Politique générale de protection des données personnelles

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 à caractère personnel 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 à caractère personnel 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 à caractère personnel 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 coeur 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. Dans cette lignée, la CDC a fait de la protection et de la sécurité des données à caractère personnel 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 à caractère personnel 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 poursuivre avec eux des relations de confiance, elle met en oeuvre un dispositif de protection des données à caractère personnel en conforme avec les dispositions législatives et réglementaires nationales et européennes 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.

Table des matières

1 - 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.

1.1 Données à caractère personnel

Les données à caractère personnel (ou données personnelles) recouvrent toute information relative à une personne physique pouvant être identifiée directement ou indirectement.
À titre d'exemple, constituent des données personnelles : le nom et prénom, le numéro de téléphone, la photographie, l'enregistrement vidéo, les empreintes biométriques, le numéro de sécurité sociale, l'adresse postale, l'adresse électronique, l'âge, les données de localisation, l'adresse IP de l'ordinateur d'un individu.
L'identification d'une personne physique peut être réalisée à partir d'une seule donnée (exemple : numéro de sécurité sociale). Cette identification peut aussi résulter du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, ayant tel numéro de téléphone, etc…).

1.2 Données à caractère personnel « sensibles »

Parmi les données personnelles figurent des catégories particulières de données, communément appelées données « sensibles ». Il s'agit des données faisant apparaître de façon directe ou indirecte les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes, ou qui sont relatives à leur santé ou à leur vie sexuelle ou orientation sexuelle, ainsi que les données génétiques et biométriques.
En principe, les traitements sur ces données sont interdits, sauf dans les cas strictement énumérés à l'article 9 du RGPD tels que, par exemple : A côté de ces catégories particulières de données régies par l'article 9 du RGPD, d'autres données qualifiées de « hautement personnelles » en raison de leur impact potentiel sur un individu, telles que les données relatives aux condamnations pénales ou aux mesures de sûreté, le numéro de sécurité sociale (NIR) ou les coordonnées bancaires, font également l'objet de précautions particulières lors d'un traitement.

- la personne concernée a donné son consentement explicite au traitement pour une ou des finalités spécifiques,
- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale,
- le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée,
- le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle,
- le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale.

1.3 Personne concernée

La personne concernée est la personne physique à laquelle se rapportent les données personnelles faisant l'objet d'un traitement.
Certaines personnes concernées par un traitement sont qualifiées de personnes « vulnérables » en raison du déséquilibre des pouvoirs accrus qu'il peut exister entre ces personnes et le responsable du traitement. Il s'agit notamment des enfants mineurs, des collaborateurs d'une entreprise, des personnes placées sous un régime de protection juridique. Des mesures particulières permettent d'encadrer la mise en oeuvre des traitements dès lors que les personnes concernées sont vulnérables. A titre d'exemple : l'usager dont la CDC gère le compte personnel de formation, le pensionné, allocataire, bénéficiaire ou éventuel ayant droit à qui la CDC verse sa retraite, le candidat dont la CDC étudie la candidature à l'occasion d'un recrutement, les collaborateurs de la CDC dont les données personnelles sont traitées pour l'édition des badges d'accès.

1.4 Responsable d'un traitement de données à caractère personnel

Le responsable du traitement est la personne, l'entité, le service ou autre organisme qui détermine les finalités et les moyens d'un traitement de données personnelles. A titre d'exemple : La CDC est responsable de traitement pour le recrutement de son personnel, la mise en place de son dispositif de vidéosurveillance.

1.5 Sous-traitant

De façon générale, un sous-traitant est toute personne, entité ou service traitant des données à caractère personnel pour le compte du responsable du traitement. A titre d'exemple : un expert-comptable qui assure la gestion comptable pour le compte de ses clients, un prestataire d'hébergement de données, un prestataire de maintenance d'une application.

