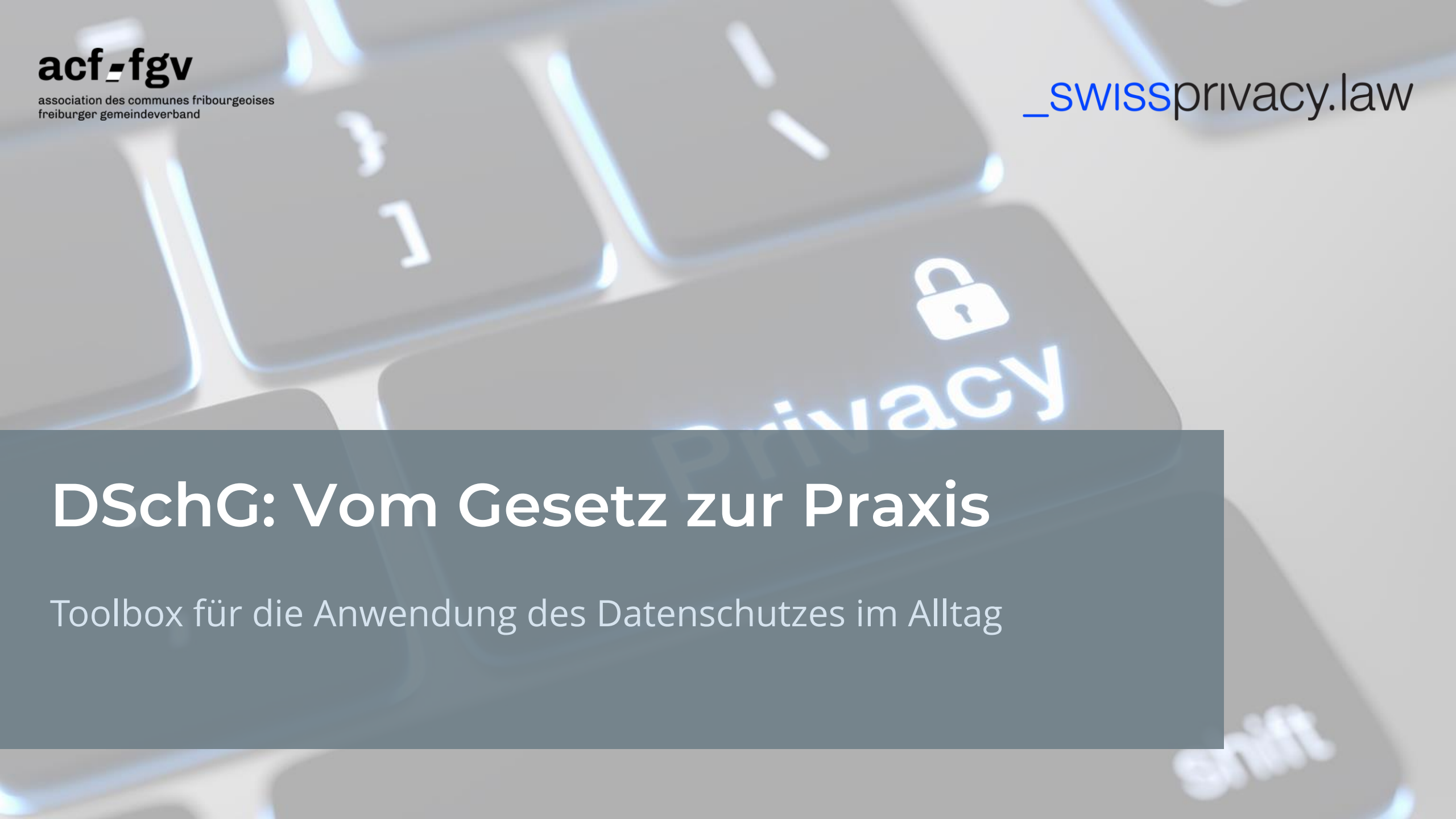
acf-fgv
association des communes fribourgeoises
freiburger gemeindeverband

_swissprivacy.law



DSchG: Vom Gesetz zur Praxis

Toolbox für die Anwendung des Datenschutzes im Alltag

Über mich

- Hermine Lacour, Dr. iur.
  - Juristin – ICT-Recht
  - Mitwirkende für www.swissprivacy.law

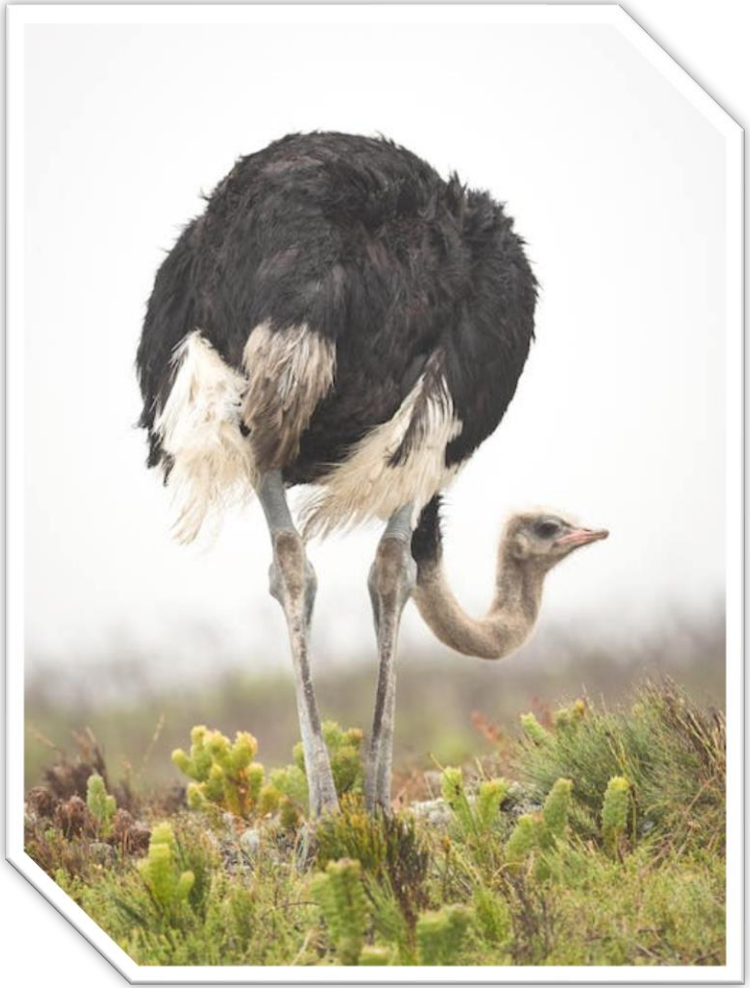
- Für mehr Informationen über Swissprivacy : www.swissprivacy.law
  - Gründer/innen : Eva Cellina, Célian Hirsch, Baptiste Favez, Kastriot Lubishtani, Frédéric Erard und Livio di Tria

