

Loi sur la protection des données (LPrD)

Révision totale

—

Soirée de présentation aux communes
Novembre 2023

Contexte de la révision

Changements sociétaux	Changements technologiques	Changements juridiques
<p>Rapport à l'information différent</p> <p>Habitudes de travail différentes</p> <p>Attentes de la population différentes</p> <p>Cyberattaques</p>	<p>Numérisation</p> <p>Digitalisation</p> <p>Plateformes électroniques (guichet virtuel, FRIAC, Dossier électronique du patient)</p> <p>Cloud</p> <p>Ordinateurs et téléphones portables</p>	<p>Révision de la loi fédérale sur la protection des données (LPD ; FF 2020 7397)</p> <p>Convention STE 108+</p> <p>Directive UE 2016/680 sur la protection des données dans les domaines de la police et de la justice</p> <p>RGPD (Règlement UE 2016/679 sur la protection des données)</p>

Objectifs de la révision

- > **Disposer d'une législation adaptée au contexte social et technologique actuel**
- > **Renforcer les droits et la protection des citoyens et des citoyennes face aux traitements toujours plus nombreux et complexes de leurs données personnelles**
- > **Mettre la législation fribourgeoise en adéquation avec les nouveaux standards applicables aujourd'hui**

Principales différences avec la loi fédérale

- > **Maintien de la protection des données des personnes morales**
 - > Motivé par des raisons à la fois pratiques et juridiques
 - > Choix identiques à Genève et à Zurich
- > **Introduction de dispositions spécifiques concernant l'usage du cloud**
 - > Reprise des dispositions introduites en 2020
 - > Situation similaire dans les cantons de Glaris, Lucerne et Zurich
- > **Maintien d'une autorité de la protection des données composée d'une Commission et d'un ou une préposé-e**
 - > Motivé par des raisons historiques
 - > Solution ayant fait ses preuves, notamment pour la coordination entre les différents domaines d'activité de l'Autorité
 - > Solution également souhaitée par l'ATPrDM

Quelques définitions et changements terminologiques (art. 4)

- > **Données personnelles** = Toutes les informations qui se rapportent à une personne identifiée ou identifiable (= la personne concernée)
- > **+/- New Données sensibles** = 1. les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales; 2. les données sur la santé, la sphère intime ou l'origine raciale ou ethnique; 3. **les données génétiques**; 4. **les données biométriques identifiant une personne physique de manière univoque**; 5. les données sur des mesures d'aide sociale; 6. les données sur des poursuites ou des sanctions pénales et administratives
- > **New Profilage** = toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne
 - > Fichier = activité de traitement
 - > Responsable du fichier = Responsable du traitement
 - > Registre des fichiers = Registre des activités de traitement
 - > Participant au fichier = co-responsable du traitement

1. Dispositions générales

1 Dispositions générales

Art. 1 But

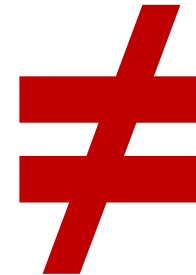
¹ La présente loi vise à protéger les droits fondamentaux des personnes dont les données personnelles font l'objet d'un traitement.



Protéger les droits fondamentaux

- Sphère privée
- Liberté de mouvement
- Liberté d'association
- Liberté d'opinion
- Autodétermination informationnelle

...



