-Mail übertragen werden, am besten wird ein **anderer Kommunikationskanal** verwendet.
- Alternativ kann auch ein Passwort im Vorfeld vereinbart werden, das fortan verwendet wird.

- Open-Source-Software (kostenlos)
- Download bspw. unter www.7-zip.org

Beim Versand sensibler Informationen <u>im E-Mail-Text</u> zu beachten:

- Beim Versand sensibler Informationen im E-Mail-Text ist eine Ende-Ende-Verschlüsselung anzuraten. Diese kann in aller Regel nur durch Zusatz Software erreicht werden.
- Bei vielen E-Mail-Anbietern kann dies relativ einfach über die Software Pretty-Good-Privacy erreicht werden. Diese ist meisten kostenlos.
- Es gibt darüber hinaus eine Vielzahl von Anbietern, die Verfahren zur Ende-zu-Ende Verschlüsselung anbieten. Meistens sind diese dienste aber kostenpflichtig, manche bieten auch Abomodelle an.

Pretty Good Privacy

→ Anerkannter Standard

→ Siehe Links für weitere Infos

https://www.security-insider.de/was-ist-pgp-a-625467/

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/De-Mail/VorteileundFunktionen/EndezuEndeVerschluesselung/EndezuEndeVerschluesselung.html