Politique interne de protection des données personnelles

Date :	2 novembre 2023

SOMMAIRE

1. PREAMBULE

Le Règlement Général sur la Protection des Données (« RGPD ») applicable dans l'ensemble des Etats membres de l'Union européenne (UE) depuis le 25 mai 2018, est venu renforcer les droits des personnes physiques sur leurs données personnelles grâce à un régime harmonisé des principes de protection au sein de l'Union européenne.

Le RGPD prévoit un principe de « responsabilité » des acteurs devant être en capacité de démontrer, à tout moment, la mise en œuvre les mesures appropriées permettant de garantir le respect des obligations leur étant imposées.

Ces exigences se matérialisent notamment par la tenue d'un registre des traitements afin de documenter la conformité des traitements de données personnelles opérés par la Carac et la mise en œuvre de mesures de sécurité renforcées. Le non-respect de ces règles pouvant conduire à des sanctions et à dégrader l'image de la Carac.

Face à ces enjeux, la Carac a décidé de se doter d'une Politique de générale de protection des données (ci-après « Politique ») destinée à garantir la protection des données personnelles des collaborateurs, des partenaires, des adhérents, des élus, des locataires des immeubles d'investissement et des fournisseurs de la Carac dans le respect du RGPD.

La protection des données personnelles contribue à pérenniser la confiance de nos collaborateurs, de nos adhérents, élus et partenaires. Il s'agit d'un enjeu significatif pour l'exercice durable de nos activités.

Le Service Juridique et en particulier le DPO sont chargés en coopération avec le RSSI de faire appliquer cette Politique au nom du Conseil d'administration.

Nous demandons donc à l'ensemble des collaborateurs de se mobiliser pour garantir sa bonne application.

Toute question relative aux modalités d'application de la Politique ou tout autre sujet relatif aux données personnelles peut être adressé à l'adresse suivante : dpo@carac.fr

2. OBJECTIFS

La présente Politique a pour objet de définir les normes de conformité, les processus, et les mesures de contrôle que la Carac met en œuvre afin de respecter la réglementation applicable en matière de protection des données personnelles (Règlement Général sur la Protection des Données du 27 avril 2016 et la Loi informatique et libertés du 6 janvier 1978 et ses modifications ultérieures, ainsi que la Directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques).

La Politique comprend l'ensemble des principes qui visent à créer au sein de la Carac un cadre commun de règles pour gérer la protection des données personnelles et d'en garantir un niveau élevé.

Les principes sont déclinés au sein de procédures opérationnelles auxquelles la Politique renvoie. Elle établit également des règles de gouvernance qui précisent les rôles et responsabilités des acteurs de la protection des données personnelles.

La mise en œuvre et le respect de la Politique sont supervisés par le DPO pour les thématiques liées à la sécurité des données personnelles.

3. DEFINITIONS

Responsable du traitement : L'organisme déterminant les finalités et les moyens des traitements, en l'espèce la Carac.

Personne concernée : Personne physique identifiée ou identifiable, directement ou indirectement par référence à une Donnée personnelle.

DPO ou Data Protection Officer : Le Délégué à la Protection des Données, garant interne en matière de conformité de la protection des données personnelles.

Donnée(s) personnelle(s) : Toute information se rapportant à une Personne concernée, par exemple un identifiant, un numéro d'adhérent, un numéro de

garantie, un nom ou un ou plusieurs éléments spécifiques propres à son identité physique, génétique, psychique, économique ou sociale.

Traitement : 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 personnelles, 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.

Limitation du traitement : Le marquage de Données personnelles conservées, en vue de limiter leur traitement futur.

Profilage : Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données personnelles pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Pseudonymisation : Le traitement de Données personnelles de telle façon que celles-ci ne puissent plus être attribuées à une Personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable.

Sous-traitant : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du Responsable du traitement.

Destinataire : La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données personnelles.

Violation de données personnelles : 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.