Protéger les données elles-mêmes

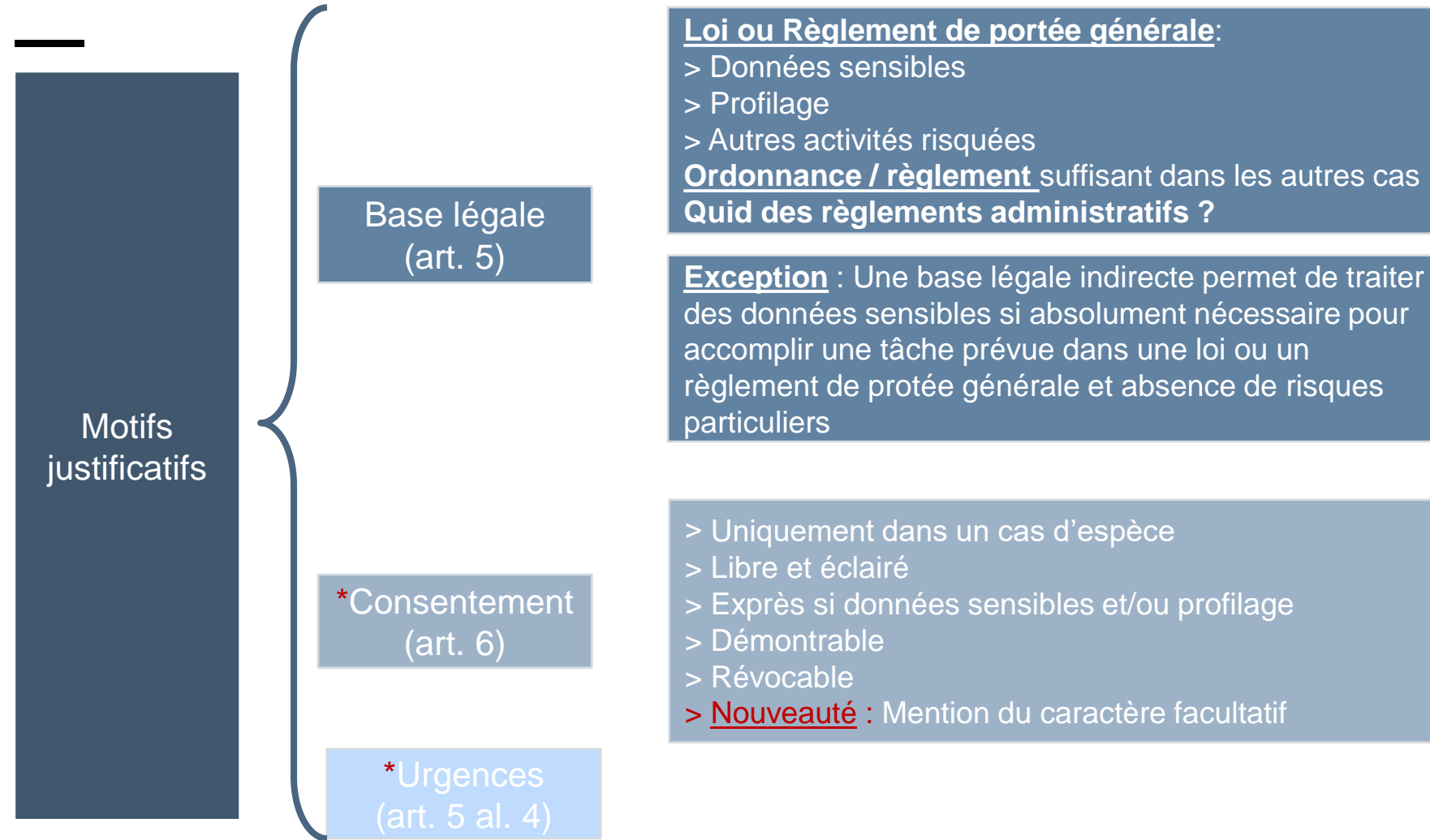
1. Dispositions générales

Champ d'application

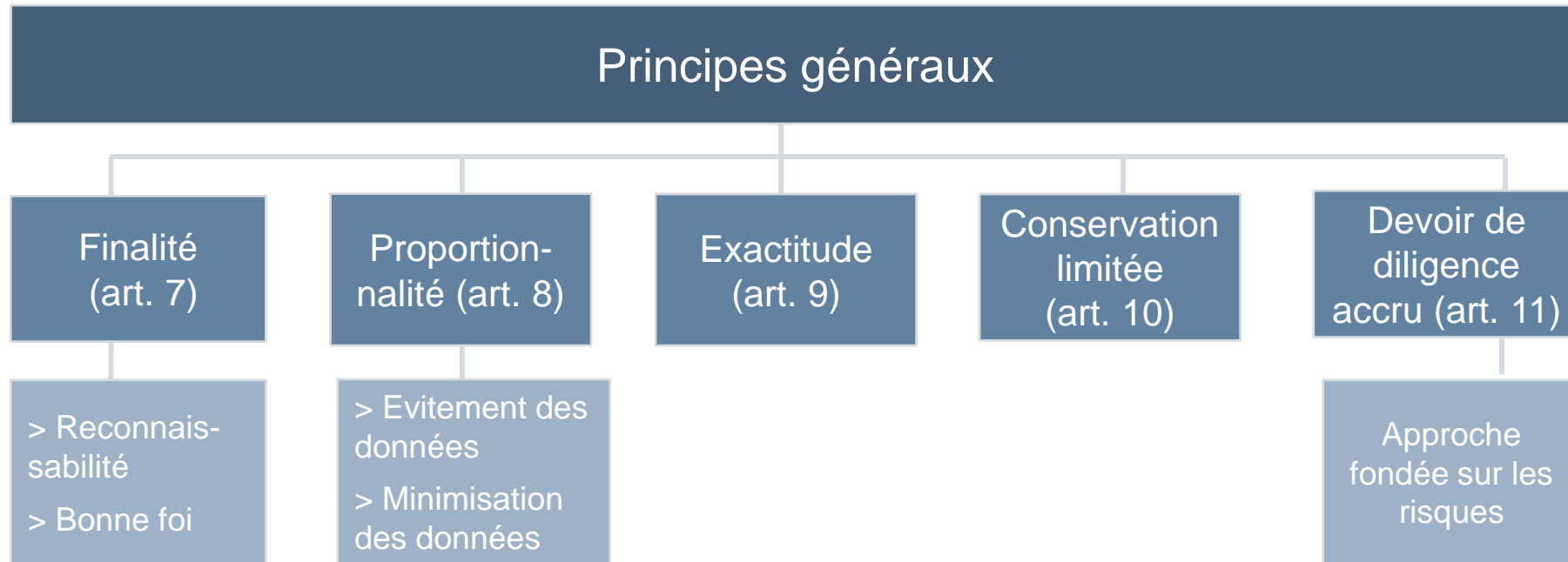
Qui ??? (art. 2)	Quoi ??? (art. 3)
<p>Idem par rapport à la LPrD actuelle</p> <ul style="list-style-type: none">> Organe et établissements public cantonaux et communaux (ég. les associations de communes, les agglomérations...)> Personnes privées chargées d'accomplir des tâches de droit public	<ul style="list-style-type: none">> Tout traitement de données accomplis par un organe soumis à la loi.> Trois exceptions :<ul style="list-style-type: none">> Procédures judiciaires en cours> Notes personnelles> Activités exercées en situation de concurrence économique → application de la LPD fédérale

