CORPS GRAND-DUCAL
INCENDIE & SECOURS

Politique de conservation des données à caractère personnel

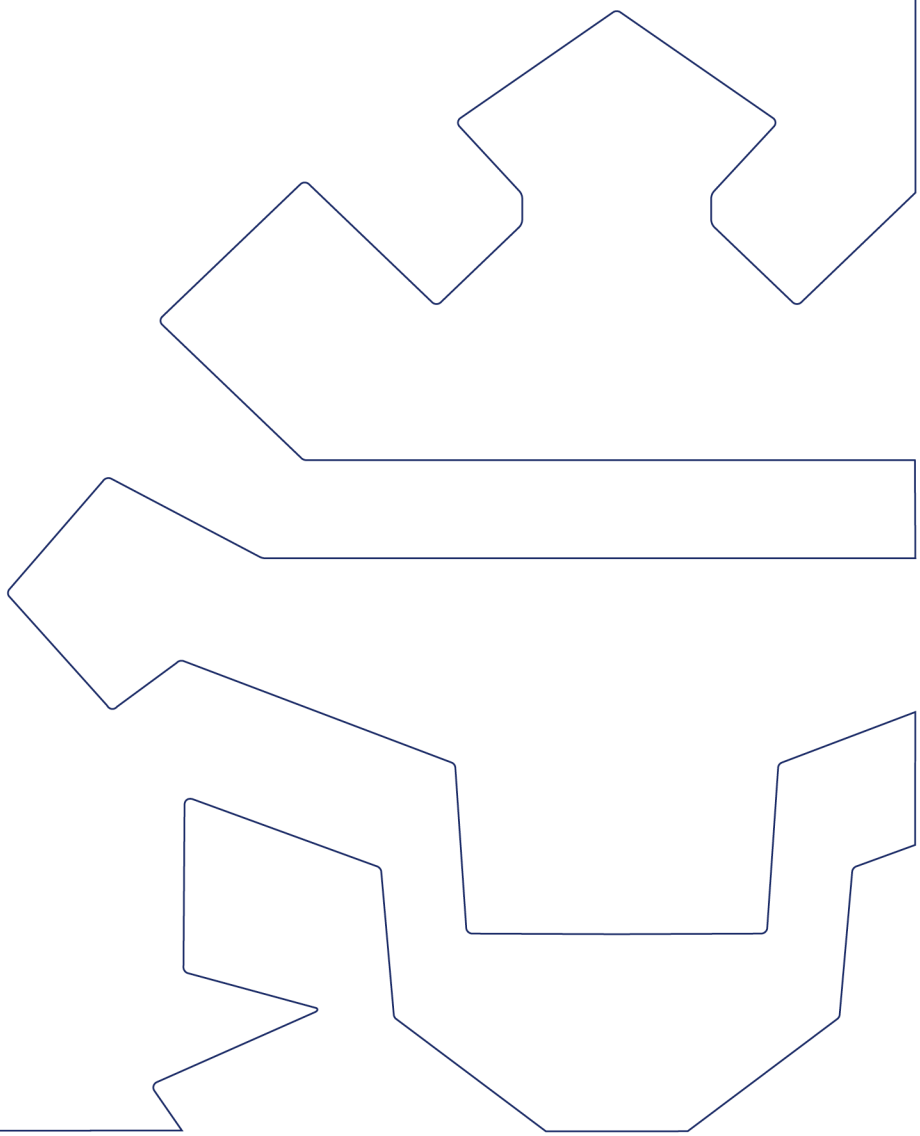

TABLE DES MATIÈRES

1 Objectif

Le Corps grand-ducal d'incendie et de secours (CGDIS) met en place la présente politique de conservation des données à caractère personnel pour garantir la suppression ou l'anonymisation des données à caractère personnel (notamment à des fins statistiques) lorsque la conservation de données à caractère personnel n'est plus justifiée.

La durée de conservation des données est déterminée au regard :

- des contraintes légales et réglementaires ;
- des contraintes contractuelles ;
- ou à défaut en fonction de ses besoins du CGDIS.

2 Champ d'application

La présente politique de gestion des données à caractère personnel s'applique :

- aux pompiers professionnels ;
- aux pompiers volontaires ;
- aux agents administratifs et techniques, quel que soit leur statut ;
- aux consultants et prestataires externes.

3 Registre

Le CGDIS tient un registre des traitements de données à caractère personnel effectués sous sa responsabilité.

Les données à caractère personnel doivent être exactes, et si nécessaire, tenues à jour.

Le CGDIS prend toutes les mesures nécessaires raisonnables afin de garantir que les données à caractère personnel inexactes soient rectifiées ou supprimées sans tarder.

4 Conservation

Conformément à la présente politique, chaque service du CGDIS est responsable des dossiers et documents qu'il crée, utilise, stocke, traite et détruit.

Les délais de conservation applicables à chaque traitement de données à caractère personnel figurent dans le registre des traitements de données à caractère personnel tenu par le CGDIS.

5 Archivage

Toutes les données à caractère personnel archivées par le CGDIS sont soit cryptées, soit verrouillées dans un endroit clos et protégé.

5.1 Documents papier

Les documents papier sont archivées dans un lieu de stockage sécurisé e, clairement étiquetés dans des boîtes d'archives mentionnant de la direction, du département ou du service et la date de destruction.

5.2 Documents électroniques

Les documents électroniques sont archivés conformément aux normes de sécurité de l'information du CGDIS en matière de contrôle d'accès et dans un format approprié pour garantir la confidentialité, l'intégrité et l'accessibilité des documents. Après l'expiration de la période d'archivage, les documents sont détruits conformément au point 4. ci-dessous.

5.3 Externalisation

Si l'archivage est externalisé, le prestataire externe doit d'abord être évalué pour s'assurer qu'il respecte nos normes de protection des données à caractère personnel et de sécurité de l'information.

5.4 Usure des supports

La possibilité que les supports de données utilisés pour l'archivage s'usent doit être prise en compte. Si des supports de données électroniques sont choisis, toutes les procédures et tous les systèmes garantissant que les informations peuvent être consultées pendant la période de conservation (tant en ce qui concerne le support d'information que la lisibilité des formats) doivent également être stockés afin de protéger les informations contre la perte résultant de changements technologiques futurs.

6 Destruction

6.1 Examen régulier

Toutes les données, qu'elles soient conservées sous un format électronique, sur les dispositifs individuels des employés ou en format papier, doivent être réexaminées régulièrement afin de décider s'il y a lieu de les détruire ou de les supprimer conformément à la période de conservation prévue. La responsabilité de la destruction des données incombe à chaque responsable de département ou de service.

6.2 Destruction sécurisée

Les données personnelles ou les informations confidentielles font l'objet d'une suppression électronique sécurisée ou d'une anonymisation.

Les documents sous format papier doivent être déchiquetés à l'aide de shredders sécurisés et verrouillés désignés, d'où les déchets sont périodiquement ramassés par le personnel et soumis à un contrôle de sécurité en vue de leur élimination.

6.3 Perte malveillante ou accidentelle

Une surveillance appropriée est mise en place pour empêcher la perte d'informations importantes à la suite d'une destruction malveillante ou involontaire de données à caractère personnel.