ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Préposée cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

Commentaire explicatif

au règlement-type d'utilisation pour la communication de données personnelles par procédure d'appel

Le présent règlement-type se fonde sur le pouvoir de conseil de la Préposée (art. 31 al. 2 let. b de la Loi du 25 novembre 1994 sur la protection des données, LPrD[1]). Il a pour but de guider les organes publics cantonaux et communaux compétents lorsqu'ils veulent instituer une procédure d'appel. Il n'est pas exhaustif et doit être complété selon les circonstances du cas particulier.

Nous vous donnons, ci-dessous, des informations sur les *bases légales nécessaires* avant d'élaborer un règlement d'utilisation (1.), puis des éléments pour élaborer ce *règlement* (2.).

1. Quant au préambule - bases légales

1.1 Type de bases légales

Le problème qui se pose est le suivant : quel type de bases légales doivent exister et que doivent-elles contenir ? Voici quelques remarques :

Il s'agit avant tout d'indiquer le *responsable du fichier* (art. 3 lit. g LPrD), c'est-à-dire l'organe compétent pour adopter le règlement d'utilisation, ce qui devrait figurer dans le préambule du règlement afin que l'utilisateur sache de qui celui-ci émane.

[1] RSF 17.1.

- Il faut ensuite déterminer les *dispositions légales existantes* (art. 4 LPrD) en la matière. Elles devraient, elles aussi, figurer dans le préambule du règlement pour assurer la clarté et la bonne compréhension pour l'utilisateur.
- Puis, il faut examiner le *type de base légale* nécessaire ce qui permettra de savoir si les bases légales existantes sont adéquates. Selon l'art. 10 LPrD, l'accès à des données personnelles au moyen d'une procédure d'appel ne peut être accordé à un destinataire que si une disposition légale le prévoit. Autrement dit, pour qu'il soit accordé un accès aux données, par le biais d'une procédure d'appel, il doit exister une disposition dans une loi ou dans une ordonnance (ou règlement).
- L'Autorité cantonale de surveillance en matière de protection de données a toujours interprété l'art. 10 al. 2 LPrD dans le sens que la base légale doit figurer dans une *loi* (base légale au sens formel) lorsqu'il s'agit d'une procédure d'appel portant sur des données *sensibles* (art. 3 lit. c et art. 8 LPrD). Cf. également ATF 122 I 360 ss.

  Dans les autres cas, on peut se contenter d'une base légale au sens matériel (ordonnance, règlement).
- Finalement, le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD)[2] prévoit à l'art. 2 la *définition* de la procédure d'appel, comme le mode de communication automatisé des données sous certaines *conditions* qui sont développées dans l'art. 21 al. 3 RSD.

  C'est sur cette base que le modèle de règlement d'utilisation vous est proposé.

1.2 **Contenu de la base légale** (formelle ou matérielle)

Voici quelques éléments qui devraient figurer dans la base légale prévoyant la procédure d'appel.

- Dans une *loi*, on pourra se limiter aux *éléments essentiels* qui justifient que l'on parle de ce sujet à cet échelon (par ex. parce que l'on traite de données sensibles) et dans le *règlement*, on donnera d'*autres précisions*.
- D'après l'art. 2 al. 1 let. c RSD, lorsque la transmission des données se fait par une procédure d'appel, elle implique la délivrance d'une *autorisation d'accès* de la part du responsable du fichier. La base légale devrait prévoir une formulation neutre (par ex., « l'accès peut être accordé au moyen d'une procédure d'appel... ») ou partant du point de vue du responsable du fichier (par ex., « X peut accorder à Y l'accès à telles données au moyen d'une procédure d'appel »). En revanche, la formule inverse basée sur le point de vue du destinataire des données est moins heureuse (par ex., « Y peut accéder par une procédure d'appel aux données détenues par X... »).
- Le *but* de l'utilisation ou réutilisation des données doit être établi de manière claire. Si la base légale définit le but uniquement de manière générale, le règlement d'utilisation devra le décrire de manière plus précise. Par ex.[3] le contrôle des

[2] RSF 17.15
[3] Les exemples proposés sont fictifs et supposent l'existence d'une loi au sens formel qui permette cette communication des données par le biais d'une procédure d'appel.

personnes ayant acquitté les amendes suite à une condamnation pénale pour une infraction particulière, en vue d'établir une statistique à la Direction de finances.