⚠ Personnes privées chargées de l'accomplissement d'une tâche de droit public cantonale ou communale : Il s'agit d'une notion juridique indéterminée dont l'interprétation dépend de cas en cas en fonction de différents critères (p. ex. la compétence de rendre des décisions ou de prélever des émoluments...) ou d'indices (p. ex. une surveillance étroite d'une collectivité publique, une reconnaissance étatique, un mandat de prestation avec une collectivité publique...)

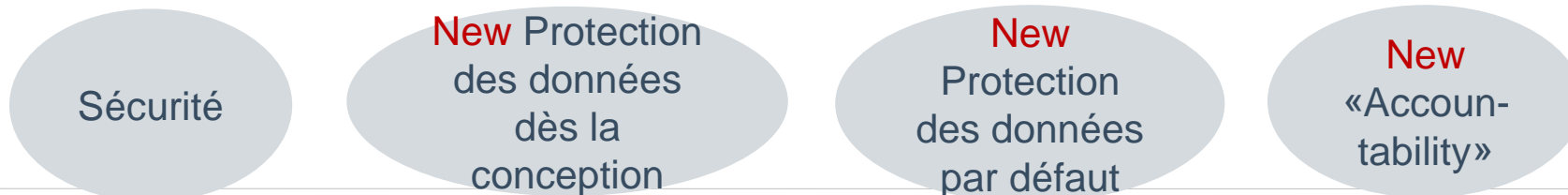
2. Principes régissant le traitement de données personnelles



2. Principes régissant le traitement de données personnelles



Section 4 sur la mise en œuvre : art. 40



2. Principes régissant le traitement de données personnelles

La collecte de données (art. 12 et 13)

- > **Abandon du principe de la collecte directement auprès de la personne**
 - > De plus en plus de collectes par entraide administrative ou procédure d'appel
- > **Devoir d'informer en cas de collecte directe / indirecte de données (art. 12)**
 - > Nouveauté : obligation d'informer si la collecte de données est obligatoire ou facultative (cf. art. 6 al. 3)
- > **Motifs d'exception au devoir d'informer (art. 13)**
 - > Principal motif d'exception : lorsque la collecte résulte d'une obligation légale

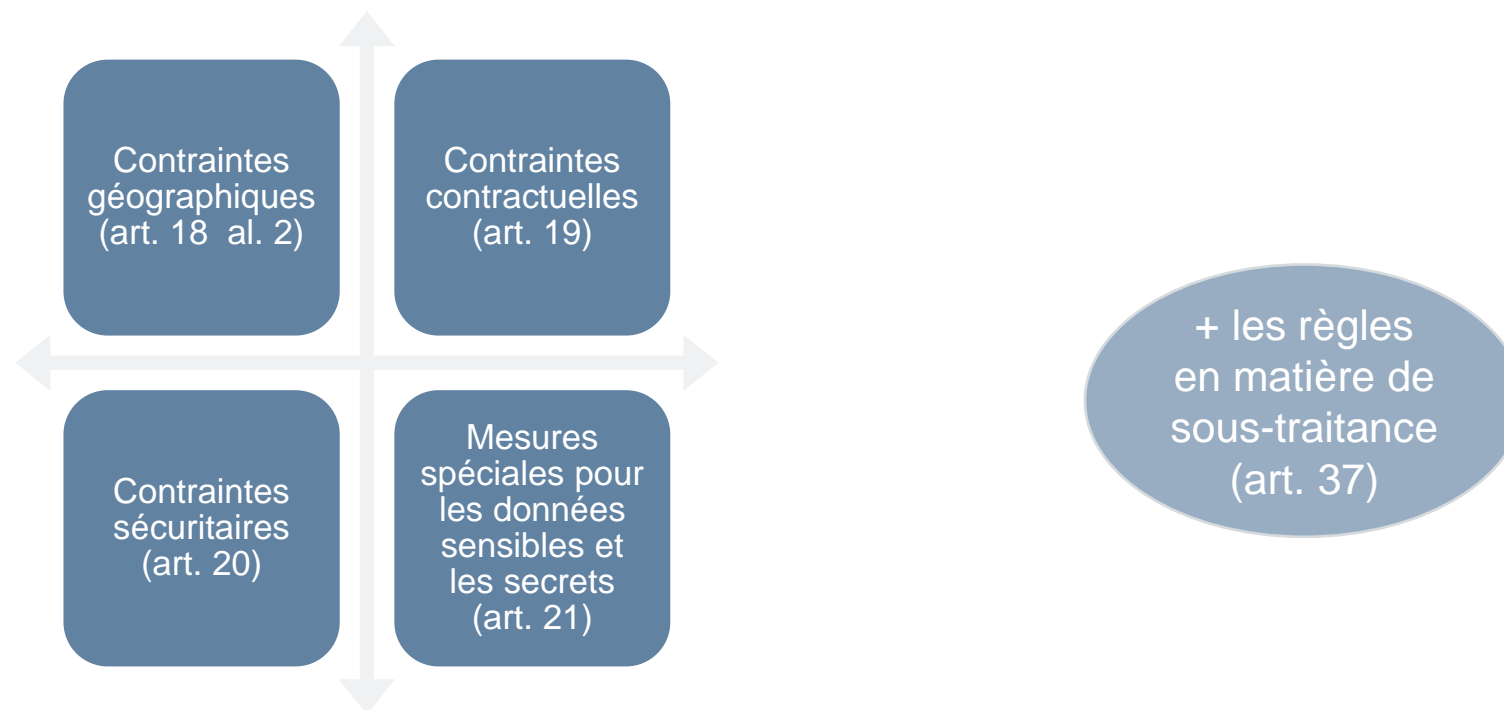
2. Principes régissant le traitement de données personnelles

