crosif.fr

Comment se mettre en conformité avec le RGPD ?

COMITÉ NATIONAL OLYMPIQUE ET SPORTIF FRANÇAIS

CROS ÎLE-DE FRANCE

RGPD

=

Règlement général sur la protection des données

crosif.fr

Présentation et définitions

CROS ÎLE-DE FRANCE

Un règlement européen

- Référence : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

- Loi n° 78-17 du 6 janvier 1978 relatif à l'informatique, aux fichiers et aux libertés modifiée.

- Modifie le cadre européen applicable au traitement des données personnelles.

- Entré en application, en droit français, le 25 mai 2018.

L’entrée en application

- La date du 25 mai 2018 n’est pas un couperet.
- Contrôle d’abord la mise en mouvement de l’association plutôt que sa complète conformité.
- Demande d’engager le processus, par la désignation d’un pilote chargé de la mise en œuvre de la réglementation.

Les objectifs

- Renforcer les droits et la protection des données à caractère personnel des personnes physiques ;

- Responsabiliser les acteurs traitant des données ;

- Moderniser le cadre européen de la protection des données afin de prendre en compte les avancées technologiques et d'harmoniser les législations des États membres.

Les grands principes

- Le renforcement des droits des personnes : recueillir le consentement ;

- L'obligation d'information : informer la CNIL et les personnes concernées dans les 72 heures suivant un piratage ;

- Des sanctions lourdes : 20 millions d'euros ou 4% du chiffre d'affaire ;

- Minimisation des données collectées : les renseignements strictement nécessaires ;

- Portabilité des données : droit de recevoir les données nous concernant ;

- Registre des données : tracer l'ensemble des données.

D’un système déclaratif à une démarche responsable

- Auparavant, système déclaratif à la CNIL avec formalités préalables à la mise en œuvre des traitements (loi de 1978 modifiée).

- Désormais, le principe de responsabilité implique que le responsable adopte des mesures techniques et organisationnelles qui garantissent le respect de la réglementation.

- Ces mesures doivent prendre en compte la nature du traitement, le contexte, la portée, les finalités et le devoir d’information aux personnes concernées.

Les cibles du RGPD

- Cibles prioritaires : entreprises qui collectent des données personnelles, parfois très sensibles, à des fins commerciales ;

- **S'applique à TOUTES les associations** (peu importe la taille, la structure ou le domaine d'activité) ;

- Association sportive avec simple liste d'adhérents : PAS dans le collimateur direct de la Commission européenne ;

Mais, le règlement fait office de loi, donc il faut s'y conformer.

Qu’est ce qu’une donnée personnelle ?

- **Définition :** Toute information se rapportant à une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique.

Un simple nom, une adresse postale, un numéro de sécurité sociale, un numéro de téléphone, une taille, une photo jusqu’à des données économiques, sociales, culturelles ou génétiques.

Les données personnelles (1/2)

- Article 5 : Les données doivent être :

- Traitées de manière licite, loyale et transparente au regard de la personne concernée ;

- Collectées pour des finalités déterminées explicites et légitimes (ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités) ;

- Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Les données personnelles (2/2)

- Exactes et, si nécessaire, tenues à jour : toutes les mesures raisonnables doivent être prises pour que les données inexactes soient effacées ou rectifiées ;

- Conservées sous une forme permettant l'identification des personnes concernées ;

- Traitées de façon à garantir une sécurité appropriée des données à caractère personnel.

Le traitement des données (1/2)

- **Définition (Art 4) :** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Le traitement des données (2/2)

- Le RGPD s’applique aux traitements réalisés sur support informatique (logiciels, sites web) mais également sur support papier.

- Collecte, enregistrement, conservation, modification, communication par transmission, etc.

- Désigne également le moyen ou l’outil de traitement (tableau excel, réseau intranet, dispositif de géolocalisation, etc.).

- Le traitement peut être automatisé ou non.

Le responsable de traitement

- Personne physique ou morale qui détermine les finalités et les moyens du traitement.

- Les obligations légales reposent sur ce responsable.

- En général, personne morale incarnée par son représentant légal.

- Sous-traitant : Traite les données personnelles pour le compte du responsable de traitement.

Pourquoi êtes-vous concernés ?

- Vous avez un fichier « membres de l'association » avec stockage de données personnelles (date de naissance, adresse mail, etc.) ;

- Vous avez un fichier de contacts à qui vous envoyez des e-mailings : newsletters, promotions, bons plans, etc. ;

- Vous avez des salariés et vous stockez leurs données personnelles.

