acf-fgv
association des communes fribourgeoises
freiburger gemeindeverband

_swissprivacy.law

LPrD : de la loi à la pratique

Boîte à outils pour appliquer la protection des données au quotidien

Présentation

- Livio di Tria
  - Juriste spécialisé en droit des nouvelles technologies.
  - Co-fondateur des blogs d'actualités en matière de protection des données www.swissprivacy.law et www.protection-donnees.ch.

- Pour plus d'informations à propos de l'association Swissprivacy : www.swissprivacy.law
  - Fondateurs : Eva Cellina, Célian Hirsch, Baptiste Favez, Kastriot Lubishtani, Frédéric Erard, Livio di Tria

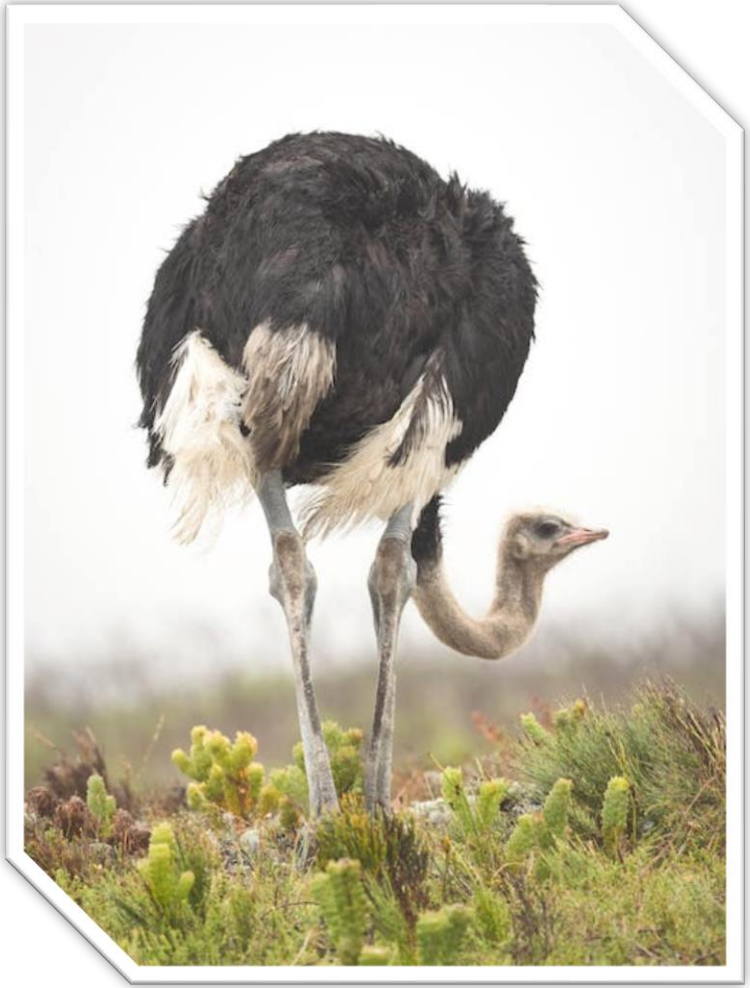
- Si vous avez des questions à propos de cette présentation, vous pouvez écrire à Livio di Tria
  - livio.ditria@swissprivacy.law

Stratégie

Anticiper

- Le responsable du traitement dispose d'un **délai de deux ans** pour se mettre en conformité.
  - Ce délai ne concerne pas les dispositions relatives aux violations de la sécurité des données.

