ETAT DE FRIBOURG
STAAT FREIBURG

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

Rue des Chanoines 2, 1700 Fribourg

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

SITES A CONTRÔLE D'ACCES

Mémorandum pour le contrôle initial

1. Objectif

Le présent Mémorandum 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) et sur la tâche de l'Autorité cantonale de surveillance de donner un *avis préalable* aux projets prévoyant la diffusion sur un site de données personnelles sensibles (art. 8 al. 3 de l'Ordonnance du 3 mai 2005 relative aux sites internet de l'Etat). Le Mémorandum a pour but d'*aider* les organes publics à fournir les informations nécessaires en vue de l'avis préalable requis.

2. Généralités

2.1 Tout organe public qui traite des données personnelles est *responsable* de la protection des données (art. 17 al. 1 Loi du 25 novembre 1994 sur la protection des données, LPrD[1], art. 4 Règlement du 29 juin 1999 sur la sécurité des données personnelles, RSD[2]). Les informations et les documents publiés sur un site à contrôle d'accès peuvent être consultés par un certain nombre de personnes autorisées situées dans ou/et hors du réseau informatique de l'Etat/de l'organe public. L'auteur du site doit en tout temps être conscient que publier des données sur un site à contrôle d'accès équivaut à les rendre accessibles largement et à en *perdre* ainsi une certaine *maîtrise* sans pour autant être délié de sa responsabilité (art. 17 al. 1 LPrD).

2.2. La diffusion de données personnelles sur un site à contrôle d'accès constitue une *procédure d'appel* au sens de l'art. 2 al. 1 let. c RSD. L'accès à ces données ne peut être accordé que si une **disposition légale** le prévoit (art. 10 al. 2 LPrD). L'organe public doit notamment faire une évaluation des risques (art. 8 RSD), définir les autorisations d'accès (art. 10 al. 2 RSD), les authentifications (art. 17 RSD). La procédure d'appel doit être documentée dans un règlement d'utilisation dont une copie est transmise à l'Autorité cantonale de surveillance en matière de protection des données. Pour le contenu, se référer à l'art. 21 al. 3 RSD.

[1] RSF 17.1
[2] RSF 17.15

3. Mesures de sécurité

3.1 En ce qui concerne la *sécurité informatique*, les systèmes utilisés doivent répondre aux exigences standard de la sécurité informatique (art. 14 al. 1 RSD). Aux termes de l'art. 17 al. 1 RSD, l'accès aux systèmes informatiques permettant le traitement de données personnelles doit être protégé par un dispositif comprenant une procédure d'authentification (identification + mot de passe) et un système de contrôle d'accès (autorisations individuelles d'accès). D'autre part, les **directives** du 16 décembre 2002 de la Direction des finances du canton de Fribourg sur les mots de passe dans l'utilisation des PC à l'Etat de Fribourg comportent les règles suivantes :

a) une procédure d'authentification comprenant au moins *l'identification* des utilisateurs et utilisatrices et l'introduction d'un mot de passe de *au moins de 7 caractères*;

b) un *changement* de mot de passe qui doit avoir lieu régulièrement;

c) la *complexité* des mots de passe doit être suffisante;

d) un *nombre minimal* de changement du mot de passe avant la réutilisation;

e) un système de *contrôle* des accès, fondé sur une définition d'autorisation individuelle d'accès.

3.2 D'autres mesures seront ajoutées selon le degré de sensibilité des données personnelles mises à disposition (par ex. cryptage des données personnelles sensibles, art. 20 RSD).

Voici ci-dessous des points exemplaires pour l'élaboration de la demande de préavis adressé l'Autorité cantonale de surveillance (art. 8 al. 3 de l'Ordonnance du 3 mai 2005 relative aux sites internet de l'Etat). Il est possible soit d'introduire les informations directement dans le document dans les cases utiles, soit de les compiler dans un document indépendant. Au besoin, l'Autorité cantonale de surveillance demandera des renseignements complé-mentaires.

