privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Guide à l'attention des autorités cantonales de la protection des données sur le principe *once-only* dans les cantons

Introduction

Les autorités et les entreprises sont constamment confrontées à la question de la possibilité d'augmenter l'efficacité induites par la numérisation. Les entreprises se préoccupent en premier lieu de la question de la rentabilité et il convient, dans le cadre de l'administration publique, d'examiner leur exploitation en rapport avec la conformité des exigences juridiques correspondantes. En ce domaine, les droits fondamentaux sont au premier plan, en particulier l'autodétermination informationnelle, mais aussi la question de la légalité.

Dans ce contexte, l'approche du caractère unique, ou justement *once-only*, est sur toutes les lèvres *;* il s'agit de la question de savoir comment éviter la communication multiple et, partant, lourde et sujette aux erreurs, de certaines données (à caractère personnel) à l'attention des autorités publiques et en veillant à ce que ces données ne soient (ou ne doivent être) communiquées *qu'une seule fois* à une autorité étatique compétente et que l'accès à ces informations par toute l'administration publique de la collectivité correspondante ou par certaines autres autorités soit assuré conformément à la protection des données et de manière appropriée (principe appelé *once-only*).

Sur mandat de *privatim*, la Conférence des Préposé(e)s suisses à la protection des données, prof. Astrid Epiney, LL.M., et Sophia Rovelli, MLaw, de l'Institut de droit européen de l'Université de Fribourg, ont établi un avis de droit sur le thème « *Once-only* et le principe de l'Etat de droit ». L'objectif du présent document de travail consiste à résumer l'avis de droit à l'attention des autorités pour la surveillance de la protection des données dans les cantons où cela s'avère pertinent et de mettre en évidence les points délicats de l'application du principe *once-only*.

L'expertise porte sur les bases juridiques du droit fédéral (Constitution et loi sur la protection des données). Par analogie, on peut se servir des conclusions relatives aux droits fondamentaux et constitutionnels dans le cas de réglementations comparables dans les cantons.

1. Avis de droit : *once-only* et le principe de l'Etat de droit[1]

L'expertise se réfère à une étude que les auteures ont effectuée sur mandat de *privatim* au sujet de la question de droit suivante :

> « L'avis de droit demandé doit s'attacher à la question de savoir si, et, le cas échéant, sous quelles conditions, l'introduction du principe dit *once-only* prévue dans la stratégie de numérisation de la Confédération et de différents cantons est en accord avec le principe de l'État de droit en général et, en particulier, avec les principes pouvant en être dérivés en matière de droit sur la protection des données. Un accent particulier devra être mis ici sur la qualification *once-only* du point de vue du droit de la protection des données, sur les barrières ou « garde-fous » constitutionnels inhérents à ladite législation, ainsi qu'après cela sur l'aménagement possible *once-only*. Une digression doit également aborder l'aménagement et l'application pratique du principe *once-only* en Estonie. »

1.1. *Once-only* : l'idée maîtresse

L'**idée maîtresse** du ***principe*** appelé ***once-only*** repose sur la communication unique d'une information (à caractère personnel) aux organes de l'Etat et sur la réutilisation ou le partage

[1] Prof. Astrid EPINEY, LL.M., Sophia ROVELLI, MLaw, Avis de droit *once only* et le principe de l'Etat de droit de mars 2021 sur mandat de *privatim*, la Conférence des Préposé(e)s suisses à la protection des données (cit. EPINEY/ROVELLI, Avis de droit privatim, n.)

des données des personnes physiques et morales ainsi collectées par les autorités.[2] L'intérêt sous-jacent du principe *once-only* se situe dans la réduction de la charge administrative pour les personnes physiques et morales et une éventuelle augmentation de l'efficacité de l'administration.[3] Apparaît ici le caractère relativement ouvert du concept, *once-only* pouvant à la fois être compris comme une collecte d'informations unique de la part de l'Etat ou comme une prescription d'enregistrement unique de données dans une base unifiée.[4]

1.2. L'exemple estonien *once-only*

L'Estonie se distingue comme étant un exemple d'application du principe *once-only*, puisque le pays peut être considéré comme un précurseur européen en matière de numérisation. Presque tous les services administratifs sont disponibles en ligne et le principe *once-only* est mis en œuvre à relativement large échelle.

