POLITIQUE GENERALE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Direction des affaires juridiques, de la conformité et de la déontologie
Janvier 2026

Caisse des Dépôts
GROUPE

Introduction

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, entré en application le 25 mai 2018, relatif à la protection des personnes physiques à l'égard des données personnelles et à la libre circulation de ces données (ci-après « RGPD ») indique dans son préambule que la protection des personnes physiques à l'égard du traitement de données personnelles (ci-après « données personnelles ») est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 1, paragraphe 1, du Traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données personnelles la concernant.

Placée sous le sceau de la Foi publique, la Caisse des Dépôts (ci-après « la CDC ») s'appuie sur une politique de responsabilité sociale exigeante placée au cœur de ses priorités stratégiques, et sur un code de déontologie engageant les collaborateurs de la CDC, quel que soit leur statut, au respect des principes et des règles de bonne conduite. Parmi ces principes, la CDC a fait de la protection et de la sécurité des données personnelles qu'elle est amenée à collecter et à traiter une de ses priorités.

Dans le cadre de ses activités, la CDC est amenée à collecter et à traiter des données personnelles relatives notamment à ses clients, ses collaborateurs, ses partenaires, ses fournisseurs, ses prestataires, les usagers de ses services, les allocataires ou bénéficiaires des prestations dont elle a la charge et leurs éventuels ayants droits. Soucieuse de préserver des relations de confiance avec eux, elle met en œuvre un dispositif de protection des données personnelles en conformité avec les dispositions européennes, et nationales en vigueur, ainsi qu'avec les délibérations, recommandations, lignes directrices et avis des autorités de protection des données - la Commission Nationale Informatique et Libertés (CNIL) en France et le Comité européen de protection des données (CEPD) à l'échelle européenne.

La présente politique s'applique aux traitements de données personnelles opérés par la CDC. Elle permet aux personnes physiques dont elle collecte et/ou traite des données personnelles dans le cadre de ses activités, de comprendre l'utilisation que la CDC fait de ces données, et les droits de ces personnes sur ces données.

01 Définitions

Pour une bonne compréhension des grands principes et droits déclinés dans cette politique, il convient au préalable de présenter la définition de ses principaux termes clés.

- **Donnée personnelle :** Toute information relative à une personne physique pouvant être identifiée directement ou indirectement.
  Exemples : Nom et prénom, numéro de téléphone, photographie, enregistrement vidéo, empreintes biométriques, numéro de sécurité sociale, adresse postale, adresse électronique, âge, données de localisation, adresse IP de l'ordinateur d'une personne physique.

  L'identification d'une personne physique peut être réalisée à partir d'une seule donnée (exemple : numéro de sécurité sociale) ou peut résulter du croisement d'un ensemble de données (exemple : une femme habitant 5, place de la Liberté à Paris, née en 1980 et exerçant le métier d'avocate).

- **Données personnelles « sensibles » :** Catégorie particulière de données dont le traitement peut engendrer un risque important pour les droits et libertés des personnes concernées.

  La CDC a une interprétation extensive des données personnelles sensibles. Elle inclut en plus des « catégories particulières de données personnelles » identifiées par le RGPD (origine raciale, opinions politiques, appartenance syndicale, données de santé, etc.), les données relatives aux condamnations pénales et aux infractions, le numéro d'inscription au répertoire national d'identification des personnes physiques (« NIR » ou « numéro de sécurité sociale ») ou encore les données « hautement personnelles » telles que les coordonnées bancaires ou les données de localisation.

- **Personne concernée :** Personne physique à laquelle se rapportent les données personnelles faisant l'objet d'un traitement.
  Exemples : Usager dont la CDC gère le compte personnel de formation ; pensionné, allocataire, bénéficiaire ou ayant droit à qui la CDC verse sa retraite ; candidat à un emploi dont la CDC étudie la candidature ; collaborateurs de la CDC dont les données personnelles sont traitées pour l'édition des badges d'accès.

  Certaines personnes concernées par un traitement sont considérées comme « vulnérables » en raison d'un déséquilibre de pouvoir avec le responsable du traitement. Cela inclut notamment les enfants mineurs, les collaborateurs d'une entreprise, les personnes sous protection juridique.

