DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

GEMEINSAM LERNEN.

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Mit der DSGVO auf du und du – praktisches Datenschutzwissen für Vereine

Sofia Vester

fix&fertig.
Datenschutzhilfen
für Zivilgesellschaft

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Wo stehe ich gerade beim Thema?

1. Beim Thema Datenschutz fühle ich mich sicher.
2. Ich habe einen guten Überblick der analogen und digitalen datenschutzrelevanten Prozesse in meinem Verein.
3. Ich weiß, wo wir auf bevorstehende Datenverarbeitung hinweisen müssen.
4. Ich weiß, wo wir eine Einwilligung zur Datenverarbeitung einholen sollten.

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Workshop - Überblick

1. Kurz-Einordnung: Wo stehe ich beim Thema?
2. Datenschutzwissen für Engagierte
    1. Welche Daten interessiert der Datenschutz?
    2. Welche Arbeitsprozesse sind davon betroffen?
3. Datenschutz in der Praxis
    1. Wo und wann muss über Datenverarbeitung informiert werden?
    2. In welchen Fällen brauche ich eine Einwilligung und wie sollte diese aussehen?
    3. Worauf muss ich bei der Auswahl & Nutzung digitaler Tools & Online-Kommunikation achten?
4. Fragen

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Oberstes Datenschutzprinzip

> Jeder Mensch
>
> soll grundsätzlich **selbst** über die
>
> Preisgabe und Verwendung
>
> seiner persönlichen Daten **bestimmen.**

→ Wird seit 2018 von der europäischen Datenschutzgrundverordnung (DSGVO) und dem daran angepassten Bundesdatenschutzgesetzt (BDSG-neu) und für Behörden von den Landesdatenschutzgesetzten (LDSGs) geregelt!

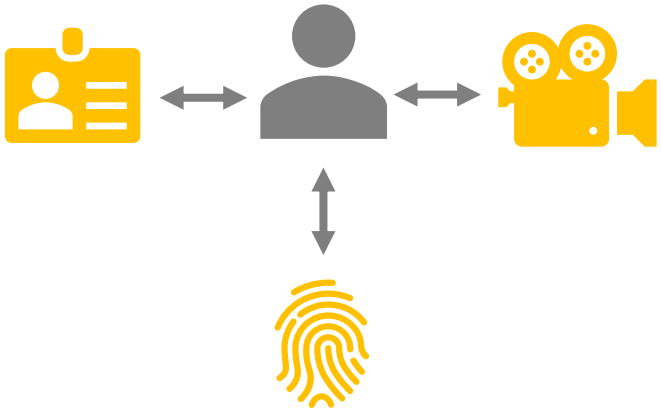
Datenschutzrechtliche Grundlage

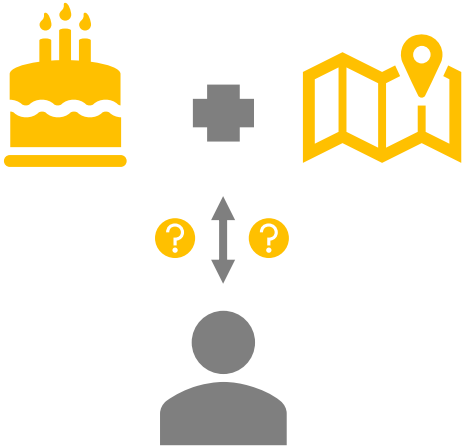
Die DSGVO regelt dabei innerhalb der EU

- Was erlaubt die Verarbeitung welcher personenbezogenen Datenkategorien unter welchen Bedingungen ?
- Für welche Zwecke dürfen personenbezogene Daten verwendet werden?
- Welche Rechte haben die Menschen, deren Daten erhoben/verwendet werden?
- Wodurch werden die Rechte von betroffenen Personen beschränkt?

Personenbezogene Daten

Welche Daten interessieren den Datenschutz?



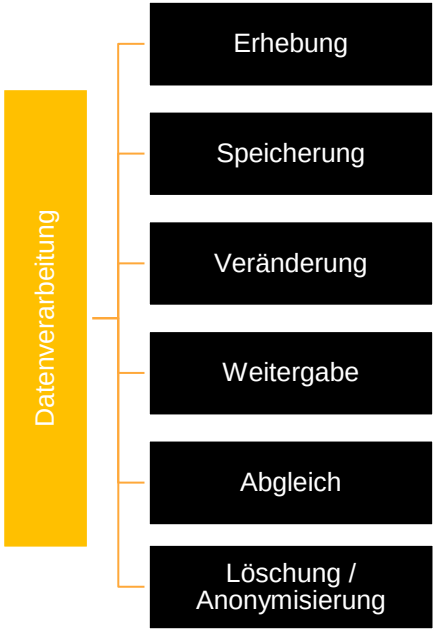


Personenbezogene Daten

Welche Daten interessieren den Datenschutz?

