FrOSCon
Free and Open Source Software Conference

STIFTUNG DATENSCHUTZ

Webbasierte Dienste datenschutzkonform betreiben

Warum Datensparsamkeit nicht genug ist, um DSGVO-konform zu sein.

Hendrik vom Lehn
Stiftung Datenschutz

Online-Vortrag, 22. August 2022
(vorbereitet für die FrOSCon, 20. + 21. August 2022)

about:Stiftung%20Datenschutz

STIFTUNG DATENSCHUTZ

DATENSCHUTZ IM EHRENAMT

Mit unserem erweiterten Informationsangebot für im Ehrenamt Aktive bieten wir konkrete Praxishilfen für die Umsetzung des Datenschutzes in der täglichen Arbeit in Vereinen und gemeinnützigen Organisationen. Ob einfache Mitgliederverwaltung, die Nutzung von Cloud-Diensten, die Öffentlichkeitsarbeit mittels Webseite und Social Media oder die Durchführung von Online-Veranstaltungen – Digitales ist bei vielen Vereinen und gemeinnützigen Organisationen inzwischen Alltag.

ÜBERBLICK

Basiswissen | Praxisratgeber | Webinare | Generator

PRAXISTHEMEN

Hauptaufgabe der Stiftung ist die Förderung effektiven und effizienten Datenschutzes. Dazu veröffentlicht die Stiftung eine Reihe von Broschüren für Betriebe und Beschäftigte sowie Handreichungen mit Erläuterungen zu den Anwendungsempfehlungen der Datenschutzkonferenz zur Umsetzung des DSGVO in der Praxis.

ÜBERBLICK

Datenschutz im Betrieb | Beschäftigtendatenschutz

Internationale Datentransfers | Standard-Datenschutzmodell

about:me

STIFTUNG DATENSCHUTZ

Background:

Informatiker und Policy-Analyst
Zertifizierter Berater für Datenschutzrecht (FernUni Hagen)

Blog:

https://vereint.digital/

Hauptberuflich:

STIFTUNG DATENSCHUTZ

Referent für Datenschutzrecht

Ehrenamtlich:

frei • föderiert • transparent
freiburg.social

Datenschutzbeauftragter

Social Media:

@hendrik@freiburg.social

hendrikvomlehn

Wenn man über digitale Souveränität spricht, kommt man an Themen wie Open Source nicht vorbei, da sich dadurch Abhängigkeiten reduzieren lassen und kritische Infrastruktur – das hat die Pandemie gezeigt – nicht in der Hand ein paar weniger Akteure liegen sollte und der Datenschutz hat dabei den Stellenwert hat, den er verdient. Offene Software ist dezentral, es wird Wert auf Datensicherheit und Privatsphäre gelegt, die Unabhängigkeit von großen Akteuren bleibt gewahrt und sorgt dadurch für die oft geforderte digitale Souveränität, die eines der strategischen Ziele der aktuellen EU-Kommission ist. Offene Software kann und sollte ein Baustein einer wirklichen digitalen Souveränität von Nut-zer*innen

STIFTUNG DATENSCHUTZ

https://www.b-b-e.de/bbe-newsletter/newsletter-nr-2-vom-2112021/staiger-digitale-souveraenitaet-open-source-gesellschaft/

Vorteile durch Open Source:

- Open Source ist anbieterunabhängig. Die Software kann weiterhin durch externe Anbieter entwickelt und gehostet werden. Die Rechte am Source Code sind jedoch offen, wodurch der Anbieter gewechselt werden kann.
- Durch Open Source ist der Bund frei in der Gestaltung der Software. Fehlt beispielsweise ein Arbeitsschritt oder kann ein Arbeitsschritt entfernt werden, so kann der Bund dies bei einem beliebigen Anbieter beauftragen und umsetzen lassen.
- Datenschutz und Sicherheit stehen an oberster Stelle. Es ist kein Vertrauen in einen Anbieter notwendig. Ein Audit kann von einem beliebigen a

https://epetitionen.bundestag.de/content/petitionen/_2022/_02/_04/Petition_130482.html

Bei der Auswahl von Video- oder Telefonkonferenzsystemen sollte aus technischer Sicht darauf geachtet werden, dass der Anbieter weder Metadaten (wer hat wann mit wem kommuniziert) noch die Inhaltsdaten der Kommunikation für eigene Zwecke auswertet oder an Dritte weitergibt. Dies können datenschutzrechtlich Verantwortliche am besten sicherstellen, wenn sie oder ihr Dienstleister (im öffentlichen Bereich sind das z.B. BITBW bei Landesbehörden oder **Komm.ONE** bei Kommunen) eine entsprechende Softwarelösung „On Premises“ – also im eigenen Rechenzentrum – bereitstellen oder aufbauen. Dadurch ist es möglich, alle Datenflüsse und Datenerhebungen selbst zu kontrollieren. Dazu bieten sich zahlreiche Lösungen auf Basis von Open-Source-Software an (z.B. Nextcloud Talk, BigBlueButton oder Matrix), die prinzipiell datenschutzgerecht einsetzbar sind.

https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

STIFTUNG DATENSCHUTZ

Bildquelle:
Markus Meier, CC-BY-SA
Zum Download bei der fsfe.