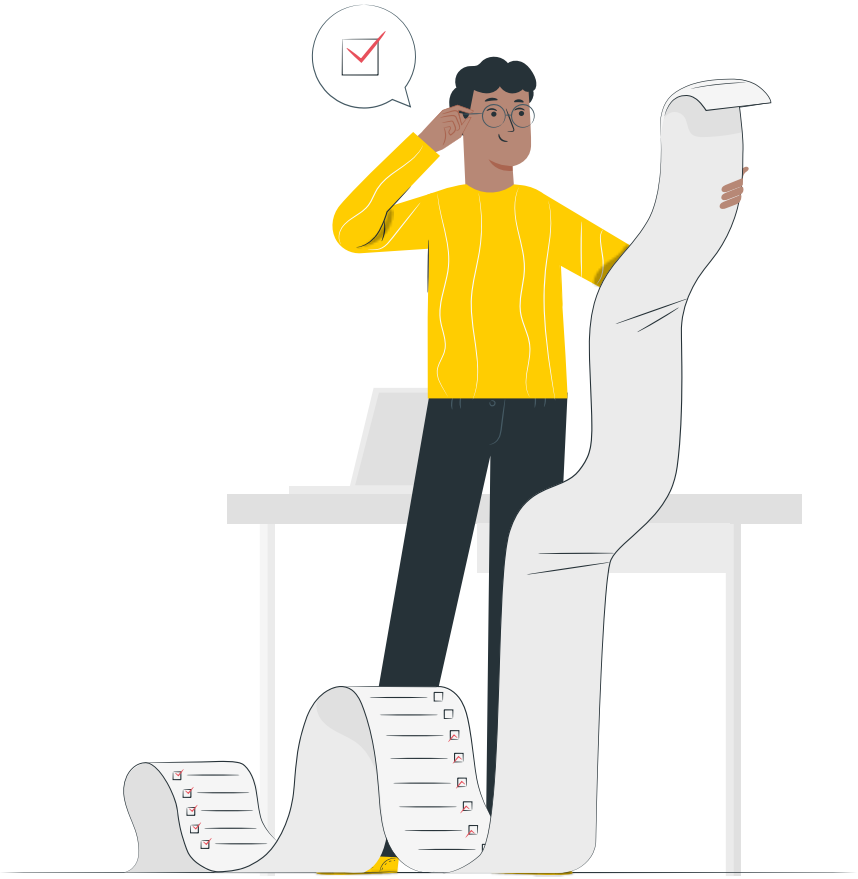
- La préparation à la conformité doit se faire de manière progressive, **par étapes**, afin de garantir une mise en œuvre efficace et durable.
  - Privilégier les « ***quick wins*** » et éviter la complexité.



Stratégie

Par étape

- Registre des activités de traitements.
- Évaluation des risques.
- Mesures de sécurité.
- Gestion des incidents de sécurité.
- Sous-traitance et externalisation.
- Autres aspects à aborder.
- Correspondant à la protection des données.
- Formation et sensibilisation.