La communication de données (art. 14 et 17)

- > **Communications systématiques de données**
 - > Base légale (art. 14 al. 1)
- > **Communications dans un cas d'espèce**
 - > Base légale ou un des motifs justificatifs prévus à l'article (14 al. 2)
- > **Communications par procédure d'appel**
 - > Base légale qui mentionne expressément ce type de communication (art. 14 al. 3)
- > **Communications transfrontières (art. 15)**
 - > Règles particulières pour les données relatives à des personnes physiques
 - > Différences selon existence ou non d'une décision d'adéquation du Conseil fédéral concernant le pays de destination
- > **Restrictions supplémentaires éventuelles (art. 16)**
- > **Réserves d'autres lois importantes (art. 17)**

2. Principes régissant le traitement de données personnelles

L'externalisation (art. 18 à 21)



2. Principes régissant le traitement de données personnelles

Nouveauté pour les communes : Projets pilotes (art. 22 + art. 35 à 35b LCyb)

Un projet pilote en matière de cyberadministration permet de tester une nouvelle solution pendant une période limitée avant, le cas échéant, de créer les bases légales formelles définitives nécessaires en vue de sa pérennisation

LCyb	LPrD
<p>Pose les principes applicables à <u>tous projets pilotes</u></p> <ul style="list-style-type: none">> Accomplissement d'une tâche publique ou d'intérêt public> Besoin d'expérimentation> Dossier pilote, phase d'évaluation, rapport d'évaluation> Règlement de portée générale d'une durée limitée dans le temps> Mesures de protection> En principe, 5 ans maximum	<p>Fixe des règles supplémentaires pour les projets pilotes qui incluent <u>le traitement de données sensibles, des activités de profilage ou d'autres traitements risqués</u></p> <ul style="list-style-type: none">> Implication de l'ATPrDM

3. Droits de la personne concernée

Droits hors procédure (art. 27 à 31)

- > **Droit d'accéder à ses propres données (art. 27-29)**
 - > Globalement inchangé
 - > **New** Contenu un peu plus élargi conformément à la LPD et au droit européen
 - > Gratuit mais possibilité pour le CE de fixer des exceptions (effort disproportionné, demandes abusives...)
 - > Restrictions possibles afin des protéger des intérêts publics ou privés prépondérants (cf. art. 29)
 - > Nouveau motif de restriction : caractère abusif de la demande (codification de la jurisprudence)
 - > Règle spéciale pour les données versées aux archives historiques (codification de la jurisprudence)
- > **Droit d'accéder aux données d'une personne décédée (art. 30)**
 - > Nouveauté
 - > Codification de la jurisprudence

3. Droits de la personne concernée

Droits hors procédure (art. 27 à 32)

- > **Droit de s'opposer à la communication de certaines données (art. 31)**
 - > **Nouveauté** : élargissement à tous les responsables du traitement
 - > Restrictions possibles, notamment si l'opposition entre en conflit avec une communication prévue par la loi ou risque de compromettre l'accomplissement d'une tâche d'un organe public (cf. art. 30 al. 2)
 - > Règles spéciales pour les communications à des personnes privée (cf. art. 30 al. 2 let. c)
 - > Mise en balances des intérêts de la personne privée qui demande les données avec les intérêts de la personne qui a exercé son droit d'opposition
 - > Décision sujette à recours
- > **Droit à la portabilité des données (art. 32)**
 - > **Nouveauté**
 - > Limité à certaines bases de données tenues selon des formats spéciaux
 - > Besoin de concrétisation dans la législation spéciale ou par le responsable du traitement