- **Responsable du traitement de données personnelles :** Personne, entité, service ou autre organisme qui détermine les finalités et les moyens d'un traitement de données personnelles.

  Exemple : La CDC est responsable de traitement pour le recrutement de son personnel, la mise en place de son dispositif de vidéosurveillance, la gestion des fonds en déshérence, la gestion des retraites.

- **Sous-traitant :** Toute personne, entité ou service traitant des données personnelles pour le compte du responsable du traitement.

  Exemple : un prestataire d'hébergement de données.

- **Traitement de données personnelles :** Toute opération ou tout ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication, diffusion, verrouillage, effacement, destruction).

  Exemple : Le traitement « Gérer les consignations et dépôts spécialisés » est un traitement de données personnelles opéré par la CDC dans le cadre de ses activités.

- **Destinataire :** Personne physique ou morale, autorité publique, service (interne) ou tout autre organisme qui reçoit communication de données personnelles.

  Exemples : Les organismes de formation sont destinataires des données des titulaires de compte personnel de formation ; la CDC est destinataire des données des comptes bancaires inactifs.

  Certaines autorités publiques sont susceptibles de recevoir communication de données personnelles dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit français. Ces autorités sont appelées « *tiers autorisés* », et ne sont pas des destinataires au sens du RGPD.

02

La gouvernance des données personnelles

Soucieuse de préserver la vie privée et la protection des données personnelles toute personne concernée dont elle traite les données, la CDC a développé une gouvernance des données personnelles permettant de prendre en compte les exigences légales et réglementaires relatives à l'utilisation et à la protection de ces données.

▪ Acteurs, rôles et responsabilités

La CDC en tant que responsable de traitement est représentée par son Directeur Général. Elle s'est dotée d'un Comité de pilotage RGPD, présidé par le Directeur des Affaires Juridiques, de la Conformité et de la Déontologie, membre du comité exécutif.

Chacun des Directeurs de la CDC est responsable de la conformité des traitements dont sa direction assure la mise en œuvre. Afin d'assurer une déclinaison opérationnelle effective de la présente Politique dans tous les métiers et directions, les Directeurs sont assistés par des correspondants métiers « Données personnelles », qui assurent le relai avec la déléguée de la protection des données de la CDC.

La CDC a désigné une déléguée à la protection des données (DPO), qui a notamment pour mission de veiller au respect de la règlementation en matière de protection des données, ainsi que d'en assurer le contrôle. La DPO est le point de contact de la CNIL avec qui elle doit coopérer sur les questions relatives aux traitements de données personnelles. Elle est également le point de contact des personnes concernées pour toute question ou demande en lien avec le traitement et la protection des données personnelles.

La DPO de la CDC peut être contactée par toute personne intéressée à l'adresse postale suivante : Caisse des dépôts et consignations - Déléguée à la protection des données (DPO) - 56 rue de Lille - 75007 Paris ; ou à l'adresse mél ci-après : dpo@caissedesdepots.fr.

▪ Un dispositif de contrôle interne

L'application de la réglementation en matière de protection des données personnelles est soumise à différents niveaux de contrôle :

- Les directions opérationnelles sont responsables du contrôle de premier niveau. Pour ce faire, elles s'appuient notamment sur les correspondants métiers « Données personnelles ».
- Le contrôle permanent au sein de la Direction des Risques déploie des contrôles de 2ème niveau sur le dispositif RGPD selon une approche par les risques.

- La DPO assure, conformément à l'article 39 du RGPD, sa mission de contrôle de l'ensemble de la règlementation relative à la protection des données personnelles, ainsi que des règles internes en matière de données personnelles.
- Au titre du contrôle périodique, l'Inspection Générale - Direction de l'Audit du Groupe réalise des audits sur le dispositif RGPD.

- **Des procédures garantes de la protection des données**

La CDC a mis en place des procédures afin de s'assurer de la bonne prise en compte, par tous ses services et collaborateurs, de l'ensemble de ses obligations en matière de protection des données personnelles.