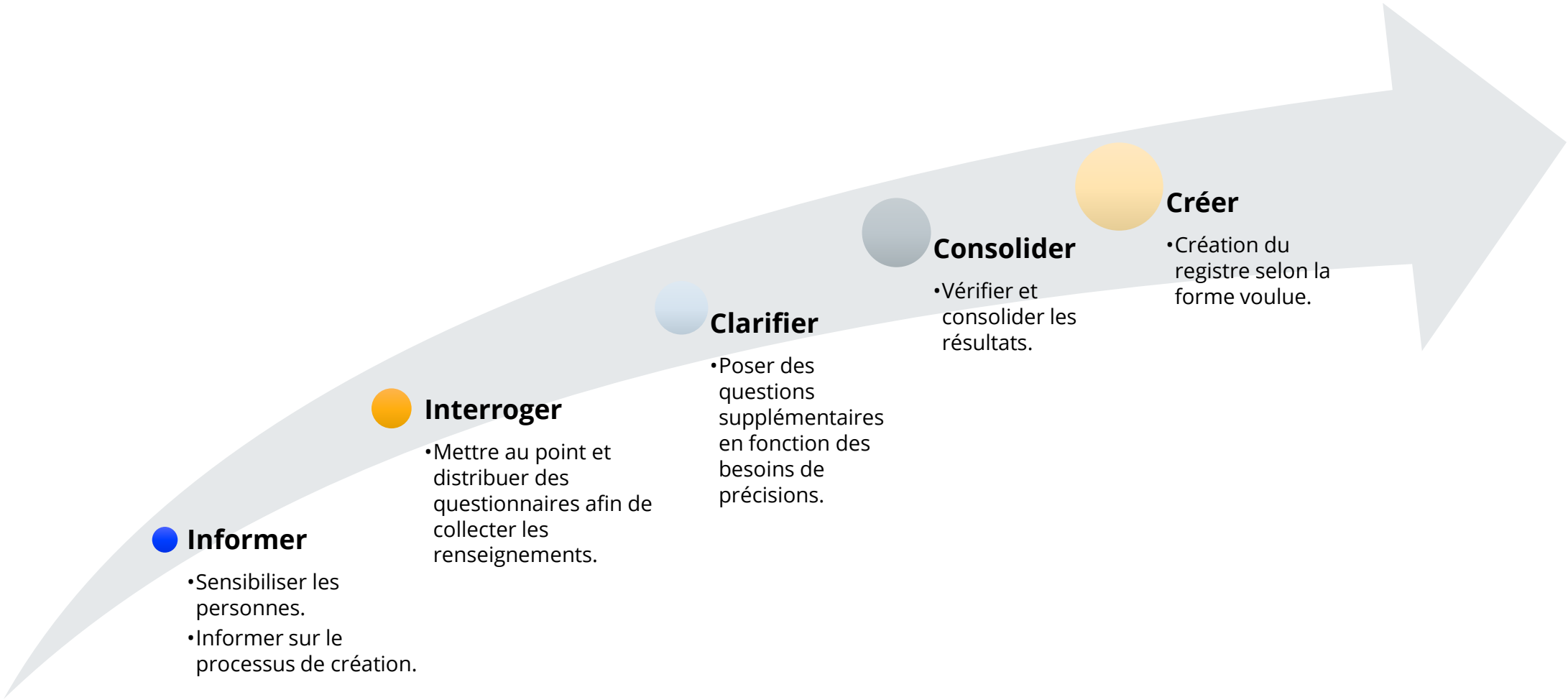
Registre des activités de traitement

Pièce maîtresse

- Pièce maîtresse, car **point de départ** :
  - Pour la mise en œuvre des autres droits et obligations ;
  - Pour l'évaluation des risques et la mise en place de mesures de sécurité ; et
  - Pour tout contrôle par l'ATPrDM.
- Vise à créer un **inventaire interne** à la commune pour chaque **activité de traitement** (registre interne).
  - Envisager une approche par département/service (p. ex. RH, Contrôle des habitants, Service technique, Service financier).
  - La loi prévoit la liste des informations minimales que le registre doit contenir (p. ex. finalité(s) du traitement, description des catégories de personnes concernées et des catégories de données personnelles traitées, destinataires réguliers de données, sous-traitants).
    - Envisager une **approche plus large**.
- Chaque responsable du traitement déclare à l'ATPrDM les activités de traitement qu'il accomplit et leurs modifications successives (registre externe).
- Exercice **dynamique** et **régulier**.

Registre des activités de traitement

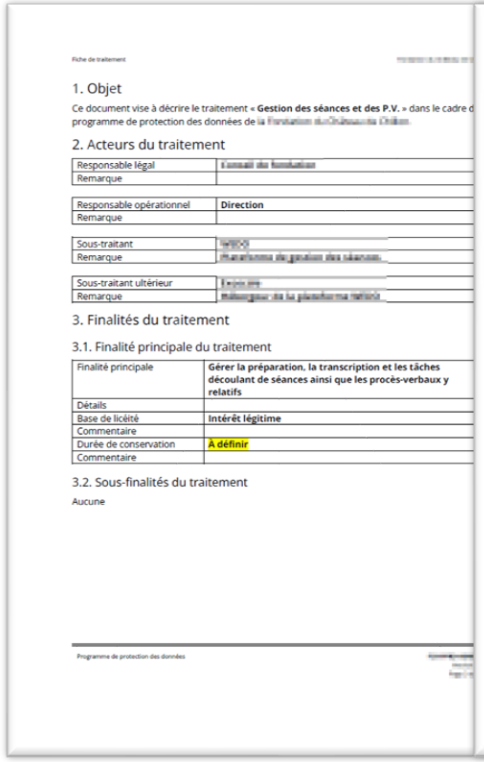
Procédure



Registre des activités de traitement

Élaboration d'un tableau synthétique et de fiches détaillées

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 Fondation du Château Orbe.

2. Acteurs du traitement

Responsable légal	Conseil de fondation
Remarque	
Responsable opérationnel	**Direction**
Remarque	
Sous-traitant	WISO
Remarque	Plateforme de gestion des séances
Sous-traitant ultérieur	Exploitant
Remarque	Hébergeur de la plateforme WISO

