ETAT DE FRIBOURG
STAAT FREIBURG

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

Réf. : RPA/FH 2016-FP-17

PRÉAVIS – FRI-PERS
du 28 février 2017

Interfaçage par webservices par le Service des curatelles d'adultes de la Ville de Fribourg (ci-après : SCFR)

I. Préambule

Vu

- les articles 16 et 16a de la Loi cantonale du 23 mai 1986 sur le contrôle des habitants (LCH) ;
- l'article 3 de l'Ordonnance cantonale du 14 juin 2010 relative à la plateforme informatique contenant les données des registres des habitants ;
- la Loi cantonale du 25 novembre 1994 sur la protection des données (LPrD) ;
- le Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD) ;
- le Préavis du 28 septembre 2016 de l'Autorité cantonale de la transparence et de la protection des données (2016-FP-13) ;
- la Décision du 3 octobre 2016 de la Direction de la sécurité et de la justice,

l'Autorité cantonale de la transparence et de la protection des données formule le présent préavis concernant la requête d'interfaçage par webservices entre l'application FRI-PERS et l'application informatique du SCFR, nommée KISS.

Le 28 septembre 2016, notre Autorité a émis un préavis favorable à l'accès aux données personnelles du profil 3 (P3), complétées par les données spéciales S1, S2, S3, S4, S5, S6, S7, S8 et S9 portant sur tout le territoire de la Ville de Fribourg ainsi que l'accès à l'historique des données de la plateforme informatique FRI-PERS. L'accès est limité aux données des habitants de la Ville de Fribourg, à savoir un accès soumis à une limitation liée au territoire du SCFR. Par décision du 3 octobre 2016, la Direction de la sécurité et de la justice a entièrement suivi notre préavis et a autorisé l'accès du SCFR aux données précitées.

Le présent préavis se base sur les éléments qui ressortent du « formulaire A2 (V1) de demande d'interfaçage par webservices de l'unité administrative entre sa base de données et la base de données FRI-PERS » daté du 9 novembre 2016 et de la séance du 31 janvier 2017 réunissant divers représentants de la Ville de Fribourg, le SITel et l'ATPrD.

Le but du présent préavis est de vérifier la licéité du traitement sous l'angle de la protection des données.

II. Interfaçage par webservices entre l'application FRI-PERS et l'application informatique de l'unité administrative concernée

Le SCFR a requis, par demande du 9 novembre 2016, l'interfaçage par webservices entre leur application informatique (KISS) et l'application FRI-PERS. Par interfaçage, il faut comprendre la consultation de l'application FRI-PERS, par l'application KISS, des données relatives au profil autorisé. En effet, l'application KISS interroge l'application FRI-PERS concernant les données d'une personne déterminée.

Il est utile de préciser que la présente demande d'interfaçage implique de simples mises à jour des données préavisées et autorisées.

III. Exigences minimales en matière de sécurité des données personnelles traitées par le SCFR

Suite à la séance du 31 janvier 2017 réunissant les différents services concernés et dans ce cas d'espèce particulier, l'autorisation doit être octroyée uniquement si les conditions ci-dessous sont respectées, dans la mesure où l'interfaçage va au-delà de la procédure habituelle.

L'article 22 LPrD rappelle que l'organe public qui traite des données personnelles doit prendre toutes les mesures d'organisation et techniques appropriées concrétisées dans le RSD.

En tant que **responsable de la sécurité des données personnelles traitées,** le SCR doit évaluer les risques encourus par le traitement qu'il envisage de faire dans l'accomplissement de ses tâches ①, doit prendre les mesures propres à assurer leur sécurité ② (art. 4 RSD) et spécifiques pour la procédure d'appel ③.