Le coup d'envoi de la mise en œuvre du principe *once-only* en Estonie est, d'une part, le recours à la technologie dite X-Road et, d'autre part, l'identification des personnes et des entreprises par l'utilisation obligatoire d'un numéro d'identification personnel et d'une ID électronique. En fait, X-Road n'est pas une base de données centralisée, mais avant tout un réseau (*data exchange layer, « couche d'échange de données »*) qui permet d'accéder à différentes bases de données.[5]

En Estonie, les **bases légales** portant sur le traitement des données personnelles se retrouvent, d'une part, dans les articles correspondants de la législation spécifique ; d'autre part, le *Public Information Act* (« Loi sur l'information du public ») et le *Personal Data Protection Act* (« Loi sur la protection des données à caractère personnel ») présentent en particulier des directives et bases légales pertinentes, qui sont spécifiées dans les directives *Estonian Data Protection Inspectorat* (« Inspection estonienne de la protection des données »). Outre le principe de transparence, le ***Public Information Act*** réglemente aussi les conditions pour la création et la gestion de bases de données, pour le respect des limitations d'accès et le monitorage de banques de données de droit public. La création et l'exploitation de **bases de données par les organes de l'Etat** requiert une **base légale,** tandis que le lancement, la modification et la suppression d'une telle base de données doivent faire l'objet d'une autorisation. Il est, par ailleurs, interdit de saisir à nouveau dans une base séparée des données déjà présentes dans l'une d'elles.[6]

Outre les droits constitutionnels, le ***Personal Data Protection Act*** est également déterminant pour la **protection des données personnelles**. Il décrit les conditions à respecter pour le traitement des données personnelles, les obligations des personnes amenées à traiter les données, ainsi que les droits des personnes concernées. Par analogie aux autres lois sur la protection des données, il statue sur les principes de base du traitement des données, comme le principe de la finalité. Cependant, un **écart par rapport à l'objectif originel est admissible** lorsqu'il existe une base légale demandant le traitement des données et que l'on tient compte du principe de proportionnalité. De plus, les **personnes concernées** peuvent poser certaines conditions à la communication des données, sont informées de l'exploitation de leurs données et ont la possibilité de consulter ces dernières sur une plate-forme. Les recherches effectuées sont, de plus, journalisées jusqu'au numéro personnel de la personne venant à intervenir. Si on présume une **atteinte à la sphère privée**, une **plainte** peut être déposée auprès de l'*Estonian Data Protection Inspectorate*, une décision négative pouvant également être attaquée en justice.

[2] EPINEY/ROVELLI, Avis de droit privatim, n. 2.
[3] EPINEY/ROVELLI, n. 7. D'autres objectifs touchent à la prévention des fraudes ainsi qu'au renforcement de la croissance économique et, au niveau européen, la charge administrative moindre devrait réduire les obstacles au marché intérieur et ainsi promouvoir la libre circulation au sein de l'UE.
[4] EPINEY/ROVELLI, Avis de droit privatim, n. 9.
[5] EPINEY/ROVELLI, Avis de droit privatim, n. 11 s.
[6] EPINEY/ROVELLI, Avis de droit privatim, n. 13.

1.3. Limites : les autres thèmes de la cyberadministration

Les systèmes de traitement des données selon le principe *once-only* prennent en charge des données personnelles de manière centralisée dans un système spécifique et les mettent à la disposition d'autres autorités pour l'exécution de tâches précises, en général lors d'une procédure d'appel. Ainsi, les données collectées servent une fois à plusieurs autorités pour l'exécution de leurs propres tâches réglementées sur le plan de la loi. Il convient de faire la distinction entre les systèmes de traitement des données qui traitent les données seulement pour une certaine exécution légale des tâches qui leur est propre et qui n'accordent aucun accès aux autres pour une nouvelle exécution des tâches. Par exemple, les portails de cyberadministration ne sont pas des systèmes de traitement des données *once-only* s'ils traitent exclusivement les données dont ils ont besoin pour l'utilisation du portail.