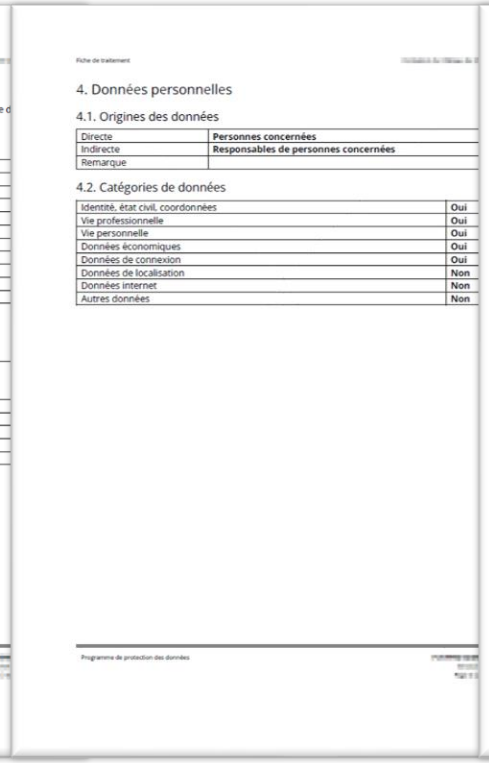
3. Finalités du traitement

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



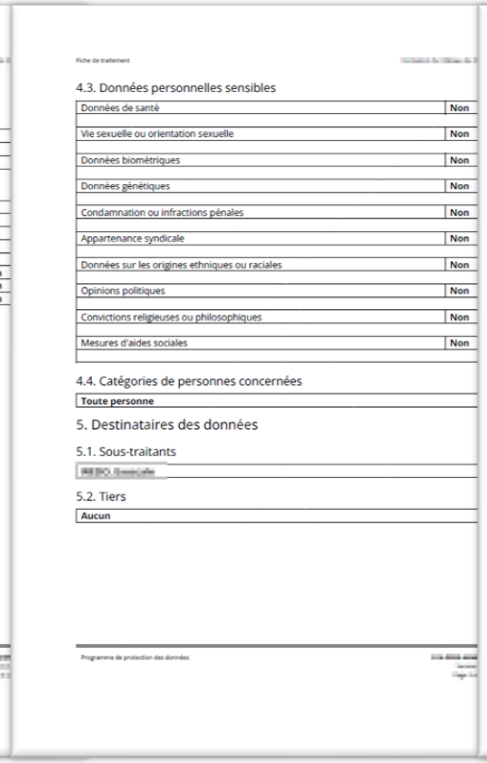
4. Données personnelles

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

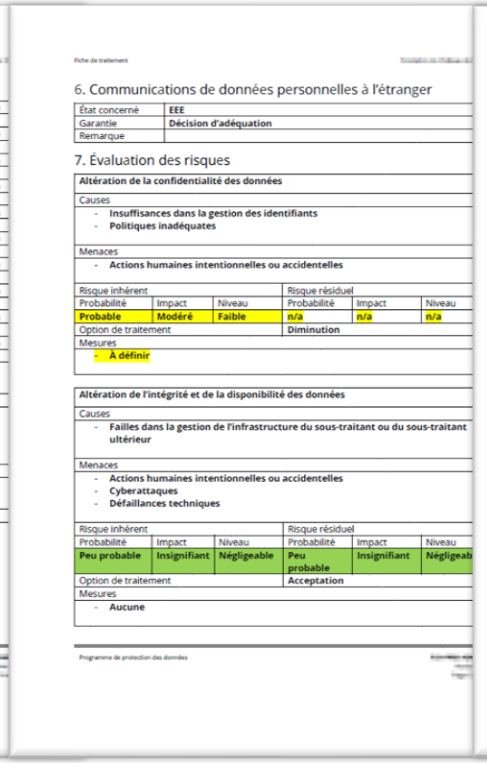
5. Destinataires des données

5.1. Sous-traitants

WISO Exploitant

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

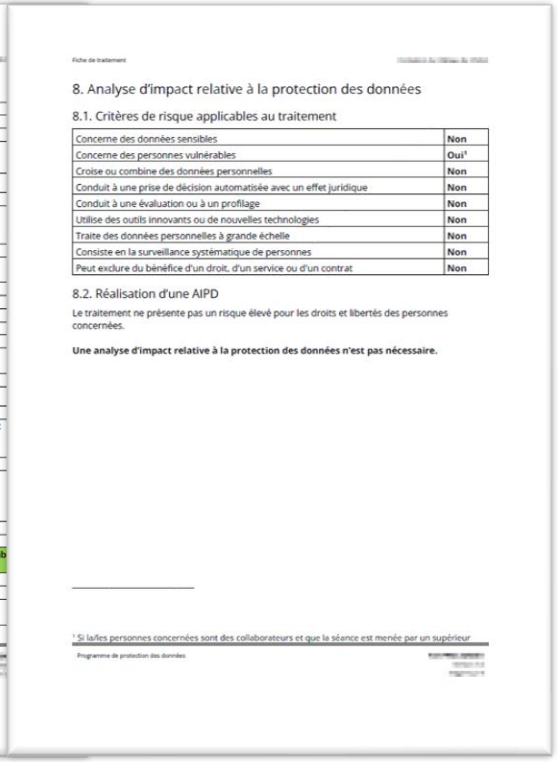
Causes
- **Failles dans la gestion de l'infrastructure du sous-traitant ou du sous-traitant ultérieur**

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

Évaluation des risques

Généralités

- Le registre des activités de traitement, si on suit une approche large, permet d'identifier les **risques inhérents** à l'activité de traitement.

Mesures de sécurité

Généralités

- Les mesures de sécurité portent généralement sur :
  - la **confidentialité** des données ;
  - la **disponibilité** des données
  - l'**intégrité** des données ; et
  - la **traçabilité** des données.
- Les mesures de sécurité doivent être fondées sur **le niveau de risque**.
- Elles peuvent être :
  - **Techniques**, telles que des pares-feux ou des logiciels ;
  - **Légales**, telles que des obligations contractuelles ;
  - **Administratives**, telles que des processus d'approbation ; ou
  - **Managériale**, telle que la formation du personnel.
- Par ailleurs, les mesures adéquates sont celles qui font consensus auprès des expert-e-s du domaine (p. ex. normes ISO 27001).