4. CHAMP D'APPLICATION

Champ d'application matériel

La présente Politique s'applique **à tout traitement de données personnelles opéré par la Carac,** quelle que soit :

- la nature de la donnée personnelle (sensible ou non, publique ou non, sécurisée ou non, pseudonyme ou non, etc.)
- les catégories de personnes concernées (adhérents, prospects, collaborateurs, candidats, prestataires, partenaires, etc.)
- la forme ou le stockage des données
- le canal de collecte de la donnée personnelle, la forme et le stockage de la donnée
- la finalité ou le type de traitement (automatisé par l'intermédiaire de supports informatiques ou manuels, y compris sous format papier).

Champ d'application territorial

La présente Politique s'applique dès lors que la Carac effectue un traitement de données personnelles sur le territoire de l'UE, que le traitement ait lieu ou non dans l'UE.

Champ d'application personnel

Tous les collaborateurs sont individuellement responsables du respect de cette Politique, y compris du respect des politiques, procédures, processus, ou autres documents annexes auxquels elle renvoie.

Le respect est obligatoire : toute violation peut donner lieu à des mesures disciplinaires dans les conditions prévues par la loi.

5. GOUVERNANCE ET PILOTAGE

Les acteurs de la protection au sein de la Carac

Toute personne travaillant chez, pour, ou avec la Carac a une part de responsabilité dans la conformité à la réglementation applicable. Cependant, certaines personnes ont des domaines de responsabilités clés.

Le Délégué à la protection des données (DPO)

La Carac a désigné un DPO joignable à l'adresse : dpo@carac.fr

Le DPO est l'interlocuteur principal pour toutes les questions concernant les données personnelles et est responsable de la définition des normes de protection des données et assure la vérification de leur application.

Au sein de la Carac, le DPO a pour mission :

- d'informer et de conseiller le responsable de traitement ainsi que les collaborateurs ;
- de contrôler le respect du présent règlement et des dispositions en matière de protection des données ;
- veiller à la bonne application du principe de protection des données dès la conception et par défaut des projets comportant un traitement de données personnelles ;
- dispenser des conseils en ce qui concerne les études d'impact sur la vie privée et en assurer la pertinence, vérifier l'exécution de celle-ci et, si besoin, de participer à sa réalisation ;
- être l'interlocuteur privilégié de l'autorité de contrôle et coopérer avec celle-ci ;
- de faire office de point de contact sur les questions relatives au traitement des données personnelles ;
- tenir l'inventaire et documenter les traitements de données à caractère personnel ;
- participer à la réalisation des notifications de violation de données personnelles et dispenser des conseils notamment concernant les éventuelles communications aux personnes concernées et les mesures à apporter ;
- remettre chaque année au responsable de traitement un rapport annuel des activités réalisées

Aux fins de la gouvernance de la protection des données personnelles, les articles 37-39 du RGPD et les lignes directrices du Conseil européen de la protection des données sont utilisés pour établir les normes minimales en ce qui concerne le statut, les obligations, les fonctions et le profil du DPO.

En particulier, la Carac s'est assuré de l'indépendance, de l'expertise et des compétences du DPO désigné.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI)

La Carac a désigné un RSSI joignable à l'adresse : rssi@carac.fr ou rthiel@carac.fr

Le RSSI travaille de concert avec l'équipe DPO pour toutes questions concernant la sécurité des données personnelles.

Au sein de la Carac, le RSSI a pour mission :

- Mettre en place la gouvernance de la cybersécurité au sein de la Carac ;
- Formaliser et contrôler la PSSI de la Carac ;
- Gérer les sujets de cybersécurité au sein de la Carac.

Le Conseil d'administration de la Carac

La Carac met également au cœur de sa gouvernance le Conseil d'administration qui s'engage à œuvrer pour la promotion d'une culture de conformité.

Pour permettre de piloter la conformité, le Conseil d'administration de la Carac s'engage notamment à :

- Associer de manière appropriée et en temps utile le DPO, le RSSI, et les comités de gouvernance à toutes les questions relatives à la protection des données.
- Aider le DPO, le RSSI et les comités de gouvernance dans l'exercice de leurs missions en :
    - Fournissant les ressources et moyens nécessaires (financier, infrastructures, personnel, temps alloués, etc.) ;
    - Fournissant l'accès aux données et aux opérations de traitement ;
    - Permettant d'entretenir leurs connaissances spécialisées et leurs capacités à accomplir leurs missions.
- Permettre au DPO et aux comités de gouvernance de faire directement rapport au niveau le plus élevé de la Carac.