Risques encourus en cas de non-respect

- Avertissement à l’encontre du responsable du traitement ;
- Mettre en demeure le responsable du traitement ;
- Limiter ou suspendre un traitement ;
- Ordonner de satisfaire aux demandes d’exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l’effacement des données ;
- Sanctions administratives (amendes jusqu’à 20 Millions d’euros).

Exemples de sanctions

- Google, janvier 2019 : Amende de 50 millions d’euros pour absence de consentement valable pour la personnalisation de la publicité ;
- Active Assurances, juillet 2019 : Amende de 180 000 euros pour avoir insuffisamment protégé les donnés des utilisateurs de son site web.

crosif.fr

Comment se mettre en conformité ?

CROS ÎLE-DE FRANCE

Désigner un délégué à la protection des données (DPO) (1/2)

- Pas obligatoire mais recommandé : pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.

- Chef d'orchestre de l'identification et de la coordination des actions à mener en matière de protection des données.

- Le délégué n'est PAS personnellement responsable : en cas de non-conformité de son organisme avec le règlement.

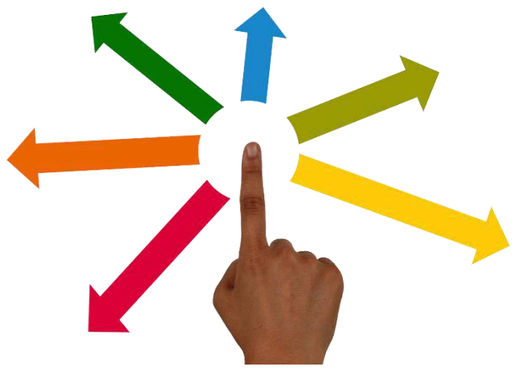
Désigner un délégué à la protection des données (DPO) (2/2)

- Désigné sur la base de ses qualités professionnelles (pas de profil type) : communiquer efficacement, expertise en matière de législations, bonne connaissance du secteur d'activité et de l'organisme et positionnement efficace en interne.

- Protéger le DPO dans l'exercice de ses missions : indépendance, positionnement hiérarchiques et pas de sanctions possibles si elles sont imposées en raison de l'exercice par le délégué de sa fonction.

- Les moyens d'action : s'assurer de son implication, lui fournir les ressources nécessaires, lui permettre d'agir de manière indépendante, lui faciliter l'accès aux données et veiller à l'absence de conflits d'intérêts.

Ses missions



- Informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;

- Contrôler le respect du règlement et du droit national en matière de protection des données ;

- Conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution ;

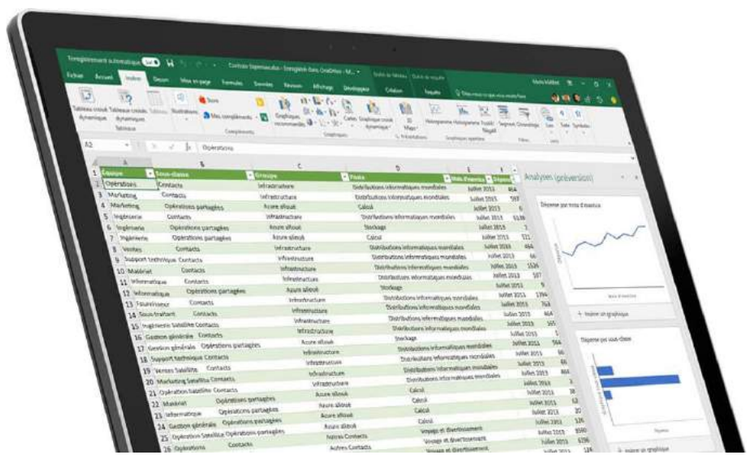
- Coopérer avec l'autorité de contrôle (CNIL) et être le point de contact de celle-ci.

Cartographier vos traitements de données personnelles (1/2)

- <u>Tenir une documentation interne complète</u> : sur les traitements de données personnelles ;

- <u>Recenser</u> : les différents traitements, les catégories, les objectifs, les acteurs (internes ou externes) et les flux de données (origine et destination) ;

- <u>Pour chaque donnée</u> Se poser les questions suivantes : Qui ? Quoi? Pourquoi ? Où ? Jusqu'à quand ? Comment ?