3. Droits de la personne concernée

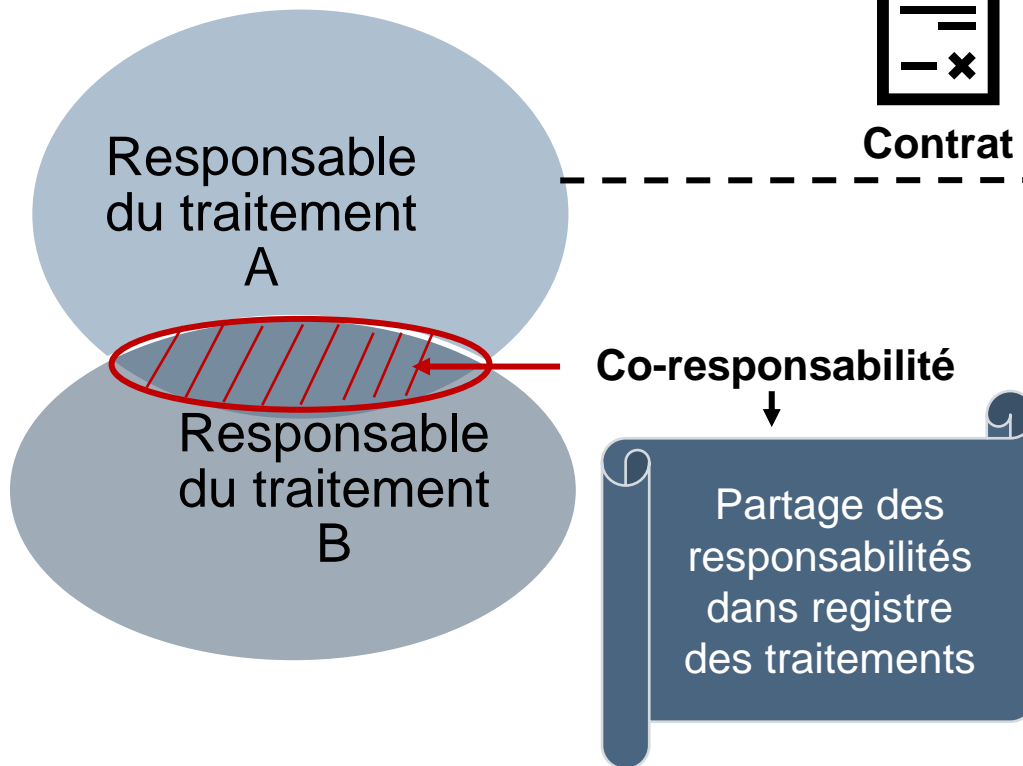
Actions défensives (art. 33-34)

- > **Face à un traitement supposément illicite**
- > **Toute personne qui dispose d'un intérêt digne de protection peut demander que le responsable du traitement :**
 - > s'abstienne de traiter les données illicitement (action préventive);
 - > cesse de traiter les données illicitement (action en cessation);
 - > constate le caractère illicite d'un traitement (action en constatation).
- > **En particulier, elle dispose des prétentions suivantes :**
 - > action en suppression des données qui n'ont plus de finalité;
 - > action en rectification des données erronées;
 - > **New** action temporaire en limitation du traitement si des clarifications sont requises;
 - > action en apposition du caractère litigieux d'une donnée;
 - > action en publication ou en communication d'une décision prise sur la LPrD.
- > **Exception :**
 - > Pas d'action en suppression et en rectification des données conservées dans des fonds d'archive
- > **Procédure et voies de droit selon CPJA et LCo**

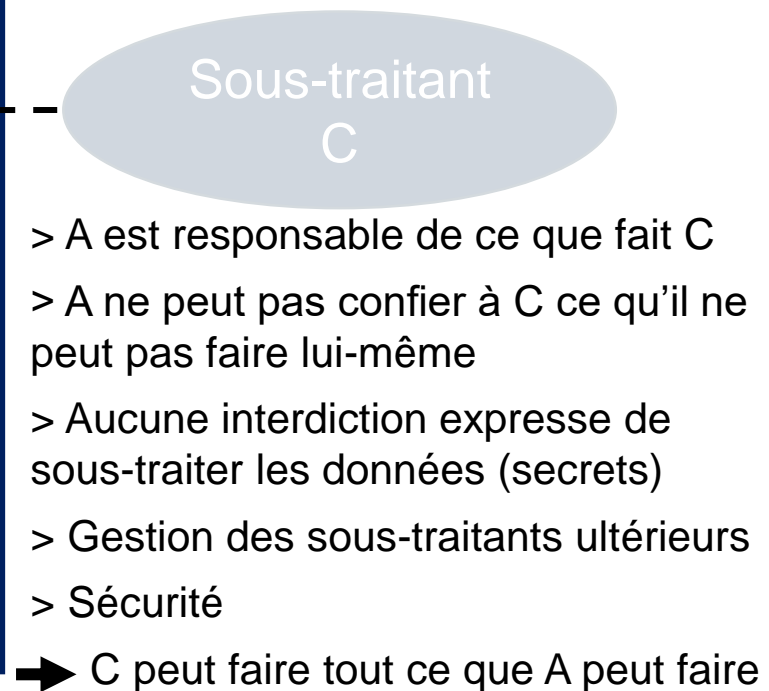
4. Mise en œuvre de la protection des données

Responsabilités (art. 36 et 37)

En général (art. 36)



Sous-traitance (art. 37)