FLOSS == datenschutzfreundlich?

STIFTUNG DATENSCHUTZ

FLOSS:

[0] Verwenden: ausführen, wie und wofür man will

[1] Verstehen: Software analysieren und anpassen

[2] Verbreiten: Kopien verteilen bzw. erhalten

[3] Verbessern: Kopien angepasster Versionen verteilen bzw. erhalten

(Die 4 Freiheiten freier Software)

DSGVO:

- *Vertraulichkeit*
- *Integrität*
- *Verfügbarkeit*
- Transparenz
- Intervenierbarkeit
- Nichtverkettung
- Datenminimierung

(Die 7 Gewährleistungsziele des SDM)

DSGVO – relevante Pflichten

STIFTUNG DATENSCHUTZ

Grundsätze
(Art. 5 DSGVO)

Rechtsgrundlagen
(Art. 6 und 9 DSGVO)

Informationspflichten
(Art. 12-14 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten
(Art. 30 DSGVO)

gemeinsame Verantwortung
Verarbeitung im Auftrag
(Art. 26 und28 DSGVO)

Übermittlung in Drittländer
(Art. 44-47 und 49 DSGVO)

Betroffenenanfragen
(Art. 15-18 und 20 DSGVO)

„technisch-organisatorische Maßnahmen“ / IT-Sicherheit
(Art. 32 DSGVO)

„privacy by design“ und „privacy by default“
(Art. 25 DSGVO)

Gute Auswahl der Software

STIFTUNG DATENSCHUTZ

Grundsätze
(Art. 5 DSGVO)

Rechtsgrundlagen
(Art. 6 und 9 DSGVO)

Informationspflichten
(Art. 12-14 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten
(Art. 30 DSGVO)

gemeinsame Verantwortung
Verarbeitung im Auftrag
(Art. 26 und28 DSGVO)

Übermittlung in Drittländer
(Art. 44-47 und 49 DSGVO)

Betroffenenanfragen
(Art. 15-18 und 20 DSGVO)

„technisch-organisatorische Maßnahmen“ / IT-Sicherheit
(Art. 32 DSGVO)

„privacy by design“ und „privacy by default“
(Art. 25 DSGVO)

Hosting in gut gewähltem Rechenzentrum

STIFTUNG DATENSCHUTZ

Grundsätze
(Art. 5 DSGVO)

Rechtsgrundlagen
(Art. 6 und 9 DSGVO)

Informationspflichten
(Art. 12-14 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten
(Art. 30 DSGVO)

gemeinsame Verantwortung
Verarbeitung im Auftrag
(Art. 26 und28 DSGVO)

Übermittlung in Drittländer
(Art. 44-47 und 49 DSGVO)

Betroffenenanfragen
(Art. 15-18 und 20 DSGVO)

„technisch-organisatorische Maßnahmen“ / IT-Sicherheit
(Art. 32 DSGVO)

„privacy by design“ und „privacy by default“
(Art. 25 DSGVO)

Software-as-a-Service

STIFTUNG DATENSCHUTZ

Grundsätze
(Art. 5 DSGVO)

Rechtsgrundlagen
(Art. 6 und 9 DSGVO)

Informationspflichten
(Art. 12-14 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten
(Art. 30 DSGVO)

gemeinsame Verantwortung
Verarbeitung im Auftrag
(Art. 26 und28 DSGVO)

Übermittlung in Drittländer
(Art. 44-47 und 49 DSGVO)

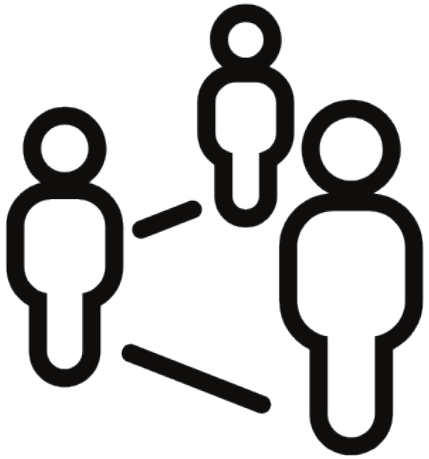
Betroffenenanfragen
(Art. 15-18 und 20 DSGVO)

„technisch-organisatorische Maßnahmen“ / IT-Sicherheit
(Art. 32 DSGVO)

