Brochure de formation initiale à la protection des données et à la sécurité des données

–

acf-fgv

association des communes fribourgeoises
freiburger gemeindeverband

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

Sommaire

01 Introduction

Objectifs de la formation

Comprendre les bases de la protection des données et de la sécurité des données.

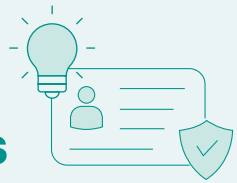
Connaître les responsabilités de chacun en matière de protection des données.

Apprendre les bonnes pratiques à adopter quotidiennement.

Importance de la protection des données

Protéger les données personnelles et assurer la sécurité des données sont essentiels pour maintenir la confiance des administré-e-s et éviter les sanctions légales.

02 Comprendre la protection des données



Définition et principes

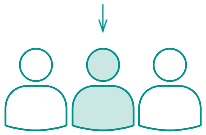
La protection des données vise à garantir que les informations personnelles (données personnelles) sont traitées de manière sûre et respectueuse de la vie privée, en conformité avec la loi.

Obligations légales

Loi du 12 octobre 2023 sur la protection des données

Règlement du 29 juin 1999 sur la sécurité des données personnelles

Droits des personnes concernées (art. 27-35 LPrD)



Droit d'accès :

Définition : Ce droit permet à toute personne de demander et d'obtenir une copie des données personnelles la concernant qui sont traitées par une organisation ou une entité cantonale ou communale.

Objectif : Il vise à permettre aux individus de vérifier si leurs données sont traitées légalement et de comprendre comment et pourquoi ces données sont utilisées.

Droit de rectification :

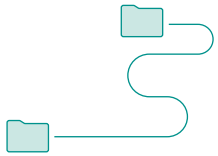
Définition : Ce droit donne à une personne le pouvoir de demander la correction ou suppression de données personnelles inexactes ou incomplètes qui sont détenues par une entité communale ou cantonale.

Objectif : Il vise à garantir que les informations personnelles sont précises et à jour, afin d'éviter toute prise de décision préjudiciable basée sur des données incorrectes.

Droit d'effacement (ou droit à l'oubli) :

Définition : Ce droit permet à une personne de demander la suppression de ses données personnelles, notamment lorsque ces données ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ou traitées.

Objectif : Il vise à permettre aux individus de contrôler la diffusion et l'utilisation de leurs données personnelles, notamment sur Internet.



Droit de portabilité :

Définition : Ce droit donne à une personne le droit de recevoir les données personnelles qu'elle a fournies à une organisation dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à une autre organisation.

Objectif : Il vise à renforcer le contrôle des individus sur leurs données personnelles.

Droit d'opposition (droit de blocage) :

Définition : Ce droit permet à une personne de s'opposer à tout moment au traitement de ses données personnelles pour des raisons liées à sa situation particulière, à moins que l'entité cantonale ou communale ne démontre des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Objectif : Il vise à offrir aux individus un contrôle supplémentaire sur l'utilisation de leurs données personnelles, en particulier lorsque cette utilisation peut avoir un impact sur leurs droits fondamentaux et libertés.

03 Principes de la sécurité des données

Confidentialité

Assurez-vous que les informations ne sont accessibles qu'aux personnes autorisées.

Intégrité

Veillez à ce que les informations soient exactes et complètes.

Disponibilité

Garantissez que les informations soient disponibles lorsqu'elles sont nécessaires.

04 Obligations et responsabilités

Employé-e-s et mandataires externes

Respecter les politiques et procédures de sécurité des données.

Utiliser des mots de passe robustes et sécurisés.

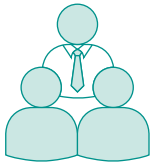
Signaler tout incident ou anomalie (violation de la sécurité des données).

Ne pas divulguer des informations à des personnes ou organisations non autorisées. Vous êtes liés au **secret de fonction** respectivement au **secret professionnel** pour les mandataires externes.

Elu-e-s communaux-ales

Appliquer les mêmes règles de confidentialité que les employé-e-s.

Suivre les dispositions spécifiques de la législation sur les communes.



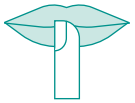
Responsables de la sécurité des données

Assurer la mise en œuvre des politiques de sécurité des données.

Former et sensibiliser les employé-e-s et les élu-e-s.

Répondre aux incidents de sécurité (violation de la sécurité des données).

05 Bonnes pratiques quotidiennes



Gestion des accès

Utilisez des mots de passe complexes.

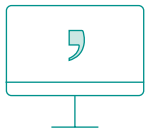
Ne partagez pas vos identifiants.

Utilisez l'authentification multi-facteurs.

Sécurité physique

Verrouillez votre poste de travail en cas d'absence.

Sécurisez les documents sensibles.

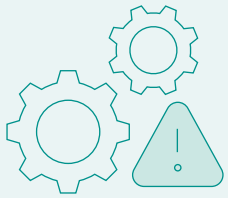


Utilisation des outils de travail

Utilisez uniquement les logiciels et équipements autorisés.

Évitez d'utiliser des dispositifs personnels pour des tâches professionnelles sans autorisation.

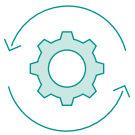
06 Gestion des incidents (violation de la sécurité des données)



Détection d'un incident

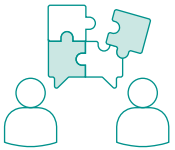
Soyez vigilant aux comportements inhabituels du système et aux emails suspects.

Signalez immédiatement tout incident.



Procédure de signalement

Informez le service informatique ou le responsable de la sécurité, ainsi que cas échéant, la préposée à la transparence et à la protection des données.



Réponse aux incidents

Prenez des mesures immédiates pour limiter les dommages.

Collaborez avec le service informatique pour résoudre le problème.

07 Ressources et contacts

Documents de référence

Loi du 12 octobre 2023 sur la protection des données

Règlement du 29 juin 1999 sur la sécurité des données personnelles

Guides pratiques de l'ATPrdM

Contacts utiles

Service informatique de la commune

Responsable de la protection des données et de la sécurité des données de la commune

8. Conclusion

Nous vous remercions de votre engagement à suivre ces directives et à protéger les données et la sécurité des données. Votre rôle est crucial pour assurer la sécurité et la confidentialité des informations sensibles.

Pour toute question ou demande d'information supplémentaire, n'hésitez pas à contacter le service informatique ou les responsables de la sécurité des données.

Note : Cette brochure fait partie intégrante de votre formation initiale. Veuillez lire attentivement chaque section et suivre les directives énoncées pour garantir la protection des données et la sécurité des données au sein de la commune.

**Autorité cantonale de la transparence,
de la protection des données et de la médiation**

Rue des Chanoines 2, 1700 Fribourg
T +41 26 322 50 08

www.fr.ch/cha/atprdm

Septembre 2024

Brochure élaborée par
Groupe de travail "Terrain" ACF-ATPrDM