- Bei Fragen zu dieser Präsentation können Sie sich an Livio di Tria schreiben.
  - livio.ditria@swissprivacy.law

Strategie
Antizipieren

- Der Verantwortliche der Datenbearbeitung hat zwei Jahre Zeit, um die Vorschriften umzusetzen.
  - Diese Frist gilt nicht für Bestimmungen über Verletzungen der Datensicherheit.

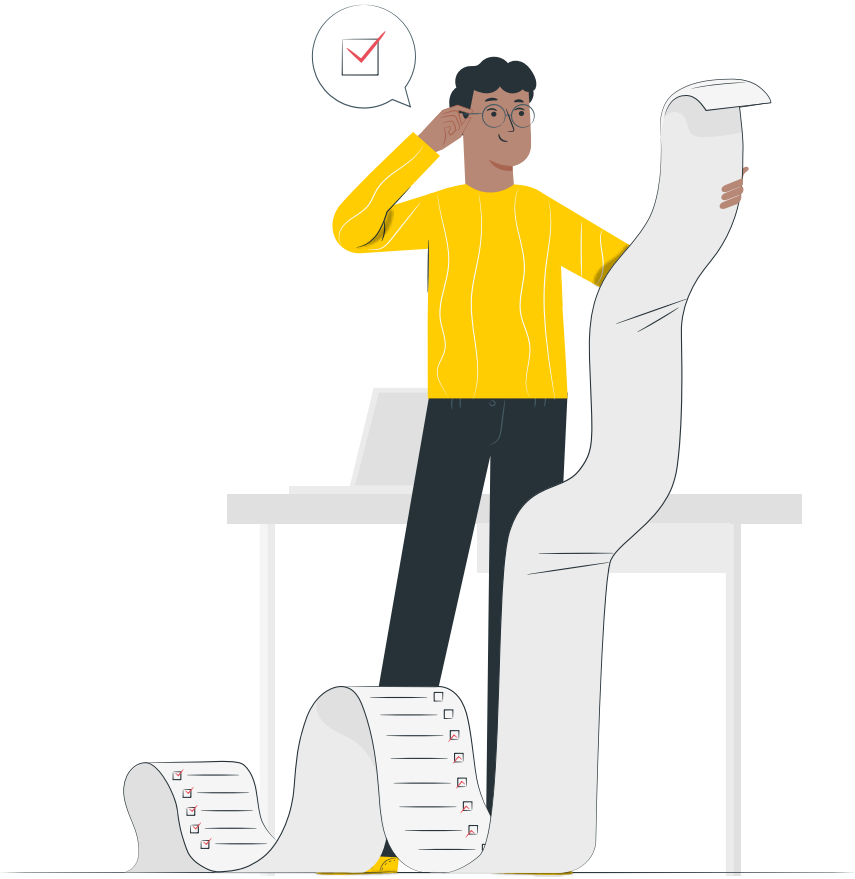
- Damit eine wirksame und nachhaltige Umsetzung gewährleistet werden kann, muss diese **schrittweise** erfolgen.
  - Bevorzugen Sie «***quick win***» und vermeiden Sie Komplexität.



Strategie

Schritt um Schritt

- Bearbeitungsregister.
- Risikobewertung.
- Sicherheitsmassnahmen.
- Management von Sicherheitsvorfällen.
- Unteraufträgen und Externalisierung.
- Weitere wichtigen Aspekte.
- Datenschutzbeauftragter.
- Schulung und Sensibilisierung.