1.6 Traitement de données à caractère personnel

Constitue un 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 toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données personnelles.
Un traitement de données personnelles est automatisé ou non. La présente politique s'applique aux traitements opérés via des fichiers papiers. À titre d'exemple : « Gérer les consignations et dépôts spécialisés » est un Traitement de données à caractère personnel opéré par la CDC dans le cadre de ses activités, et identifié par la finalité poursuivie.

1.7 Destinataire

Le destinataire est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. À titre d'exemple : une société mère, une administration, un service peuvent être destinataires de données.

2 - La gouvernance des données personnelles

Soucieuse de préserver la vie privée et la protection des données personnelles de ses clients, collaborateurs, partenaires, fournisseurs, prestataires, usagers, allocataires ou bénéficiaires dont elle traite des données, ou de toute autre 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.

Ainsi, la CDC a mis en place une organisation interne destinée à gérer les différentes problématiques posées par la protection des données personnelles. La CDC a ainsi mis en place des procédures internes permettant la bonne application des exigences du RGPD, telles qu'en matière de gestion et notification des violations de données, ou de gestion des demandes d'exercice des droits des personnes concernées.

La CDC a également mis en place une comitologie et un réseau de relais internes gages de respect des grands principes de protection des données.

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 du Groupe. Chacun des Directeurs de la CDC est responsable de la conformité des traitements dont sa direction assure la mise en oeuvre. 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 » (RDCP), qui assurent le relai avec la DPO CDC.

La CDC a désigné une déléguée à la protection des données (DPO). La DPO de la CDC a notamment pour mission, en collaboration avec les départements juridiques de la Direction des Affaires Juridiques, de la Conformité et de la Déontologie (DAJCD), 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 : à l'attention de la Déléguée à la protection des données (DPO) - 56 rue de Lille - 75007 Paris, ou à l'adresse mél ci-après : dpo @ caissedesdepots.fr

3 - Les grands principes applicables aux données personnelles

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 utilisation légitime et proportionnée

Les données personnelles collectées par la CDC le sont uniquement pour des finalités déterminées, explicites et légitimes liées à son activité.

La collecte de données personnelles au sein de la CDC est destinée à l'exercice de ses activités dans le cadre de ses relations avec ses clients, ses collaborateurs, ex-collaborateurs, candidats, partenaires, fournisseurs et prestataires, usagers de ses services, allocataires ou bénéficiaires des prestations dont elle a la charge et leurs éventuels ayants droits.

Ces données ne sont pas utilisées ultérieurement de manière incompatible avec ces finalités.

3.2 Une collecte loyale et transparente

Dans un souci de loyauté et de transparence vis-à-vis de ses clients, ses collaborateurs, ses partenaires, ses fournisseurs et ses prestataires, ou de toute autre personne concernée dont elle traite les données, la CDC prend soin d'informer les personnes concernées de chaque traitement qu'elle met en oeuvre 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 données personnelles sont collectées loyalement par la CDC. Aucune collecte n'est effectuée à l'insu des personnes concernées et sans qu'elles n'en soient dument informées.

3.3 L'adéquation et la minimisation des données collectées

Les données personnelles collectées sont strictement nécessaires à l'objectif poursuivi par la collecte des données. La CDC s'attache à minimiser les données collectées, à les tenir exactes et à jour.

La CDC ne collecte et ne traite que les données à caractère personnel dont elle a besoin pour assurer la finalité du traitement.

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 à caractère personnelle 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 L'intégrité et la confidentialité des données

Les données personnelles sont traitées par la CDC de façon à garantir une sécurité appropriée de ces données, y compris la protection contre le traitement non autorisé de ces données par des tiers, la perte, la destruction, l'altération de ces données ou tout incident qui rendrait ces données indisponibles, susceptible de causer un préjudice pour les personnes concernées.

Les mesures prises visent notamment à conserver ces données intègres et à apporter une confidentialité à ces données appropriée au regard de leur nature et de leur sensibilité, afin de limiter tout accès par des tiers non autorisés à ces données.

3.6 Une protection des données personnelles dès la conception et par défaut

La CDC met en œuvre des mesures ayant vocation à respecter les principes de protection des données personnelles dès la conception et les principes de protection des données personnelles par défaut.