- L'organe public détermine les *tâches* à accomplir par les responsables du fichier et par les destinataires (art. 10 RSD). Par ex. la Direction de la sécurité et de la justice fixe la mise à jour des fichiers du Service de l'exécution de peines à X fois par mois, en vue d'effectuer le contrôle des amendes acquittées.
- Le cercle des *destinataires* concernés doit être suffisamment défini dans la base légale. Par ex. les destinataires sont les collaborateurs du Service de la statistique de la Direction de finances.
- Les *catégories des données* nécessaires à l'accomplissement de la tâche doivent être précisées. Par ex. les données communiquées par la procédure d'appel sont les données d'identité du condamné, la nature de l'infraction, les données comptables (versements).

2. Quant au règlement d'utilisation

Voici d'abord quelques remarques générales, puis des remarques particulières article par article.

- Le *but* du « règlement-type d'utilisation » est de servir de canevas à suivre lors de la mise en place de la communication automatisée des données par le biais d'une procédure d'appel. Il est possible de le modifier, de le compléter par ex. par une grille ou un tableau mentionnant qui accède à quoi et quand.
- Selon le caractère de confidentialité des données à communiquer et le type de traitement des données transmises, le règlement sera *adapté* ou *complété* pour répondre aux exigences de la LPrD.
- Les *variantes* prévues à l'art. 1 proposent l'introduction d'une annexe au règlement. Celle-ci devra suivre la même procédure que le règlement en cas de modification.
- Plus précisément, un règlement d'utilisation doit *au moins régler* toutes les informations prévues dans *l'art. 21 RSD*. Ce sont les suivantes :

Art 1 Responsable du fichier et destinataires

Al. 1. Mentionner *l'organe responsable du fichier* et les noms ainsi que la fonction des *personnes chargées des contacts avec les destinataires* et des *contrôles*. Il est également possible de faire figurer la liste nominative en annexe selon la variante.

Al. 2. Mentionner les *destinataires* concernés par l'autorisation du responsable du fichier et indiquer les *personnes autorisées à accéder aux données* et leurs fonctions. Le destinataire est en général un organe public ou privé. Il est également possible de faire figurer la liste nominative des personnes autorisées en annexe selon la variante.

Al. 3. Préciser *l'étendue de la consultation* : entière ou partielle, champ ou informations autorisés. Dans le cas où elle diffère selon les personnes, il est préférable d'indiquer

l'étendue de la consultation qui correspond à chaque personne dans l'annexe et utiliser la variante proposée.

Art 2 Données mises à disposition

Al. 1. et 2. Préciser la nature des *données personnelles* (art. 3 let. a LPrD), par ex. : données d'identité telles que nom, prénom, date et lieu de naissance, adresse, sexe, état civil, statut en Suisse, etc. et/ou des *données sensibles* (art. 3 let. c LPrD), à savoir : opinions ou activités religieuses, philosophiques, politiques ou syndicales ; santé, sphère intime ou appartenance à une race ; mesures d'aide sociale ; sanctions pénales ou administratives et procédures y relatives. Indiquer également lorsque aucune donnée personnelle sensible n'est mise à disposition.

Al. 3. Préciser le *nombre* approximatif des personnes concernées sur lesquelles il existe des données dans le fichier en question.

Art 3 Traitement des données

Al. 1. L'organe public est responsable des données et doit, par souci de sécurité et d'efficacité, établir la *fréquence* des communications ou interrogations. En particulier, il détermine selon les circonstances soit un nombre maximum d'interrogations, soit des événements précis qui justifient l'interrogation, par ex. lorsqu'il n'est pas possible d'obtenir ces données d'une autre manière et que celles-ci sont absolument nécessaires à l'accomplissement de la tâche de l'organe public.

Al. 2. Il décide également s'il y a un *droit d'impression et de reproduction* des données consultées.

Lorsque un tel droit est *admis,* le traitement de ces données doit ensuite suivre les principes généraux de la protection des données, en particulier la nécessité d'une base légale, le principe de proportionnalité et le principe de finalité (art. 4, 5 et 6 LPrD). La communication des données est traitée aux art. 10 et 11 LPrD alors que la destruction et l'archivage des données sont soumis aux art. 13 LPrD et 13 RSD. En pratique, ces données peuvent soit être classées dans différents fichiers existants, soit être classées ensemble. Dans ce dernier cas, elles ont une vie propre et constitue un nouveau fichier qui doit être à son tour déclaré auprès de l'Autorité cantonale de surveillance en matière de protection des données conformément à l'art. 19 LPrD.