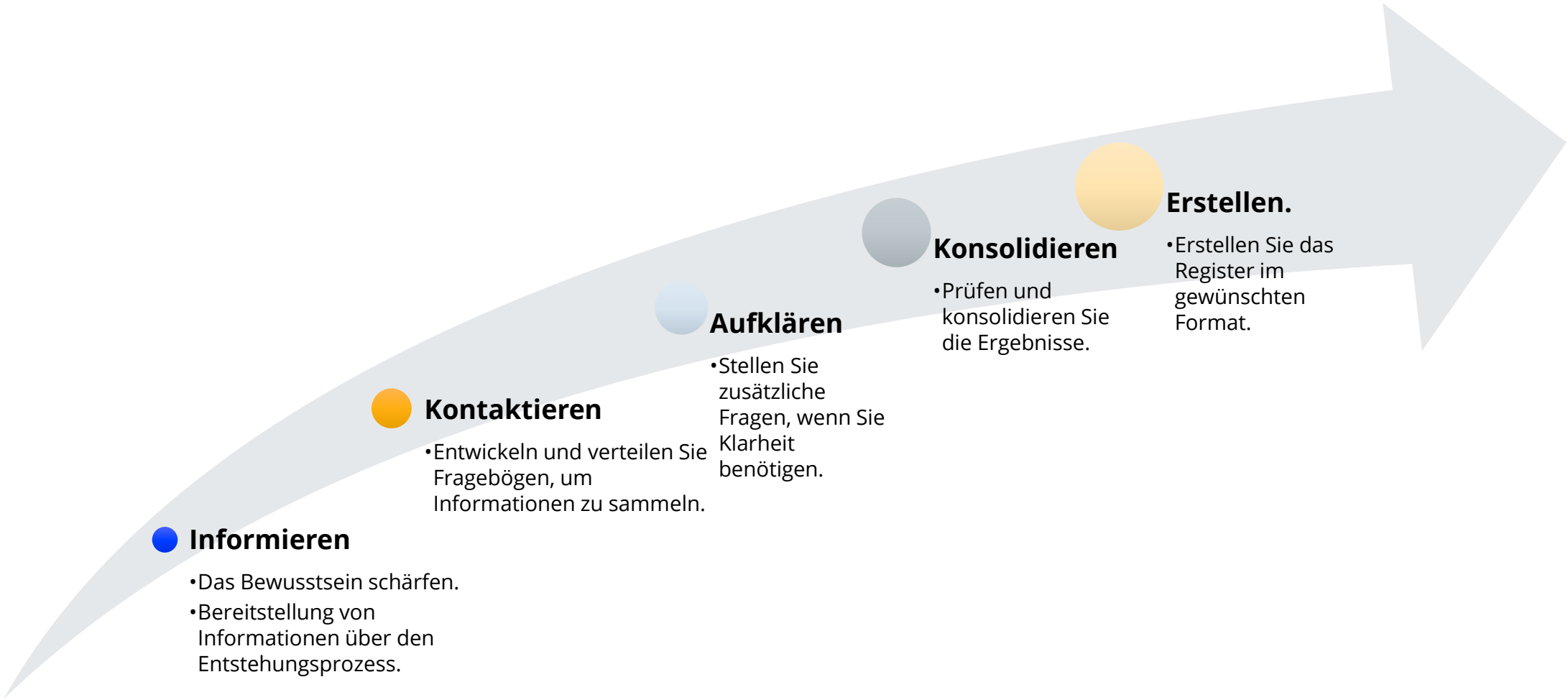
Bearbeitungsregister

Schlüsselelement

- Stellt ein Schlüsselelement dar, denn es ist der **Ausgangspunkt**:
  - für andere Rechte und Pflichten;
  - für die Risikobewertung und die Durchführung von Sicherheitsmassnahmen;
  - für alle Kontrollen der kantonalen Behörde für Öffentlichkeit, Datenschutz und Mediation (ÖDSMB).
- Ziel ist die Erstellung eines **internen Inventars** für jede **Bearbeitung** innerhalb der Gemeinde (internes Register).
  - Erwägen Sie einen Ansatz nach Abteilung/Dienststelle (z. B. Personalabteilung, Einwohnermeldeamt, Technischer Dienst, Finanzdienst).
  - Im Gesetz sind die Mindestangaben aufgeführt, die das Register enthalten muss (z. B. Zweck(e) der Verarbeitung, Beschreibung der Kategorien von betroffenen Personen und der Kategorien von verarbeiteten personenbezogenen Daten, regelmässige Empfänger von Daten, Auftragsverarbeiter).
    - Erwägen Sie einen **umfassenderen Ansatz**.
- Jeder Verantwortliche meldet dem ÖDSMB die von ihm durchgeführten Verarbeitungstätigkeiten und deren nachfolgende Änderungen (externes Register).
- Keine statische Aufgabe – **regelmässige** und **dynamische** Registerführung.

Bearbeitungsregister

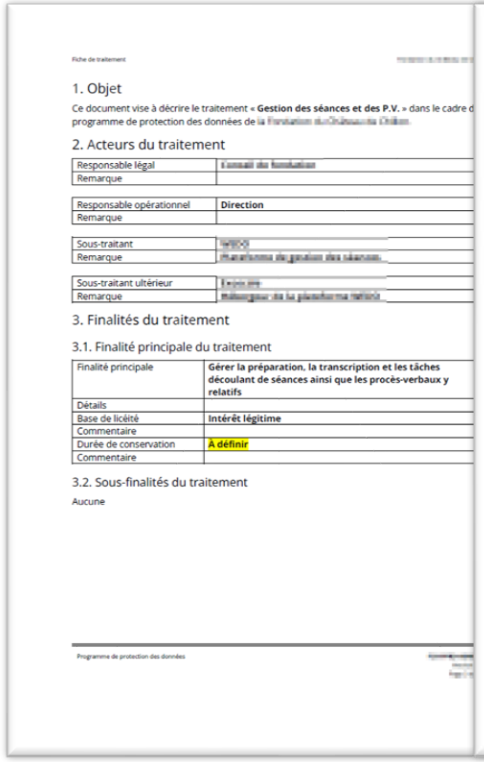
Verfahren



Bearbeitungsregister

Schaffung einer Übersichtstabelle und detaillierter Dokumente

Statut	Référence	Traitement	Responsable opérationnel du traitement	Finalité	Base de licéité	Durée de conservation	Catégories de données	Données sensibles	Catégories de personnes	Catégories de destinataires	AIPD	Comm. à l'étranger
Projet	ADM001	Gestion des séances et des P.V.	Direction	Gérer la préparation, la transcription et les tâches découlant de séances ainsi que les procès-verbaux y relatifs	Intérêt légitime	à définir	Identité, état civil, coordonnées Vie professionnelle Vie personnelle Données économiques Données de connexion	non	Toute personne	Sous-traitants Sous-traitants ultérieurs	non	oui



1. Objet

Ce document vise à décrire le traitement « **Gestion des séances et des P.V.** » dans le cadre d
programme de protection des données de la [illegible]

2. Acteurs du traitement

Responsable légal	[illegible]
Remarque	
Responsable opérationnel	**Direction**
Remarque	
Sous-traitant	[illegible]
Remarque	[illegible]
Sous-traitant ultérieur	[illegible]
Remarque	[illegible]

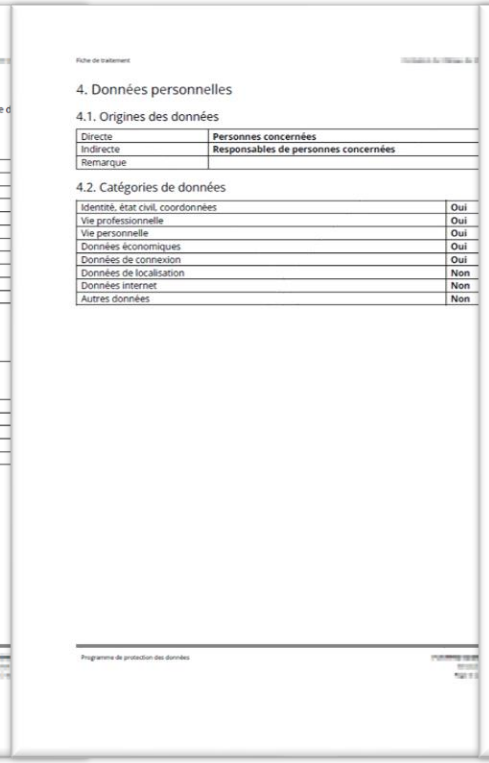
3. Finalités du traitement

3.1. Finalité principale du traitement

Finalité principale	**Gérer la préparation, la transcription et les tâches découlant de séances ainsi que les procès-verbaux y relatifs**
Détails	
Base de licéité	**Intérêt légitime**
Commentaire	
Durée de conservation	**À définir**
Commentaire	