1.4. Bases : le principe de l'Etat de droit et la protection des données

« Le principe de l'État de droit implique l'existence d'une base légale pour toute action de l'État. De plus, le traitement de données personnelles par les organes de l'État tombe sous le coup du domaine de protection de l'art. 13, al. 2 Cst. Par ailleurs, les conditions préalables à une **restriction des droits fondamentaux** doivent être respectées conformément à l'art. 36 Cst. La loi sur la protection des données concrétise ces exigences de droit constitutionnel pour le traitement de données personnelles. La communication de telles données à des tiers constitue à cet égard une forme particulière de traitement des données. Si des données personnelles sont communiquées de manière automatisée, des exigences plus rigoureuses sont alors applicables à la base légale, car l'examen de proportionnalité préalable par le propriétaire des données n'a pas lieu dans chaque cas, augmentant ainsi le risque d'atteinte à la personnalité ».[7]

1.5. Implications du principe de l'Etat de droit pour l'aménagement du *once-only*

1.5.1. *Once-only* en tant que communication automatique des données

Lors de la communication automatique des données dans le cadre du *once-only*, il convient d'appliquer des exigences plus rigoureuses à la base légale. Ce principe a cours à cause du danger plus important d'atteinte à la personnalité même après la suppression de la prescription expresse du droit fédéral pour la procédure d'appel (art. 19, al. 3 aLPD).[8]

1.5.2. Respect du contenu essentiel de l'autodétermination informationnelle

L'aménagement du *once-only*, dans lequel des quantités très importantes de données personnelles sont partagées avec de nombreux organes de l'Etat, sans conditions, serait problématique en considérant le contenu essentiel de l'art. 13 Cst. Une surveillance généralisée et l'établissement d'un profil de personnalité complet (citoyens transparents, « gläserne Bürger ») doivent être empêchés.[9]

1.5.3. Nécessité d'une base légale

L'introduction du principe *once-only* – du moins jusqu'à un certain point et pour autant que le recours à ce principe est obligatoire – requiert une base légale formelle. Les aspects importants suivants doivent être définis avec une précision suffisante dans la législation spécifique :

- but du traitement
- étendue du traitement des données
- catégories des accédants autorisés

[7] EPINEY/ROVELLI, Avis de droit privatim, n. 38.
[8] EPINEY/ROVELLI, Avis de droit privatim, n. 41.
[9] EPINEY/ROVELLI, Avis de droit privatim, n. 45 ss.

- catégories de données
- droits des personnes concernées
- durée de la conservation
- suppression

Une interaction entre loi et ordonnance (grandes lignes dans la loi, précision dans l'ordonnance) est possible. Une clause générale, en vertu de laquelle toutes les autorités pourraient communiquer toutes les données dont elles ont besoin pour l'exécution des tâches, ne serait pas conforme à la Constitution.[10]

1.5.4. Intérêt public

L'amélioration de l'efficacité peut être considérée comme un intérêt public.[11]

1.5.5. Proportionnalité

L'aménagement de diverses mises en œuvre du principe *once-only* est envisageable. La question de la proportionnalité d'une mise en œuvre concrète doit être évaluée au moyen des critères mentionnés ci-après.

1.5.5.1. Aptitude

La mise en œuvre peut générer un gain d'efficacité dans l'administration, ce qu'il faut évaluer en fonction des circonstances concrètes.[12]

1.5.5.2. Nécessité

La nécessité doit être vérifiée au moyen des critères suivants :

- les données ne doivent être traitées que dans une mesure correspondant à l'exécution des tâches ;
- les requêtes individuelles doivent être privilégiées par rapport aux requêtes sous forme de listes ;
- la mise en œuvre la plus sûre doit être choisie d'un point de vue technique ;
- le risque d'abus doit être réduit par des mesures appropriées (p. ex. réduction des catégories d'accédants autorisés, mise en place de barrières d'accès, limitation du volume de données consultables selon l'unité administrative ou encore selon la fonction du destinataire des données) ;
- un système de gestion des données, qui permet aux personnes concernées d'exercer un certain contrôle, peut s'avérer utile (sans pour autant remplacer la base légale !) ;
- les droits des personnes concernées doivent être renforcés par une transparence élevée et la traçabilité ;
- une mise en œuvre optionnelle est à préférer à une mise en œuvre obligatoire.[13]

1.5.5.3. Proportionnalité *stricto sensu*

L'acceptabilité doit être vérifiée en tenant compte d'une pesée généralisée des intérêts suivants :

