Datenschutz im Verein

Beispielsfall

Kulturverein „Demo“ e.V.:

- 500 Mitglieder
- Ausstellungsraum mit Büro (Räume werden von Dritten mitgenutzt)
- Website mit Mitgliederlogin + Mail-Newsletter
- Twitter, Facebook, Instagram
- Alle 2 Wochen Veranstaltungen
- 5 Teilzeit-Mitarbeiter (Kassenwart, Mitgliederverwaltung, Öffentlichkeitsarbeit)
- 1 Vorsitzender

Datenschutz – Wer macht‘s?

- **Brauchen wir einen DSB?**
  - Bestellpflicht für Vereine besteht, sobald > 20 Personen regelmäßig mit personenbezogenen Daten arbeiten Mitgliederverwaltung, Finanzen, Werbung etc. (§ 38 BDSG)
  - Verhältnis DSB – Verarbeitungen vorab festlegen: Beratung/Risikoeinschätzung <> Verantwortung

- Was passiert, wenn wir keinen DSB bestellen müssen?
  - Datenschutzvorgaben müssen auch ohne DSB eingehalten werden

- **Empfehlung: 1-2 Personen haben das Thema im Blick, können ggf. freiwillig als DSB bestellt werden**

Wo fangen wir an?
Übersicht über Datenverarbeitungen erstellen

Prozesse

Mitgliederverwaltung
Digital und/oder Papier?

Fotos, Filme auf Veranstaltungen
Wer macht die Fotos?

Social Media
Facebook, Twitter, Instagram

Website, Mitgliederlogin
Wer gestaltet die Website?

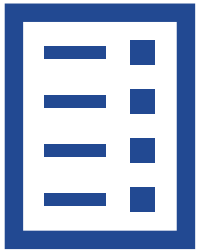
Beitragszahlungen
Wer hat Einsicht in Bankdaten?

Wo fangen wir an?
Übersicht über Datenverarbeitungen erstellen

Prozesse

Vorhandene personenbezogene Daten

- Mitgliederverwaltung: Name, Vorname, Adresse, ggf. weitere Daten je nach Verein
- Beitragszahlungen → IBAN!
- Website: Fotos / Filme, IP-Adressen, Login-Daten



Wo fangen wir an?
Übersicht über Datenverarbeitungen erstellen

Prozesse

↓

Vorhandene personenbezogene Daten

↓

Übersicht erstellen

Prozess	Beschreibung	pb. Daten
Mitglieder-verwaltung	…	Name, Vorname, Adressdaten…
Website + E-Mail	Newsletter, Mitgliederlogin für Kalender-verwaltung…	IP-Adresse, Login-Daten (Mail, Passwort), Name, Vorname…
…		

Einzelne Prozesse betrachten

Welche Datenarten werden wofür benötigt?

Geburtsdaten: Mindestalter, Altersvorschriften?
Adressdaten: Briefversand, Identifizierung?
Beitragszahlungen: IBAN → Höheres Missbrauchs**risiko**

Dauerhafte Speicherung notwendig oder einmalige Abfrage ausreichend?

Nicht benötigte Daten löschen, soweit keine Einwilligung vorliegt

Erforderliche Daten absichern

Löschen

Schredder für Papierunterlagen

Ausgemusterte **Festplatten** formatieren + ggf. physisch zerstören

Nicht (mehr) benötigte Daten löschen

USB-Sticks formatieren / vernichten

Doppelte Datenhaltung vermeiden

<>

Backups von wichtigen Datensätzen

Löschen

Nicht mehr benötigte Daten löschen

Datenbestände (Papier + elektronisch) **regelmäßig** auf Erforderlichkeit prüfen und ggf. löschen / schreddern

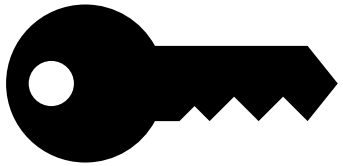
Daten, die nicht (mehr) für die Durchführung von Vereinstätigkeiten erforderlich sind, dürfen nur aufbewahrt werden, wenn die betroffene Person **eingewilligt** hat

Technisch-organisatorische Maßnahmen

„Erforderliche Daten sichern“

Papierakten

Aktenordner nicht offen aufbewahren
Abschließbarkeit Büro / Schreibtisch
Schredder anschaffen



Zugang und Zutritt

Wer hat Zugang zum Büro? → Personal, Reinigung, Hausmeister…
Zugang Büro = Zugang Akten? → Ggf. Schreibtisch / Schrank separat abschließen
Wer muss Daten einsehen können? → Vergabe von Büroschlüsseln und Zugangsdaten für Computer