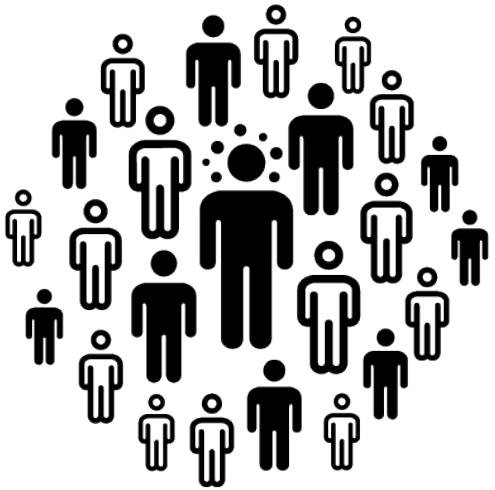
„privacy by design“ und „privacy by default“
(Art. 25 DSGVO)

DSGVO – Rollen und Verantwortlichkeiten

Auftragsverarbeiter

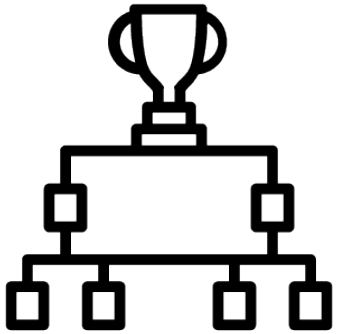


Verantwortlicher



Betroffene

Auftragsverarbeiter (Kette)



Eigener Verantwortlicher

Was tun? (beim Betrieb)

STIFTUNG DATENSCHUTZ

Als Verantwortlicher:

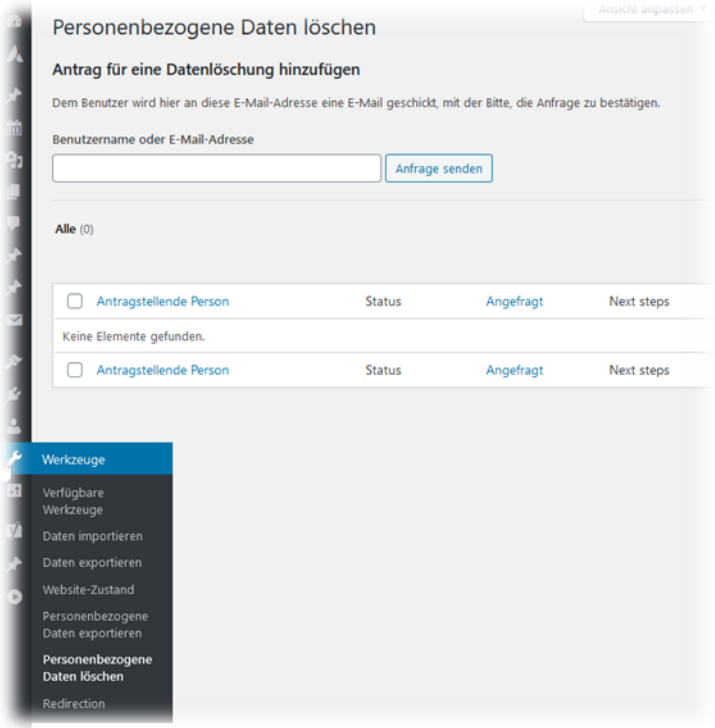
1. Software sorgfältig auswählen
2. Passende Ebene des Hostings wählen
    a) Guten Hoster wählen und AV-Vertrag abschließen
    b) Ggf. den eigenen Betrieb sicher aufstellen
3. Interne Zuständigkeiten und Zugriffsregelungen klären
4. Rechtsgrundlagen klären
5. VVT ergänzen
6. Datenschutzhinweise zur Verfügung stellen (auch online/über den Dienst selbst)
7. Eventuelle Betroffenenanfragen beantworten

Für andere Organisationen: (als Auftragsverarbeiter)

1. Den eigenen Betrieb sicher aufstellen
2. Ggf. AV-Vertrag mit Hoster abschließen
3. AV-Vertrag mit Organisation abschließen
4. VVT als Auftragsverarbeiter erstellen
5. Unterstützung bei Betroffenenanfragen
6. Ggf. Muster für Datenschutzhinweise (bei SaaS)

Was tun? (als Entwickler)

- Zumindest Möglichkeiten zur Verlinkung von Impressum und Datenschutzhinweisen einbauen.
- DSGVO-kompatible Templates für Datenschutzhinweise zur Verfügung stellen.
  - Wenn möglich, in den Setup-Prozess mit einbauen.
- Dafür sorgen, dass Daten gezielt gelöscht werden können.
- Tools für den Umgang mit Betroffenenanfragen bereit stellen (siehe z.B. Wordpress →).
- Guide erstellen, was als Nutzer der Software für DSGVO-konformen Betrieb notwendig ist.



Fazit

- Freie Software ist oft datensparsam, aber DSGVO-Compliance ist mehr.
- Obliegt letztendlich dem „Verantwortlichen“.
- ABER, als Entwickler kann man unterstützen.

- Gedanken zur digitalen Zivilgesellschaft und politischen Rahmenbedingungen: https://vereint.digital/digitale-infrastruktur-fuer-die-zivilgesellschaft-gedanken-zur-rolle-von-open-source-software-und-datenschutz/