Gestion des incidents

Distinction entre l'incident et la violation

- **Incident** de la sécurité des données.
  - Événement indésirable ou inattendu qui peut compromettre la sécurité des données.
  - Ne conduit pas nécessairement à la perte de données personnelles, à leur modification, à leur effacement ou leur destruction, à leur divulgation ou un accès non autorisé à ces données (≠ Violation).
    - Sans intervention, aurait cependant pu y conduire.
- **Violation** de la sécurité des données
  - Toute violation de la sécurité entraînant de manière accidentelle ou illicite une altération de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des données.

Gestion des incidents

Mesures à prendre dans le cas d'une violation de la sécurité des données

- Mesures à prendre en présence d'une **violation** de la sécurité des données, et ce dans **tous les cas** :
  1. Prendre immédiatement les **mesures appropriées** afin de mettre fin à la violation et d'en minimiser les effets.
  2. Consigner dans un **document interne** la nature de la violation, le type de données concernées, les catégories de personnes touchées, les conséquences probables pour ces dernières et les mesures prises pour y remédier.
- Mesures à prendre en présence d'une **violation** de la sécurité des données, et ce dans **certains cas :**
  1. **Annoncer à l'ATPrDM** la violation entraînant un risque élevé pour les droits fondamentaux de la personne concernée.
  2. **Annoncer à la personne concernée** la survenance d'une violation lorsque cette mesure s'impose pour des **motifs de transparence** et/ou pour permettre à la personne concernée de prendre les **mesures utiles à la sauvegarde de ses intérêts**.

Gestion des incidents

Procédure

1. **Préparation** : plan de réponse.
2. **Identification** : mesures de surveillance.
3. **Évaluation** : évaluer la gravité.
4. **Intervention** : stopper l'incident, minimiser les dégâts et récupérer les données.
5. **Notification** : informer les parties concernées si nécessaire.
6. **Analyse post-incident** : tirer des leçons et améliorer les mesures.

Gestion des incidents

Plan de réponse

- Domaines clés d'un **plan de réponse** pour éviter la panique :
  - Fournir des **informations** sur la manière dont la commune devra réagir à tout incident affectant la sécurité de ses données.
  - Déterminer les **rôles et les responsabilités** des personnes chargées de répondre à tout incident.
  - Fournir des **informations** sur les installations disponibles qui pourraient être utilisées pour aider à gérer l'incident.
  - Fournir des **stratégies** à utiliser pour la communication interne et externe de manière efficace.
  - Déterminer les **mesures** qui devraient être prises après l'incident.