- intérêt privé à la protection des données personnelles
- intérêt public à la protection des données personnelles
- efficacité dans l'administration
- accomplissement des tâches en vertu de la loi
- prise en compte du potentiel externe et interne d'abus et d'attaque[14]

[10] EPINEY/ROVELLI, Avis de droit privatim, n. 55.
[11] EPINEY/ROVELLI, Avis de droit privatim, n. 56.
[12] EPINEY/ROVELLI, Avis de droit privatim, n. 60 s.
[13] EPINEY/ROVELLI, Avis de droit privatim, n. 68.
[14] EPINEY/ROVELLI, Avis de droit privatim, n. 73 ss.

1.5.6. Finalité

La réutilisation potentielle de données une fois prélevées par les autorités dans un but autre que celui pour lequel elles ont été collectées devrait donc, au moins dans les grandes lignes, être déjà réglée sur le plan de la loi lors de la collecte initiale et être reconnaissable ou en tout cas conciliable avec le but originel. Les nouveaux buts précisément définis peuvent être traités ensuite dans une nouvelle base légale avec les champs d'application individuels du principe *once-only*.

Une admissibilité sans limites de la modification ultérieure ne serait pas constitutionnelle.[15]

1.5.7. « Protection des données par la technique » et sécurité des données

Le risque d'abus encouru en cas de possibilité de requête automatique doit être affronté en garantissant un niveau de protection technique et organisationnel élevé. La sécurité des données constitue un principe intrinsèque constitutionnellement fondé en matière de droit de la protection des données (art. 8 LPD) et elle joue un rôle essentiel aussi bien dans le cadre de la proportionnalité que dans l'optique des exigences envers la base légale. Des mesures de sécurité à appliquer en cas de communication automatisée des données doivent ainsi être décrites dans la base légale.[16]

2. Mise en œuvre concrète dans les cantons et exemples *once-only*

2.1. BE : LFDP

Avec la Loi sur les fichiers centralisés de données personnelles (LFDP, RSB 152.05, en vigueur depuis le 1er mars 2021), le canton de Berne a créé une base légale pour ce que l'on appelle les fichiers centralisés de données personnelles, dont les données sont systématiquement à la disposition de plusieurs autorités pour qu'elles puissent accomplir leurs tâches légales (art. 5, al. 2 LFDP). Le traitement « efficace » des données personnelles fait expressément partie du but de la loi (art. 1, al. 1, lettre a LFDP). Cependant, les autorités ne peuvent accéder (selon une procédure d'appel) à certaines données du système de gestion centrale des personnes (profils selon l'art. 6 LFDP) uniquement s'il existe une règlementation spécifique des droits (art. 8 ss. LFDP), qu'elles puissent prouver que les données demandées sont nécessaires pour l'accomplissement de leurs tâches légales ou, dans le cas de données personnelles particulièrement dignes de protection, qu'elles sont impérativement nécessaires (art. 5, al. 4 LFDP) et qu'il existe une base légale suffisante pour le traitement des données dans la loi spécialisée conformément à la législation sur la protection des données (art. 9, al. 1, lettre a LFDP).

La LFDP est une loi-cadre pour les fichiers centralisés de données personnelles ; elle désigne les prescriptions que le Conseil-exécutif doit régler par voie d'ordonnance pour chaque fichier centralisé de données personnelles (art. 7 LFDP). L'ordonnance sur la plate-forme des systèmes des registres communaux (O GERES, RSB 152.051) pour la plate-forme cantonale GERES, qui contient les données du contrôle des habitants des communes, est un exemple d'application. En s'appuyant sur la délégation du Conseil-exécutif, les Directions, la Chancellerie d'Etat et la Justice peuvent fixer elles-mêmes les accès pour leurs autorités (offices, unités administratives, etc.) au moyen d'une réglementation sur les droits (Ordonnance de Direction selon l'art. 8, al. 2, lettre a LFDP). Pour chaque accès, celle-ci doit prouver sa nécessité pour l'accomplissement des tâches et l'existence de bases légales suffisantes dans tous les actes législatifs.

