ETAT DE FRIBOURG
STAAT FREIBURG

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

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

Rue des Chanoines 2, 1700 Fribourg

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

—

Ref: MS/al 2024-PrD-323
T. direct: +41 26 305 59 73
E-Mail: secretariatatprdm@fr.ch

Freiburg, 3 septembre 2024

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

I. Fondements

Les présentes instructions sont édictées sur la base du pouvoir de conseil de la préposée cantonale à la transparence et à la protection des données (art. 54 al. 1 let. d de la loi du 12 octobre 2023 sur la protection des données ; ci-après : LPrD ; RSF 17.1). À considérer comme lignes de conduite, ces instructions ont pour but de guider les services compétents lorsqu'ils communiquent des données personnelles et sensibles des personnes concernées par courrier électronique. Les autorités communales peuvent également s'y référer.

II. Généralités

Avant de traiter des données personnelles et sensibles, les organes publics doivent tenir en considération ce qui suit :

1. Les données personnelles sont définies comme étant toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 4 al. 1 let. a LPrD).
2. 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*).
3. L'organe public qui traite des données personnelles doit prendre des mesures organisationnelles et des mesures techniques appropriées contre tout traitement non autorisé des données (art. 40 LPrD).
4. L'organe public qui traite des données sensibles au sens de l'article 4 alinéa 1 lettre c LPrD doit prendre toutes les dispositions nécessaires pour prévenir le risque accru d'atteinte qu'implique le traitement de telles données (art. 11 LPrD).

III. La transmission de données personnelles et de données confidentielles

La confidentialité et l'intégrité des données personnelles et sensibles doit être garantie lors de leur transmission électronique (art. 3 al. 1 et 17 al. 1 let. a et b du Règlement du 29 juin 1999 sur la sécurité des données RSD ; RSF 17.15).

IV. La transmission de données personnelles sensibles

Il est essentiel de s'assurer que les informations confidentielles sont correctement protégées.

Le courrier électronique n'est en principe pas considéré comme un moyen de transmission sécurisé.

Les données personnelles sensibles et les informations confidentielles ne devraient donc pas être transmises par courrier électronique. Si ce canal de communication doit malgré tout être utilisé, la confidentialité et l'intégrité des données et des documents transmis doivent être garanties.

Les conditions pour une utilisation du courrier électronique conforme à la protection des données pour les données personnelles sensibles et les documents confidentiels sont les suivantes :

1. Garantie de l'identification des partenaires de communication (émetteur et récepteur)
2. Identité de l'expéditeur (proof of origin)
3. Connexion de transport sécurisée
4. Cryptage du contenu du courriel ainsi que des pièces jointes
5. Garantie de l'intégrité des données et des documents
6. Réglementation claire de l'utilisation et de la configuration des appareils privés (si ceux-ci sont autorisés).

Il existe des possibilités techniques pour la mise en œuvre concrète de ces exigences.[1]

1. Garantie de l'identification des partenaires de communication (émetteur et récepteur)

Les partenaires de communication internes utilisent leur ID personnelle (xxx.xxx@fr.ch) et un mot de passe conforme aux directives relatives aux mots de passe. Pour les partenaires de communication externes, une authentification forte doit être utilisée. Ex : SMS. Cette mesure permet entre autres d'éviter qu'un courriel envoyé par erreur à une fausse adresse ne puisse être ouvert par le/la destinataire.

2. Identité de l'expéditeur ou de l'expéditrice

Se faire passer pour un expéditeur/une expéditrice soi-disant digne de confiance est aujourd'hui un risque majeur (courriels fake). Pour les contenus et les annexes confidentiels et sensibles, il est important de pouvoir identifier clairement l'expéditeur. Cela se fait en général par une signature numérique de l'expéditeur ou de l'expéditrice.

[1] Exemple : https://www.bit.admin.ch/fr/swiss-government-pki-fr ; https://www.bit.admin.ch/fr/sg-pki-swiss-government-pki-trust-service-provider-tsp-fr

3. Connexion de transport sécurisée

La connexion de transport doit être cryptée en tant que cryptage de bout en bout (E2EE) ; c'est-à-dire de client à client.

4. Cryptage du contenu du courriel et des pièces jointes

Les contenus confidentiels doivent être transmis et déposés sous forme cryptée. Le simple cryptage de transport n'est pas suffisant, car les courriels sont sinon stockés en clair chez le destinataire et l'expéditeur.

5. Garantir l'intégrité des données et des documents

Le contenu confidentiel et sensible des données et des documents ne doit pas être modifié. Le ou la destinataire doit pouvoir vérifier qu'il ou elle a bien reçu les données originales.

6. Réglementation claire sur l'utilisation et la configuration des appareils privés (si ceux-ci doivent être autorisés).

La manière dont les courriels professionnels, y compris leurs annexes, peuvent être gérés sur des appareils privés doit être clairement définie. En particulier, la suppression des données et le mélange de données privées et professionnelles comportent des risques élevés pour la protection des données et la sécurité de l'information.

Canaux de transmission alternatifs : des portails peuvent être utilisés comme alternative au courrier électronique pour l'échange de documents et de données confidentiels, à condition qu'ils répondent aux exigences de sécurité.

V. L'accès aux données personnelles et aux données personnelles sensibles (transfert de courrier électronique)

Dans le cadre de l'utilisation du courrier électronique, les utilisateurs et utilisatrices doivent être conscients qu'ils traitent des données confidentielles et sensibles et qu'ils doivent donc faire preuve d'une diligence particulière. Il n'est pas permis de les transmettre à ses propres adresses de courriels privés, ni de les envoyer à des personnes qui ne sont pas autorisées à traiter ces données.