Ainsi, lors de l'élaboration de projets comme de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données personnelles, la CDC prend en compte l'ensemble des principes et droits à la protection des données personnelles. Elle s'assure notamment que les éditeurs/fournisseurs de produits et solutions informatiques ou digitales répondent aux prescriptions légales et permettent d'assurer la protection des données qui y seront traitées.

À titre d'exemple : la CDC a mis en place un dispositif de protection dès la conception qui assure une mise en oeuvre des principes du RGPD en amont de chacun de ses projets, et dont l'application est vérifiée lors de chaque comité d'engagement concerné.

4 - Les fondements juridiques des traitements mis en œuvre par la CDC

Tout traitement mis en oeuvre par la CDC repose sur une base juridique.Ainsi, les traitements effectués par la CDC ne sont mis en oeuvre que si au moins une des conditions suivantes est remplie :

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

L'article 6 du RGPD vise parmi les traitements de données personnelles licites les traitements de données qui sont nécessaires 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.

Les traitements de données personnelles effectuées par la CDC peuvent par exemple 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 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 de traitements de la CDC fondés sur une mission d'intérêt public :

Gérer les consignations et les dépôts spécialisés : Mission d'intérêt public fondée sur l'art. L518-2 du code monétaire et financier (CMF)

Finalité | Base juridique

- Gérer les consignations et les dépôts spécialisés | Mission d'intérêt public fondée sur l'art. L518-2 du code monétaire et financier (CMF)
- Gérer les retraites | Mission d'intérêt public fondée sur l'art. L518-2 du CMF
- Mon Parcours Handicap | Mission d'intérêt public fondée sur 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 ou de l'exercice de l'autorité publique dont elle est investie, et spécifiquement liés à celle-ci.

4.2 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 en tant que responsable de traitement.

A titre d'exemple : les obligations légales ou réglementaires relatives aux traitements de lutte anti- blanchiment ou contre le financement du terrorisme, ou relatives aux déclarations aux organismes sociaux par la CDC en sa qualité d'employeur.

4.3 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. A titre d'exemple : les intérêts légitimes poursuivis par la CDC peuvent notamment consister à piloter et superviser ses activités, mesurer la qualité des services rendus, améliorer le service rendu.

Dans ce cas de figure, ces traitements sont mis en oeuvre 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.

4.4 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. A titre d'exemple : un contrat de travail entre la CDC et un collaborateur.

4.5 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 à caractère personnel 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.

5 - Les destinataires des données personnelles confiées à la CDC

Le destinataire d'un traitement de données est la personne, le service, la direction, l'entité, qui de manière habituelle reçoit communication des données.

La CDC a mis en place une politique et des règles d'habilitation strictes. Au sein des différentes directions de la CDC, les données personnelles ne sont ainsi accessibles ou transmises qu'aux seules personnes autorisées à en prendre connaissance au regard de leurs missions.

Pour ce qui concerne les destinataires des données tiers à la CDC, la CDC veille à ce que tout tiers ayant connaissance des données ait été préalablement autorisé par la CDC à prendre connaissance de ces données.

Par ailleurs, certaines données personnelles peuvent être adressées à des tiers pour satisfaire aux obligations légales, réglementaires ou conventionnelles s'imposant à la CDC, ou aux autorités légalement habilitées.

Les personnes concernées sont informées par la CDC des destinataires de leurs données, conformément à leur droit à l'information sur le traitement de leurs données au titre des articles 13 ou 14 du RGPD.

6 - Les sous-traitants de la CDC en matière de données personnelles

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

La CDC choisit ses sous-traitants avec soin et 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 oeuvre 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.

7 - La sécurité des données personnelles

La CDC accorde une importance particulière à la sécurité des données personnelles.

Elle met en place des mesures techniques et organisationnelles adaptées au degré de sensibilité des données personnelles, en vue d'assurer l'intégrité et la confidentialité des données et de les protéger contre toute intrusion malveillante, toute perte, altération ou divulgation à des tiers non autorisés.