Technisch-organisatorische Maßnahmen

„Erforderliche Daten sichern“

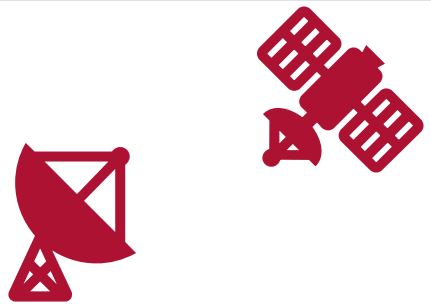
Smartphones / Messenger

Alternativen zu WhatsApp z.B.
Signal / Threema

Sparsam mit Dritt-Apps auf Smartphones/Tablets umgehen

Internetnutzung

Nur auf vertrauenswürdigen Internetseiten surfen
„**https**“ = Transportverschlüsselung
URL vor Klick überprüfen
Temporäre Dateien / Cookies regelmäßig/automatisch löschen



Technisch-organisatorische Maßnahmen

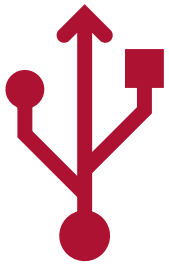
„Erforderliche Daten sichern“

Mobile Datenträger

Laptops wegschließen / abschließen
Sparsam mit USB-Sticks und mobilen Festplatten umgehen

Computer

Aktuelles **Betriebssystem**, WinXP-Rechner nicht ans Internet/WLAN hängen
Virenscanner installieren, **Firewall** (z.B. Windows Defender) angeschaltet lassen
Auf „kostenlose“ Drittanbieter-**Add-Ins** für Browser/Office möglichst verzichten
Sicherheitsupdates sofort installieren



Technisch-organisatorische Maßnahmen

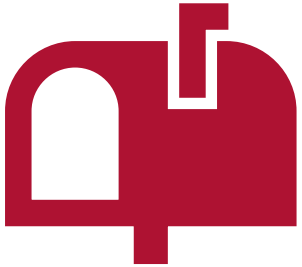
„Erforderliche Daten sichern“

Passwörter

Windows-Passwort für jeden Benutzer: > 8 Zeichen, Groß/klein, Ziffern, Sonderzeichen
Sensible Dokumente mit (anderem!) Passwort schützen, z.B. Excel mit Bankdaten
Passwörter nicht mit Post-It am Bildschirm oder im Büro aufbewahren
Router- + **WLAN-Passwörter** ändern (>20 Zeichen bei WPA)

E-Mails

Vorsicht vor **Phishing** / **Spam!**
Keine unbekannten Mailanhänge öffnen
Absenderadressen kontrollieren (z.B. I l |)



Fotos und Filmaufnahmen auf Wettkämpfen / Veranstaltungen

- **Datenschutzhinweise** zu Foto-/Filmaufnahmen an Eingängen **sichtbar** anbringen → v.a. Ansprechpartner für Widerspruch
  - Muster: https://datenschutz-generator.de/fotohinweis
  - FAQ: https://www.baden-wuerttemberg.datenschutz.de/faq-fotografieren-und-datenschutz-wir-sind-im-bild/

- **Einwilligung** auf Teilnahmeantrag anbringen --> Wozu werden die Daten verarbeitet und wo werden sie veröffentlicht?

- Einwilligung **Minderjähriger** nur durch gesetzliche Vertreter

Fotos und Filmaufnahmen auf Wettkämpfen / Veranstaltungen

- **Externe Fotografen**
  - Vertraulichkeit im Dienstleistungsvertrag, besser: **Auftragsverarbeitungsvertrag**
    - Muster: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf

- Zu einzelnen Fallgruppen siehe auch die hessische **Vereins-FAQ**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20180613_Datenschutz%20im%20Verein_1.pdf

Websitegestaltung

- **Einbindung von externem Content** → Youtube / Facebook embedding / framing
  - Youtube: „erweiterter Datenschutzmodus“ (blockt aber nicht alle Google-Cookies)
  - Like/Share-Button Facebook, Twitter, Xing: „Shariff“-Lösung → https://de.wordpress.org/plugins/shariff/
  - Besser: Fotos / Videos selbst hosten

- **Tracking** → Cookie-Verwaltung erstellen, nicht nur Banner mit „OK“

Websitegestaltung

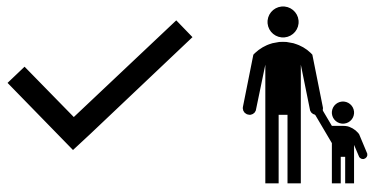
- Login und Newsletter → „**Double-Opt-In**“
  - „Double-Opt-In“ = Nutzer gibt E-Mail-Adresse auf Website ein und erhält Aufforderung zur Bestätigung an diese Mail, erst nach 2. Bestätigung erfolgt Registrierung / Newsletterversand

