Hinweise zum Umgang mit Datenschutz und Anleitung für (ehrenamtliche) Mitarbeitende

Stand: 17.02.2021

Dieser Handzettel wurde erstellt, denn mit Datenverarbeitung beschäftige Personen, auch (ehrenamtliche) Mitarbeitende, sind zum Datengeheimnis verpflichtet. Dieses besteht auch nach Beendigung der Tätigkeit fort.

1. ALLGEMEIN ZUM DATENSCHUTZ

- Datenschutz soll **vor Missbrauch schützen** (z.B. vor Manipulation, Benachteiligung und Stigmatisierung) und **die eigene Freiheit schützen**
- **Wichtige Richtlinien**:
  - BDSG (Bundesdatenschutzgesetz), gibt es seit 1978, Neufassung 2018
  - DSGVO (EU-Datenschutz-Grundverordnung), anzuwenden seit 2018: einheitliche Regeln in allen EU-Ländern, stärkere Rechte, z.B. gut aufbereitet unter https://deinedatendeinerechte.de/
- Datenschutz ist ein **Grundrecht in Europa**, in vielen außereuropäischen Ländern, (z.B. USA, China) nicht, d.h.:
  - außereuropäische Angebote/Firmen/Server müssen nicht den EU-Richtlinien folgen und gelten vorwiegend als unsicher
  - Als Verein, der seinen Sitz in Europa hat, gelten europäische Datenschutzrichtlinien auch für Betroffene im außereuropäischen Ausland und wir müssen diese ermöglichen

2. PERSONENBEZOGENE DATEN

- Daten, die verarbeitet werden und einem Menschen zugeordnet werden können:
  - **Allgemeine Personendaten:** Name, Geburtsdatum, Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer, Handynummer, Zeugnisse, Zertifikate, Nachweise, Urkunden
  - **Kennnummern jeder Art:** Sozialversicherungsnummer, Steueridentifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer, Matrikelnummer, Mitgliedsnummer
  - **Bankdaten:** Kontonummer, IBAN-Nummer, Kreditinformationen, Kontostand, Schließfachnummer, Angaben zur Bonität (SCHUFA)
  - **Sämtliche Online-Daten:** IP-Adresse, Standortdaten
  - **Persönliche Merkmale:** Haarfarbe, Größe, Statur, Gewicht, Augenfarbe, Geschlecht, sexuelle Orientierung
  - **Merkmale gegenständlicher Art:** Fahrzeugdaten, Immobilien- und Grundbesitzangaben, Eintragungen im Grundbuch, Autokennzeichen, Zulassungsdaten
  - **Kundendaten:** Kundennummer, Bestellhistorie, Adressdaten, Lieferdaten, Kontodaten
- Zu den **Daten mit erhöhtem Schutzbedarf** gehören zum Beispiel:
  - Angaben zur **ethnischen Herkunft** einer Person
  - **Politische** Ansichten und Haltungen
  - **Religiöse**, philosophische sowie weltanschauliche Ansichten und Einstellungen
  - Angaben zur aktiven Zugehörigkeit oder Unterstützung einer **Gewerkschaft** o.ä.
  - **Krankheits-, Gesundheits- und Patientendaten jeder Art**
  - Angaben zu **sexuellen** Präferenzen und Praktiken
- DSGVO sieht vor und **verpflichtet zu**:
  - Verbot mit Erlaubnisvorbehalt („Alles ist verboten, außer es ist ausdrücklich erlaubt“)
  - Zweckbindung und Zweckbestimmung
  - Prinzip der Erforderlichkeit
  - Prinzip der Datensparsamkeit
- Datenerhebung **ist zulässig, wenn** erlaubt durch:
  - BDSG, z.B. öffentlich zugängliche Daten (Telefonbuch, Presse, Aushänge)
  - andere Rechtvorschrift, wie andere vertragliche Regelungen
  - Einwilligung der Betroffenen, z.B. Einverständniserklärung