Toute nouvelle réglementation des droits d'accès doit être présentée pour vérification (art. 11 LFDP) au Bureau cantonal pour la surveillance de la protection des données (BPD). Si des

[15] EPINEY/ROVELLI, Avis de droit privatim, n. 80.
[16] EPINEY/ROVELLI, Avis de droit privatim, n. 83.

différences considérables et insolubles sont constatées, le Bureau cantonal pour la surveillance de la protection des données peut porter la réglementation jusque devant le Tribunal administratif. La vérification juridique de l'admissibilité est ainsi assurée.

En tant que systèmes de traitement des données, les fichiers centralisés de données personnelles sont soumis en outre au contrôle préalable par le Bureau cantonal pour la surveillance de la protection des données en vertu de l'art. 17a de la Loi sur la protection des données (LCPD, RSB 152.04) au cas où on a affaire à des risques élevés (données particulièrement dignes de protection, données soumises à des obligations particulières de garder le secret ou recours à des moyens techniques présentant des risques particuliers pour les droits des personnes concernées [en particulier le Cloud]).

2.2. BS : marché des données ; DMV

L'Ordonnance sur le marché des données (DMV « Verordnung über den Datenmarkt », RS 153.310) a permis de créer une plate-forme centralisée qui met des données personnelles, factuelles et actualisées à la disposition des organes publics, lorsqu'elles sont requises par plus d'un organe public pour l'accomplissement des tâches légales.

Les organes publics sont tenus de mettre à la disposition du marché des données, sans frais, les données qu'ils génèrent dans une application spécialisée sur la base d'un mandat légal et qui sont aussi requises par un autre organe public ou plusieurs autres organes publics en vue de l'accomplissement de leurs tâches légales.

La remise des données a lieu par une procédure d'appel ou par une attribution unique et nécessite l'autorisation du détenteur des données. Les autorisations doivent être soumises à l'autorité pour la surveillance de la protection des données du canton BS pour un contrôle préalable.

2.3. FR : Référentiel cantonal

Le Référentiel cantonal est une infrastructure numérique qui traite principalement des données de référence concernant des personnes ou des organisations. Sous données de référence, il faut comprendre les données qui servent à identifier, recenser, localiser, contacter ou représenter la personne ou l'organisation. Le Référentiel cantonal contient en plus des données factuelles impersonnelles d'utilité générale telles que des informations sur les organes des collectivités publiques (noms et adresses des communes et des unités administratives, etc.), adresses postales, liste des pays et des nomenclatures standardisées (appellations, sexes, nationalités, types de personnes morales, etc.).

Le Référentiel est à la disposition des organes des collectivités publiques et des particuliers qui accomplissent des tâches officielles.

Les personnes concernées peuvent remettre des données supplémentaires sur elles-mêmes dans certains buts et demander la suppression ou la rectification de données personnelles erronées. L'ajout de données personnelles dans le Référentiel cantonal requiert le consentement libre et éclairé de la personne concernée ; en outre, l'administration doit avoir besoin de ces données et doit préciser chaque fois leur but.

Durant la phase pilote de deux ans, l'Autorité cantonale de la transparence et de la protection des données (ATPrD) est régulièrement consultée au sujet de l'évolution de la mise en œuvre et de l'exploitation du Référentiel cantonal. Elle peut intervenir en tout temps pour exiger le respect des dispositions relatives à la protection des données.

2.4. ZH : plate-forme cantonale des données sur les habitants ; MERG

La plate-forme cantonale des données sur les habitants (« Kantonale Einwohnerdaten-plattform ») représente la mise en œuvre du *once-only* dans une mesure limitée et dans une structure optionnelle.

La plate-forme cantonale des données sur les habitants représente une copie centralisée du registre communal des habitants. Les organes publics autorisés peuvent demander des données personnelles à cette plate-forme cantonale. Cependant, la souveraineté des données reste auprès des communes.

La base légale de la plate-forme cantonale des données sur les habitants découle du § 22 ss. de la Loi cantonale sur la communication et le registre des habitants (« kantonales Gesetz über das Meldewesen und die Einwohnerregistrer », MERG, LS 142.1). Les organes publics peuvent demander un accès à cette plate-forme pour certaines catégories de données. La connexion est accordée si la vérification par l'office communal indique qu'il existe une base légale pour le traitement des catégories de données souhaitées. L'autorité zurichoise pour la surveillance de la protection des données a vérifié le processus de connexion.