Elle a notamment mis en place un dispositif de protection des données dès la conception et par défaut, qui assure que pour tout projet de conception, de sélection et d'utilisation d'applications, de services et de produits qui reposent sur le traitement de données personnelles, l'ensemble des principes de protection des données personnelles sont bien pris en compte avant la mise en œuvre opérationnelle du traitement. A cette occasion, la CDC s'assure, entre autres, que les éditeurs/fournisseurs de produits et solutions informatiques ou digitales répondent aux prescriptions légales et garantissent la protection des données qui y seront traitées. Des comités d'engagement permettent de vérifier le suivi du dispositif par les équipes projets.

03 La mise en conformité des traitements à la CDC

La CDC s'attache au respect des principes prévus à l'article 5 du Règlement (UE) 2016/648 dans le cadre de la collecte et l'utilisation des données personnelles.

3.1 Une finalité déterminée, explicite et légitime

Lorsque la CDC met en œuvre un traitement de données personnelles, elle définit de manière précise un objectif, qui correspond à la finalité du traitement. Cette finalité doit être explicite - c'est-à-dire compréhensible par tout le monde - et légitime - c'est-à-dire au service des missions de la direction de la CDC qui met en œuvre le traitement.

Les données collectées ne peuvent pas être utilisées ultérieurement de manière incompatible avec la finalité définie. Dès lors, si la CDC prévoit d'effectuer un traitement ultérieur des données personnelles pour une finalité autre que celle pour laquelle elles ont été collectées, elle s'assurera de la compatibilité de cette nouvelle finalité avec les finalités initiales du traitement. La CDC fournira au préalable à la personne concernée les informations au sujet de ce nouveau traitement.

3.2 La licéité du traitement

Pour être licite, un traitement de données personnelles doit reposer sur une base légale qui autorise sa mise en œuvre. Sans base légale valide, un traitement de données personnelles est jugé illicite.

Six bases légales sont définies par l'article 6 du RGPD pour encadrer les traitements des données personnelles. Les traitements mis en œuvre par la CDC reposent sur cinq de ces bases légales (décrites ci-après). La sixième base légale, relative à la sauvegarde des intérêts vitaux d'une personne physique, ne s'applique à aucun traitement de données mis en œuvre par la CDC à ce jour.

- **Les missions d'intérêt public ou l'autorité publique dont est investie le responsable de traitement**

Les traitements de données personnelles effectuées par la CDC peuvent être nécessaires à l'exécution d'une mission d'intérêt public dont est investie la CDC. Cette mission d'intérêt

public est définie par le droit français ou européen.

L'article L.518-2 du code monétaire et financier (CMF) prévoit en effet que la CDC et ses filiales sont « *au service de l'intérêt général* » et que le groupe « *remplit des missions d'intérêt général en appui des politiques publiques conduites par l'Etat et les collectivités territoriales* ». Ces missions d'intérêt général peuvent s'analyser comme des missions d'intérêt public au regard des critères retenus par la jurisprudence et la doctrine des autorités de protection.

Exemples : le traitement « Gérer les consignations et les dépôts spécialisés » fondé sur une mission d'intérêt public au titre de l'art. L518-2 du CMF ; le traitement « Gérer les retraites » fondé sur une mission d'intérêt public au titre de l'art. L518-2 du CMF ; le traitement « Mettre à disposition un portail d'information et d'orientation sur le Handicap » fondé sur une mission d'intérêt public au titre de l'art. 42 de la loi n°2021-502.

Lorsque des traitements de données personnelles sont réalisés par la CDC sur le fondement de cette base légale, la CDC s'assure que ces traitements de données soient strictement nécessaires à l'exécution de la mission d'intérêt public dont elle est investie, et spécifiquement liés à celle-ci.

- **Des obligations légales ou réglementaires**

Certains traitements de données personnelles effectués par la CDC peuvent être nécessaires pour le respect des obligations légales ou réglementaires s'imposant à la CDC dans le cadre de certains champs de son activité.

Exemple : les obligations légales ou réglementaires relatives aux traitements de lutte anti-blanchiment ou contre le financement du terrorisme en tant qu'organisme assujetti, ou celles relatives aux déclarations aux organismes sociaux par la CDC en sa qualité d'employeur.