3. VERPFLICHTUNGEN ALS TEIL DER ARVC-SELBSTHILFE

- **Wichtigste Frage:** Welche Daten müssen überhaupt gesammelt werden?
- **Betroffene haben Rechte** auf transparente Information und Kommunikation, Auskunft, Information, Berichtigung, Löschung von und Beschwerde zu ihren Daten
- **Löschung von Daten** (Standardlöschfristen):
  - 3 Jahre (allgemeine Verjährungsfrist): Projektinhalte, E-Mails, z.B. auch Teilnahmelisten
  - 7 Jahre: Handelsbriefe und Verträge
  - 10 Jahre: Buchhaltungsdaten, Rechnungen und Stammdaten, z.B. Mitgliederlisten
- **Technische und organisatorische** Maßnahmen (TOMs) nach §9 BDSG gewährleisten:
  - Zutrittskontrolle, z.B. Schloss an der Türe
  - Zugangskontrolle, z.B. sicheres Passwort
  - Zugriffskontrolle, z.B. sichere Aufbewahrung von Datenträgern
  - Eingabekontrolle, z.B. Protokollierung der Anwendungen
  - Trennungsgebot, d.h. unterschiedlich erhobene Daten an anderen Orten aufbewahren
  - Weitergabekontrolle, also Art des Versands von Daten
  - Auftragskontrolle (Wer beauftragt wen und schickt was weiter?)

4. CHECKLISTE: WAS KANNST DU TUN?

- ☐ Geh mit personenbezogenen Daten sorgfältig um und folge dem Prinzip der **Datensparsamkeit**.
- ☐ Gib Deine **Benutzerkennungen** nicht weiter.
- ☐ Verwende **sichere Passwörter** und ändere diese regelmäßig (mindestens einmal pro Jahr).
- ☐ Achte darauf, dass niemand die Daten **mitlesen** kann, die/der das nicht soll.
- ☐ Schütze Deinen (Arbeitsplatz-)**Rechner**.
- ☐ **Trenne** ggf. geschäftliche und private Daten.
- ☐ **Verschlüssle** E-Mail und E-Mail-Anlagen, auch auf Laptops und Smartphones.
- ☐ **Sichere** Deine Daten regelmäßig, z.B. auf einer externen Festplatte.
- ☐ Führe regelmäßig (automatische) **Softwareupdates** durch.
- ☐ Denk an die **Sicherheit von Datenträgern**, auch von ausgedrucktem Papier, und prüfe auch analoge Maßnahmen, wie z.B. abgesperrte Schränke oder entsorgtem Papier.
- ☐ Nutze für Kommunikation **sichere Messengerdienste** (z.B. Signal, Telegram) und verzichte auf unsichere (z.B. WhatsApp, Facebook, Instagram, Snapchat, etc.).
- ☐ Sei Dir bewusst, dass **E-Mails** und E-Mailanhänge, wie frei lesbare Postkarten im Internet sind. **Telefonate** gelten ebenso als unsichere Kommunikation, insbesondere, wenn sie über Skype oder WhatsApp durchgeführt werden.
- ☐ **Videokonferenzen** können sicher über Jitsi, BigBlueButton oder YuLinc durchgeführt werden. Falls Du Zoom oder Microsoft Teams (nicht EU-datenschutzkonform) nutzen möchtest, gib acht auf Folgendes:
  - Zu Meetings erst kurz vorher Links rausschicken (max. 1 Tag vorher) und Link nur über Personenkreis verschicken, der Link braucht
  - Meetings mit Passwort schützen (wenn kurze Frist eingehalten wird, muss Passwort nicht unbedingt in Extramail verschickt werden)
  - Wartebereiche in Meetings einrichten und kontrollieren wer eintritt
  - Aufklärung der Teilnehmer über die Nutzung und Nachteile des Tools
- ☐ Falls Du personenbezogene Daten teilen möchtest, nutze dazu bspw. **cloud- oder drivebasierte Optionen** (z.B. Nextcloud), worüber das Dokument passwortgeschützt zur Verfügung gestellt werden kann. Das Passwort kann in einer separaten Kommunikationsform mitgeteilt werden.
- ☐ Falls Du personenbezogene Daten in Deinem **privaten E-Mailaccount** nutzt, bist Du für die Verarbeitung haftbar. Lösche E-Mails mit personenbezogenen Daten sofort nach Verwendung und nutze ggf. einen sicheren E-Mailanbieter (z.B. Posteo, aikQ, RiseUp, Autistici)

Falls Du viele Verarbeitungstätigkeiten (bspw. als Solopreneur:in) durchführen musst, lohnt es sich ein **Datenverarbeitungsverzeichnis** zu erstellen. Ein Beispiel des Anwaltvereins: https://anwaltverein.de/de/praxis/datenschutz?file=files/anwaltverein.de/downloads/praxis/datenschutz/dav-merkblatt-umsetzung-datenschutz-grundverordnung.pdf

Eine gute, aber **sehr ausführliche Checkliste** des Bayerischen Landesamts für Datenschutztaufsicht bietet Hilfestellung bei weiteren Datenschutzmaßnahmen: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf