

Broschüre zur Grundausbildung Datenschutz und Datensicherheit

—

acf - fgv

association des communes fribourgeoises
freiburger gemeindeverband



ETAT DE FRIBOURG
STAAT FREIBURG

**Autorité cantonale de la transparence, de la protection des données
et de la médiation ATPrDM**

**Kantonale Behörde für Öffentlichkeit, Datenschutz
und Mediation ÖDSMB**



Inhaltsverzeichnis

1. Einführung	3
2. Datenschutz verstehen	4
3. Grundsätze der Datensicherheit	6
4. Pflichten und Verantwortlichkeiten	7
5. Gute alltägliche Praktiken	8
6. Verwaltung von Vorfällen (Datensicherheitsverletzungen)	9
7. Ressourcen und Kontakte	10
8. Schlussfolgerung	11

01 Einführung



Ziele der Ausbildung

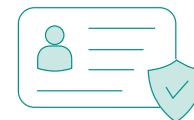
Die Grundlagen des Datenschutzes und der Datensicherheit verstehen.

Kenntnis der Verantwortlichkeiten jedes Einzelnen in Bezug auf den Datenschutz.

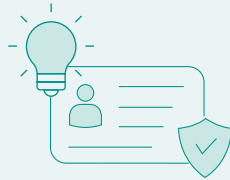
Lernen Sie gute Praktiken, die Sie täglich anwenden können.

Bedeutung des Datenschutzes

Der Schutz personenbezogener Daten und die Gewährleistung der Datensicherheit sind entscheidend, um das Vertrauen der BürgerInnen aufrechtzuerhalten und gesetzliche Sanktionen zu vermeiden.



02 Datenschutz verstehen



Definition und Prinzipien

Der Datenschutz soll sicherstellen, dass persönliche Informationen (Personendaten) sicher, datenschutzgerecht und gesetzeskonform verarbeitet werden.

Gesetzliche Verpflichtungen

Gesetz vom 12. Oktober 2023 über den Datenschutz

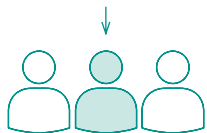
Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten

Rechte der betroffenen Personen (art. 27-35 DschG)

Zugangsrecht:

Definition: Dieses Recht ermöglicht es jeder Person, eine Kopie der sie betreffenden Personendaten, die von einer Organisation oder Einrichtung verarbeitet werden, zu beantragen und zu erhalten.

Ziel: Es soll Einzelpersonen ermöglichen, zu überprüfen, ob ihre Daten rechtmässig verarbeitet werden, und zu verstehen, wie und warum diese Daten verwendet werden.



Recht auf Berichtigung:

Definition: Dieses Recht ermöglicht es jeder Person, die Berichtigung oder Löschung unrichtiger oder unvollständiger Personendaten zu verlangen, die sich im Besitz einer kantonalen oder kommunalen Einheit befinden.



Zweck: Es soll sicherstellen, dass Personendaten genau und aktuell sind, damit keine schädlichen Entscheidungen auf der Grundlage unrichtiger Daten getroffen werden können.

Recht auf Löschung (oder Recht auf Vergessen):

Definition: Dieses Recht ermöglicht es einer Person, die Löschung ihrer Personendaten zu verlangen, insbesondere wenn diese Daten für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr erforderlich sind.

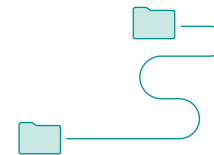
Ziel: Es soll Einzelpersonen ermöglichen, die Verbreitung und Verwendung ihrer Personendaten, insbesondere im Internet, zu kontrollieren.



Recht auf Übertragbarkeit:

Definition: Dieses Recht ermöglicht es einer Person, die Personendaten, die sie einer kantonalen oder kommunalen Einheit zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Ziel: Es soll die Kontrolle des Einzelnen über seine Personendaten stärken.



Widerspruchsrecht (Recht auf Sperrung):

Definition: Dieses Recht ermöglicht es einer Person, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Bearbeitung ihrer Personendaten Widerspruch einzulegen, es sei denn, die Organisation weist zwingende schutzwürdige Gründe für die Bearbeitung nach, die die Interessen und Rechte der betroffenen Person überwiegen, oder es dient der Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht.

Ziel: Es soll Einzelpersonen zusätzliche Kontrolle über die Verwendung ihrer Personendaten geben, insbesondere wenn diese Verwendung Auswirkungen auf ihre Grundrechte und Freiheiten haben kann.



03 Grundsätze der Datensicherheit



Datenschutz

Stellen Sie sicher, dass nur berechtigte Personen auf die Informationen zugreifen können.



Integrität

Achten Sie darauf, dass die Informationen richtig und vollständig sind.



Verfügbarkeit

Stellen Sie sicher, dass Informationen verfügbar sind, wenn sie benötigt werden.

04 Pflichten und Verantwortlichkeiten



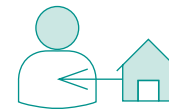
Angestellte und externe AuftragsbearbeiterInnen

Beachten Sie die Sicherheitsrichtlinien und -verfahren.

Verwenden Sie starke und sichere Passwörter.

Melden Sie alle Vorfälle oder Anomalien (Datensicherheitsverletzung).

Informationen nicht an unbefugte Personen oder Organisationen weitergeben. Sie sind an das **Amtsgeheimnis** bzw. das **Berufsgeheimnis** für externe AuftragsbearbeiterInnen gebunden.



GemeinderätInnen

Wenden Sie die gleichen Vertraulichkeitsregeln an wie Ihre Angestellten.

Befolgen Sie die spezifischen Bestimmungen der Gemeindegesetzgebung.



Datensicherheitsbeauftragte

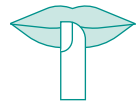
Gewährleistung der Umsetzung von Sicherheitsrichtlinien (Datensicherheit).

Schulung und Sensibilisierung von Mitarbeitenden und gewählten VertreterInnen.

Auf Sicherheitsvorfälle reagieren (Datensicherheitsverletzung).



05 Gute alltägliche Praktiken



Verwaltung von Zugängen

- Verwenden Sie komplexe Passwörter.
- Geben Sie Ihre Logins nicht weiter.
- Verwenden Sie die Multi-Faktor-Authentifizierung.



Physische Sicherheit

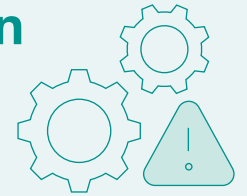
- Sperren Sie Ihren Arbeitsplatz, wenn Sie nicht da sind.
- Sichern Sie sensible Dokumente.



Nutzung von Arbeitsmitteln

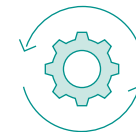
- Verwenden Sie nur erlaubte Software und Geräte.
- Vermeiden Sie es, persönliche Geräte ohne Erlaubnis für berufliche Aufgaben zu verwenden.

06 Verwaltung von Vorfällen (Datensicherheitsverletzung)



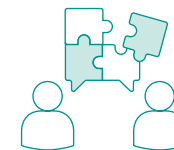
Erkennen eines Vorfalls

- Achten Sie auf ungewöhnliches Systemverhalten und verdächtige E-Mails.
- Melden Sie jeden Vorfall sofort.



Verfahren für die Meldung

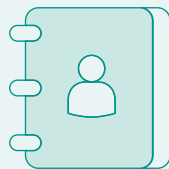
- Informieren Sie die IT-Abteilung oder den Datensicherheitsbeauftragten.
- Befolgen Sie die Verfahren zur Dokumentation der Vorfälle.



Reaktion auf Vorfälle

- Ergreifen Sie sofort Massnahmen, um den Schaden zu begrenzen.
- Arbeiten Sie mit der IT-Abteilung zusammen, um das Problem zu lösen.

07 Ressourcen und Kontakte



Referenzdokumente

Gesetz vom 12. Oktober 2023 über den Datenschutz

Reglement vom 29. Juni 1999 über die Sicherheit
der Personendaten

Leitfäden der ÖDSMB



Nützliche Kontakte

IT-Abteilung der Gemeinde

**Verantwortliche Person für den Datenschutz
und die Datensicherheit in der Gemeinde**

8. Schlussfolgerung



Wir danken Ihnen für Ihr Engagement, diese Richtlinien zu befolgen und die Daten und die Datensicherheit. Ihre Rolle ist entscheidend, um die Sicherheit und Vertraulichkeit sensibler Informationen zu gewährleisten.

Wenn Sie Fragen haben oder weitere Informationen benötigen, wenden Sie sich bitte an die IT-Abteilung oder die mit der Datensicherheit beauftragte Person.

Hinweis: Diese Broschüre ist Bestandteil Ihrer Grundausbildung. Bitte lesen Sie jeden Abschnitt sorgfältig durch und befolgen Sie die aufgeführten Richtlinien, um den Datenschutz und die Datensicherheit) in unserer Gemeinde zu gewährleisten.

**Kantonale Behörde für Öffentlichkeit und,
Datenschutz und der Mediation**

Rue des Chanoines 2, 1700 Fribourg
T +41 26 322 50 08

www.fr.ch/de/sk/oedsmb

September 2024



Broschüre erstellt von
Arbeitsgruppe SGV/ÖDSMB