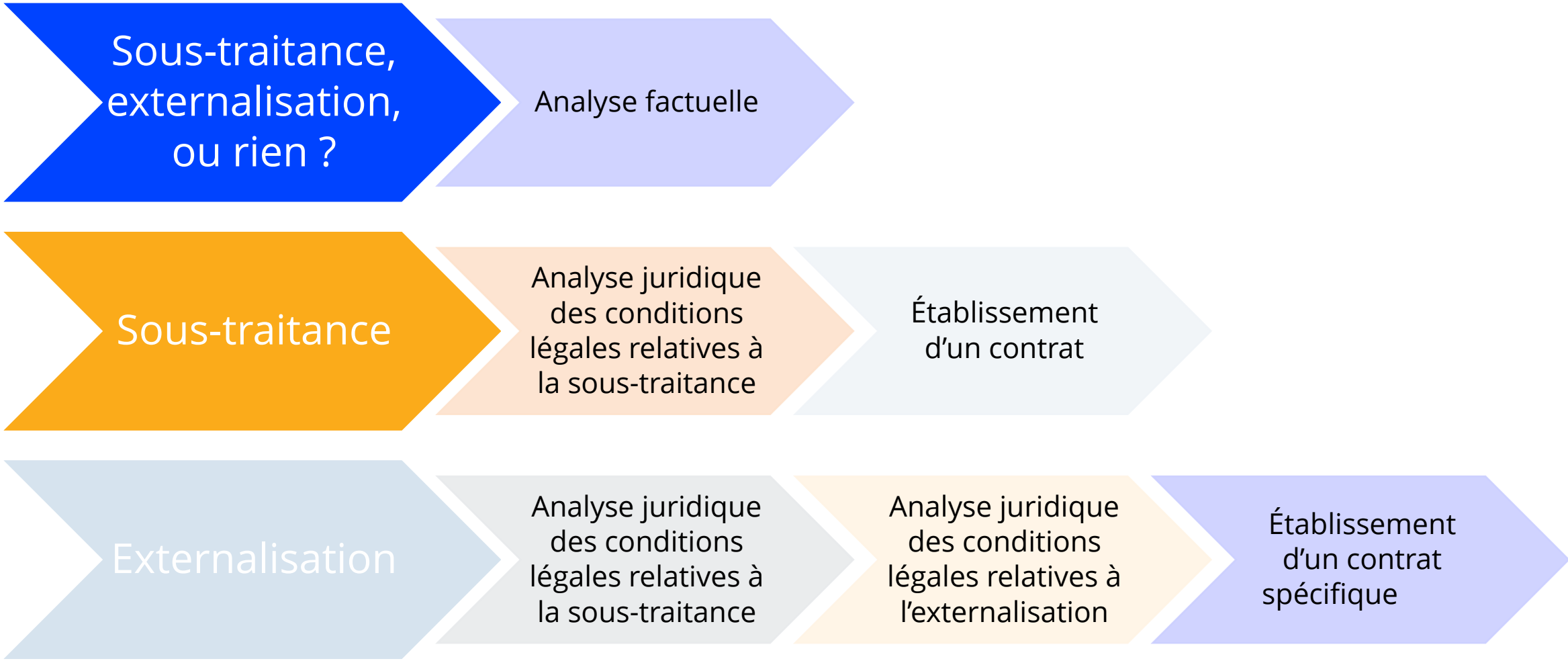
Sous-traitance et externalisation

Quelle(s) différence(s) ?

- La **sous-traitance** est le procédé selon lequel une entité publique confie une partie de ses activités de traitements à une entreprise externe (p. ex. fiduciaires, agences de recrutement, agences marketing) ou une collectivité publique tierce.
  - Efficacité opérationnelle, réduction des coûts, spécialisation, flexibilité.
- L'externalisation est une **forme qualifiée** de sous-traitance.
  - Tout ce qui implique l'utilisation de ressources informatiques pour stocker, traiter et partager des données.
  - Vise les services dits de « ***cloud computing*** ».

Sous-traitance et externalisation

Étapes



Sous-traitance et externalisation

Contrat de sous-traitance

Pas de description minimale pour le **contrat de sous-traitance**. Recommandations ?

1. Préambule.
2. Définitions.
3. Champ d'application et objet (objet, durée, nature).
4. Obligations du sous-traitant (instructions, obligation de confidentialité, mesures de protection, obligations d'assistance, droit d'audit).
5. Lieu de l'exécution du traitement.
6. Intervention de sous-traitants ultérieurs.
7. Sort des données.
8. Droit de résiliation extraordinaire.
9. Dispositions finales.

Autres aspects à aborder

Devoir d'informer et déclaration de protection des données

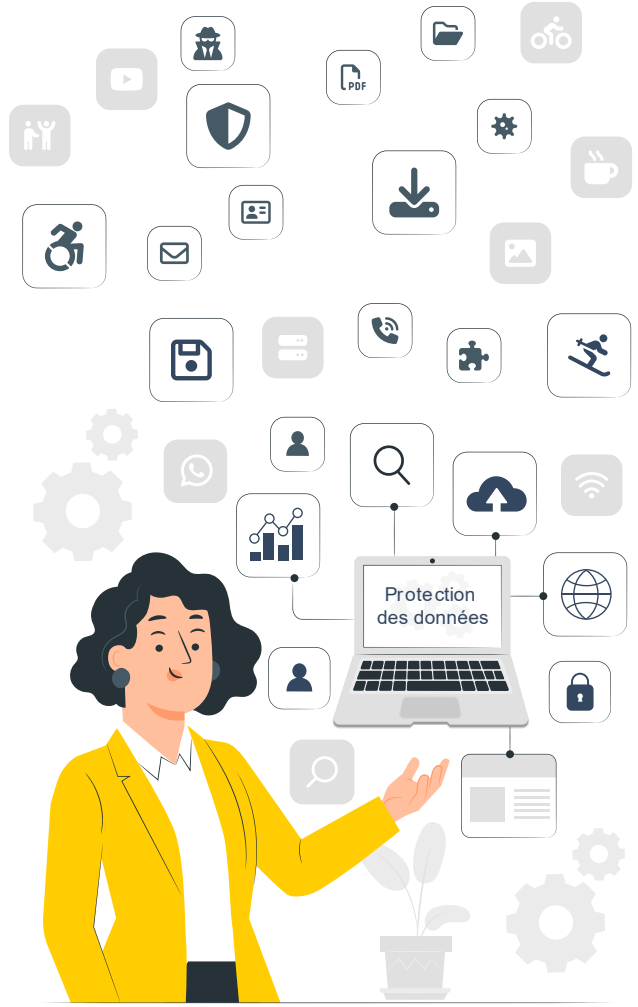
- Le responsable du traitement doit informer la personne concernée en lui fournissant notamment :
  - ses coordonnées ;
  - la finalité du traitement ;
  - les destinataires ou les catégories de destinataires auxquels les données personnelles sont transmises ; et
  - le caractère obligatoire ou facultatif de la collecte des données.
- Pas besoin notamment si la collecte résulte d'une **obligation légale** (majorité des cas).
  - Ne concerne pas le cas des sites web
    - Nécessité d'avoir une déclaration de la protection des données en fonction des traitements (p. ex. cookies obligatoires, cookies statistiques).