4. Informations à fournir pour la demande d'avis préalable à l'Autorité cantonale de surveillance

4.1. Informations sur le site et les données traitées

Nom de l'organe public responsable	
Nom du site	
But du site	
Une telle publication est-elle nécessaire à l'accomplissement des tâches légales ? Quelles en sont	

les raisons (art. 5 et 6 LPrD) ?	
Le site à contrôle d'accès contient-il des données personnelles ? Lesquelles (art. 3 let. a LPrD) ? Le site à contrôle d'accès contient-il des données sensibles ? Lesquelles (art. 3 let. c LPrD) ?	
Les personnes concernées sont-elles informées ? Par quel moyen ? A quel moment ? Le consentement de ces personnes est-il requis (art. 10 LPrD) ? Comment ?	

4.2. Bases légales

Existe-t-il des bases légales autorisant le traitement et la publication de telles données ? Lesquelles (art. 4 LPrD) ? Ces bases légales permettent-elles l'accès à ces données au moyen d'une procédure d'appel en ligne (art. 10 al. 2 LPrD) ?	

4.3. Responsabilité

Nom de la personne en charge du contenu du site Un traitement conjoint de plusieurs organes est-il prévu ? Si oui, la répartition des responsabilités a-t-elle été déterminée par écrit (art. 17 al. 2 LPrD et 6 RSD) ?	

4.4. Autorisation

Les personnes autorisées à accéder aux fichiers sont-	

elles définies ? L'étendue de leurs accès est-elle définie (consulter, copier, introduire, modifier, etc.) (art. 10 RSD)[3] ?	
En cas de traitement de données sensibles, ces données sont-elles publiées sur le site à contrôle d'accès avec l'autorisation du responsable dans chaque cas ? Ces autorisations sont-elles individuelles ? (art. 21 al. 1 RSD)	
Existe-t-il un engagement écrit des personnes autorisées par lequel elles s'engagent à respecter les mesures de sécurité?	

4.5. Sécurité

Des mesures de sécurité ont-elles été prises ? Lesquelles (art. 3 RSD) ? A-t-on effectué une analyse des risques (art. 4 al. 2 RSD) ? Laquelle ? Un règlement d'utilisation a-t-il été prévu (art. 21 al. 3 RSD) ? Existe-t-il des directives écrites à l'attention des personnes autorisées (art. 3 RSD) ? Merci de nous fournir le document Est-il prévu de vérifier régulièrement si les mesures de sécurité sont respectées par les utilisateurs (art. 4 al. 3 RSD) ?	
L'organe public responsable du contenu du site a-t-il pris les mesures d'organisation appropriées contre tout traitement non autorisé des données (art. 22 LPrD) ? A-t-il pris les mesures organisationnelles et techniques nécessaires (art. 11 RSD) ? Est-il prévu de réévaluer ces mesures (art. 12 RSD) ?	

[3] Exemple de grille dans le Guide à l'attention des organes publics – concept – La protection des données personnelles dans mon service, avril 2006, Préposée à la protection des données du canton de Fribourg.

Le service informatique compétent a-t-il pris les mesures techniques appropriées contre tout traitement non autorisé (art. 3 al. 1 RSD) ? Des mesures de cryptage ou de chiffrement sont-elles prévues ?	

4.6. Conservation des données personnelles - surveillance

Quelle est la durée prévue pour le site à contrôle d'accès ?	
Si la durée est indéterminée, a-t-on prévu une réévaluation périodique des risques et des mesures (art. 12 RSD) ?	
La conservation, respectivement la destruction des données personnelles est-elle prévue ? En cas d'archivage informatique, des délais de destruction sont-ils prévus ? Qu'est-ce qui est détruit ? Elimination totale ? Aussi les copies de sauvegarde ? Une reconstitution des données est-elle possible ?	
Des mesures de contrôle, respectivement de surveillance sont-elles prévues ?	

4.7. Organismes privés[4]

Une procédure par outsourcing est-elle prévue (hébergement du site à contrôle d'accès par un organisme privé externe) ? ***Attention**. Si tel est le cas, l'organisme en question est également soumis à la législation sur la protection des*	

[4] www.fr.ch/sprd sous : pour en savoir plus, mandat (outsourcing)

données (art. 2 al. 1 let. b LPrD).	
L'organe public participe-t-il à un site à contrôle d'accès créé par un organisme privé ? ***Attention**. Si tel est le cas, l'organe public est également soumis à la législation sur la protection des données (art. 2 al. 1 let. a LPrD).*	