- **Les intérêts légitimes de la CDC**

Les intérêts légitimes de la CDC ou d'un tiers peuvent parfois être de nature à justifier un traitement de données personnelles par la CDC.

Exemple : piloter la sécurité des systèmes informatique de la CDC dans le but de détecter et prévenir les incidents de sécurité, mesurer la qualité des services rendus, améliorer le service rendu.

Dans ce cas de figure, ces traitements sont mis en œuvre par la CDC en prenant en compte les intérêts et les droits fondamentaux des clients, collaborateurs, partenaires, fournisseurs et prestataires ou toute autre personne concernée par le traitement. A ce titre, ils s'accompagnent de mesures et garanties pour assurer la protection des intérêts et droits de la personne concernée permettant un équilibre avec les intérêts légitimes poursuivis par la CDC.

- **L'exécution du contrat ou des mesures précontractuelles avec la personne concernée**

Certains traitements de données personnelles effectués par la CDC peuvent parfois être fondés, lorsque cela est adéquat au regard du contexte, sur l'exécution du contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Dans ces cas de figure, le traitement est licite s'il est strictement nécessaire à l'exécution d'un contrat liant la CDC avec la personne concernée, ou à l'exécution de mesures précontractuelles à sa demande, le cas échéant.

Exemple : un contrat de travail entre la CDC et un collaborateur.

- **Le consentement de la personne concernée**

Certains traitements de données personnelles effectués par la CDC peuvent être fondés, de manière marginale, sur le consentement de la personne concernée. Dans le cas où un traitement de données personnelles requiert le consentement de la personne concernée comme base de licéité du traitement, le consentement de la personne, pour une ou plusieurs finalités spécifiques, doit répondre à des conditions particulières pour être valable, conformément à l'article 7 ; et le cas échéant, à l'article 8 du RGPD.

Pour ces traitements, la CDC s'assure notamment que le consentement est libre, éclairé, non équivoque et donné par un acte positif clair, par exemple au moyen d'une déclaration écrite, y compris par voie électronique. De même, la CDC s'assure que le consentement de la personne peut être retiré à tout moment.

3.3 La minimisation des données collectées

Les données personnelles collectées par la CDC doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité poursuivie par le traitement.

A ce titre, lorsque la CDC a défini la finalité d'un traitement à mettre en œuvre, elle identifie et évalue les données personnelles qui vont lui permettre d'atteindre cette finalité. Elle exclut alors toute donnée non essentielle ou superflue. Lorsque c'est possible elle recourt notamment à la pseudonymisation (suppression des données directement identifiantes) ou bien encore à l'anonymisation des données (suppression de toute donnée directement ou indirectement identifiante).

En minimisant la collecte de données personnelles, la CDC limite la quantité de données personnelles stockées sur son système d'information. Cette mesure permet ainsi de réduire les impacts pour les personnes concernées en cas de violation de données personnelles.

3.4 La limitation de la durée de conservation des données

La CDC conserve les données personnelles qu'elle collecte uniquement pendant la durée nécessaire au regard des finalités du traitement considéré, et en accord avec la législation nationale applicable notamment concernant les durées de prescription légale ou réglementaire.

La CDC étant un organisme public, elle est soumise aux dispositions du code du patrimoine concernant les archives publiques. Elle peut ainsi avoir à conserver de manière illimitée des données personnelles pour des finalités archivistiques dans l'intérêt public. L'archivage intermédiaire ou définitif des données se fait, le cas échéant, en accord avec les règles définies

par le département interne des archives de la CDC, qui est l'autorité d'archivage en la matière, et dans le respect de la doctrine des autorités de protection, notamment le guide sur les durées de conservation de la CNIL rédigé en partenariat avec le Service interministériel des archives de France (SIAF).

3.5 La collecte loyale et transparente

Dans un souci de loyauté et de transparence, la CDC prend soin d'informer les personnes concernées de chaque traitement qu'elle met en œuvre par des mentions d'information. Ces mentions peuvent être affichées ou indiquées sur différents supports : site internet, formulaire de collecte, notices d'information, etc.