Cartographier vos traitements de données personnelles (2/2)

- Participe à la documentation de la conformité.

- Permet d’identifier :

- les parties prenantes ;
- les catégories de données traitées ;
- à quoi servent les données ?
- qui accède aux données ?
- à qui sont elles communiquées ?
- les durées de conservation ;
- comment sont-elles sécurisées ?

Le registre des données personnelles (1/4)

- Modèle sur le site de la CNIL
- Mentionner :

1) <u>Noms et coordonnées du responsable du traitement</u>

La personne physique ou morale qui détermine les finalités et les moyens du traitement.

2) <u>Les différents traitements de données personnelles</u>

Exemple : collecte des informations et stockage sur un tableur, etc.

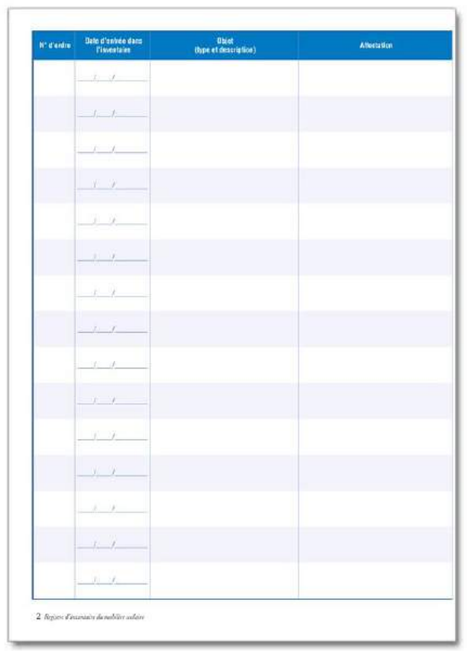
Le registre des données personnelles (2/4)

3) <u>Les catégories de données personnelles traitées</u>

Données d'identification, informations d'ordre économique et financière, données de connexion, etc.

4) <u>Les différentes catégories de personnes concernées</u>

Adhérents, bénévoles, salariés, etc.



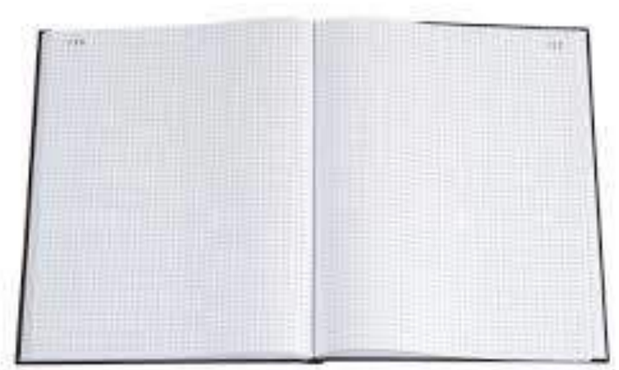
Le registre des données personnelles (3/4)

5) <u>Les objectifs poursuivis par les opérations de traitement des données</u>

Suivi du paiement de la cotisation annuelle, envoi d'informations relatives à la vie de l'association, remboursement des frais de transports pour les réunions organisées par l'association, etc.

6) <u>Les acteurs (internes ou externes) qui traitent ces données</u>

Identification des sous-traitants éventuels.



Le registre des données personnelles (4/4)

7) Les durées de conservation

8) La description générale des mesures de sécurité techniques et organisationnelles pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées.

Les traitements licites (1/2)

- Le traitement est licite **SI** une de ces conditions est remplie :

1) La personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques ;

2) Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie prenante ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

3) Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

Les traitements licites (2/2)

4) Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

5) Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

6) Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Les traitements

- Seules les informations adéquates, pertinentes et nécessaires à la finalité peuvent faire l’objet d’un traitement.

- Établir une durée de conservation en fonction de la finalité de chaque fichier.

- N’autoriser la consultation des données que par les personnes habilités à y accéder en raison de leurs missions.

- Toujours être en mesure de démontrer que la personne a donné son consentement (dans le cas où son recueil était nécessaire).

Prioriser vos actions

- Assurez-vous que seules les données strictement nécessaires, à la poursuite de vos objectifs, sont collectées et traitées ;

- Identifiez la base juridique de votre traitement (consentement, intérêt légitime, contrat, obligation légale) ;

- Révisez vos mentions d'information ;

- Vérifiez que vos sous-traitants éventuels connaissent leurs nouvelles obligations ;

- Prévoyez les modalités d'exercice des droits des personnes concernées ;

- Vérifiez les mesures de sécurité mises en place.

