ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

La Préposée cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm

PROCÉDÉ POUR LES CONTRÔLES

I. Introduction

La préposée cantonale à la protection des données (ci-après: la préposée) a notamment pour tâche de contrôler l'application de la législation relative à la protection des données auprès des organes de l'Etat et des communes (art. 31 al. 2 let. a et al. 3 de la Loi cantonale du 25 novembre 1994 sur la protection des données, ci-après: LPrD; RSF 17.1).

Le but de ces contrôles est de sensibiliser, d'informer et conseiller les organes sur la problématique de la protection des données, dans un esprit de collaboration. Ces contrôles peuvent prendre différentes formes : un contrôle planifié, à savoir annoncé et organisé, un contrôle spontané qui fait notamment suite à une faille de sécurité, une dénonciation ou un risque accru d'atteinte aux droits fondamentaux des personnes concernées, un contrôle général voire un contrôle limité à certaines activités de l'organe public. Ainsi, ces contrôles peuvent avoir comme objet les traitements des données personnelles de tout un service, être restreints (limités) à une section d'un service ou à un ou plusieurs traitements spécifiques ou domaines ou à certains aspects d'un traitement (p.ex. les droits et profils d'accès ou l'externalisation sous l'angle contractuel).

A la suite d'un contrôle, un rapport est transmis par la préposée à la Commission cantonale de la transparence, de la protection des données et de la médiation (ci-après: la Commission) qui en prend connaissance. Selon l'art. 30a al. 1 let. c LPrD, la Commission peut, le cas échéant, formuler des recommandations (mesures à prendre adressées à l'organe contrôlé et dont le non-respect peut faire l'objet d'une procédure judiciaire) ou des propositions (mesures dont le seul but est d'améliorer la situation). En aucun cas des procédures disciplinaires ou judiciaires ne sont entamées contre des collaborateurs.

Le présent document sert de guide à la préposée pour préparer et réaliser de façon optimale des contrôles. Il décrit les étapes à suivre et les tâches à effectuer, mais la préposée reste libre de l'adapter en fonction de la situation. Ce document s'inspire de l'expérience acquise par la préposée ainsi que de la méthodologie développée pour le groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre des accords d'association à Schengen (art. 54 s. de l'ordonnance sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE; Ordonnance N-SIS, RS 362.0).

Il est à souligner que la préposée recueille toutes les informations nécessaires à ce but, notamment demander des renseignements, exiger la production de documents, procéder à des

inspections et se faire présenter des traitements de données. Le secret de fonction ne peut lui être opposé (art. 31 a. 3 LPrD).

II. Avant le contrôle

1. Choix de l'organe à contrôler

En raison du grand nombre d'organes (services cantonaux, communes, etc.) pour lesquels la LPrD s'applique et qui sont susceptibles d'être contrôlés par la préposée, l'activité de contrôle ne peut pas être réalisée simultanément pour tous. Il est dès lors nécessaire de déterminer régulièrement auprès de quel organe un contrôle est effectué et s'il s'agit d'un contrôle global du respect de la protection des données ou si le contrôle se limite à certains aspects voire à un traitement spécifique.

Si le contrôle se limite à certains aspects spécifiques de la protection des données, notamment lors du déploiement d'un nouveau système de traitement ou d'accès à une plateforme, le même contrôle peut être effectué auprès de plusieurs organes ou services afin de veiller à un traitement cohérent et uniforme, et conforme aux exigences légales.

Les critères retenus pour déterminer cet organe sont notamment les suivants:

1.1 la sensibilité des données traitées par l'organe;
1.2 la quantité de données traitées par l'organe;
1.3 la fréquence du traitement effectué par l'organe;
1.4 la nouveauté du traitement effectué par l'organe;
1.5 le potentiel de violation des dispositions en matière de protection des données;
1.6 la connaissance d'un état de fait susceptible de ne pas être en adéquation avec les principes fondamentaux de la protection des données;
1.7 l'existence d'un contrôle similaire effectué dans un autre canton (comparaison);
1.8 le déploiement d'un nouveau système d'information auquel différents organes ou services peuvent accéder ;
1.9 l'existence de bases légales confiant des tâches spécifiques à l'Autorité ou à la préposée en matière de protection des données (cf. Référentiel cantonal de données, FriPers etc.).
1.10 l'actualité, notamment les évolutions dans le cadre de la digitalisation et de la cyberadministration.

Le choix de l'organe peut être proposé par la préposée à la Commission, qui peut demander des précisions concernant le contrôle. La Commission peut également proposer un organe à contrôler dans le cadre de ses attributions (art. 30a al. 1 let. b LPrD).