Les informations contenues dans les mentions sont les suivantes :

- L'identité et les coordonnées de la CDC, le cas échéant du ou des responsable(s) conjoint(s) ;
- Les coordonnées de la déléguée à la protection des données de la CDC ;
- Les finalités du traitement ;
- La base légale du traitement ;
- Le cas échéant, les intérêts légitimes poursuivis par la CDC ou par un tiers ;
- En cas de collecte indirecte des données, les catégories de données personnelles concernées et la source de ces données.
- Le caractère obligatoire ou facultatif du recueil des données, ainsi que les conséquences éventuelles de la non-fourniture de des données ;
- Les destinataires ou catégories de destinataires auxquels les données personnelles sont communiquées ;
- Le cas échéant, les transferts de données existants ou envisagés hors Union européenne ;
- La durée de conservation des données personnelles ou lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- Les droits dont disposent les personnes concernées au titre de la règlementation ;
- Le cas échéant, l'existence d'une prise de décision automatisée, y compris un profilage, et toute information utile concernant la logique sous-jacente, l'importance et les conséquences prévues de ce traitement pour la personne concernée ;
- Le cas échéant, si un traitement ultérieur des données personnelles pour une finalité autre que celle pour laquelle elles ont été collectées est prévu.

La CDC n'a pas l'obligation d'informer les personnes concernées si celles-ci disposent déjà des informations ou que la communication de ces informations se révèle impossible ou exigerait des efforts disproportionnés

3.6 La sécurité des données

La CDC met en place des mesures techniques et organisationnelles adaptées aux risques que fait porter chaque traitement sur les personnes concernées et leurs données, en prenant notamment en compte la sensibilité des données et le contexte dans lequel elles sont traitées.

Ces mesures doivent permettre de garantir une sécurité appropriée des données personnelles et plus précisément :

- Leur confidentialité (protection contre tout accès illégitime aux données ou divulgation non autorisé) ;
- Leur intégrité (protection contre toute altération intentionnelle ou accidentelle rendant les données incomplètes ou inexactes) ;
- Leur disponibilité (protection contre toute destruction ou perte, intentionnelle ou accidentelle des données).

Ces mesures de sécurité sont notamment :

- Une authentification forte systématiquement privilégiée ;
- Un contrôle d'accès physique pour sécuriser les locaux ;
- La gestion des droits d'accès avec des profils différenciés en fonction des besoins et des missions des utilisateurs ;
- Des mécanismes de sauvegarde pour assurer la résilience des données.

La CDC effectue également régulièrement des contrôles internes afin de vérifier la bonne application opérationnelle des règles relatives à la sécurité des données.
Elle peut être amenée à effectuer des audits permettant de vérifier la bonne application des règles de sécurité par ses sous-traitants, conformément aux obligations définies dans leurs contrats les liant à la CDC.

La sécurité des données personnelles repose également sur le respect par les collaborateurs de la CDC de la Charte d'utilisation des ressources informatiques de la CDC. Tout collaborateur de la CDC, quel que soit son statut, doit prendre connaissance et signer cette charte avant de commencer à travailler pour la CDC et s'engage à la respecter tout au long de sa collaboration avec la CDC. De même, les collaborateurs de la CDC sont régulièrement formés à la sécurité des données et des systèmes d'information de la CDC, dans le cadre de formations obligatoires. Le respect de ces règles est également susceptible d'être vérifié dans le cadre du contrôle interne appliqué par la CDC.

En outre, la CDC a édicté des Règles de Sécurité des Systèmes d'Information pour les Prestataires de Services (RSSIPS), qui sont opposables par contrat à tout prestataire utilisant les systèmes d'information de la CDC.

3.7 L'encadrement de la sous-traitance

Des prestataires de services de la CDC, d'autres entités du groupe CDC ou tout autre tiers sont parfois amenés à traiter les données personnelles pour le compte de la CDC.

Lorsque la CDC choisit ses sous-traitants, elle leur impose :

- Un niveau de protection des données personnelles équivalent à celui qu'elle accorde elle-même aux données ;
- Une utilisation des données personnelles uniquement pour assurer la gestion des services qu'ils doivent fournir ;
- Un respect strict de la législation et de la règlementation applicable en matière de confidentialité, de secret bancaire, de secret des affaires et de protection des données personnelles ;
- La mise en œuvre de toutes les mesures adéquates pour assurer la protection des données personnelles qu'ils peuvent être amenés à traiter ;
- La définition des mesures techniques, organisationnelles nécessaires pour assurer la sécurité de ces données.