Effectuer une analyse d'impact relative à la protection des données (AIPD)

- Description du traitement étudié et de ses finalités ;

- Évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

- Évaluation des risques pour les droits et libertés des personnes concernées et évaluation des mesures envisagées pour faire face à ces risques.

- Modèles disponibles sur le site de la CNIL

Organiser les processus internes

- Prendre en compte la protection des données personnelles dès la conception d’une application ou d’un traitement : minimalisation de la collecte de données, cookies, durée de conservation, mentions d’information, recueil du consentement, sécurité et confidentialité des données.

- Sensibiliser et organiser la remontée d’informations (plan de formation et communication).

- Traiter les réclamations et les demandes des personnes concernées quand à l’exercice de leurs droits (acteurs et modalités).

- Anticiper les violations de données (notifier à l’autorité dans les 72 heures).

Documenter la conformité

- Documentation de vos traitements de données personnelles (registre des traitements, les AIPD et l'encadrement des transferts) ;

- Information des personnes (mentions d'information, recueil du consentement et procédures mises en places pour l'exercice des droits) ;

- Les contrats qui définissent les rôles et les responsabilités des acteurs (les contrats avec les sous-traitants, les procédures internes en cas de violation des données et les preuves que les personnes concernées ont donné leur consentement).

crosif.fr

Le respect des droits des personnes

CROS ÎLE-DE FRANCE

L’information et la transparence

- Connaitre la raison de la collecte des différentes données nous concernant ;

- Comprendre le traitement qui sera fait de nos données ;

- Assurer la maitrise de nos données, en facilitant l’exercice de nos droits.

Dans quels cas devez-vous informer ?

- **<u>En cas de collecte directe des données</u>** auprès des personnes (ex : formulaires, achat en ligne, souscription d'un contrat) ou via des dispositifs d'observation de l'activité des personnes (ex : vidéosurveillance, analyse de la navigation Internet, géolocalisation, etc.) ;

- **<u>En cas de collecte indirecte des données</u>** personnelles (ex : auprès de partenaires commerciaux, de sources accessibles au public ou d'autres personnes).

A quels moments ?

- **<u>Dans le cadre de la collecte</u> :** Au moment du recueil (ou dès que possible dans le délai d'un mois) ;

- **<u>En cas de modification substantielle ou d'événement particulier</u>** : nouvelle finalité, nouveaux destinataires, changement dans les modalités d'exercice des droits, violation de données…

- Une information régulière participe de l'objectif de transparence !

Quelles informations ?

- Identité et coordonnées de l’organisme (responsable du traitement)
- Finalités
- Base légale

- Caractère obligatoire ou facultatif du recueil des données
- Destinataires ou catégories de destinataires des données
- Durée de conservation des données
- Droits des personnes concernées
- Coordonnées du DPO
- Droit d’introduire une réclamation auprès de la CNIL

La forme de l’information

- Veiller à ce que l’information soit compréhensible : vocabulaire simple et adapté au public visé ;

- Délivrer une information concise : court et lisible ;

- Garantir l’accessibilité de l’information : permettre aux personnes de voir immédiatement comment accéder à l’information.

Le droit à l’information

L’association doit informer ses adhérents sur la/les finalités du traitement et les droits dont elle dispose.

Le droit d’accès

- Droit d’obtenir la confirmation que les données à caractère personnel ne sont pas traitées

OU

- Droit d’obtenir l’accès aux données personnelles qui sont traitées et à certaines informations (les finalités du traitement, les catégories de données et les destinataires des données).

Le droit de rectification

- Droit d’obtenir, dans les meilleures délais, que les données inexactes soient rectifiées ;

- Droit d’obtenir que les données incomplètes soient complétées.

Le droit d’opposition, de communication

- Toute personne peut s’opposer, pour un motif légitime, à ce que des données la concernant soient traitées, sauf si le traitement concerné présente un caractère obligatoire ;
- Droit d’obtenir du responsable du traitement une copie des donnés leur appartenant.

Le droit à l'effacement, droit à l'oubli

- Droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant.