① Le SCFR doit évaluer les risques d'atteinte à la confidentialité des données et les risques de traitement non autorisé ; suivant les besoins, il évalue également les risques d'atteinte à l'intégrité et à la disponibilité des données (art. 8 RSD). Constituent notamment de tels risques : les risques de falsification, de vol ou d'utilisation illicite ; les risques de modification, de copie ou d'accès non autorisés ; les risques de perte accidentelle et d'erreurs techniques. Le SCFR attribue ainsi un degré de confidentialité selon l'échelle suivante : a) 1er degré : accessible au public ; 2ème degré : à usage interne ; 3ème degré : confidentiel ou secret. Pour ce faire, le SCFR se fonde sur la nature des données personnelles traitées, sur le but, l'étendue et les formes du traitement, ainsi que sur les préjudices qu'un usage abusif des données peut causer aux personnes concernées (art. 9 RSD). Notre Autorité est d'avis que les données personnelles traitées par le SCFR sont **classées confidentielles** ; cette classification entraîne une **protection accrue.** Ainsi, le SCFR doit prendre les mesures techniques qui ne permettent pas aux tiers d'accéder aux données contenues dans l'application KISS. Il est toutefois nécessaire de sécuriser la transmission des données entre les applications FRI-PERS et KISS par un cryptage (art. 20 RSD). Entre outre, l'accès aux données de KISS doit être autorisé par le SCFR aux collaborateurs désignés selon la fonction et les tâches. Si l'application KISS devait être liée à d'autres applications, il est de la responsabilité du Chef de service de faire une scission claire au stockage des données.

② Pour assurer la sécurité des données, le SCFR détermine, en fonction des tâches qu'elles sont appelées à exécuter, les personnes autorisées à accéder aux fichiers ainsi que l'étendue de leur accès. L'autorisation d'accès peut également, notamment lors d'un traitement informatisé des données, porter

sur des données ou des catégories de données spécifiques (art.10 RSD). Notre Autorité distingue les catégories suivantes :

- le Chef de Service a accès à tous les dossiers des clients ;
- les curateurs ont accès uniquement aux dossiers des clients qui leur sont attribués. Ces derniers auront l'accès à l'intégralité du dossier du client ;
- le comptable, selon sa tâche : si comptabilité du client, il a accès uniquement aux informations du dossier du client nécessaires à sa tâche ; si comptabilité du Service, il a accès à l'adresse du client, à la liste de frais et à l'adresse de l'Autorité compétente mais pas aux autres éléments du dossier ;
- l'administration a accès seulement aux données administratives des clients et non à leur dossier complet. Selon l'organisation interne, la personne s'occupe uniquement des dossiers clients qui lui sont attribués.

Les mesures techniques et organisationnelles peuvent porter aussi bien sur les personnes et les locaux que sur le matériel et la sécurité informatique (art.11 RSD).

③ Comme il s'agit d'une procédure d'appel, des mesures techniques et organisationnelles supplémentaires doivent être prises (art. 21 RSD).

Concernant l'authentification et le contrôle des accès, l'accès aux systèmes informatiques permettant le traitement de données personnelles doit être protégé dans un dispositif comprenant : a) une procédure d'authentification comprenant au moins l'identification des utilisateurs et l'introduction d'un mot de passe ainsi que b) un système de contrôle des accès, fondé sur une définition d'autorisations individuelles d'accès. L'accès aux applications et/ou fichiers doit également être protégé par un tel dispositif lorsque les données classées confidentielles sont traitées (art. 17 RSD). **Dans la mesure où les données traitées sont classées comme confidentielles, une authentification et un contrôle des accès doivent être prévus.**

S'agissant du SPoMi, ce dernier doit veiller à ce que les destinataires ne puissent pas modifier les données ni en entrer de nouvelles et qu'ils n'aient accès qu'aux données correspondant aux autorisations d'accès (lecture ou consultation). En outre, 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 (art. 21 RSD).

Le SITel doit garantir la traçabilité de la transmission des données entre l'application FRI-PERS et l'application KISS.

En matière de contrôle, il est nécessaire de rappeler que l'autorité supérieure doit contrôler la bonne application de ces règles. Dans le cas d'espèce, il s'agit du Conseil communal de la Ville de Fribourg. De plus, un contrôle par notre Autorité conformément aux articles 29ss LPrD et par le SITel conformément à l'article 27 RSD peut à tout moment être effectué.

IV. Nécessité de la requête

Afin d'être en mesure d'appliquer la législation fédérale et cantonale en matière de protection de l'adulte, le SCFR a besoin d'avoir accès à des données actualisées et exactes. Ainsi, l'interfaçage par webservices sollicité lui permettra d'obtenir des données régulièrement actualisées de ses clients et de les utiliser dans le cadre de ses activités.

