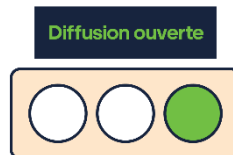


— Politique de protection des données personnelles — SMSI ISO 27001

Classification : données neutres

Diffusion : ouverte



Cycle de vie du document

Version	Date	Auteurs	Objet de la révision	Validation
V1.0	06/05/2025	Aurélie Araujo Stéphane Locatelli	Rédaction initiale	Frank Gaudet

Diffusion

- Collaborateurs, adhérents et clients, partenaires

1. Introduction

11. Objet du document

La politique de protection des données personnelles vise à assurer la conformité aux exigences légales, statutaires, réglementaires et contractuelles relatives aux aspects de la sécurité de l'information portant sur la protection des données à caractère personnel.

12. Documents de référence

La politique de protection des données personnelles fait notamment appel aux références suivantes :

- ISO 27002:2022 §5.34 : Protection de la vie privée et des données à caractère personnel

13. Définitions

« **Données à caractère personnel** » (ci-après « DCP ») : toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement.

« **Données à caractère personnel sensibles** » : les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

« **Traitement de données à caractère personnel** » : 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.

« **Responsable de traitement** » : organisation qui détermine les finalités et les moyens du traitement des données à caractère personnel.

« **Sous-traitant** » : personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

« **Finalité** » : la finalité du traitement est l'objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

« **Bases légales** » : la base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement. Six bases légales sont prévues par le RGPD : le consentement, le contrat, l'obligation légale, la sauvegarde des intérêts vitaux, l'intérêt public et les intérêts légitimes.

« **Consentement** » : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

« **Violation de données à caractère personnel** » : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

2. Finalités des traitements

CDER, ou toute autre entité du Groupe CDER, utilise les données à caractère personnel afin :

- de délivrer et facturer les produits et services commandés (expertise comptable, paie RH, droit et fiscalité, conseil aux chefs d'entreprise),
- d'assurer la gestion de la relation contractuelle avec ses clients et adhérents ou clients (adhésion, enquête de satisfaction, forums expertise et emploi, ateliers du conseil, assemblée générale, etc.),
- d'assurer les obligations contractuelles avec ses collaborateurs (paie, formation, recrutement, etc.),
- d'assurer les actions de communication internes et externes.

CDER assure le traitement des données à caractère personnel uniquement aux fins mentionnées ci-dessus.

3. Données collectées et durées de conservation

31. Adhérents et clients

CDER, ou toute autre entité du Groupe CDER, en tant que responsable de traitement ou sous-traitant, peut collecter des données à caractère personnel lorsque un adhérent ou client souscrit à l'offre de services dans le cadre d'un abonnement ou d'une prestation ponctuelle.

L'information sur la nature des données collectées et leurs durées de conservation sont précisées dans :

- L'article 10 des Conditions Générales de Vente de la Demande de prestation ponctuelle
- L'article 6 des conditions générales annexées à la Lettre de mission ou de son avenant
- La charte de confidentialité annexée aux [Conditions Générales d'Utilisation du portail MyCDER](#)

32. Collaborateurs

CDER, ou toute autre entité du Groupe CDER, en tant que responsable de traitement peut collecter des données à caractère personnel dans le cadre de la gestion de son personnel.

L'information sur la nature des données collectées et leurs durées de conservation sont précisées dans le contrat de travail ou son avenant.

33. Autres personnes

CDER, ou toute autre entité du Groupe CDER, en tant que responsable de traitement peut collecter des données à caractère personnel lorsqu'une personne :

- s'inscrit à la newsletter,
- postule ou candidate sur le portail emploi,
- remplit le formulaire de contact disponible sur le site,
- participe à des événements dans lesquels le Groupe CDER est présent,
- échange avec les équipes commerciales.

Les données à caractère personnel peuvent être également collectées indirectement lors de l'utilisation de cookies et d'autres technologies. Il est collecté des informations telles que le nombre de visiteurs, ainsi que la date de la dernière visite de l'utilisateur et la page consultée.

L'information sur la nature des données collectées et leurs durées de conservation sont précisées dans la [Charte de confidentialité du site web CDER](#).

4. Sécurité des données personnelles

Dans le cadre de son système de gestion de la sécurité de l'information certifié ISO 27001, CDER met en œuvre des mesures de sécurité techniques et organisationnelles appropriées ainsi que des actions nécessaires afin de protéger les données à caractère personnel collectées.

Les données à caractère personnel sont traitées de façon à ce que leur disponibilité, leur intégrité et leur confidentialité soient assurées au regard de leur niveau de sensibilité par la mise en œuvre de mesures administratives, techniques et physiques pour prévenir la perte, la destruction, le vol, l'utilisation, la divulgation ou la modification non-autorisées.

CDER s'assure que les outils qui permettent le traitement des données à caractère personnel garantissent un niveau de protection optimal desdites données.

La Politique de Sécurité de l'Information du Groupe CDER est disponible sur simple demande à l'adresse suivante : rgpd@cder.fr

Les données personnelles traitées peuvent être communiquées aux personnes suivantes :

- à une société du Groupe CDER ;
- aux membres du personnel de CDER habilités à traiter cette information ;
- à l'un des sous-traitants de CDER pour la fourniture du service concerné ;

- à l'un des partenaires de CDER pour établir une communication ou effectuer une transaction que la personne concernée a demandé ou autorisé ;
- à des prestataires de services externes qui ont été spécifiquement autorisés à traiter les données personnelles ;
- aux autorités judiciaires, dans les cas où la loi l'impose ou l'autorise.

5. Droits des personnes concernées

Les personnes concernées par le traitement disposent des droits suivants :

- le droit d'être informé concernant le traitement des données à caractère personnel.
- le droit d'accéder aux données à caractère personnel traitées par le Groupe CDER
- le droit de demander la rectification et la correction des données à caractère personnel.
- le droit à l'oubli qui permet d'exiger la suppression des données à caractère personnel par le Groupe CDER.
- le droit à la limitation du traitement qui permet de contrôler la façon dont les données à caractère personnel sont traitées.
- le droit d'opposition au traitement des données à caractère personnel.
- le droit de retirer son consentement lorsque le traitement se fait sur la base du consentement.
- le droit de définir le sort des données après le décès de l'utilisateur.
- le droit à la portabilité.
- le droit à l'image.

CDER a nommé un délégué à la protection des données personnelles que vous pouvez contacter en lui adressant un message à l'adresse suivante : rgpd@cder.fr

Pour exercer ses droits, la personne concernée doit contacter le service de protection des données personnelles de CDER à l'aide de l'adresse ci-dessus. Elle dispose également du droit de déposer une réclamation auprès de la Cnil.

6. Procédure en cas de violation de données à caractère personnel

Si la violation n'entraîne pas de risque pour les droits et libertés des personnes concernées, CDER en tant que responsable du traitement ou sous-traitant :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- ne doit pas notifier cette violation ni à la CNIL, qui peut en revanche contrôler cette documentation interne, ni aux personnes concernées.

Si la violation entraîne un risque pour les droits et libertés des personnes concernées, CDER en tant que responsable du traitement ou sous-traitant :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h.

Si la violation entraîne un risque élevé pour les droits et libertés des personnes concernées, CDER en tant que responsable du traitement ou sous-traitant :

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL, au plus tôt et dans un délai maximal de 72h ;
- doit communiquer la violation aux personnes concernées, au plus tôt.