La CDC s'engage à conclure avec ses sous-traitants des contrats définissant précisément les conditions et modalités de traitement des données personnelles effectués pour son compte, conformément à l'article 28 du RGPD.

3.8 L'encadrement des transferts de données en dehors de l'Espace Economique Européen (EEE)

Les données personnelles traitées par la CDC dans le cadre de son activité peuvent faire l'objet d'un transfert vers une entité située en dehors de l'Espace Economique Européen (c'est-à-dire, en dehors de l'Union Européenne, de la Norvège, du Lichtenstein et de l'Islande).

Lorsque les données personnelles sont transférées hors de l'EEE, ces données personnelles peuvent être soumises à des législations ou réglementations dont le niveau de protection vis-à-vis des données personnelles varie, et n'est pas toujours reconnu comme équivalent à celui offert par le droit de l'Union européenne.

Dans le cadre d'un tel transfert vers un pays hors de l'EEE, des mesures assurant la protection et la sécurité des données transférées sont mises en place par la CDC, afin que ces transferts soient licites au regard des exigences du RGPD et de la doctrine des autorités de protection en la matière.

Pour sécuriser ces transferts hors de l'EEE, la CDC peut, par exemple, avoir recours aux clauses contractuelles types (CCT) publiées par la Commission européenne. Ces CCT sont alors annexées aux contrats conclus entre la CDC et les importateurs de données personnelles.

Si le contexte du transfert l'exige (en particulier la législation du pays importateur ne présente pas des garanties suffisantes en matière de protection des données personnelles), ces CCT sont complétées par des mesures supplémentaires d'ordre juridique, organisationnel et/ou technique afin d'assurer un niveau de protection adéquat aux données, conformément au droit de l'Union européenne.

Les personnes concernées sont informées des transferts de leurs données effectués par la CDC, le cas échéant, conformément à leur droit à l'information visé aux articles 13 et 14 du RGPD.

04 La gestion des droits des personnes

La CDC a mis en place un dispositif permettant de garantir l'exercice des droits dont bénéficient les personnes concernées. Toutefois, les droits ne sont pas toujours exerçables par la personne concernée car ils dépendent de la base légale du traitement.

4.1 Identification et applicabilité des droits

Les personnes concernées disposent des droits suivants :

- **Droit d'accès :** Toute personne concernée peut interroger la CDC pour savoir si celle-ci traite des données la concernant. Le cas échéant, elle peut demander communication de toutes ses données et obtenir toutes les informations sur les caractéristiques du traitement (finalités, base légale, destinataires, etc.).

- **Droit de rectification :** Toute personne concernée demander la rectification de ses données personnelles qui sont inexactes ou incomplètes.

- **Droit à l'effacement :** Toute personne peut faire effacer les données la concernant notamment lorsque 1) les données ne sont plus nécessaires au regard de la finalité du traitement, 2) elle retire son consentement, 3) elle exerce son droit d'opposition, 4) le traitement s'avère être illicite, 5) une obligation légale impose l'effacement, ou bien 6) le traitement concerne les mineurs dans le cadre de l'offre de services de la société de l'information, notamment les réseaux sociaux.

- **Droit à la limitation du traitement :** Toute personne peut demander la suspension du traitement de ses données lorsqu'elle 1) conteste l'exactitude des données et que la CDC doit procéder aux vérifications 2) s'oppose à l'effacement des données d'un traitement qui s'est avéré illicite, 3) a besoin des données pour la constatation, l'exercice ou la défense de ses droits, ou bien, 4) s'est opposée au traitement et que les motifs de l'opposition sont en cours de vérification. Lorsque le droit à la limitation est mis en œuvre, les données ne peuvent plus être utilisées, modifiées ou supprimées. Seule la conservation est permise.

- **Droit à la portabilité des données :** Toute personne a le droit de recevoir une copie de ses données sous un format structuré, courant, lisible par machine pour transmission à un

autre responsable de traitement ou bien d'obtenir du responsable de traitement la transmission directe de ses données à un autre responsable de traitement.