- Donner une importance aux analyses et conseils en matière de protection des données personnelles dispensées par le DPO, le RSSI, et les comités de gouvernance et, dans le cas où les recommandations ne seraient pas retenues, à en documenter les raisons.
- S'assurer de l'avis du DPO, du RSSI, et des comités de gouvernance avant mise en œuvre de tout nouveau projet impliquant ou appelé à impliquer des données personnelles.
- Veiller à l'indépendance du DPO, du RSSI et des comités de gouvernance.

Les comités :

Un comité de protection des données doit se réunir à minima une fois par an afin de présenter la stratégie relative à la protection des données personnelles au sein de la Carac et pour permettre le suivi de cette dernière.

Le Comité RGPD assure la cohérence de la mise en œuvre de la protection des données par les opérationnels de la Carac. Il permet d'orienter et de valider les demandes et besoins des métiers en fonction des problèmes rencontrés par les différentes activités techniques et métiers de la Carac en matière de protection des données.

Le comité RGPD est composé :

- Du Responsable de la fonction « Sécurité de l'Information » / Responsable de la Sécurité des Systèmes d'Information (FSI/RSSI) ;
- Du Responsable de la Fonction Clé « Gestion des risques » ;
- Du Responsable de la Fonction Clé « Vérification de la conformité » ;
- Du Délégué à la Protection des données (DPO) ;
- Du Responsable de la fonction clef « Audit Interne »
- Du Directeur de la Transformation Stratégique ;
- Du Responsable du Département Systèmes d'Information ;
- Du Responsable de la Production Informatique ;
- Du Responsable MOA ;
- Du Responsable Gestion des projets stratégiques.

Les outils de la mise en conformité

La Carac met en œuvre un ensemble d'outils, de procédures, de politiques, de processus afin d'assurer la conformité à la réglementation applicable et notamment au principe de responsabilisation.

Toute la documentation permettant à la Carac de démontrer sa conformité est disponible au sein d'un espace dédié à la protection des données pour les registres des traitements.

Les collaborateurs ont également accès à toute documentation utile leur permettant de connaître les règles applicables et les processus à suivre au quotidien.

La Carac met en place dans le Teams CARAC RGPD :

- Un registre des traitements de données personnelles (en tant que responsable de traitement). Le registre est mis à disposition de la CNIL sur demande
- Une procédure de gestion des demandes d'exercice des droits
- Un registre de suivi des demandes d'exercice des droits
- Une procédure de gestion des violations des données personnelles
- Un registre de suivi des violations de données personnelles
- Une cartographie permettant l'identification des AIPD (Analyse d'Impact relative à la protection des Données personnelles) en cas de traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques)
- Un modèle d'annexe RGPD pour les sous-traitants
- Un support de formation et plan de formation
- Un référentiel de durée de conservation
- Une procédure de contrôle CNIL

La Carac a également élaboré et déployé des processus, des politiques et des procédures en matière de sécurité, notamment :

- d'une politique de sécurité du système d'information (PSSI) ;
- d'un plan de reprise d'activité (PRA) ;
- d'un plan de continuité d'activité (PCA).

Le principe de responsabilisation est un processus continu. Par conséquent, toute cette documentation est mise à jour de manière continue pour s'assurer

qu'elle reste conforme, exacte et à jour (e.g., évolution des traitements, changement de prestataire, changement de mesures techniques ou organisationnelles de sécurité applicables, etc.).

Le DPO est également joignable à l'adresse suivante mise à disposition de tous les collaborateurs : dpo@carac.fr

Les mécanismes de contrôle

Contrôles et audit internes

Le DPO mène régulièrement des contrôles et des audits internes de conformité à la réglementation applicable et à la présente Politique.

Le DPO, avec l'appui du RSSI le cas échéant, testent, analysent, et évaluent les mesures juridiques, techniques et organisationnelles afin de vérifier leur efficacité.

Contrôle et audits des sous-traitants

La Carac pourra effectuer le contrôle de ses sous-traitants et sous-traitants ultérieurs afin de vérifier le respect des obligations contractuelles convenues ainsi que de la réglementation applicable.