La CDC effectue régulièrement des contrôles internes afin de vérifier la bonne application opérationnelle des règles relatives à la sécurité des données, notamment des données personnelles. 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.

Ainsi, elle s'engage à prendre les mesures de sécurité physiques, logiques, techniques et organisationnelles nécessaires pour protéger ses activités, préserver la sécurité des données personnelles de ses clients, ses collaborateurs, ses partenaires, ses fournisseurs, ses prestataires ou de toute autre personne physique dont elle traite les données, contre tout accès, modification, divulgation, destruction ou accès non autorisés des données personnelles qu'elle détient.

À titre d'exemple : la protection des applications par une authentification forte, l'accès aux locaux sécurisés, la mise en place de profils distincts selon les besoins d'accès aux données des utilisateurs, les mesures de sauvegarde des données.

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 sont également susceptibles d'être vérifiées dans le cadre du contrôle interne appliqué par la CDC.

Cette sécurité des données personnelles passe aussi par le respect par ses prestataires des règles de sécurité définies par la CDC. Ces règles sont rappelées dans les Règles de Sécurité des Systèmes d'Information pour les Prestataires de Services (RSSIPS) à la CDC, que la CDC rend opposable par contrat à tout prestataire utilisant les systèmes d'informations de la CDC.

8 - Les droits des personnes

Les personnes physiques dont la CDC traite les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données et les traitements qui en sont fait. La CDC est particulièrement soucieuse du respect de ces droits conformément à la législation et à la règlementation applicable en la matière, et, dans ce cadre, elle assure le respect des droits suivants :

- le droit à l'information sur le traitement,
- le droit d'accès,
- le droit de rectification,
- le droit à l'effacement ou « droit à l'oubli »,
- le droit à la limitation du traitement,
- le droit à la portabilité,
- le droit d'opposition au traitement,
- le droit de retirer son consentement à tout moment,
- le droit de définir des directives relatives à la conservation, l'effacement et la communication de ses données personnelles après sa mort,
- le droit de réclamation et de recours.

8.1 Les modalités d'exercice des droits

La CDC donne aux personnes physiques dont elle traite les données les moyens d'exercer effectivement leurs droits sur ces données.

Ces droits peuvent être exercés par courrier en s'adressant au centre de la CDC de Bordeaux à l'adresse suivante : Caisse des Dépôts - Données personnelles – 6 place des citernes - 33059 Bordeaux Cedex, ou par courriel via mesdonneespersonnelles@caissedesdepots.fr.

Pour les demandes autres que les demandes au titre du droit à l'information, la personne concernée doit justifier de son identité en indiquant clairement ses nom et prénoms, l'adresse à laquelle elle souhaite que la CDC lui réponde, et y joindre la photocopie d'un titre d'identité valide portant sa signature, sauf en cas d'autre moyen moins impactant de vérifier son identité. Ces éléments sont fournis à la CDC afin d'être certain de respecter la confidentialité des données de la personne et de ne pas les envoyer à un tiers.

Par principe, la personne concernée pourra obtenir sans frais l'accès à ses données personnelles, sauf demande manifestement infondée ou excessive, leur rectification ou leur effacement, ou la réponse à l'exercice de tout autre de ses droits visés aux articles 15 à 22 du RGPD, dans les meilleurs délais et au plus tard dans le délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prorogé de deux mois, compte tenu de la complexité et du nombre de demandes, 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 :

Concernant le droit à l'information, la CDC n'aura pas l'obligation d'y donner suite lorsque :

Au titre de l'exercice du droit d'accès, la CDC fournit à l'intéressé une copie des données personnelles le concernant faisant l'objet d'un traitement. Toutefois, elle peut être amenée à demander le paiement de frais raisonnables basés sur les coûts administratifs engendrés par la demande, pour toute copie supplémentaire demandée par la personne concernée.

La CDC informera la personne concernée dans le cas où elle ne peut donner suite à ses demandes et de la possibilité pour cette dernière d'introduire une réclamation devant l'autorité de contrôle et de former un recours juridictionnel.

- exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications, ou prendre les mesures demandées, ou
- refuser de donner suite à ces demandes.
- le demandeur dispose déjà de ces informations,
- la communication d'informations au demandeur se révèle impossible ou exigerait des efforts disproportionnés.

8.2 Le droit à l'information

Dans l'objectif de garantir un traitement équitable et transparent, la personne concernée dont les données sont traitées par la CDC, reçoit de la CDC des informations précises et complètes relatives :

Lorsque la CDC a l'intention d'effectuer un traitement ultérieur des données personnelles de la personne concernée pour une finalité autre que celle pour laquelle ses données personnelles ont été collectées, la CDC veillera au respect de l'exigence de compatibilité de cette nouvelle finalité de traitement avec les finalités initiales du traitement, et fournira au préalable à la personne concernée les informations au sujet de ce nouveau traitement.

- à l'identité et aux coordonnées du responsable de traitement, de son représentant légal et de son délégué à la protection des données, le cas échéant ;
- aux finalités du traitement ainsi qu'à la base juridique du traitement ;
- le cas échéant, aux intérêts légitimes poursuivis par le responsable de traitement ou par un tiers ;
- en cas de collecte indirecte de ses données : aux catégories de données personnelles concernées ;
- en cas de collecte des données directement auprès de la personne : au caractère obligatoire ou facultatif du recueil des données, ainsi que sur les conséquences éventuelles de la non-fourniture de des données ;
- aux destinataires ou catégories de destinataires auxquels les données personnelles sont communiquées ;
- le cas échéant, à l'existence de transferts de données vers un pays tiers à l'Union européenne ou une organisation internationale, l'existence d'une décision d'adéquation couvrant ce transfert, ou à défaut les garanties appropriées mises en place pour encadrer ce transfert et la possibilité d'en obtenir une copie ;
- lorsque cela est possible, à la durée de conservation des données personnelles envisagée ou, lorsque ce n'est pas possible, aux critères utilisés pour déterminer cette durée ;

- à l'existence du droit de demander au responsable du traitement l'accès à ses données personnelles, la rectification ou l'effacement de celles-ci, une limitation du traitement de ses données, la portabilité de ses données ; du droit de s'opposer au traitement de ses données dans certaines conditions ; du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage ; du droit de définir des directives particulières quant au sort de ses données après sa mort ; lorsque le traitement est fondé sur le consentement de la personne ; du droit de retirer son consentement à tout moment ; ainsi que du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- si les données personnelles ne sont pas collectées auprès de la personne concernée, à toute information disponible quant à leur source ;
- à l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, aux informations utiles concernant la logique sous-jacente, l'importance et les conséquences prévues de ce traitement pour la personne concernée.

8.3 Le droit d'accès et de rectification

La personne concernée dispose auprès de la CDC d'un droit d'accès et de rectification.

Au titre du droit d'accès, elle peut avoir la confirmation que des données personnelles la concernant sont ou ne sont pas traitées et lorsqu'elles le sont, l'accès auxdites données ou leur communication ainsi que les informations citées au point « 8.2 – le droit à l'information ».

La personne concernée peut demander à la CDC à ce que les données personnelles soient, selon les cas, rectifiées ou complétées si elles sont inexactes, incomplètes, équivoques ou obsolètes.

8.4 Le droit à l'effacement (droit à l'oubli)

Sur demande recevable de la personne concernée, la CDC procèdera à l'effacement des données personnelles la concernant, dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

Néanmoins, elle est informée que l'exercice de ce droit à l'effacement ne sera pas recevable lorsque la conservation des données personnelles est nécessaire soit :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a) du RGPD, ou à l'article 9, paragraphe 2, point a) du RGPD, et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1 du RGPD et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 du RGPD ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;

- les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel la CDC est soumise ;
- les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 du RGPD.
- à l'exercice du droit à la liberté d'expression et d'information,
- au respect d'une obligation légale qui requiert le traitement prévu par la législation ou la règlementation applicable ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investie la CDC,
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique à des fins statistiques,
- à la constatation, à l'exercice ou à la défense de droits en justice.