Dans le cas contraire, l'*interdiction* formelle de faire des impressions et copies doit être mentionnée, de même que les mesures de sécurité y relatives.

Al. 3. Les ***destinataires*** n'ont pas le pouvoir d'introduire ou modifier des données dans le fichier (art. 21 al. 2 RSD). Si tel devait être le cas, il ne s'agirait plus de destinataires dans une procédure d'appel mais de ***participants*** qui auraient des responsabilités partagées avec le responsable du fichier (art. 3 let. h LPrD).

Art 4 Procédure d'authentification

Celle-ci devrait contenir au moins *l'identification des destinataires* par le biais de l'introduction d'un mot de passe personnel. Ce mot de passe doit être changé régulièrement. Il s'agit d'exigences comparables à celles de l'art. 17 RSD.

Art 5 Autres mesures de sécurité

Al. 1. Indiquer les *mesures de sécurité générales et spécifiques* prises par l'organe responsable du fichier. Il s'agit de déterminer les mesures organisationnelles et techniques mises en place pour assurer la confidentialité, la disponibilité et la sécurité des données. Ces mesures doivent notamment prévenir la destruction des données, le vol, l'accès non identifié, la falsification ou toute autre utilisation illicite ou de traitement non autorisé. Il s'agit par ex. du travail des données anonymes, codées, ou chiffrées.

Al. 2 Le terme de *« journalisation »* est défini à l'art. 2 al. 1 RSD. Ce procédé permettra ensuite de vérifier (art. 6) si les destinataires ont accédé uniquement aux données qui leur étaient nécessaires.

Art 6 Mesures de contrôle

Mentionner les *mesures de contrôle*, leur fréquence et l'organe de contrôle qui veillera à ce que l'utilisation réponde aux buts de consultation. La journalisation prévue à l'art. 5 sera particulièrement utile à la vérification.

Art 7 Communication et copie du règlement

Indiquer les éventuels destinataires d'une *copie du règlement,* par ex. le service destinataire ou bénéficiaire de la procédure d'appel.

Une copie doit parvenir à l'Autorité cantonale de surveillance en matière de protection des données. Dans l'art. 21 al. 3 RSD in fine, il est prévu qu'une copie du règlement d'utilisation est transmise à l'Autorité cantonale ou communale de surveillance en matière de protection de donnés. Il s'agit pour cette Autorité de pouvoir, le cas échéant, vérifier la conformité du contenu du règlement avec les dispositions en matière de protection des données et s'assurer que l'utilisation de ces données n'entraîne pas des atteintes illicites à la personnalité.

<u>Remarque supplémentaire</u>

Nous signalons qu'il convient de procéder, si nécessaire, à une analyse éventuelle des coûts pour évaluer l'opportunité de la procédure d'appel dans le cas d'espèce.

Annexe au commentaire explicatif

Les principales bases légales générales pour l'établissement d'un règlement d'utilisation sont les suivantes :

Loi du 25 novembre 1994 sur la protection des données (LPrD) (RSF 17.1)

Art. 10 Communication

a) Conditions

[1] …

[2] L'accès à des données personnelles au moyen d'une procédure d'appel, notamment un accès en ligne, ne peut être accordé à un destinataire que si une disposition légale le prévoit.

Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD) (RSF 17.15)

Art. 2 Définitions

[1] Au sens du présent règlement, on entend par :

a) …

b) *journalisation* l'enregistrement, à des fins de contrôle ou de reconstitution, de tout ou partie des activités effectuées sur un système ou sur une application informatiques ;

c) *procédure d'appel* le mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication.

[2] …

Art. 21 b) Procédure d'appel

[1] **...**

[2] **...**

[3] La procédure d'appel doit être documentée dans un règlement d'utilisation, qui précise notamment les personnes autorisées à accéder aux données, les données mises à leur disposition, la fréquence des interrogations, la procédure d'authentification, les autres mesures de sécurité ainsi que les mesures de contrôle. Une copie du règlement est transmise à l'autorité cantonale ou communale de surveillance en matière de protection des données.