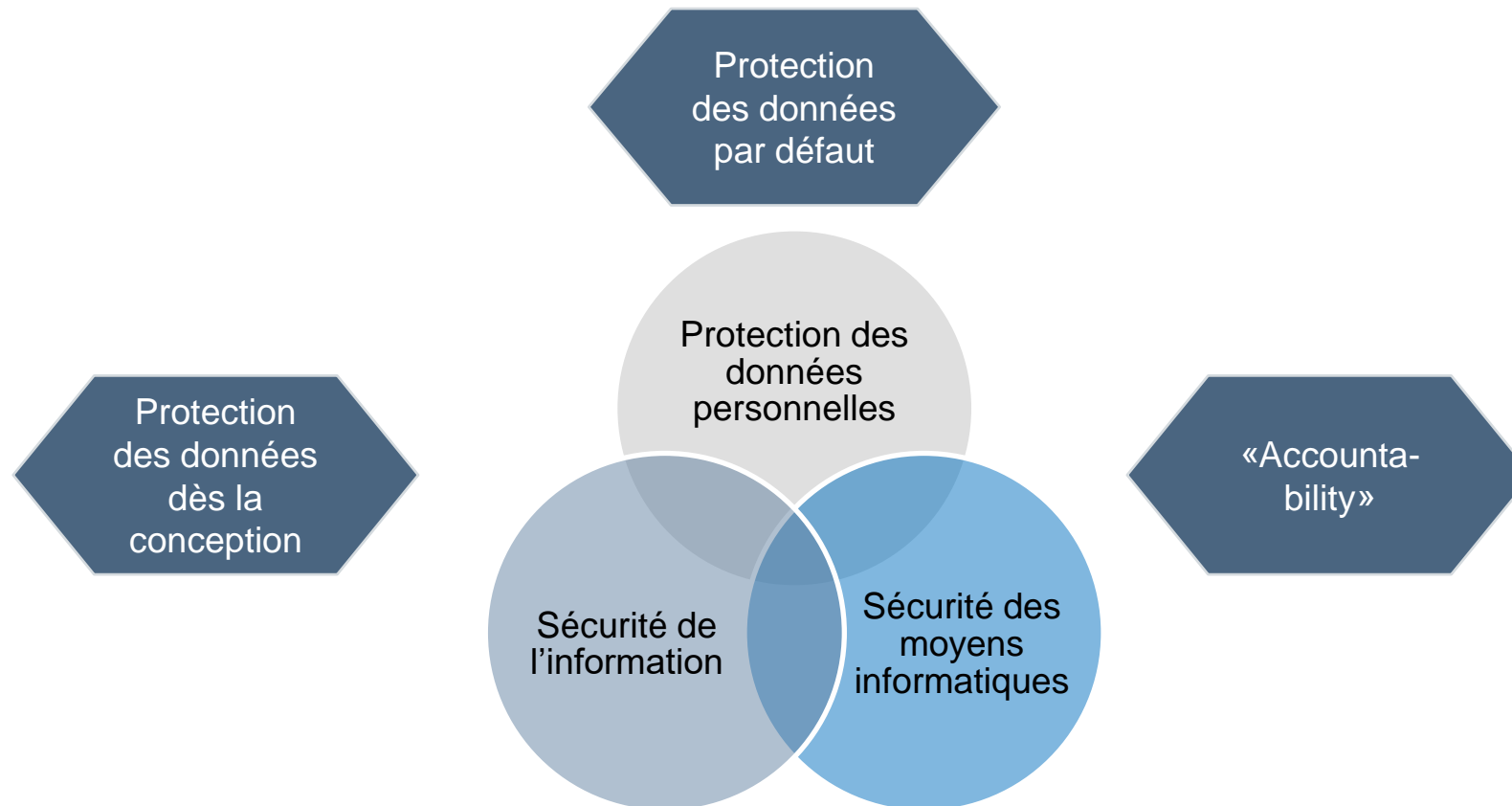
4. Mise en œuvre de la protection des données

Registre des activités de traitement (art. 38 et 39)

- > **Cartographie des traitements de données**
- > **Traitements accomplis par les organes publics cantonaux et communaux et par les délégués d'une tâche publique**
- > **Obligation de déclarer les traitements à l'ATPrDM**
- > **Exceptions pour traitements de moindre importance (cf. art. 39)**
- > **Registre déjà existant (registre des fichiers / ReFi) et accessible en ligne**

4. Mise en œuvre de la protection des données

+/- New Mesures organisationnelles et techniques (art. 40)



4. Mise en œuvre de la protection des données

Nouveauté : Analyse d'impact relative à la protection des données (art. 41 et 42)

- > **Analyse d'impact nécessaire si un nouveau traitement de données fait naître la suspicion d'un risque élevé pour les droits fondamentaux**
- > **Analyse selon les circonstances; la loi fixe quatre situations dans lesquelles il existe une présomption de risque élevé**
- > **Contenu de l'analyse d'impact**
 - > Description du traitement
 - > Evaluation des risques techniques et juridiques
 - > Mesures prévues pour protéger les droits fondamentaux
- > **Si analyse confirme existence d'un risque élevé, consultation de l'ATPrDM**
- > **Prise de position de l'ATPrDM dans délai de 2 mois, prolongeable d'un mois**
- > **Responsable du traitement informe l'ATPrDM de la suite apportée**