2. Préparation interne du contrôle par la Préposée

2.1 Recherche des dispositions légales pertinentes

La préposée recherche l'ensemble des dispositions légales qui s'appliquent dans le cadre du traitement de données par l'organe contrôlé. Il s'agit de dispositions fédérales, cantonales ou communales. Elles peuvent se trouver dans des lois, ordonnances ou règlements.
Les dispositions légales sont pertinentes lorsque :

2.1.2 elles décrivent l'organe (sa composition, son fonctionnement, ses liens avec d'autres organes, etc.);
2.1.3 elles énumèrent les activités de l'organe;
2.1.4 elles accordent des droits à l'organe;

2.1.5 elles imposent des obligations à l'organe;
2.1.6 elles traitent de la protection des données pour l'organe en général ou pour une de ses tâches en particulier (p. ex. un article de loi prévoyant que l'organe communique d'office certaines informations à d'autres organes);
2.1.7 elles traitent de la mise en œuvre d'un système d'information (p.ex. registre, plateforme, référentiel) dont l'organe a besoin, ou dispose d'un accès, pour l'accomplissement de ces tâches ;
2.1.8 elles concernent la digitalisation et la cyberadministration ;
2.1.9 elles soumettent l'organe à un secret de fonction, secret professionnel ou autre devoir de discrétion.

2.2 Recherche de jurisprudence

Il est également important de savoir s'il existe de la jurisprudence qui a un impact sur l'organe concerné en matière de protection des données.

2.3 Recherche d'informations diverses

Les informations de source non juridiques peuvent apporter des renseignements sur l'organe contrôlé. Il est ainsi possible de consulter le site Internet, les médias ou les autres moyens de communication.

2.4 Synthétisation des recherches

Après avoir collecté diverses informations, il est important de les synthétiser pour connaître le fonctionnement de l'organe et les activités qu'il doit exercer et qui ont un impact sur la protection des données. Il est indispensable d'avoir une connaissance aussi précise et étendue que possible de l'organe contrôlé pour effectuer un contrôle de qualité, être crédible et montrer un intérêt envers l'organe contrôlé. Il en va de même si le contrôle a pour objet un traitement spécifique respectivement un système d'information.

2.5 Détermination des points à contrôler

Sur la base de l'expérience de la préposée, des expériences menées dans d'autres cantons ou auprès d'autres organes fédéraux, une liste des points précis à contrôler doit être établie. Il peut s'agir par exemple de:

2.5.1 l'existence d'une information du personnel en lien avec la protection des données;
2.5.2 la conscience de la sensibilité de certaines informations et des risques potentiels;
2.5.3 l'existence d'une liste de personnes ayant accès à certaines données;
2.5.4 l'existence de restrictions d'accès à des données sensibles;
2.5.5 l'existence d'une liste des traitements effectués avec les données;
2.5.6 l'existence d'une liste des personnes à qui sont communiquées des données et de quelle façon;
2.5.7 l'existence d'un inventaire des applications informatiques et bases de données utilisées ;
2.5.8 en cas d'externalisation, l'existence des contrats garantissant la protection des données ;
2.5.9 du règlement d'utilisation d'un système informatique;
2.5.10 la concordance entre la pratique et ce qui est prévu.

Il est possible de limiter le contrôle à certaines activités, à l'exclusion d'autres qui ne présentent pas de risques ou de problèmes particuliers.

2.6 Rédaction de questions à poser et énumération des éléments à contrôler

En fonction de l'analyse des risques potentiels et en vue du contrôle effectif à réaliser, une liste contenant les points suivants est établie:

2.6.1 questions précises à poser lors du contrôle;
2.6.2 éléments spécifiques à contrôler (p. ex visite des locaux, consultation des logfiles ; consultation des contrats des prestataires externes);
2.6.3 informations à dispenser.

2.7 Personnel nécessaire

Si le contrôle nécessite des compétences particulières (p. ex. en informatique), la préposée mandate des spécialistes en la matière.

3. Prise de contact avec l'organe

3.1 Annonce préliminaire par oral

Dans un premier temps, un contact oral avec la personne responsable de l'organe ou la personne de contact annonce le contrôle. Le but est de :

3.1.1 se présenter brièvement;
3.1.2 informer l'organe de l'existence de cette tâche de contrôle et qu'il a été retenu;
3.1.3 informer l'organe de la date du contrôle prévu ;
3.1.4 de préciser qu'un courrier contenant de plus amples informations quant au déroulement du contrôle suivra prochainement.