3.2. Sous-finalités du traitement

Aucune



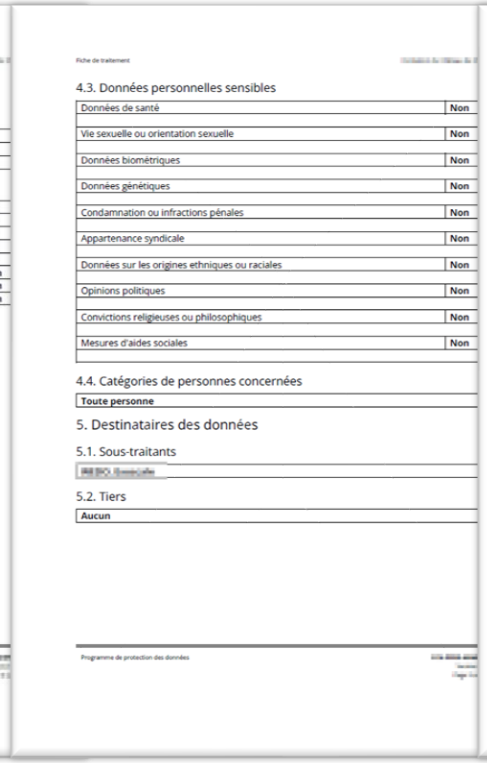
4. Données personnelles

4.1. Origines des données

Directe	**Personnes concernées**
Indirecte	**Responsables de personnes concernées**
Remarque	

4.2. Catégories de données

Identité, état civil, coordonnées	**Oui**
Vie professionnelle	**Oui**
Vie personnelle	**Oui**
Données économiques	**Oui**
Données de connexion	**Oui**
Données de localisation	**Non**
Données internet	**Non**
Autres données	**Non**



4.3. Données personnelles sensibles

Données de santé	**Non**
Vie sexuelle ou orientation sexuelle	**Non**
Données biométriques	**Non**
Données génétiques	**Non**
Condamnation ou infractions pénales	**Non**
Appartenance syndicale	**Non**
Données sur les origines ethniques ou raciales	**Non**
Opinions politiques	**Non**
Convictions religieuses ou philosophiques	**Non**
Mesures d'aides sociales	**Non**

4.4. Catégories de personnes concernées

Toute personne

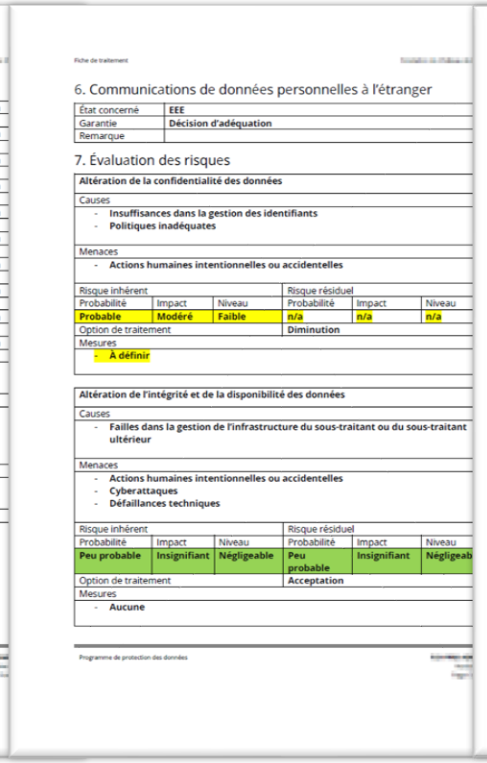
5. Destinataires des données

5.1. Sous-traitants

[illegible]

5.2. Tiers

Aucun



6. Communications de données personnelles à l'étranger

État concerné	**EEE**
Garantie	**Décision d'adéquation**
Remarque	

7. Évaluation des risques

Altération de la confidentialité des données

Causes
- **Insuffisances dans la gestion des identifiants**
- **Politiques inadéquates**

Menaces
- **Actions humaines intentionnelles ou accidentelles**

Risque inhérent			Risque résiduel		
Probabilité	Impact	Niveau	Probabilité	Impact	Niveau
Probable	**Modéré**	**Faible**	**n/a**	**n/a**	**n/a**

Option de traitement: **Diminution**

Mesures
- **À définir**

Altération de l'intégrité et de la disponibilité des données

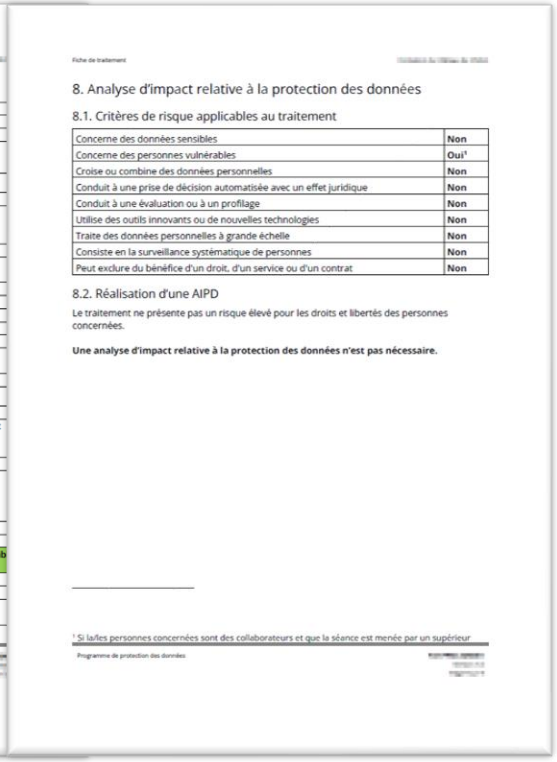
Causes
- **Failles dans la gestion de l'infrastructure du sous-traitant ou du sous-traitant ultérieur**