4. Mise en œuvre de la protection des données

Nouveauté : Violation de la sécurité des données (art. 43 et 44)

Mesures à prendre	Obligations d'annonce
<ul style="list-style-type: none">> Identifier> Corriger> Minimiser les effets> Consigner> Communiquer ?	<ul style="list-style-type: none">> Du sous-traitant au responsable du traitement> Du responsable du traitement à l'ATPrDM si vraisemblance d'un risque élevé> * Du responsable du traitement au centre national suisse pour la cybersécurité (NCSC) s'il s'agit d'une cyberattaque (74b LSI)> Du responsable du traitement à la personne concernée si nécessaire pour des motifs de transparence, pour protéger ses droits ou si l'ATPrDM l'exige> Exceptions à l'obligation d'annonce> Possibilité d'une annonce publique

Définition d'une violation de la sécurité des données à l'article 4 al. 1 let. k

4. Mise en œuvre de la protection des données

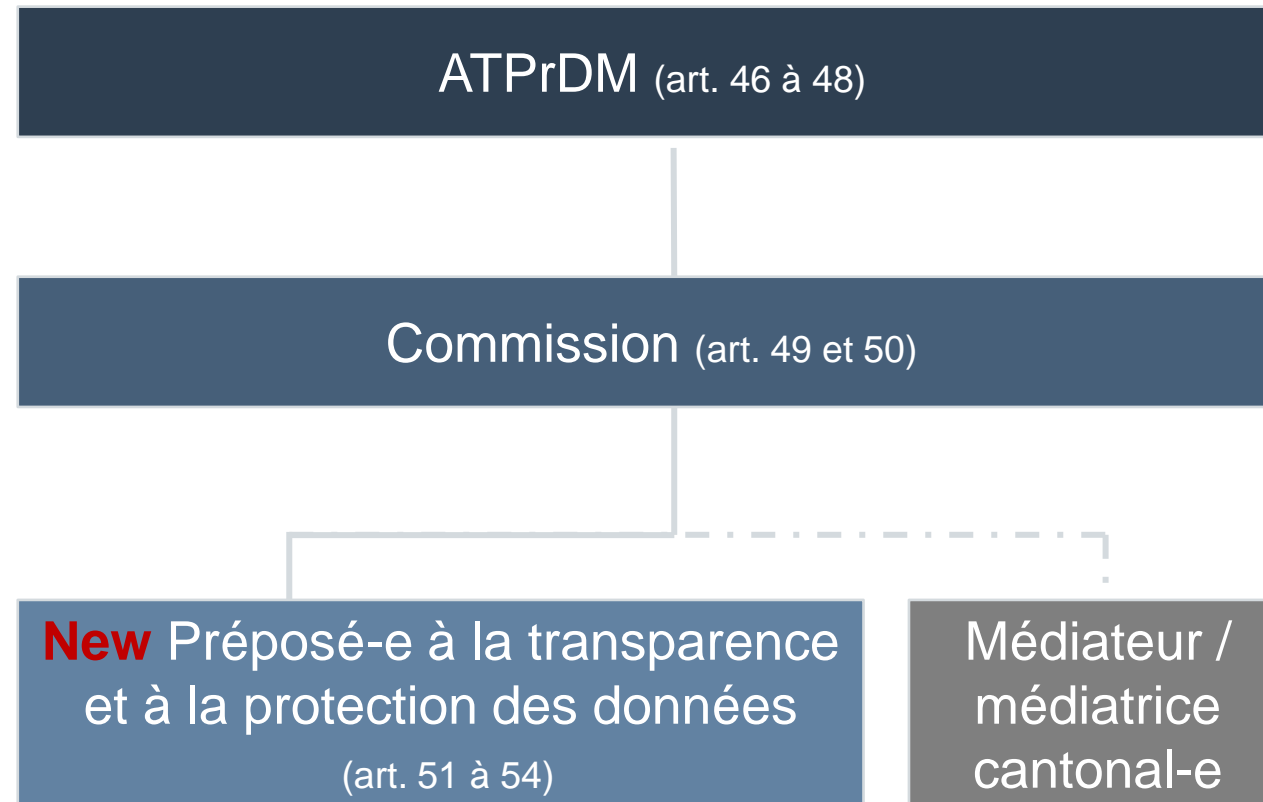
Demi-nouveauté : Correspondants et correspondantes à la protection des données (art. 45)

- > Professionnalisation de la protection des données au sein des Directions
- > Une personne par Direction
- > Tâches de sensibilisation et de conseil, participation à la réalisation des analyses d'impact et contact avec l'ATPrDM
- > Certaine autonomie reconnue
- > Création d'un réseau de compétence au sein de l'administration

Pas d'obligation pour les communes... mais pas interdit non plus...

