R.G.P.D. CHATAIN & Associés

REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

POLITIQUE INTERNE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

MAJ 2/2022.02

Rgpd Chatain & Associés 20, rue de la République, 69270 Couzon au Mont d'Or
SAS au capital de 15 000 € SIREN 843 404 914 RCS LYON SIRET du siège 843404914 00023

Table des matières

1. Introduction

La protection des données à caractère personnel est à la fois un défi et un enjeu pour l'ensemble des acteurs du monde contemporain. Pour nous, et l'ensemble de nos personnels.

Elle constitue autant un critère d'amélioration des services existants qu'un facteur de confiance en interne que vis-à-vis des tiers.

De ce fait, la mairie s'est engagée dans une voie d'innovation et de modernisation fondée sur le respect de valeurs éthiques fortes : la protection des données à caractère personnel et de la vie privée font désormais également partie de ses priorités.

La présente 'Politique interne de protection des données à caractère personnel' définit les règles de bonne conduite attendues par ses personnels pour assurer la protection des données à caractère personnel que nous gérons.

Cette politique détaille le comportement responsable et éthique que chaque personnel doit observer lors de la collecte et du traitement de données à caractère personnel.

Elle évoluera naturellement en fonction du contexte légal et réglementaire applicable.

2. Définitions

Les concepts majeurs de la protection des données à caractère personnel sont les suivants.

1. Données à caractère personnel

Toute information se rapportant à une personne physique directement ou indirectement identifiable :
- Directement : (exemple : nom et prénom) ;
- Indirectement : un numéro de téléphone ou de plaque d'immatriculation, un identifiant (le numéro de sécurité sociale), une adresse postale ou un courriel, mais aussi la voix ou l'image.

L'identification d'une personne physique peut être réalisée :
- À partir d'une seule donnée (exemple : nom) ;
- À partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).

2. Données à caractère personnel sensibles

Il s'agit des données à caractère personnel faisant apparaître de façon directe ou indirecte les origines raciales, ethniques, les opinions politiques, philosophiques, religieuses, l'appartenance syndicale des personnes ou qui sont relatives à leur santé ou à leur vie sexuelle.

3. Personne concernée :

La personne concernée désigne la personne à laquelle se rapportent les données qui font l'objet d'un traitement.

4. Responsable d'un traitement de données à caractère personnel :

Il s'agit de la personne qui détermine les finalités et les moyens d'un traitement : le Président pour l'association CROS AURA.

5. Sous-traitant :

Toute société traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant.

6. Traitement de données à caractère personnel :

Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toutes autres formes de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

3. Principes

Le Règlement Général sur la Protection des Données décline plusieurs grands principes que chaque personnel se doit d'observer scrupuleusement.

3.1 Légalité

La réalisation de traitement à partir de données collectées de manière illicite est interdite.

Pour chaque nouveau traitement, le personnel doit s'assurer de la base légale de son traitement et de la conformité du traitement en lui-même.

3.2 Loyauté et transparence

Les données à caractère personnel ne doivent pas être collectées et traitées à l'insu des personnes concernées.

Avant la mise en œuvre de tout traitement, le salarié doit vérifier l'adéquation de son traitement et des informations données à la personne concernée.

Il doit également valider l'existence de la prise de connaissance effective par la personne concernée des informations lui permettant d'exercer ses droits le cas échéant.

Il est interdit de se procurer des données à caractère personnel auprès de tiers sans s'être assurer au préalable des droits nécessaires pour collecter et traiter de telles données.

3.3 Finalité et légitimité

Les objectifs des traitements doivent être clairement exprimés, explicites et légitimes.
Les données collectées doivent uniquement être collectées pour répondre exclusivement aux finalités recherchées.

Utiliser une base de données pour des finalités non prévues avec la finalité initiale est interdit.

3.4 Nécessité et proportionnalité

Seules peuvent être collectées les données à caractère personnel strictement nécessaires à la réalisation du traitement.

Il est nécessaire de définir dès la création d'un traitement la durée de conservation des données à caractère personnel pour pouvoir réaliser les finalités à atteindre.

3.5 Qualité

Chaque personnel doit s'assurer que les données à caractère personnel qu'il est amené à traiter dans le cadre de son activité sont exactes et ne sont pas périmées. Au besoin, il est impératif de les mettre à jour.

Les zones de commentaires libres sont à bannir au maximum au profit des choix à cocher.

3.6 Respectez les droits des personnes

Les personnes concernées ont un droit d'accès, de rectification, de mise à jour, d'opposition lorsque que le droit l'autorise, à l'effacement ou droit à l'oubli, à la limitation de traitement, au retrait de leur consentement, à la portabilité de leurs données lorsque les possibilités le permettent.

Respecter les procédures mises en place est une obligation pour chacun des personnels en faisant remonter toute demande au Délégué à la Protection des Données (DPO externe), au Référent RGPD le cas échéant.

3.7 Sécurité et confidentialité

Chaque personnel traitant des données à caractère personnel se doit, à son niveau, de garantir la sécurité, l'intégrité et la confidentialité des informations personnelles qu'il gère.
Le respect de la Politique d'utilisation des systèmes d'information et de communication et la remontée d'information auprès de sa hiérarchie en cas de violation de données ou de découverte de failles de sécurité sont des éléments essentiels de la préservation des droits des personnes.

Chaque personnel doit veiller :

- À garantir la confidentialité des données à caractère personnel qu'il traite.
- À ne pas divulguer d'informations auprès d'autres services de tiers qui ne seraient pas habilités à en prendre connaissance,
- À utilise au quotidien les mesures de sécurité prévues.

La transmissions d'informations à caractère personnel dans le cadre d'un contrat de sous-traitance impose la mise en œuvre d'obligations contractuelles.

3.8 Encadrement des transferts hors Union Européenne

La gestion des flux hors Union Européenne de données à caractère personnel est encadrée. Il est possible d'héberger des données personnelles sur des serveurs situés en dehors de l'Union européenne.

Chaque personnel doit, pour chaque traitement concerné, la maitriser.
Avant de transférer des données à caractère personnel vers un autre pays, il est nécessaire de vérifier auprès du Délégué à la Protection des Données/ du référent RGPD le cas échéant si et dans quelles conditions il y a une possibilité de le faire.

Dans tous les cas se présentant, toutes les mesures nécessaires à la préservation de l'intégrité et de la sécurité des données à caractère personnel doivent être prise pour s'assurer que le destinataire :

- Est situé dans un État considéré comme adéquat par la Cnil ;
- Présentent des garanties suffisantes validées par la Cnil quant à la protection des Données à caractère personnel transmises.

4. Support interne

En cas de difficulté dans la compréhension des présentes règles, le référent Délégué à la Protection des Données (DPO, le référent RGPD le cas échéant) est à la disposition de chaque personnel pour la bonne application de la présente politique.

5. Entrée en vigueur

La présente politique entre en vigueur le 15 septembre 2023.

CROS
Auvergne-Rhône-Alpes
Maison Régionale des Sports
68 Avenue Tony Garnier / CS21001
69304 LYON Cedex 07

Le Responsable de Traitement

LEVARLET Christian, Président du CROS AURA