2.5. Un Service national des adresses

Au niveau fédéral, il convient de créer une base légale pour l'instauration d'un Service national des adresses (SNA) des personnes physiques, que l'Office fédéral de la statistique tiendrait et qui serait à la disposition de la Confédération, des cantons et des communes, ainsi qu'aux tiers habilités, pour l'accomplissement de leurs tâches publiques. La procédure de consultation s'est déroulée en automne 2019. Le message sur la Loi sur le service des adresses (LSAdr) devrait être adopté par le Conseil fédéral au début 2022.

3. « Garde-fous » pour le recours au principe *once-only*

Le principe de l'Etat de droit ne s'oppose pas fondamentalement au *once-only*. En accord avec les prescriptions constitutionnelles et relevant du droit de la protection des données, *once-only* peut être mis en œuvre si l'on observe les garde-fous mentionnés ci-dessous.

À RESPECTER IMPÉRATIVEMENT :

- **Respect de l'essence de l'art. 13 Cst** : éviter les profils de personnalité complets

- **Base légale** : lorsque *once-only* concerne plusieurs applications ou s'il est obligatoire : créer une base légale formelle. Des précisions sont possibles par voie d'ordonnance. La loi doit stipuler elle-même les points suivants :
  - finalité du traitement
  - étendue du traitement des données
  - catégories des accédants autorisés
  - catégories de données
  - droits des personnes concernées
  - durée de la conservation
  - suppression
  - responsabilités

- **Proportionnalité :** dans un cas concret d'application, choisir un aménagement proportionnel. Les éléments suivants sont possibles :
  - mise en œuvre optionnelle à titre d'option moins intrusive
  - droits d'accès différentiés
  - processus de l'examen de la proportionnalité des accès et des communications de données (comme dans la LFDP BE, dans l'ordonnance sur le marché des données BS et autres)

- transparence (« dashboard », tableau de bord)

- **Finalité** : réglementer légalement dans les grandes lignes la réutilisation dans un but autre déjà lors de la collecte initiale, rendre reconnaissable ou, en tout cas, vérifier qu'elle soit conciliable avec le but originel. Traiter en plus les nouveaux buts dans une nouvelle base légale. A cet égard, il faut tenir compte, en particulier, de la création de bases légales suffisamment « claires » pour le traitement et la communication de données personnelles sensibles dans les systèmes *once-only*.

À ÉVITER IMPÉRATIVEMENT :

- la création de « citoyens transparents »
- le remplacement de la base légale par des mécanismes de contrôle (« dashboard », tableau de bord) ou le consentement
- le démantèlement du principe de finalité par l'admissibilité sans limites de la modification ultérieure de la finalité du traitement
- le manque ou l'insuffisance (densité normative insuffisante) des bases légales pour le traitement et la communication des données dans les systèmes *once-only*, en particulier dans le cas de données personnelles sensibles

INTÉGRATION de l'autorité pour la surveillance de la protection des données

- Si un projet *once-only* est lancé dans l'administration, il convient d'y inclure l'autorité pour la surveillance de la protection des données en fonction de la législation cantonale sur la protection des données. En règle générale, cette autorité doit être consultée en vue d'une prise de position dans le cas d'un projet de loi et le responsable doit effectuer une analyse d'impact relative à la protection des données pour le projet concret en question.

- Si des accès aux données d'une base de données *once-only* doivent être accordés ou modifiés, nous suggérons de lancer une procédure de demande. Les demandes motivées doivent être adressées à l'organe responsable ou compétent de l'exploitation du système *once-only*. Les motifs doivent faire état de sa nécessité pour l'exécution des tâches, avec une justification suffisamment précise, en particulier lors d'une demande de données personnelles sensibles. Les demandes doivent être soumises pour avis à l'autorité pour la surveillance de la protection des données. Si aucun consensus n'est trouvé, la demande doit être présentée à l'organe supérieur compétent conformément aux règles de procédure cantonales en matière de clarification des questions en lien avec la législation sur la protection des données et une décision doit être prise. Les organes possédant un accès doivent supprimer, auprès de l'organe responsable ou compétent, les droits d'accès qui ne sont pas nécessaires, par exemple dans le cas d'un changement important dans la procédure. Une procédure de cette nature pourrait se dérouler comme suit :