Menaces
- **Actions humaines intentionnelles ou accidentelles**
- **Cyberattaques**
- **Défaillances techniques**

Risque inhérent			Risque résiduel		
Probabilité	Impact	Niveau	Probabilité	Impact	Niveau
Peu probable	**Insignifiant**	**Négligeable**	**Peu probable**	**Insignifiant**	**Négligeab**

Option de traitement: **Acceptation**

Mesures
- **Aucune**



8. Analyse d'impact relative à la protection des données

8.1. Critères de risque applicables au traitement

Concerne des données sensibles	**Non**
Concerne des personnes vulnérables	**Oui**[1]
Croise ou combine des données personnelles	**Non**
Conduit à une prise de décision automatisée avec un effet juridique	**Non**
Conduit à une évaluation ou à un profilage	**Non**
Utilise des outils innovants ou de nouvelles technologies	**Non**
Traite des données personnelles à grande échelle	**Non**
Consiste en la surveillance systématique de personnes	**Non**
Peut exclure du bénéfice d'un droit, d'un service ou d'un contrat	**Non**

8.2. Réalisation d'une AIPD

Le traitement ne présente pas un risque élevé pour les droits et libertés des personnes concernées.

Une analyse d'impact relative à la protection des données n'est pas nécessaire.

[1] Si la/les personnes concernées sont des collaborateurs et que la séance est menée par un supérieur

Risikobewertung

Allgemein

- Das Bearbeitungsregister ist umfassend und ermöglicht, die **mit der** Verarbeitungstätigkeit **verbundenen Risiken zu** ermitteln.

Sicherheitsmassnahmen

Allgemein

- Die Sicherheitsmassnahmen umfassen im Allgemeinen :
  - **Vertraulichkeit**;
  - **Verfügbarkeit**;
  - **Integrität**;
  - **Nachvollziehbarkeit.**
- Die Sicherheitsmassnahmen müssen sich **nach dem Risikoniveau richten**.
- Zum Beispiel:
  - **Technisch**, z. B. Firewalls oder Software;
  - **Rechtlich**, z. B. vertragliche Verpflichtungen;
  - **Regulatorisch**, z.B. Genehmigungsverfahren;
  - **Führungsaufgaben**, z. B. die Ausbildung des Personals.
- Am besten sind Massnahmen geeignet, über die sich die Experten einig sind (z. B. ISO 27001-Normen).

Behandlung von Zwischenfällen

Unterscheidung zwischen Vorfall und Verletzung

- **Vorfall der Datensicherheit**.
  - Unerwünschtes oder unerwartetes Ereignis, das die Datensicherheit gefährden kann.
  - Führt nicht notwendigerweise zum Verlust personenbezogener Daten, zu deren Änderung, Löschung oder Vernichtung, zur Offenlegung oder zum unbefugten Zugriff auf diese Daten (≠ Verletzung).
    - Ohne Intervention hätte dies jedoch zu einem solchen Ergebnis führen können.
- **Verletzung** der Sicherheit von Personendaten.
  - Jede Verletzung der Sicherheit, die zu einer zufälligen oder unrechtmässigen Änderung der Vertraulichkeit, Verfügbarkeit, Integrität oder Rückverfolgbarkeit von Daten führt.

Behandlung von Zwischenfällen

Massnahmen im Falle einer Verletzung der Sicherheit von Personendaten

- Massnahmen, die im Falle einer **Verletzung** der Sicherheit von Personendaten in **allen Fällen** zu ergreifen sind:
  1. Sofortiges Ergreifen **geeigneter Massnahmen zur** Beendigung des Verstosses und zur Minimierung seiner Auswirkungen.
  2. Halten Sie in einem **internen Dokument** die Art des Verstosses, die Art der betroffenen Daten, die Kategorien der betroffenen Personen, die voraussichtlichen Folgen für sie und die ergriffenen Massnahmen zur Behebung der Situation fest.
- Massnahmen, die im Falle einer **Verletzung** der Sicherheit von Personendaten in **bestimmten Fällen zu** ergreifen sind:
  1. **Benachrichtigung des ÖDSMB über** jede Verletzung, die ein **hohes Risiko** für die Grundrechte der betroffenen Person darstellt.
  2. **Benachrichtigung der betroffenen Person** über das Auftreten einer Verletzung, wenn dies aus **Gründen der Transparenz** erforderlich ist und/oder um die betroffene Person in die Lage zu versetzen, selbst **geeignete Massnahmen zur Wahrung ihrer Interessen zu** ergreifen.

Behandlung von Zwischenfällen

Verfahren

1. **Vorbereitung**: Reaktionsplan.
2. **Identifizierung**: Überwachungsmassnahmen.
3. **Bewertung**: Beurteilung des Schweregrads des Problems.
4. **Intervention**: Beendigung des Vorfalls, Minimierung des Schadens und Wiederherstellung der Daten.
5. **Benachrichtigung**: Benachrichtigung der Betroffenen, falls erforderlich.
6. **Analyse nach einem Zwischenfall**: Lehren ziehen und Massnahmen verbessern.

Behandlung von Zwischenfällen

Reaktionsplan

- Schlüsselelemente eines **Reaktionsplans** zur Vermeidung von Panik :
  - Stellen Sie **Informationen** bereit, wie die Gemeinde auf einen Vorfall der Beeinträchtigung der Datensicherheit reagiert.
  - Legen Sie die **Aufgaben und Zuständigkeiten** der Personen fest, die für die Reaktion auf einen Vorfall verantwortlich sind.
  - Geben Sie **Informationen** über verfügbare Einrichtungen, die bei der Bewältigung des Vorfalls helfen können.
  - Stellen Sie **Strategien** für eine effektive interne und externe Kommunikation bereit.
  - Legen Sie fest, welche **Massnahmen** nach dem Vorfall ergriffen werden sollen.