Verarbeitung personenbezogener Daten

Was bedeutet Datenverarbeitung überhaupt?



- Eine Datenverarbeitung kann automatisiert, halbautomatisch oder analog geschehen.
- Neben digitalen Daten betrifft Datenschutz auch Akten, Notizen, Adresskarteien und vor allem auch Bild-, Ton- oder Videoaufnahmen.
- Anonymisierte Daten fallen nicht unter die DSGVO.
- Die Datenverarbeitung zwischen Familienmitgliedern fällt nicht unter den Datenschutz.

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Leitmotiv
Erwartbarkeit

Kann die betroffene Person auf Basis der Ihr zur Verfügung stehenden Informationen die stattfindende oder bevorstehende Verarbeitung ihrer Daten erwarten?

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Mit welchen Daten habt Ihr zu tun?

1. Mit welchen Daten habt Ihr vor allem zu tun?
2. Habt Ihr es mit besonders schützenswerten Daten zu tun?
    1. Gesundheitsdaten, genetischen Daten, biometrischen Daten, Weltanschauung, Gewerkschaftszugehörigkeit, Zugehörigkeit zu politischen Gruppen, Religionszugehörigkeit, sexuelle Identität, sexuelle Orientierung, Herkunft, nationale Zugehörigkeit, „Race“ (im Sinne der Critical Race Theory) oder rassifizierend genutzte Merkmale
    2. Verarbeitet Ihr Daten von Kindern und Jugendlichen unter 16 Jahren?
    3. Macht Ihr Videoaufnahmen / nutzt eine Überwachungskamera?

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Beispiele analoger Datenverarbeitung

1. Telefonbuch, Visitenkartensammlung
2. Notizen
3. Ein- und ausgehende Post
4. Verträge und Akten der Finanz- & Lohnbuchhaltung
5. Personalakten (inkl. Bewerbungsunterlagen, Daten von ehrenamtlich Engagierten & Praktikant:innen)
6. Protokolle von Vorstandssitzungen
7. Mitgliedschaftsdokumente
8. Ausgedruckte Fotos, Ton- oder Videobänder
9. …

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

DSEE-AKADEMIE

Beispiele digitaler Arbeitsprozesse

1. Emails
2. Kalenderorganisation
3. Webseite
4. Social Media Seiten
5. W-LAN-Bereitstellung intern und für Gäste
6. Online-Fundraising
7. Online-Veranstaltungen / Online-Videokonferenzen
8. Online-Projektmanagement
9. Messengerdienste
10. …

DEUTSCHE STIFTUNG FÜR ENGAGEMENT UND EHRENAMT

Datenschutzanforderungen

Welche Rechte haben betroffene Personen?

- **Recht auf Auskunft**
- **Berichtigung**
- **Recht auf Einschränkung der Verarbeitung***
- **Recht auf Widerspruch***
- **Löschung***
- **Recht auf Vergessenwerden***

→ Nur bei zweifelsfreier Identifizierung und im Rahmen eines leistbaren Aufwands.

→ * Nur wenn keine sonstige Rechtsgrundlage das Speichern erlaubt/fordert.

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

DSEE-AKADEMIE

Wessen Daten verarbeitet Ihr?

1. Vereinsmitglieder
2. Dienstleister:innen
3. Mitarbeitende / Praktikant:innen / Honorarkräfte
4. Engagierte / Helfer:innen / Partner-Organisationen
5. Zielgruppen Eures Engagements
6. Spender:innen / Förderinstitutionen
7. Webseitenbesucher:innen
8. Soziale Medien-Seiten-Besucher:innen
9. W-LAN-Nutzer:innen
10. Veranstaltungsteilnehmende (ggf. in Präsenz oder online)
11. …

DEUTSCHE STIFTUNG FÜR ENGAGEMENT UND EHRENAMT

Datenschutzanforderungen

Welche Rechtsgrundlagen erlauben eine Verarbeitung?