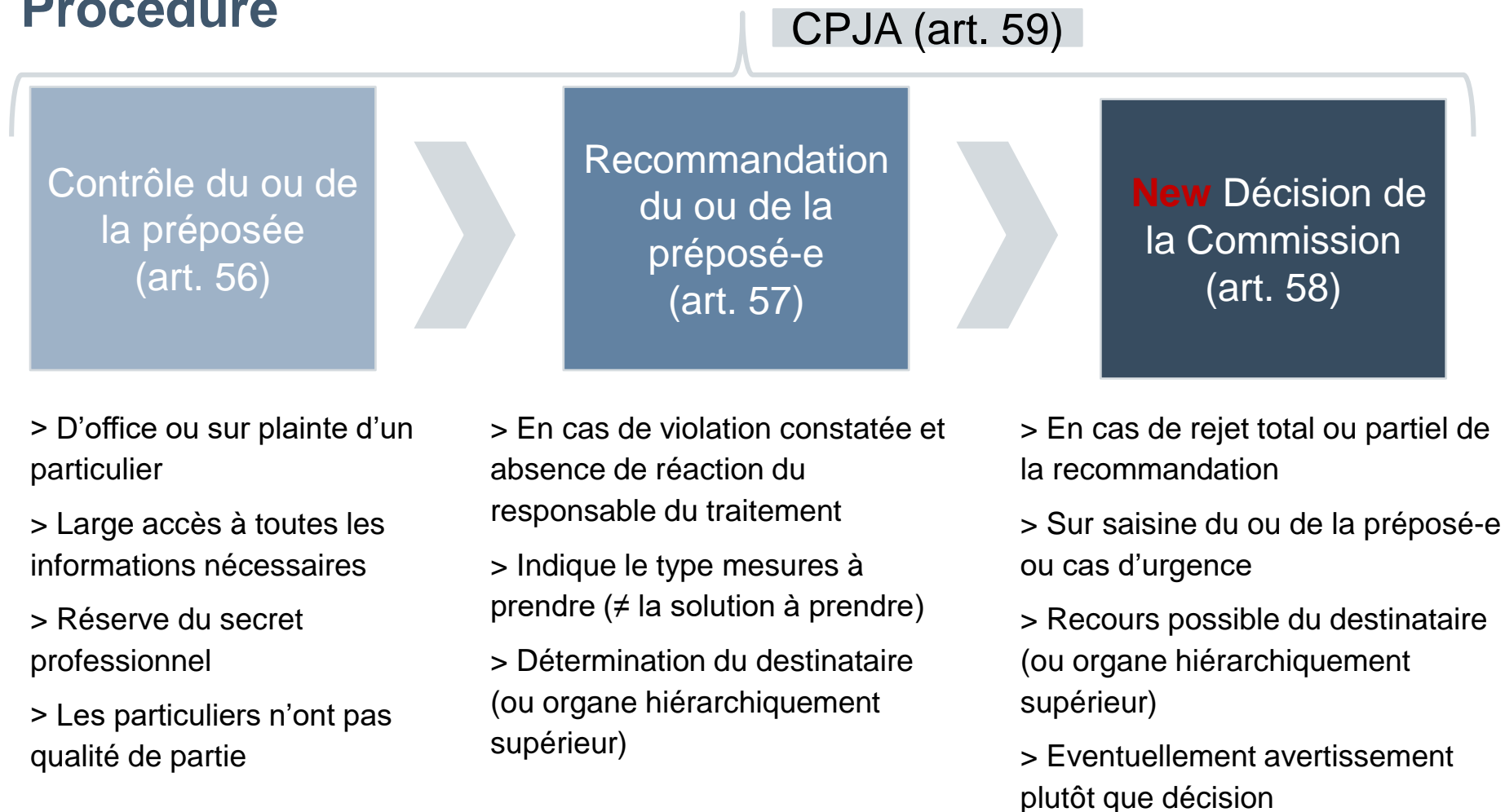
5. Surveillance

Autorité compétente



5. Surveillance

Procédure



6. Dispositions finales et transitoires

- > **Règlementation d'exécution (art. 61)**
 - > Annonce l'adoption d'une ordonnance d'exécution
- > **Droit transitoire (art. 62)**
 - > Délai de mise en conformité de deux ans
 - > Absence de délai de mise en conformité pour les traitements soumis aux accords de Schengen-Dublin
- > **Adaptation de la législation (art. 63)**
 - > Délai de mise en conformité de deux ans

7. Modifications d'autres lois concernant les communes

- > **Loi sur les communes (LCo)**
 - > Base légale pour l'exploitation d'un système de gestion des affaires (cf. art. 102a)
- > **Code de juridiction et de procédure administrative (CPJA)**
 - > Transparence en cas de recours dans le cadre d'une procédure à des outils d'aide à la décision reposant sur des algorithmes + droit à l'information (art. 66a)
 - > Transparence en cas de décision prise intégralement par une machine + droit à l'information + droit à un réexamen gratuit si suspicion d'erreur commise par la machine (art. A1-4a)
- > **Loi sur la vidéosurveillance (LVid)**
 - > Rappel des règles sur l'analyse d'impact (cf. art. 4 al. 3)
 - > Cosmétique législative (préfet / préfète)
- > **Loi sur la cyberadministration (LCyb)**
 - > Reprise des dispositions modifiées sur le cloud computing introduites à l'article 19 LPrD (cf. art. 35a et 35b)
 - > Dispositions sur les projets pilotes (cf. slide 15)