8.5 Le droit à la portabilité

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à la CDC, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement, sans que la CDC à laquelle les données à caractère personnel de la personne ont été communiquées y fasse obstacle.

Ce droit est toutefois limité aux traitements effectués à l'aide de procédés automatisés, basés sur le consentement ou sur un contrat et aux données personnelles relatives à la personne concernée communiquée par cette personne. Par exemple, les données des collaborateurs traitées par l'employeur, sur la base d'un intérêt légitime ou d'obligations légales, ne sont pas concernées par le droit à la portabilité. Les demandes de portabilité doivent donc être analysées au cas par cas par la CDC.

Des données personnelles dérivées, calculées ou inférées peuvent être créées par la CDC à partir de données brutes fournies directement par la personne concernée. Le droit à la portabilité n'inclut pas ces données personnelles dérivées, calculées ou inférées.

Ce droit permet à une personne : Les données concernées par la portabilité intéressent les catégories suivantes :

En cas d'exercice du droit à la portabilité au profit de la CDC, la personne concernée a la possibilité de transmettre à la CDC les données personnelles la concernant préalablement fournies à un autre responsable de traitement.

Lorsque ce droit est exercé au profit d'un organisme tiers, la personne concernée est informée que la CDC n'est pas responsable du traitement réalisé par l'organisme responsable de traitement qui reçoit les données personnelles.

Après l'exercice de ce droit, la CDC n'a pas l'obligation de conserver des données personnelles, et ne devra pas en tout état de cause les conserver plus longtemps que nécessaire.

Malgré l'exercice de ce droit, la personne concernée pourra continuer à utiliser les services proposés par la CDC et pourra exercer ses droits tant que subsiste le traitement.

- de récupérer les données la concernant traitées par un organisme, pour son usage personnel, et de les stocker sur un appareil ou un cloud privé par exemple. Ce droit permet de gérer plus facilement et par soi-même ses données personnelles.
- de transférer ses données personnelles d'un organisme à un autre. Les données personnelles peuvent ainsi être transmises à un nouvel organisme :
    - soit par la personne elle-même,
    - soit directement par l'organisme qui détient les données, si ce transfert direct est « techniquement possible ».
- uniquement les données personnelles (sont par conséquent exclues les données anonymisées ou les données qui ne concernent pas le demandeur),
- les données personnelles fournies par la personne concernées (tel que par exemple, l'adresse électronique, le nom d'utilisateur, l'âge, etc.),
- les données personnelles ne portant pas atteinte aux droits et libertés de tiers, telles que celles protégées par le secret des affaires.

8.6 Le droit d'opposition

La personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, à un traitement de données personnelles la concernant lorsque le traitement est fondé sur l'intérêt légitime du responsable de traitement y compris le profilage. Le droit d'opposition ne s'applique pas lorsque le traitement est fondé sur une obligation légale (exemple : traitement relatif à la mise en oeuvre du Compte personnel de formation)

En cas d'exercice d'un tel droit d'opposition, la CDC cessera le traitement de ces données sauf lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et droits et les libertés de la personne concernée ou pour la constatation, l'exercice ou la défense d'un droit en justice.

8.7 Le droit à la limitation du traitement

La personne concernée a la possibilité de demander la limitation du traitement de ses données personnelles, c'est-à-dire qu'elle a le droit de demander le gel temporaire du traitement de ses données personnelles :

La limitation entraine en principe l'exclusion de toute utilisation des données personnelles à l'exception de la conservation de ces données, sauf si la personne concernée donne son consentement à une autre opération de traitement de ces données personnelles.

- quand elle conteste l'exactitude des données personnelles et ce pendant une durée permettant à la CDC de vérifier l'exactitude des données personnelles,
- si le traitement est illicite et qu'elle s'oppose à l'effacement de ses données personnelles mais exige une limitation de leur utilisation,
- si la CDC n'a plus besoin des données personnelles aux fins du traitement mais celles-ci restent nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice,

- pendant la durée de vérification ayant pour objet de confirmer que les motifs légitimes poursuivis par la CDC prévalent sur ceux de la personne concernée si elle s'est opposée au traitement en vertu de son droit d'opposition.