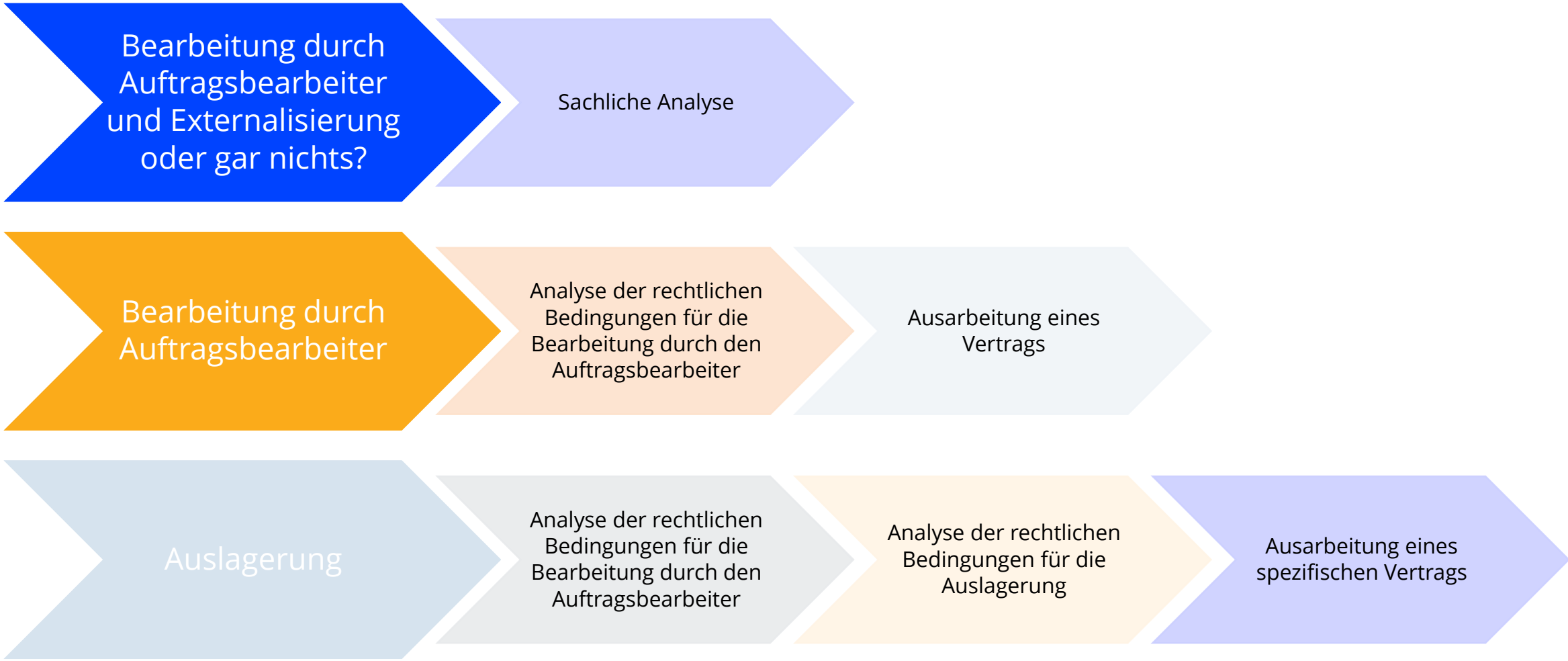
Unteraufträgen und Externalisierung

Was ist der Unterschied?

- **Bearbeitung durch Auftragsbearbeiter (Unterauftragsnehmer):**
- Vorgang, bei dem eine öffentliche Einrichtung einen Teil ihrer Beitungstätigkeiten an ein externes Unternehmen (z. B. Treuhänder, Personalvermittlungsagenturen, Marketingagenturen) oder an eine dritte öffentliche Einrichtung überträgt.
  - Betriebliche Effizienz, Kostensenkung, Spezialisierung, Flexibilität.
- **Externalisierung:** Form der Vergabe von Unteraufträgen.
  - Alles, was die Nutzung von IT-Ressourcen zur Speicherung, Verarbeitung und gemeinsamen Nutzung von Daten beinhaltet.
  - ***Cloud*** Computing-Dienste.

Unteraufträgen und Externalisierung

Etappen



Unteraufträgen und Externalisierung

Verträge zur Bearbeitung durch Auftragsbearbeiter

Keine Mindestvorgaben für den **Vertrag**. Empfehlungen?

1. Präambel.
2. Definitionen.
3. Umfang und Gegenstand (Zweck, Dauer, Art).
4. Verpflichtungen des Unterauftragnehmers (Anweisungen, Geheimhaltungspflichten, Schutzmassnahmen, Mitwirkungspflichten, Recht auf Prüfung).
5. Ort, an dem die Bearbeitung durchgeführt wird.
6. Nachträgliche Vergabe von Unteraufträgen.
7. Art der bearbeiteten Daten.
8. Ausserordentliches Kündigungsrecht.
9. Schlussbestimmungen.