- **Muster-Datenschutzhinweise**:
  - https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenschutzhinweise-Websites/Muster-Datenschutzhinweise-Websites---Juli-2019.pdf
  - https://datenschutz-generator.de/datenschutzerklaerung/
  - https://www.mein-datenschutzbeauftragter.de/datenschutzerklaerung-konfigurator/

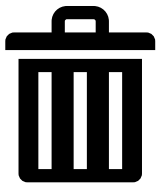
Social Media
Facebook, Twitter, Instagram

- Fotos / Videos → Über Veröffentlichung auf FB / Twitter / Youtube **bei Erstellung der Aufnahmen** informieren

- Veröffentlichung von Bildern in Social Media, auf denen Personen nicht nur „Beiwerk“ sind (Bsp.: Läufer bei Marathon) nur mit **Einwilligung**



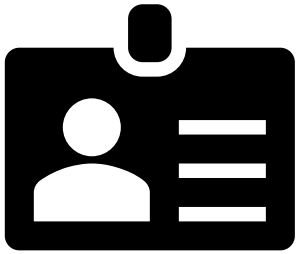
- **Nur einen Account** verwenden, damit Fotos zumindest auf diesem ggf. wieder gelöscht / geändert werden können



- Stellungnahme LfDI BaWü zu Twitter: https://www.baden-wuerttemberg.datenschutz.de/twitter-datenschutzfolgenabschaetzung/

Social Media
Facebook, Twitter, Instagram

- Nutzung im Übrigen
  - **Volle Namen** nach Möglichkeit vermeiden
  - Keine **Adressdaten** von Personen
  - Keine **sensiblen** Informationen → Finanzdaten und Daten nach Art. 9 DSGVO: Gesundheitsinformationen, Herkunft etc.
  - Informationen nach **TMG** mit aufnehmen → Datenverarbeitungen, Ansprechpartner usw.



- BVerwG zu Facebook-Fanpages: https://www.bverwg.de/pm/2019/62

Dokumentation

- **Verarbeitungsverzeichnis** für jeden Prozess, bei dem personenbezogene Daten verarbeitet werden
  - **Muster**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Verantwortlicher.docx
  - **Ausfüllhinweise**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Hinweise%20zum%20Verzeichnis%20von%20Verarbeitungstätigkeiten_1.pdf
  - **Gesamtübersicht** anlegen, z.B. Excel

- **Auftragsverarbeitungsverträge**
  - **Muster**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf
  - **Anwendungsfälle** → Fotografen, IT (Hosting), jede Datenweitergabe an Dritte, die im Auftrag des Vereins tätig sind
  - **AVV** zusammen mit jeweiliger Verarbeitungsbeschreibung ablegen

Dokumentation

- **Datenschutzfolgenabschätzung (DSFA):**
  - **Positiv-Liste DSK**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/DSFA_muss_Liste_DSK_de.pdf
  - **Positiv-Liste Hessen**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorgänge%20-Muss-Liste%20Berlin%20%28002%29.pdf
  - **„Demo" BayLDA**: https://www.lda.bayern.de/media/themen/03_dsfa_fallbeispiel_baylda_iso29134.pdf

Weitere Infos

- **Hessischer Beauftragter für Datenschutz und Informationsfreiheit**: https://datenschutz.hessen.de/
- **Übersicht Landesregierung Hessen**: https://www.gemeinsam-aktiv.de/img/GA-Datenschutz_V8_1018_web.pdf
- **HBDI zu Vereinen**: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/20180613_Datenschutz%20im%20Verein_3.pdf
- **LfDI RP**: https://www.datenschutz.rlp.de/de/themenfelder-themen/vereine/
- **LfDI BaWü**: https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/

Weitere Infos

- **Muster für Einwilligungen**: https://www.tlfdi.de/mam/tlfdi/themen/anwendungsbeispiel_einwilligung_.pdf

- **Infos zu Phishing**:
  - https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html
  - https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073

- **Datenschutz für Eltern + Kinder**: https://www.youngdata.de/# (Soziale Medien, Apps, Sicherheit im Internet uvm.)

Verschlüsselung

Allgemein zu Verschlüsselung:
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Datenverschluesselung/datenverschluesselung_node.html

Nachtrag speziell zu Bitlocker:
Die HDD-Verschlüsselung für Windows ist nur in den Win7/10 Professional und Enterprise-Versionen enthalten, also nicht in "Home".
Tutorial zur Einrichtung von Heise:
https://www.heise.de/tipps-tricks/BitLocker-auf-Windows-10-Festplatte-richtig-verschluesseln-4325375.html

Mailverschlüsselung (kostenlos + Open Source):
https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptotechnologie/Gpg4win/gpg4win_node.html

HEAG

Gebündelte Kompetenz.

Vielen Dank für Ihre Aufmerksamkeit!