Autres aspects à aborder

Devoir d'informer et déclaration de protection des données

Déclaration de protection des données

1. Introduction
2. Qui sommes-nous et comment nous contacter ?
3. Quel est notre rôle en matière de protection des données ?
4. Quand et comment collectons-nous vos données ?
5. Quelles catégories de données traitons-nous ?
6. Pourquoi traitons-nous vos données ?
7. Quels sont vos droits ?
8. Comment sécurisons-nous vos données ?
9. Où vos données sont-elles stockées ?
10. Combien de temps conservons-nous vos données ?
11. À qui communiquons-nous vos données ?
12. Quels cookies utilisons-nous ?
13. Quels réseaux sociaux utilisons nous ?



Autres aspects à aborder

Droits et procédures

- Droits notamment prévus :
  - Droit d'accès ;
  - Droit à la portabilité ;
  - Droit d'opposition par avance à la communication à des tiers de données déterminées ;
  - Droit à la limitation temporaire du traitement en cas de traitement supposément illicite ;
  - Droit de rectification.
- Il est conseillé pour chaque droit d'avoir une **procédure en place** pour être en mesure d'y répondre.

#	Étape	Description
1	Réception de la demande.	
2	Enregistrer la demande de la personne concernée.	La demande de la personne concernée est enregistrée dans un registre des demandes de la personne concernée.
3	Confirmer l'identité de la personne concernée.	L'identité de la personne concernée devrait être vérifiée et confirmée. Si l'identité ne peut être vérifiée, il est nécessaire de demander à la personne concernée des compléments.
4	Évaluer la validité de la demande de la personne concernée.	La demande devrait être évaluée. En particulier, il est important d'analyser si des restrictions sont applicables (=> En cas de refus, décision sujette à recours).
5	Recueillir les informations demandées.	Les informations demandées devraient être recueillies. Il faut le faire dans le délai légal, tout en gardant une marge de manœuvre pour la sixième étape.
6	Prendre les mesures nécessaires et fournir les informations demandées.	La demande de la personne concernée est exécutée et les informations lui sont fournies selon les modalités prévues.
7	Clore la demande de la personne concernée.	Lorsque la demande est finalisée, elle doit être enregistrée dans le registre des demandes de la personne concernée, avec la date de clôture de la demande (nécessaire pour savoir si la demande a un caractère répétitif).

Correspondant à la protection des données

Chef d'orchestre

- **Aucune obligation** pour les communes de désigner un correspondant à la protection des données.
  - Mais représente une **aide précieuse**.
- Que peut faire le correspondant ?
  - Former.
  - Sensibiliser.
  - Conseiller et assister.
  - Participer à la réalisation d'une AIPD.
  - Être l'interlocuteur principal.
- Les communes peuvent envisager une mutualisation des coûts en engageant un professionnel.
  - La protection des données, et plus largement la sécurité de l'information, est un **métier**.
    - Nécessité de disposer des connaissances professionnelles spécifiques.
    - Nécessité de ne pas exercer des tâches incompatibles avec ses tâches de correspondant à la protection des données.
    - Nécessité d'exercer sa fonction de manière indépendante (p. ex. ne pas recevoir d'instruction).

Formation et sensibilisation

Objectifs

Formation

- L'objectif d'un programme de formation est d'aider un individu à acquérir les connaissances, les compétences et le comportement nécessaire pour répondre à des exigences spécifiques.

Sensibilisation

- L'objectif d'une séance de sensibilisation est de faire prendre conscience au public cible d'une préoccupation et éventuellement d'un changement d'approche et de comportement

Formation et sensibilisation

Méthodes de formation

Programme de protection des données

Nécessité d'aller plus loin

- Le **programme de protection des données** est un ensemble de mesures et d'activités visant à atteindre un objectif à long terme.
- L'objectif ne devrait pas être simplement « la conformité » mais un équilibre entre la **protection des droits et libertés** des personnes concernées et le **fonctionnement quotidien de la commune**.
- Il s'agit d'une approche GRC (Gouvernance, Risques, Conformité).