Andere wichtige Aspekte

Informationspflicht und Datenschutzerklärung

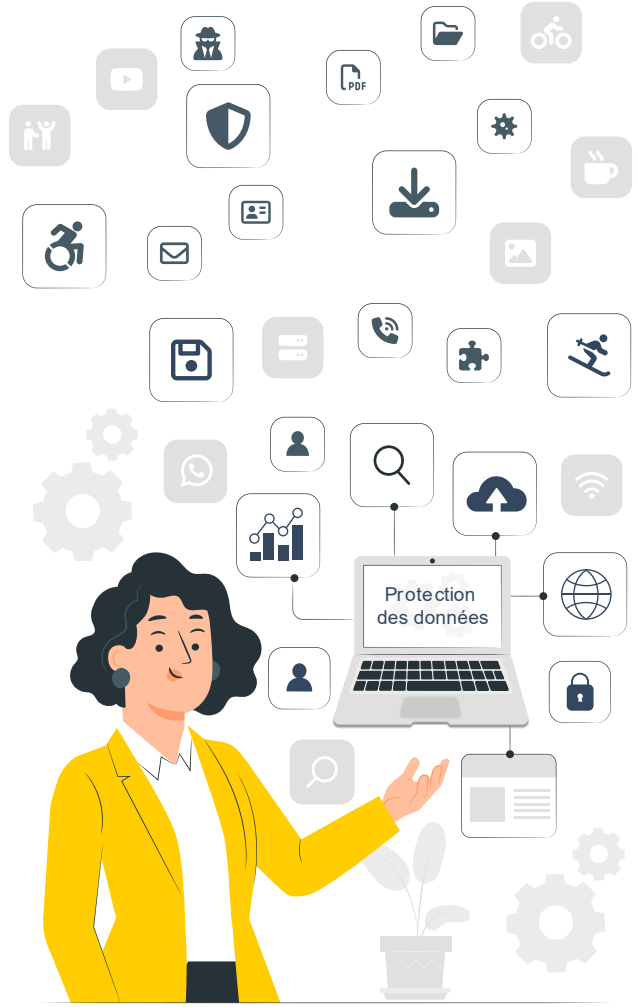
- Der für die Bearbeitung Verantwortliche muss die betroffene Person informieren, insbesondere durch die Bereitstellung von Informationen:
  - Kontaktinformationen;
  - Zweck der Verarbeitung;
  - Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten übermittelt werden;
  - obligatorische oder fakultative Datenerhebung.
- Nicht notwendig, wenn die (Daten-)Erhebung aufgrund einer **gesetzlichen Verpflichtung erfolgt** (in den meisten Fällen).
  - Gilt nicht für Webseiten
    - Notwendigkeit einer Datenschutzerklärung je nach Verarbeitung (z. B. obligatorische Cookies, statistische Cookies).

Andere wichtige Aspekte

Informationspflicht und Datenschutzerklärung

Erklärung zum Datenschutz

1. Einführung
2. Wer wir sind und wie Sie uns kontaktieren können.
3. Was ist unsere Rolle beim Datenschutz?
4. Wann und wie erheben wir Ihre Daten?
5. Welche Kategorien von Daten verarbeiten wir?
6. Warum verarbeiten wir Ihre Daten?
7. Welche Rechte haben Sie?
8. Wie sichern wir Ihre Daten?
9. Wo werden Ihre Daten gespeichert?
10. Wie lange bewahren wir Ihre Daten auf?
11. Mit wem teilen wir Ihre Daten?
12. Welche Cookies verwenden wir?
13. Welche sozialen Netzwerke nutzen wir?



Andere wichtige Aspekte

Rechte und Verfahren

- Rechte im Besonderen:
  - Recht auf Zugang;
  - Recht auf Übertragbarkeit;
  - Recht, der Weitergabe bestimmter Daten an Dritte im Voraus zu widersprechen;
  - Recht auf vorübergehende Einschränkung der Bearbeitung im Falle einer angeblich unrechtmässigen Bearbeitung;
  - Recht auf Berichtigung.
- Es ist sinnvoll, für jedes Recht ein **Verfahren festzulegen, mit** dem Sie reagieren können.

#	Schritt	Beschreibung
1	Eingang des Antrags.	
2	Registrieren Sie den Antrag der Person.	Der Antrag der betroffenen Person wird in ein Register der Anträge der betroffenen Person aufgenommen.
3	Bestätigen Sie die Identität der betroffenen Person.	Die Identität der betroffenen Person sollte überprüft und bestätigt werden. Wenn die Identität nicht überprüft werden kann, muss die betroffene Person um weitere Informationen gebeten werden.
4	Bewerten Sie die Gültigkeit des Antrags der betroffenen Person.	Der Antrag sollte auf seine Gültigkeit geprüft werden. Insbesondere ist zu prüfen, ob Beschränkungen bestehen (=> bei Ablehnung ist die Entscheidung anfechtbar).
5	Sammeln Sie die gewünschten Informationen.	Die angeforderten Informationen müssen gesammelt werden. Dies muss innerhalb des gesetzlichen Zeitrahmens geschehen, wobei ein gewisser Spielraum für die sechste Stufe bestehen muss.
6	Ergreifen Sie die erforderlichen Massnahmen und übermitteln Sie die angeforderten Informationen.	Dem Antrag der betroffenen Person wird nachgekommen und die Informationen werden in der angegebenen Weise bereitgestellt.
7	Schliessen Sie den Antrag der betroffenen Person.	Sobald der Antrag abgeschlossen ist, muss er in das Register der Anträge der betroffenen Person eingetragen werden, zusammen mit dem Datum, an dem der Antrag abgeschlossen wurde (dies ist notwendig, um festzustellen, ob es sich um einen sich wiederholenden Antrag handelt).

Datenschutzbeauftragter

Leiter

- Die lokalen Behörden sind **nicht verpflichtet**, einen Datenschutzbeauftragten zu benennen.
  - Aber es ist eine **wichtige Unterstützung**.
- Was kann der Datenschutzbeauftragte tun?
  - Ausbilden.
  - Das Bewusstsein schärfen.
  - Beraten und unterstützen.
  - Mitwirken an der Erstellung einer Datenschutz-Folgenabschätzung (DSFA).
  - Der Hauptansprechpartner sein.
- Lokale Gebietskörperschaften können in Erwägung ziehen, die Kosten zu bündeln und gemeinsam einen Datenschutzbeauftragten anzustellen.
  - Datenschutz, und im weiteren Sinne auch Informationssicherheit, ist ein **Beruf**.
    - Besondere Fachkenntnisse sind erforderlich.
    - Er darf keine Aufgaben wahrnehmen, die mit seinen Pflichten als Datenschutzbeauftragter unvereinbar sind.
    - Muss seine Funktion selbständig ausüben können (z. B. keine Anweisungen erhalten).

Schulung und Sensibilisierung

Ziele

Ausbildung

- Ziel eines Ausbildungsprogramms ist, dem Einzelnen zu helfen, sich die Kenntnisse, Fähigkeiten und Verhaltensweisen anzueignen, die für die Erfüllung bestimmter Anforderungen erforderlich sind.

Bewusstsein schärfen

- Ziel der Sensibilisierung ist, die Zielgruppe auf ein Problem aufmerksam zu machen und möglicherweise ihre Einstellung und ihr Verhalten zu ändern.