Anbahnung & Abschluss von Verträgen

Erfüllung von Rechtsvorschriften
Bspw.: Steuerrecht, Arbeitsrecht, Vergaberecht, Presserecht

Einwilligung
Bspw.: Newsletter-Abonnement, zu veröffentlichendes Interview, Vernetzung mit Dritten

Berechtigtes Interesse
Bspw.: Sicherheitsdienst & Einlasskontrollen, Beratungsgespräche, Öffentlichkeitsarbeit (mit Beschränkungen)

Sonderregelungen für Wahrnehmung einer Aufgabe im öffentlichen Interesse
Bspw.: für Forschungs-, Archiv-, historische, statistische, journalistische und literarische Zwecke

Schutz lebenswichtiger Interessen

Pflicht zur Datenminimierung & Zweckbindung

1. Es dürfen immer nur zwingend Daten erhoben werden, die für den Zweck erforderlich sind (bspw. Kontakt- & Kontodaten bei Spende – sonst nichts).

2. Bei der Nutzung technischer Programme sind datensparsame Voreinstellungen zu wählen (bspw.: nur Email-Adresse für Newsletter als Pflichtfeld).

3. Es dürfen Daten nur so lange gespeichert werden wie für den Zweck erforderlich ist.
   Außer: Daten müssen aufbewahrt werden (bspw. Steuerrecht), es besteht ein berechtigtes Interesse (bspw. Bewerbungsdokumente, Teilnahmelisten) oder eine Einwilligung

4. Löschpflichten für personenbezogene Daten sollten weitmöglichst eingehalten werden und die Löschung immer sicher geschehen (bspw. mithilfe professioneller Aktenvernichtung)

Ein Löschkonzept mit Erinnerungshilfen im Kalender kann dabei unterstützen, die wichtigsten Löschpflichten einzuhalten (bspw. Aufbewahrungspflicht in der Finanzbuchhaltung mit 10 Jahren als maximaler Richtwert oder 6 Monate für Bewerbungsunterlagen).

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Für welche Zwecke verarbeitet Ihr Daten?

1. Durchführung der Vereinszwecke laut Satzung?
2. Mitgliederverwaltung?
3. Interne Organisation und Absprachen?
4. Öffentlichkeitsarbeit?
5. Fundraising?
6. Veranstaltungen?
7. …

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Datenschutzanforderungen

Pflicht zur Transparenz - Datenschutzinformationen

Wenn möglich sollte im vorhinein über bevorstehende Datenverarbeitung aufgeklärt werden.
Die Informationen sollten leicht zugänglich digital oder schriftlich (auch gesprochen) und möglichst präzise, transparent und verständlich in einer klaren und einfachen Sprache bereitgestellt werden.

- ✓ Welche Daten werden zu welchen Zwecken erhoben/verarbeitet und auf welcher Rechtsgrundlage?
- ✓ **Werden die Daten an Dritte weitergegeben oder ist der Zugriff darauf durch Dritte möglich?**
- ✓ Wie lange werden die Daten gespeichert?
- ✓ Welche Rechte haben betroffene Personen?
- ✓ Wer ist für die Datenverarbeitung verantwortlich (in der Regel = Verantwortliche:r im Sinne des Presserechts)?
- ✓ Wie kann man zum Thema Datenschutz in Kontakt treten (Kontaktinformation für Datenschutzanfragen muss kein Name sein, es reicht eine E-Mail-Adresse bspw. datenschutz@verein.de)?

Wann immer Ihr Daten wollt – braucht‘s vorher Infos!

Pflicht zum Schutz der Daten

Personenbezogene Daten sollten geschützt verarbeitet werden. Dies bedeutet vor allem einen unberechtigten Zugriff Dritter und eine Verarbeitung über den vereinbarten/berechtigten Zweck hinaus zu verhindern. Bei der Nutzung von Cloud-Diensten (Speicherkapazitäten & Tools) muss darauf geachtet werden, wo die Daten verarbeitet werden.

- Ein vergleichbares Schutzniveau kann in allen EU-Mitgliedstaaten vorausgesetzt werden.
- Für weitere Länder wurde durch die EU ein angemessenes Datenschutzniveau bestätigt (bspw.: Andorra, Argentinien, Israel, Neuseeland, Japan, das Vereinigte Königreich und Südkorea).

ACHTUNG: Für die USA gibt es aktuell keine gültige Länderregelung!

Aufgrund der Zugriffsmöglichkeiten US-amerikanischer Geheimdienste, erfüllen Cloud-basierte Programme oder Speicherkapazitäten, Messenger-Dienste und Soziale Medien, deren Daten von US-amerikanischen Firmen oder auf Servern in den USA verarbeiten, dieses Schutzniveau nicht.