Programme de protection des données

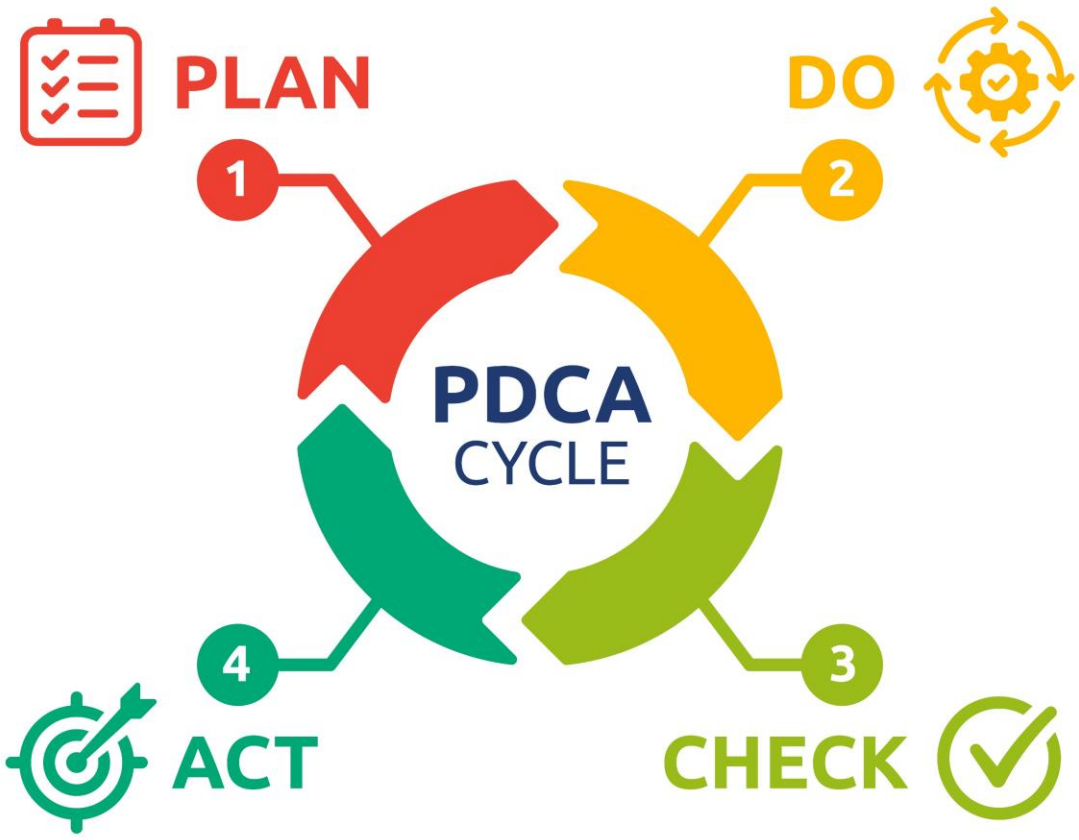
Avantages

- **Réduire** les **risques** pour les personnes concernées et pour l'entité publique.
- **Limiter** l'exposition aux **violations de la sécurité des données** et aux incidents.
- **Limiter** l'exposition de l'entité publique à des **plaintes** de personnes concernées.
- **Protéger** les **actifs informationnels** de l'entité publique.
- **Améliorer** ou **maintenir** la confiance du **public** et des **partenaires**.

Programme de protection des données

Construction

1. Déterminer le cadre légal.
2. Identifier les données et les traitements.
3. Identifier les sous-traitants et les destinataires.
4. Créer le registre des activités de traitement.
5. Évaluer les risques.
6. Réaliser une analyse des écarts.
7. Élaborer une stratégie de protection des données.
8. Mobiliser des ressources et obtenir l'engagement de l'Exécutif
9. Mettre en œuvre les mesures.
10. Former et sensibiliser les collaborateurs.
11. Mettre en place des mécanismes de surveillance.
12. Gérer les incidents.
13. Réviser et améliorer en continu.



Conclusion

Check-list

- ❑ Établir un registre des activités de traitement.
- ❑ Évaluer les risques et définir des mesures de sécurité.
- ❑ Établir un plan de réponse en cas de violation de la sécurité des données.
- ❑ Établir les déclarations et procédures de protection des données (p. ex. déclaration de protection des données pour le site web, procédure en cas de droit d'accès).
- ❑ Examen des contrats qui sont en lien avec la protection des données (p. ex. sous-traitance).
- ❑ Vérification des directives internes (p. ex. conservation des données).
- ❑ Analyse d'impact relative à la protection des données si nécessaire.
- ❑ Sensibilisation et formation.

Conclusion

Mais encore…

- Exemple de formation approfondie (gratuite).
  - Atelier organisé par l'Association des communes fribourgeoises (à venir).
- Exemples de formations approfondies (payantes).
  - 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).
- Littérature et modèle
  - ATPRdM
  - www.swissprivacy.law
  - www.protection-donnees.ch
  - www.protectiondesdonnees.guide
  - www.datenrecht.ch


Conseil Municipal
Pétaouchnok
UN VOLONTAIRE POUR ÊTRE RESPONSABLE CYBERSÉCURITÉ
Boucherie