Durée de conservation des données

- Déterminer la durée de conservation en fonction de l'objectif ayant conduit à la collecte de ces données ;

- Droit commun : **3 ans** pour les données personnelles des personnes inactives ;

- **1 mois** : vidéosurveillance ;

- **5 ans** : données relatives à un salarié ;

- **10 ans** : dossier médical à compte de la consolidation du dommage ;

- Ces durées doivent être limitées et définies en fonction de la finalité de leur traitement.

Délais de réponse

- Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises dans un délai d'un mois à compter de la réception de la demande.

- Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes.

- Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

- Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies en retour par voie électronique lorsque cela est possible.

Mentions à faire apparaitre dans un formulaire de collecte de données

Les informations recueillies dans le questionnaire sont enregistrées dans un fichier informatisé par **[coordonnées du responsable de traitement]**. La base légale du traitement est **[base légale du traitement]**.

Les données marquées par un astérisque dans le questionnaire doivent obligatoirement être fournies. Dans le cas contraire, **[préciser les conséquences éventuelles en cas de non-fourniture des données].**

Les données collectées seront communiquées aux seuls destinataires suivants : **[destinataires des données].**
Elles sont conservées pendant **[durée de conservation des données prévue par le responsable du traitement ou critères permettant de la déterminer]**.

Vous pouvez accéder aux données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données. **(en fonction de la base légale du traitement, mentionner également : Vous pouvez retirer à tout moment votre consentement au traitement de vos données ; Vous pouvez également vous opposer au traitement de vos données ; Vous pouvez également exercer votre droit à la portabilité de vos données)**

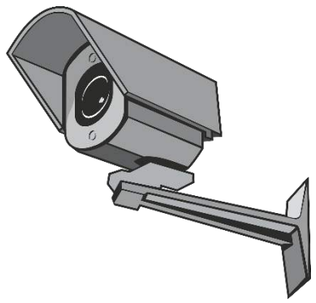
Consultez le site cnil.fr pour plus d'informations sur vos droits.

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter **(le cas échéant, notre délégué à la protection des données ou le service chargé de l'exercice de ces droits) : [adresse électronique, postale, coordonnées téléphoniques, etc.]**

Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

Dispositif de vidéosurveillance

- Deux niveaux d'information : Panneau d'affichage à l'entrée des locaux et règlement intérieur de l'association.



- **Panneau d'affichage :**

Etablissement placé sous vidéosurveillance par X pour la sécurité des personnes et des biens.
Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de X et par les forces de l'ordre.
Pour exercer vos droits Informatique et Libertés, notamment votre droit d'accès aux images qui vous concernent, ou pour toute information sur ce dispositif, vous pouvez contacter notre délégué à la protection des données (DPO) (ou, si vous n'avez pas désigné de DPO, une personne identifiée par sa fonction) en écrivant à dpo@X.fr ou à l'adresse postale suivante : XXXX.

- **Règlement intérieur :**

- ***Objet du traitement (finalité et base légale) :*** *sécurité des personnes et des biens*
- ***Données et catégories de personnes concernées :*** *employés et visiteurs occasionnels*
- ***Destinataires :*** *personnel habilité + forces de l'ordre*
- ***Durée de conservation :*** *1 mois ou plus en cas d'incident*
- ***Droits des personnes :*** *droit d'accès, d'effacement, d'opposition, limitation du traitement, etc*

Politique de confidentialité et de protection des données

- Article 13 du règlement ;

- Insérer un lien en bas de page d’accueil du site de la structure à côté de la page contact ;

- Doit être accessible en « 2 clics » sur votre site Internet.

Les cookies

- Fichier texte généré par le serveur du site lorsque vous le visitez (ou par application tierce) : permet un historique et une personnalisation de la navigation ;

- Tolérance de la CNIL jusqu'à l'été 2020 sur les cookies et les traceurs ;

- Jusqu'à cette date : Poursuite de la navigation vaut expression du consentement au dépôt de cookies.

Nous contacter

Emile BENIZEAU
Chargé de mission Juridique et Sport Santé
Coordinateur territorial Île-de-France CNOSF

Mail : emile.benizeau@crosif.fr

Téléphone : 01 49 85 84 99

COMITÉ NATIONAL OLYMPIQUE ET SPORTIF FRANÇAIS

CROS ÎLE-DE FRANCE

Comité Régional Olympique et Sportif Île-de-France
1, rue des Carrières - 94250 Gentilly
01 49 85 84 90 | crosif@crosif.fr | www.crosif.fr