3.2 Information du contrôle par courrier

Dans un deuxième temps, un courrier est adressé à l'organe contrôlé pour l'informer du contrôle et lui communiquer des détails. Le courrier contient :

3.2.1 les raisons du contrôle (tâches de la préposée, choix de l'organe, etc.);
3.2.2 le déroulement du contrôle (pour plus de détails voir ci-dessous point III. 6);
3.2.3 les éléments/aspects qui seront contrôlés;
3.2.4 une remarque sur le fait que, éventuellement en fonction du déroulement effectif du contrôle, celui-ci pourra être étendu à d'autres éléments;
3.2.5 la liste des documents pertinents à envoyer de manière préalable au contrôle, si certaines informations pour préparer le contrôle ne sont pas disponibles lors de la phase « recherche »;
3.2.6 une requête d'éventuelles précisions nécessaires pour le bon déroulement du contrôle (p. ex. emplacement géographique de certains systèmes traitant des données, existence de documents internes, etc.);
3.2.7 la proposition d'une date pour le contrôle, qui devrait se dérouler environ 5 à 6 semaines après l'envoi du courrier (1 semaine pour prendre connaissance du courrier et y répondre, 3 semaines pour faire parvenir d'éventuels documents supplémentaires à la préposée et pour qu'elle puisse en prendre connaissance et en tenir compte pour ajuster le déroulement du contrôle. Les 5 semaines seront nécessaires pour que l'organe en question puisse également se préparer). Le contrôle s'effectuera, si possible, hors des vacances usuelles;
3.2.8 une information sur la présence des personnes participant au contrôle (la préposée, un informaticien, un(e) juriste, un(e) collaborateur (trice), etc.);

3.2.9 la requête de la présence de certaines personnes de l'organe (chef, personne de contact, informaticien, collaborateur, etc.). La préposée peut établir le planning et la liste des personnes à interviewer.

L'organe hiérarchiquement supérieur ou l'organe de surveillance est informé du contrôle par envoi d'une copie du courrier précité.

3.3 Confirmation par téléphone

Quelques jours avant la date convenue entre les parties pour le contrôle, un entretien téléphonique confirme et rappelle le contrôle.

4. Ajustement de l'analyse préparatoire du contrôle

En fonction des documents éventuellement envoyés par l'organe contrôlé, le déroulement du contrôle est ajusté et les points à contrôler sont complétés. La préposée peut demander des documents ou informations supplémentaires, par écrit ou par oral.

III. Le contrôle

1. Localisation

Le contrôle s'effectue en principe dans les locaux de l'organe.

2. Déroulement

Un procès-verbal est rédigé de façon la plus neutre possible : aucun commentaire subjectif n'est consigné.

Le contrôle se déroule de la façon suivante :

2.1 la préposée décrit brièvement son rôle;
2.2 l'organe peut se présenter et expliquer la façon dont il aborde, de façon générale, les problèmes liés à la protection des données;
2.3 les questions prévues sont posées et les éléments examinés;
2.4 les éventuelles remarques ou questions finales de la part de l'organe sont récoltées;
2.5 la préposée requiert éventuellement de la part de l'organe contrôlé des documents ou informations supplémentaires, utiles à la rédaction du rapport du contrôle;
2.6 l'organe contrôlé est informé qu'un exemplaire du procès-verbal lui sera transmis et qu'il pourra y apporter des précisions ou corrections.

IV. Après le contrôle

3. Envoi du procès verbal

L'envoi du procès-verbal a lieu le plus vite que possible. Les éventuelles propositions de corrections que souhaitent apporter l'organe contrôlés sont envoyées à la préposée dans un délai fixé par cette dernière. Si la préposée décide de ne pas intégrer ces propositions dans le procès-verbal, celles-ci y sont annexées.

4. Analyse du contrôle

Sur les bases du procès verbal accepté par l'ensemble des parties, la préposée analyse la situation et relève :

4.1 les points positifs;
4.2 les points négatifs ou à améliorer.

Si des documents supplémentaires sont nécessaires ou de nouvelles questions apparaissent, la Préposée contacte l'organe contrôlé.

5. Rédaction d'un rapport final

Un rapport final comprenant un résumé du contrôle et l'analyse de ce dernier est rédigé. Le rapport est soumis à la Commission, puis à l'organe contrôlé pour d'éventuelles remarques.

6. Élaboration de recommandations et de propositions

Si nécessaire et en fonction du rapport final, la Commission élabore des recommandations ou des propositions.

7. Information de l'organe contrôlé

L'envoi du rapport final et des éventuelles recommandations ou propositions est effectué dès que possible. L'organe supérieur est informé du résultat du contrôle en joignant le rapport.

8. Publication du rapport final

Le rapport final peut faire l'objet d'une information générale dans le rapport d'activité; la question de l'information du public sera examinée en temps voulu à la lumière des résultats du rapport final et de la Loi du 9 septembre 2009 sur l'information et l'accès aux documents (RSF: 17.5), en prenant en compte la protection des données et la protection des intérêts publics.

V. Suivi

1. La préposée veille à ce que les éventuelles recommandations ou propositions soient suivies.
2. Lorsque le contrôle est terminé, la préposée en informe l'organe concerné ainsi que l'organe supérieur.

Florence Henguely
Préposée cantonale à la protection des données

Fribourg, le 5 avril 2022