En outre, il est important de rappeler que le numéro AVS ne peut être utilisé en tant qu'identificateur universel pour procéder à la mise à jour des données entre les applications FRI-PERS et KISS. En effet, l'utilisation du numéro AVS à cette fin est interdite par le droit fédéral. Le nom, la date de naissance et la localité suffisent dans la mesure où ces données permettent d'identifier une personne et d'accéder à ses données administratives actuelles.

V. Conclusion

L'Autorité cantonale de la transparence et de la protection des données préavise **favorablement** la demande d'interfaçage par webservices entre l'application FRI-PERS et l'application KISS :

pour les données du profil 3 (P3) complétées par les données spéciales S1 à S9 portant uniquement sur le territoire de la Ville de Fribourg ainsi que l'accès à l'historique des données de la plateforme informatique FRI-PERS ;

aux conditions suivantes :

- **seules les données des clients enregistrés dans la base de données KISS du SCFR seront mises à jour par l'export des données de l'application FRI-PERS ;**
- **le Chef du SCFR peut mettre à jour quotidiennement les données de la base de données KISS par les données FRI-PERS. Lors de l'attribution de nouveaux clients au Service, le Chef aura la tâche de créer un nouveau dossier en y insérant le nom, le prénom, l'adresse et la date de naissance de la personne concernée pour pouvoir accéder à ses données. Lorsque la mesure est levée, la personne décédée ou tout autre motif permettant de clore un dossier, il est de la responsabilité du Chef de Service de fermer le dossier et de vérifier que les données du client concerné ne soient plus mises à jour ;**
- **l'accès est restreint comme suit par le SCFR :**
  - **le Chef de Service a accès à tous les dossiers des clients ;**
  - **les curateurs ont accès uniquement aux dossiers des clients qui leur sont attribués. Ces derniers auront accès à l'intégralité du dossier client ;**
  - **le comptable, selon sa tâche : si comptabilité du client, il a accès uniquement aux informations du dossier du client nécessaires à sa tâche ; si comptabilité du Service, il a accès à l'adresse du client, à la liste de frais et à l'adresse de l'Autorité compétente mais pas aux autres éléments du dossier ;**
  - **l'administration a accès seulement aux données administratives des clients et non à leur dossier complet. Selon l'organisation interne, la personne s'occupe uniquement des dossiers clients qui lui sont attribués** ;
- **le Chef du SCFR est responsable du traitement des données provenant de FRI-PERS par les personnes autorisées à accéder à l'application KISS ;**
- **chaque collaborateur est responsable des données qu'il traite (clause de confidentialité et secret de fonction) ;**

- **le Règlement d'utilisation devra contenir l'obligation du responsable à prendre les mesures nécessaires et la responsabilité du Chef de service devra clairement y ressortir ;**
- **les mesures techniques et organisationnelles précitées devront être prises et respectées.**

Il est, en outre, rappelé que le numéro AVS ne peut être utilisé en tant qu'identificateur universel pour procéder à la mise à jour des données entre les applications FRI-PERS et KISS. En effet, l'utilisation du numéro AVS à cette fin est interdite par le droit fédéral. Le nom, la localité et la date de naissance suffisent dans la mesure où ces données permettent d'identifier une personne et d'accéder à ses données administratives actuelles.

VI. Remarques

> Les dispositions légales pertinentes doivent être respectées, notamment celles en matière de protection des données. Les données qui sont accessibles au service requérant ne doivent être consultées que pour l'accomplissement de ses tâches. Les dispositions pénales sur le secret de fonction s'appliquent: les données consultées ne doivent pas être communiquées à d'autres organes publics ou à des personnes privées.

> Toute modification de l'accès devra être annoncée et notre Autorité se réserve le droit de modifier son préavis.

> Les dispositions figurant aux art. 22a et 30a al. 1 let. c LPrD sont réservées.

> Le présent préavis sera publié.

Alice Reichmuth Pfammatter
Préposée cantonale à la protection des données