→ **Es sollte die Nutzung US-amerikanischer Cloud-Dienste geprüft, ggf. darüber informiert werden und wenn möglich eine entsprechende Einwilligung eingeholt werden!**

Auswahl & Verwendung von Cloud/Online-Diensten?

1. **Vor allem für Pflicht-Aktivitäten**: möglichst EU-Dienstleistungen & EU-Serverstandorte

2. Wo aus Gründen der Praktikabilität auf US-Online-Dienste oder Online-Dienste mit Datenverarbeitung auf US-amerikanischen Servern zurückgegriffen wird
   → **darüber informieren und möglichst (implizite) Einwilligung einholen (bspw. Zoom)**

3. **Schaut Euch immer die Einstellungsmöglichkeiten an!** Oft geht‘s datensparsamer, bspw. sind Server-Standorte wählbar oder eine bessere Verschlüsselung möglich und Nutzerrechte auf die nötigen Personen einschränkbar

- **ACHTUNG: Aktuelle Abmahnungswelle wegen der Einbettung von GoogleFonts auf Webseiten → auf https://sicher3.de/google-fonts-checker/ Webseite prüfen und ggf. von Webseiten-Host lokal hosten lassen**

- ACHTUNG: Auch öffentliche Social Media Seiten (Fan-Pages) sind aktuell nicht DSGVO-konform zu nutzen. → Unbedingt in den Datenschutzinformationen der Webseite mit aufführen & Rechtsdurchsetzung / mögliche Abmahnwelle im Auge behalten!

Beispiel Messengerdienste

Unterschiede beim Datenschutz by design & by default

1. WhatsApp & Signal: Ende-zu-Ende-Verschlüsselung: Auch die Betreiber:innen haben keinen Zugriff auf den Inhalt der Nachrichten. Aber im Fall von WhatsApp sehr wohl auf alle Kontakte – ohne deren Einwilligung!
2. Signal nutzt weitere Maßnahmen, um Datensparsamkeit durch Technikgestaltung und gewählte Voreinstellungen zu unterstützen. Das sog. Zero-Knowledge-Prinzip stellt sicher, dass auch die Betreiber:innen keinen Zugriff auf die Nutzerdaten haben.
    1. Langzeitverschlüsselung: Mittels Perfect Forward Secrecy wird sichergestellt, dass es nicht möglich ist, bei Bekanntwerden eines eigentlich geheimen persönlichen User:innen-Schlüssels ältere Nachrichten zu entschlüsseln. Aus der Ende-zu-Ende-Verschlüsselung heraus werden für jede Nachricht temporäre Schlüssel erstellt, die nach Zustellung der Nachricht wieder gelöscht werden.
    2. Verschlüsselte Nutzerprofile: Nur autorisierte Kontakte des / der Signal-User:in können das eigene Nutzerprofil sehen und erhalten darauf Zugriff. Auch der Zugriff durch die Betreiber:innen ist hierdurch ausgeschlossen.
    3. Telefonbuch: Die Telefonbuch-Kontakte der Signal-User:innen werden nicht auf die Betriebsserver geladen.
    4. PIN: Die persönlichen Informationen bei Signal werden mit einem persönlichen PIN gesichert und geschützt.
    5. Gesprächsverschlüsselung: Diese erfolgt wie bei den Nachrichten über das Signal-Protokoll.
    6. Tracking: Signal setzt ausdrücklich keine Tracking-Technologien ein. Das heißt, dass auch Ihre Meta-Daten (wie Geräteinformationen oder Art und Häufigkeit der Nutzung) bei Signal nicht ausgewertet werden.

Die Allgegenwärtigkeit von Online-Diensten

1. Speicherkapazitäten →	Dropbox, Google Drive, Microsoft OneDrive, YourSecureCloud, NextCloud, etc.
2. Emails & Kalender →	Outlook, Gmail, Yahoo Mail, Web.de, Telekom Mail, Posteo, mailbox, etc.
3. Soziale Medien →	Facebook, Instagram, Twitter, TicToc, YouTube, LinkedIn, Xing, Pinterest, etc.
4. Messengerdienste →	WhatsApp, Telegram, Signal, Snapchat, Skype, Threema, Wire, etc.
5. Projektmanagement →	Trello, Asana, Meistertask, Zenkit To Do, todoist, etc.
6. Videokonferenzen →	Jitsi / fairmeeting, BigBlueButton, Teams, Zoom, Alfaview, Skype, etc.
7. Veranstaltungsmanagent →	eventbrite, eventim, guestoo
8. Newsletter →	sendinblue, CleverReach, Rapidmail, Mailchimp
9. Fundraising →	RaiseNow, FundraisingBox, betterplace, GRÜN spendino, Twingle

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Welche Cloud/Online-Dienste werden wie verwendet?

