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

Aide-mémoire N° 4

COMMUNICATION DES DONNEES PAR COURRIER ELECTRONIQUE

Aide-mémoire concernant la communication des données personnelles par courrier électronique

Objectif

Les présentes instructions sont prises sur la base du 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). A considérer comme ligne de conduite, ces instructions ont pour but de guider les services compétents lorsqu'ils communiquent des données personnelles des personnes concernées par courrier électronique. Les autorités communales de protection des données peuvent également s'y référer.

2. Généralités

a) Les données qui ne sont pas des données personnelles ne font pas l'objet de restrictions au sens de la LPrD (art. 1 LPrD a contrario).
b) L'organe public qui traite des données personnelles (toute information qui se rapporte à une personne identifiée ou identifiable) doit prendre des mesures d'organisation et les mesures techniques appropriées contre tout traitement non autorisé des données (art. 22 al. 1 LPrD).
c) L'organe public qui traite des données sensibles (données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, des sanctions pénales ou administratives et les procédures y relatives, art. 3 let.c LPrD), doit prendre toutes les dispositions nécessaires pour prévenir le risque accru d'atteinte qu'implique le traitement de telles données (art. 8 LPrD).

3. La communication des données personnelles

L'accessibilité de données personnelles par transmission électronique doit être protégée contre toute atteinte à leur confidentialité et contre tout traitement non autorisé (art. 3 al. 1 et 17 al. 1 lit. a et b

du règlement sur la sécurité des données personnelles du 29 juin 1999, RSD). Les directives du 27 novembre 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 et la brochure d'avril 2002 du DSB+CPD.CH "Sécurité et outils modernes de communication" 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.

4. La communication des données sensibles
Les données sensibles et les informations confidentielles ne doivent en principe pas être transmises par courrier électronique. Dans le cas où une telle communication doit avoir lieu par cette voie, les moyens suivants doivent être mis en oeuvre pour assurer la confidentialité de la communication:

a) Si la communication n'emprunte que le réseau cantonal (Intranet) :

1. Les documents échangés doivent être chiffrés; le chiffrement (ou cryptage) d'un message le rend illisible à toute personne qui ne dispose pas du code secret (la clé) qui a servi au chiffrement (à défaut de chiffrement, on pourrait admettre la protection attachée au document par mot de passe).

b) Si la communication transite par les réseaux publics (Internet) :

1. Les documents échangés doivent être chiffrés.
2. Il devrait y avoir vérification de l'intégrité du message, autrement dit la garantie doit être donnée que l'information n'a pas été dénaturée, accidentellement ou intentionnellement lors de son cheminement sur le réseau.
3. Enfin, des mécanismes d'authentification devraient garantir que l'expéditeur est bien celui qu'il prétend être.

5. L'accès aux données personnelles et sensibles
L'accès aux données personnelles et sensibles est strictement protégé. Seul/e le ou la titulaire peut donner l'autorisation à un tiers d'avoir accès à la communication transmise. L'accès doit être accordé en précisant au moins les points suivants :

a) le but pour lequel les données sont communiquées,
b) la désignation des données auxquelles se réfère l'autorisation,
c) le bénéficiaire de l'accès et la personne responsable du traitement.

6. Points particuliers
L'utilisation de blinds copies ou copies cachées peut poser un certain nombre de problèmes, notamment ceux concernant la non connaissance par le destinataire du message par courrier électronique, d'autres copies cachées à d'autres éventuelles personnes. Nous conseillons de les éviter dans la mesure du possible.

Pour d'autres informations cf. les instructions no 2 sur le droit d'accès.