8.8 Le droit de retirer son consentement à tout moment

Lorsque les traitements de données que la CDC met en oeuvre sont fondés sur le consentement de la personne concernée, celle-ci est en droit de retirer ce consentement à n'importe quel moment.

Le cas échéant, la CDC cessera de traiter les données personnelles de la personne, sans que la validité des opérations de traitement antérieures auxquelles la personne avait consenti ne soit remise en cause.

8.9 Le droit de définir des directives quant au sort de ses données après sa mort

La personne concernée est informée qu'elle a la possibilité de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données personnelles après son décès.

À ce titre, elle peut définir des directives générales ou particulières. Les directives générales concernent l'ensemble des données personnelles relatives à la personne et sont établies auprès d'un tiers de confiance, certifié et chargé de faire respecter la volonté du défunt (par exemple un notaire).

Les directives particulières sont directement enregistrées auprès de la CDC et mises en œuvre pour les données personnelles concernées.

8.10 Le droit d'introduire toute réclamation ou tout recours

La personne concernée a le droit d'introduire une réclamation auprès d'une autorité de protection des données, par exemple la CNIL en France, et ce, sans préjudice de tout autre recours administratif ou juridictionnel.

Elle peut effectuer ce recours auprès de l'autorité de protection au sein de l'Etat membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise.

9 - L'encadrement des flux transfrontières

Les données personnelles traitées par la CDC dans le cadre de son activité peuvent faire l'objet d'un transfert vers une entité située dans un autre pays de l'Union Européenne, ou hors de l'Union Européenne (plus particulièrement de l'Espace Economique Européen, qui comprend les pays de l'Union européenne, la Norvège, le Lichtenstein et l'Islande).

Lorsque les données personnelles sont transférées vers des pays non-membres de l'Espace Economique Européen, 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 Espace Economique Européen, 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'Espace Economique Européen, 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.

Les CCT de la Commission européenne sont disponibles sur le site de la CNIL (www.cnil.fr), notamment à l'adresse suivante.

Lorsque le contexte du transfert l'exige, par exemple, lorsque le niveau de protection des données personnelles prévu par le droit auquel est soumis l'importateur des données personnelles ne permet pas de garantir l'effectivité des dispositions prévues aux CCT, 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.

10 - La notification 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 à caractère personnel 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 à caractère personnel 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.

À cet effet, la CDC a mis en place une procédure interne permettant de respecter ses obligations, notamment en termes de délais, en matière de gestion des violations de données personnelles.

Elle tient également un registre des violations de données permettant de consigner toute violation de données personnelles, c'est-à-dire les faits concernant la violation de données, ses effets et les mesures prises pour y remédier. Elle tient ce registre à disposition de la CNIL en cas de contrôle.

De manière générale, la CDC met en place toutes les mesures nécessaires pour prévenir les violations de données et réagir de manière appropriée en cas d'incident.

11 - Le dispositif de contrôle interne

La CDC met en oeuvre les moyens nécessaires pour assurer la conformité de ses traitements au regard de la règlementation relative à la protection des données.

Les directions opérationnelles sont responsables du contrôle de premier niveau. Pour ce faire, elles s'appuient notamment sur les relais 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 au regard du RGPD, de l'ensemble de la règlementation relative à la protection des données à caractère personnel, 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.

12 - Diffusion et évolution de la présente Politique

La présente Politique est accessible sur le site Internet de la CDC ainsi que sur l'intranet Next pour l'ensemble des collaborateurs. Elle est examinée par le Comité exécutif (COMEX) et la Commission de surveillance.

Elle est actualisée régulièrement pour prendre en compte les évolutions des pratiques et traitements de la CDC, ses évolutions organisationnelles et techniques, ainsi que les potentielles évolutions législatives et réglementaires applicables aux données personnelles.