  - Lancement de la procédure de demande, *le cas échéant*, par l'organe compétent du système *once-only*
  - Dépôt des demandes motivées (octroi, suppression, modification des accès) auprès de l'organe compétent
  - Examen par l'organe compétent et prise de position
  - Remise de la demande à l'autorité pour la surveillance de la protection des données
  - Examen par l'autorité pour la surveillance de la protection des données et prise de position
  - Décision, en cas de conflit, sur la demande par l'organe compétent selon les règles de procédure
  - Octroi des accès après la prise de position de l'autorité pour la surveillance de la protection des données ou après la décision déterminant la procédure par l'organe compétent

4. Liste de contrôle de la procédure législative

4.1. Introduction du principe *once-only*

Les conditions en cas de restriction des droits fondamentaux doivent être respectées dans la procédure législative. La nécessité d'une base légale pour introduire le principe *once-only* est au centre de l'attention. Le niveau de norme et la précision de la base doivent satisfaire aux exigences constitutionnelles.

Niveau de norme : tout principe *once-only* exige une base légale expresse (formelle). La promulgation d'une loi formelle est obligatoirement nécessaire si des données personnelles sensibles ou des données comportant un devoir de secret sont concernées, si *once-only* est aménagé en tant que principe obligatoire ou s'il est possible que des profils de personnalité soient établis.

Précision : le degré de précision nécessaire ne peut cependant être fixé de manière abstraite. Il dépend d'un grand nombre de facteurs tels que :

- la diversité et la complexité des points à réglementer,
- la responsabilité globale du système,
- les données concernées, les catégories de données,
- les fonctionnalités d'un système (comme l'historique, le profilage),
- les destinataires de la norme,
- la prévisibilité des décisions en l'occurrence nécessaires,
- la gravité de l'atteinte,
- l'aménagement technique ou
- la communication automatisée des données.

4.2. Base du traitement réglée par une loi spéciale

En plus de la base du principe *once-only*, il faut créer des bases juridiques supplémentaires dans une loi spécifique (p. ex. pour le traitement spécifique des données selon les tâches qui légitimise la réception des données à partir du système *once-only* ou la remise de ses propres données dans un système de cette nature). Ces réglementations doivent être aménagées au moyen des prescriptions de la législation sur la protection des données dans le canton en tant que base légale directe ou indirecte pour le traitement des données.

Dans ce contexte, il faut tenir compte notamment des aspects suivants :

1. Définition de la **finalité du traitement** ;
2. Evocation de la **nature et de l'étendue du traitement des données** avec, en particulier, l'aménagement de la communication des données ;
3. Catégories **d'autorités ou de personnes impliquées dans le traitement des données**, notamment les accédants autorisés ayant besoin d'un accès pour l'accomplissement de leurs tâches légales ; de même que la réglementation de la procédure d'attribution des autorisations d'accès ;
4. Précision des **catégories de données concernées ou traitées**, en particulier en présence de données personnelles sensibles, de profils de personnalité ou d'un éventuel profilage ;
5. **Intégration appropriée de l'autorité pour la surveillance de la protection des données** (voir LFDP BE, l'ordonnance sur le marché des données BS) ;
6. Réglementation de la **conservation et de la suppression** des données ;
7. Garantie des **droits des personnes concernées** ;
8. **Moyens utilisés pour la mise en œuvre de la procédure ou de la communication automatisée**, en particulier les mesures de sécurité devant être prises, ainsi que les responsabilités et compétences pour le système technique.

Annexe 1 Autres informations

Organisation	Titre	État
Université de Fribourg, Institut de droit européen	*Once-only* et le principe de l'État de droit Avis de droit établi sur mandat de *privatim*, la Conférence des Préposé(e)s suisses à la protection des données - prof. Astrid Epiney, LL.M. - Sophia Rovelli, MLaw	Mars 2021
privatim	Guide pour les portails web de l'administration publique	V 1.0/Juin 2018
Office fédéral de la statistique OFS	I14Y Plate-forme d'interopérabilité I14Y Plate-forme d'interopérabilité (admin.ch)	Dernière visite le 30 juin 2021