Schulung und Sensibilisierung

Schulungsmethoden

Datenschutzprogramm

Notwendigkeit, weiter zu gehen

- Das **Datenschutzprogramm** ist ein Bündel von Massnahmen und Aktivitäten, mit denen ein langfristiges Ziel erreicht werden soll.
- Das Ziel sollte nicht nur die «Einhaltung der Vorschriften» sein, sondern die Schaffung eines Gleichgewichts zwischen dem **Schutz der Rechte und Freiheiten** der betroffenen Personen und der **täglichen Arbeit der lokalen Behörde**.
- GRC-Ansatz (Governance, Risk and Compliance).

Datenschutzprogramm

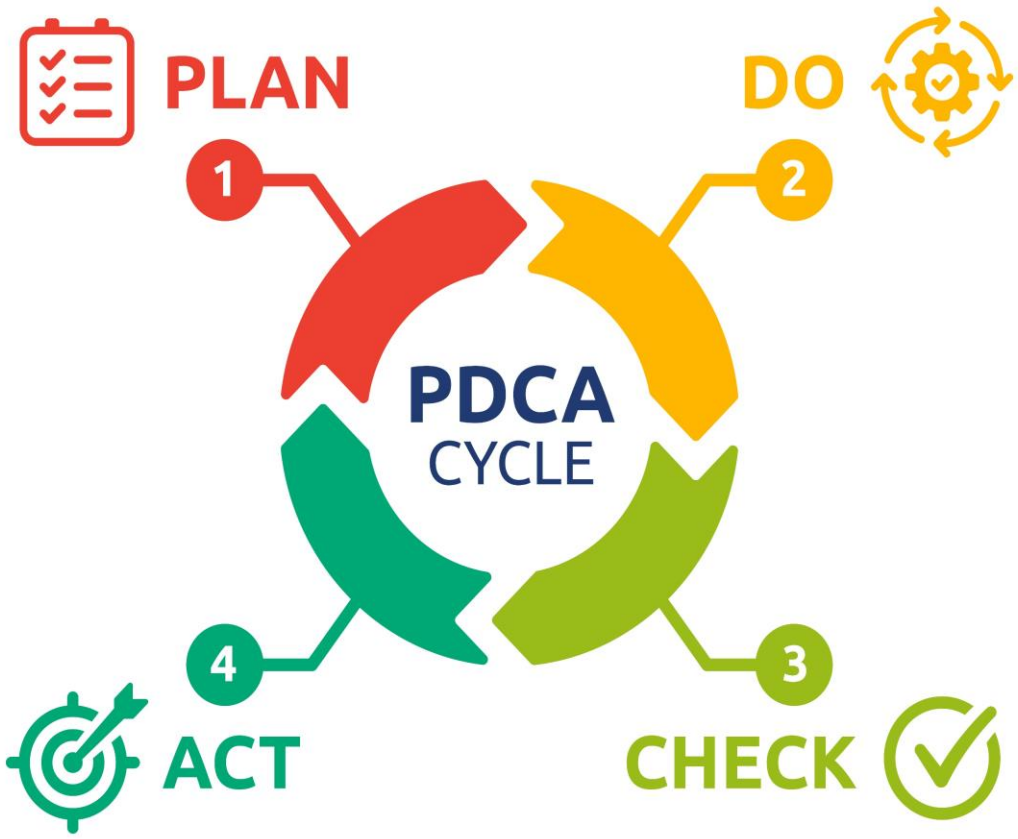
Vorteile

- **Verringerung** der **Risiken** für die betroffenen Personen und für die öffentliche Einrichtung.
- **Begrenzung des** Risikos von **Datensicherheitsverletzungen** und -**vorfällen**.
- **Begrenzung** der Anfälligkeit der öffentlichen Einrichtung für **Beschwerden** von Betroffenen.
- **Schutz der Informationswerte** der öffentlichen Einrichtung.
- Verbesserung und Erhaltung des Vertrauens **der Öffentlichkeit** und der **Partner**.

Datenschutzprogramm

Ausarbeitung

1. Festlegung des rechtlichen Rahmens.
2. Identifizierung von Daten und Bearbeitungen.
3. Identifizierung von Unterauftragnehmern und Empfängern.
4. Schaffung des Registers der Verarbeitungstätigkeiten.
5. Risikobewertung.
6. Durchführung einer Lückenanalyse.
7. Entwicklung einer Datenschutzstrategie.
8. Mobilisierung von Ressourcen und Unterstützung der Exekutive.
9. Durchführung der Massnahmen.
10. Schulung und Sensibilisierung der Mitarbeiter.
11. Einrichtung von Überwachungsmechanismen.
12. Umgang mit Vorfällen.
13. Kontinuierliche Überprüfung und Verbesserung.



Fazit

Checkliste

- ❑ Einführung eines Registers der Bearbeitungstätigkeiten.
- ❑ Bewertung der Risiken und Festlegung von Sicherheitsmassnahmen.
- ❑ Schaffung eines Reaktionsplans für den Fall einer Verletzung der Datensicherheit.
- ❑ Ausarbeitung von Datenschutzerklärungen und -verfahren (z. B. Datenschutzerklärung für die Webseite, Verfahren im Falle eines Auskunftsanspruchs).
- ❑ Überprüfung von Verträgen in Bezug auf den Datenschutz (z. B. Vergabe von Unteraufträgen).
- ❑ Überprüfung der internen Richtlinien (z. B. Vorratsdatenspeicherung).
- ❑ Erforderlichenfalls Durchführung einer Datenschutz-Folgenabschätzung.
- ❑ Sensibilisierung und Schulung.

Fazit

Aber noch mehr...

- Beispiel für eine vertiefte Ausbildung (kostenlos).
  - Vom Freiburger Gemeindeverband organisierter Workshop (wird noch bekannt gegeben).
- Beispiele für vertiefende Ausbildungen (kostenpflichtig).
  - Correspondant en matière de protection des données et de transparence pour les administrations publiques du canton de Fribourg (SEC Formation Fribourg)
  - CAS en Protection des données (Unidistance)
  - Responsable de la protection des données / DPO (UNIGE)
  - CAS Datenschutz (Unidistance)
- Literatur und Modell
  - ÖDSMB
  - www.swissprivacy.law
  - www.protection-donnees.ch
  - www.protectiondesdonnees.guide
  - www.datenrecht.ch

acf-fgv
association des communes fribourgeoises
freiburger gemeindeverband

_swissprivacy.law

Danke vielmals!

www.swissprivacy.law