- **Droit d'opposition :** Toute personne a le droit de s'opposer à tout moment au traitement des données personnelles la concernant.

- **Droit de refuser une décision fondée exclusivement sur un traitement automatisé :** Toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui a un effet juridique ou qui l'affecte sensiblement. La personne qui a fait l'objet d'une telle décision peut la contester, demander à connaitre la logique et les critères employés pour prendre la décision et demander qu'une personne humaine intervienne pour réexaminer la décision.

- **Droit de décider du sort de ses données après sa mort :** Toute personne concernée peut définir des directives (générales ou particulières) relatives à la conservation, à l'effacement et à la communication de ses données à personnelles après son décès.

Le tableau ci-dessous présente les droits applicables selon la base légale du traitement (cf. *3.2 La licéité du traitement*) :

Droits	Consentement	Contrat	Intérêt légitime	Obligation légale	Mission d'intérêt public
Accès	OUI	OUI	OUI	OUI	OUI
Rectification	OUI	OUI	OUI	OUI	OUI
Effacement	OUI	OUI	OUI	NON	OUI
Limitation du traitement	OUI	OUI	OUI	OUI	OUI
Portabilité	OUI	OUI	NON	NON	NON
Opposition	*Retrait du consentement*	NON	OUI	NON	OUI
Décider du sort de ses données après sa mort	OUI	OUI	OUI	OUI	OUI
Refuser une décision exclusivement automatisée	Cas particulier : l'applicabilité de ce droit dépend de l'existence d'une prise de décision automatisée et non de la base légale du traitement				

4.2 Les modalités d'exercice des droits

Les personnes concernées peuvent exercer leurs droits :

- par courrier postal à : Caisse des Dépôts et Consignations – Données Personnelles - Établissement de Bordeaux – 6, place des Citernes – 33059 BORDEAUX CEDEX ;
- par e-mail à mesdonneespersonnelles@caissedesdepots.fr ;
- par un formulaire en ligne disponible à l'adresse : https://www.caissedesdepots.fr/demande-d-exercice-de-droits

Pour faciliter la gestion de la demande, la personne concernée est invitée à indiquer toute information permettant de justifier son identité et sa demande (a minima nom, prénom, le cas échéant n° client et service(s) ou traitement(s) concerné(s)). En cas de doute raisonnable sur son identité, la CDC pourra demander des informations ou des documents complémentaires (exemple : pièce d'identité).

La personne concernée pourra obtenir une réponse à sa demande dans les meilleurs délais, et au plus tard, dans le délai d'un mois à compter de la réception de la demande qualifiée de recevable. Ce délai peut être prorogé de deux mois, en cas de complexité de la demande et du nombre de demandes simultanées, auquel cas la personne concernée est informée de cette prolongation et des motifs du report.

Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives notamment en raison de leur caractère répétitif, la CDC pourra :

- exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour faire droit à ses demandes.
- refuser de donner suite à ses demandes.

La personne concernée a le droit d'introduire une réclamation auprès d'une autorité de protection des données au sein de l'Etat membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation de données aurait été commise. En France l'autorité de protection des données compétente est la Commission Nationale Informatique et Libertés (CNIL).

05 La gestion des violations de données personnelles

Une violation de données personnelles se définit comme : « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données » (art.4 §12 du RGPD).

Conformément à l'article 33 du RGPD, la CDC en tant que responsable de traitement a l'obligation de documenter toute violation de données personnelles dont elle aurait connaissance. Elle doit aussi notifier à la CNIL dans les meilleurs délais et au plus tard dans les 72h après en avoir pris connaissance, toute violation de données susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Lorsque ce risque est élevé, la CDC doit par ailleurs en informer les personnes concernées.

A cet effet, la CDC a mis en place une procédure interne permettant de respecter ses obligations en la matière, notamment en termes de délais.
Elle tient également un registre permettant de consigner toute violation de données personnelles avec mention des faits, des effets de la violation et des mesures prises pour y remédier. Elle tient ce registre à disposition de la CNIL en cas de contrôle.