

Process interne

Gestion des demandes et incidents relatifs aux données personnelles

Le : ...

1. Objet

Cette procédure décrit la manière dont la CPTS [Nom] gère :

- Les demandes d'exercice de droits des personnes concernées (articles 12 à 22 du RGPD),
- Les incidents ou violations de données personnelles (articles 33 et 34 du RGPD).

Elle vise à garantir une réaction rapide, documentée et conforme aux obligations légales, ainsi qu'une traçabilité complète des actions menées.

2. Champ d'application

Cette procédure s'applique à l'ensemble des traitements de données personnelles réalisés par la CPTS, qu'ils soient numériques (logiciels, formulaires, fichiers, plateformes), ou papiers (documents d'adhésion, feuilles de présence, questionnaires).

Elle concerne tous les adhérents, salariés, coordinateurs et sous-traitants ayant accès à des données personnelles dans le cadre de leurs missions.

3. Responsabilités et acteurs

Tous les utilisateurs sont responsables de signaler sans délai tout incident ou demande.

Acteur	Rôle et responsabilités
Pilote RGPD / DPO	Réception, analyse et suivi des demandes et incidents. Centralise les registres (droits / violations).
Coordinateur ou salarié de la CPTS	Informe immédiatement le pilote RGPD de toute demande ou incident observé.
Présidence	Valide les notifications externes (CNIL, personnes concernées).
Sous-traitants	Informent la CPTS sans délai en cas d'incident concernant des données traitées pour son compte.

4. Gestion des demandes d'exercice de droits

4.1 Réception de la demande

Les demandes peuvent être adressées à la CPTS par [\[Mail\]](#) ou par courrier CPTS [\[Nom\]](#) – [\[Adresse postale complète\]](#).

Elles doivent préciser l'identité du demandeur, la nature du droit exercé et, si possible, le traitement concerné.

4.2 Vérification de l'identité

Le responsable de traitement peut demander un justificatif d'identité en cas de doute raisonnable sur l'identité.

Le délai de réponse est suspendu jusqu'à réception des éléments permettant cette vérification.

4.3 Analyse et réponse

Le pilote RGPD analyse la demande et coordonne la réponse. - Délai de réponse : 1 mois, prolongeable de 2 mois en cas de complexité. - Si la demande est refusée (infondée, excessive ou répétitive), la décision est motivée. Le refus est accompagné de l'information sur le droit d'introduire une réclamation auprès de la CNIL.

4.4 Enregistrement et archivage

Chaque demande est consignée dans le registre des droits.

Les échanges sont conservés 5 ans à des fins de preuve de conformité.

5. Gestion des violations de données personnelles

5.1 Signalement immédiat

Tout membre ou sous-traitant qui constate une perte, un vol, une divulgation ou une erreur d'envoi impliquant des données personnelles doit le signaler immédiatement au pilote RGPD.

5.2 Qualification de l'incident

Le pilote RGPD évalue la gravité selon les critères suivants :

- Nature de la violation (confidentialité, intégrité, disponibilité),
- Volume et type de données concernées,
- Nombre de personnes impactées,
- Conséquences potentielles (préjudice matériel ou moral).

5.3 Déclaration des incidents

Cas n°1 : absence de risque

Si la violation ne présente aucun risque pour les droits et libertés des personnes : la CNIL n'est pas notifiée ; les personnes concernées ne sont pas informées ; l'incident est néanmoins documenté dans le registre des violations.

Cas n°2 : risque pour les droits et libertés

Si la violation présente un risque pour les droits et libertés des personnes : la CNIL est notifiée dans un délai de 72 heures après en avoir pris connaissance ; la notification est réalisée via le téléservice officiel de la CNIL ; l'incident est documenté dans le registre des violations.

L'information des personnes concernées n'est pas obligatoire à ce stade, sauf si des mesures techniques rendent les données incompréhensibles (ex : chiffrement).

Cas n°3 : risque élevé pour les droits et libertés

Si la violation est susceptible d'engendrer un risque élevé pour les personnes concernées : la CNIL est notifiée dans les 72 heures ; les personnes concernées sont informées dans les meilleurs délais, de manière claire et compréhensible ; des mesures correctives immédiates sont mises en œuvre pour limiter les conséquences.

5.4 Mesures correctives

Quelle que soit la situation, la CPTS met en œuvre des mesures adaptées :

- Sécurisation ou suppression des accès concernés,
- Modification des mots de passe,
- Récupération ou neutralisation des données exposées,
- Sensibilisation des personnes impliquées,
- Ajustement des procédures si nécessaire.

5.5 Traçabilité et cloture

Toute violation, qu'elle donne lieu ou non à notification, est consignée dans le registre des violations de données personnelles, avec : la description de l'incident, l'analyse du risque, les décisions prises, les mesures correctives mises en œuvre.

Les dossiers sont conservés 5 ans à des fins de preuve de conformité.

6. Documentation et suivi

Le pilote RGPD veille à leur mise à jour régulière et à leur archivage sécurisé,

Les registres (droits et violations) sont accessibles uniquement aux personnes habilitées,

Un bilan annuel RGPD est présenté au bureau de la CPTS pour le suivi global de conformité.