1. Welche Online-Dienste / Tools verwendet Ihr, bei denen digitale personenbezogene Daten verarbeitet werden?
2. Welche davon sind aus den USA oder nutzen dortige Speicherkapazitäten?
3. Nutzt Ihr bereits datenschutzfreundliche Einstellungen?
4. Nutzt Ihr den Dienst nur intern oder werden Daten externer Personen verarbeitet?
5. Wenn extern: auf welche Dienste geht Ihr bereits in den Datenschutzinformationen auf der Webseite ein – welche sollten evtl. ergänzt werden?
6. Welche Dienste solltet Ihr noch einmal prüfen?

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

Was macht eine korrekte Einwilligung aus?

- **informiert** (auf Basis Datenschutzhinweisen)
- **aktiv** (keine vorgesetzten Haken, kein „opt-out“ sondern „opt-in“)
- **zweckspezifisch** (alle vorgesehenen Zwecke sollten aufgeführt sein)
- **nachweisbar** (möglichst digital mit „Zeistempel“ oder als Vermerk)
- **durch die betroffene Person selbst** (Ausnahme Kinder & Jugendliche unter 16 Jahren oder Menschen mit Vormund, dann durch Erziehungsberechtigte/Vormund)

Die Vereins-Webseite

- In den **Datenschutzinformationen** der Webseite können alle Datenschutzinformationen zu relevanten Datenverarbeitungsprozessen gesammelt bereitgestellt werden
  (Empfehlung: Teil-Überschriften als Anker für einzelne Abschnitte zu nutzen, bspw. Datenverarbeitung im Zusammenhang mit der Spendenbearbeitung, Newsletter, Social Media Kanäle, Teilnahme an digitalen Veranstaltungen, etc.)

- Überall, wo Ihr Besucher:innen der Webseite zur Kontaktaufnahme einladet oder Daten abfragt (Kontaktformular, Spendenformular, Adresse, Newsletter-Abo, etc.) sollte dann zu (entsprechendem Abschnitt in den) Datenschutzinformationen verlinkt werden (→ Hinweise zur Datenverarbeitung finden Sie hier in unseren Datenschutzinformationen)

- Werden externe Programme („Cookies“) in die Webseite eingebunden (bspw. Social-Media-Plug-Ins, Google Analytics), so dürfen diese erst nach einer Einwilligung aktiviert werden → mithilfe des sogenannten **„Cookie-Banners“** können Besucher:innen entscheiden, ob sie nur die technisch notwendige Datenverarbeitung erlauben oder dem Einsatz darüber hinausgehender Datenverarbeitung zu (gewerblichen) Analysezwecken einwilligen

- **ACHTUNG: Aktuelle Abmahnungswelle wegen der Einbettung von GoogleFonts auf Webseiten! → Mit Webseiten-Host klären ob GoogleFonts bereits lokal gehostet werden.**

Beispiele

Datenschutzhinweise abseits der Webseite?

1. Vereinsmitglieder (im Mitgliedschaftsantrag)
2. Zu veröffentlichte Interviews
3. Im Zusammenhang mit Spendenwerbung abseits der Webseite
4. Im Zusammenhang mit Veranstaltungen (digital vor Anmeldung, bei Vor-Ort-Anmeldung ausgedruckt ausliegend)
5. ...

Zusammenfassendes Leitmotiv – Erwartbarkeit

Kann die betroffene Person davon ausgehen, dass ihre Daten …

- für die vorgesehenen Zwecke und
- durch die vorgesehenen Beteiligten (ggf. genutzte Cloud-Dienste oder externe Auftragsdatenverarbeitende nicht vergessen)
- auf vorgesehene Weise und unter gegebenen Bedingungen
- über einen vorgesehenen Zeitraum
- angemessen geschützt
- und wo nötig nur auf Basis einer Einwilligung

… verarbeitet werden?

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

DSEE-AKADEMIE · DSEE-AKADEMIE ·

fix&fertig.

Datenschutzhilfen für Zivilgesellschaft

Sofia Vester | fixundfertig@posteo.de | www.fixundfertig.online

Datenschutzberatung | begleitete DSGVO-Umsetzung | Team-Qualifizierung
für Engagierte in Vereinen, NGOs und Stiftungen

DEUTSCHE STIFTUNG
FÜR ENGAGEMENT
UND EHRENAMT

DSEE-AKADEMIE · DSEE-AKADEMIE ·

VIELEN DANK