Ces contrôles et audits sont documentés et font l'objet de rapports d'audits. Lorsque des mesures correctives doivent être adoptées et implémentées par le sous-traitant ou le sous-traitant ultérieur, cela fait l'objet d'un plan d'actions ou de remédiation suivi par le DPO avec l'appui du RSSI, le cas échéant. Les résultats de ces contrôles pourront être mis à disposition de l'autorité de contrôle compétente (la CNIL en France).

Modèle d'annexe RGPD pour les sous-traitants

6. PRINCIPES DE PROTECTION DES DONNEES MIS EN ŒUVRE PAR LA CARAC

Principes fondamentaux de protection des données

La Carac à travers chaque collaborateur, doit mettre en œuvre les principes de protection des données suivants lors de la conception de tout projet.

Le respect de ces principes implique toujours le DPO de la Carac et, le cas échéant, le service juridique, les comités de gouvernance et le Conseil d'administration.

Limitation des finalités : finalités déterminées, explicites et légitimes

La Carac s'assure que les données personnelles sont collectées pour des finalités déterminées, explicites et légitimes, et qu'elles ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités.

A ce titre, lors de la mise en place d'une nouvelle activité de traitement, les collaborateurs doivent expliquer tous les objectifs et les finalités au DPO afin de garantir des conseils précis sur la conformité à la réglementation applicable et à la présente Politique.

Si une nouvelle finalité n'a pas été prévue ou communiquée au DPO, les collaborateurs ne pourront pas utiliser les données jusqu'à ce qu'un nouvel examen soit effectué.

Registre des traitements de données personnelles 

Licéité du traitement de données personnelles : bases légales et dérogations

La Carac s'assure que les données personnelles sont traitées de manière licite, loyale et transparente. En particulier, la Carac est garante de la licéité des traitements qu'elle réalise.

Cela signifie que la Carac s'assure que les traitements sont fondés sur l'une des bases légales édictées par la réglementation applicable :

Consentement	La personne concernée a donné son consentement, soit toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne accepte, par une déclaration ou par un acte positif clair, que ses données personnelles fassent l'objet d'un traitement (ex : prospection commerciale B2C, cookies et autres traceurs, etc.).
Contrat	Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée.
Respect d'une obligation légale	Le traitement est nécessaire au respect d'une obligation légale à laquelle la Carac est soumise. Un texte légal rend obligatoire la mise en œuvre de certains traitements (ex : la tenue du registre unique du personnel).
Intérêt légitime	Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par la Carac ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (ex : la vidéosurveillance ou la gestion de la fraude).
Sauvegarde des intérêts vitaux	Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ou d'une autre personne (ex : la gestion des risques d'épidémie). En principe, cette base légale n'est pas utilisable par la Carac au regard de son activité quotidienne.
Exécution d'une mission d'intérêt public	Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement (ex : les traitements mis en œuvre par une collectivité locale ou une administration). En principe, cette base légale n'est pas utilisable par la Carac au regard de son activité quotidienne

A ce titre, lors de la mise en place d'une nouvelle activité de traitement, les collaborateurs doivent expliquer tous les objectifs et les finalités au DPO afin de

garantir des conseils précis sur la base légale applicable et les conséquences subséquentes de ce choix.

Le consentement et l'intérêt légitime sont d'ailleurs des bases légales qui doivent être utilisées de manière très prudente. En effet, des conditions et des exigences strictes doivent être respectées, par exemple le respect des conditions de validité du consentement ou encore la conduite d'une balance des intérêts.

Le DPO porte également une attention particulière lorsque des données sensibles sont appelées à être traitées puisque des exigences additionnelles seront à respecter. En effet, le principe étant l'interdiction de traiter ces données sensibles, il conviendra de répondre strictement à l'une des dérogations édictées par la réglementation applicable et respecter de surcroît des exigences spécifiques pouvant provenir d'autres textes juridiques.

Les données sensibles visent toutes les informations de nature à révéler l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques ou biométriques, les données concernant la santé, la vie ou l'orientation sexuelle d'une personne.

Minimisation des données : adéquation, pertinence et limitation

La Carac s'assure que les données collectées sont adéquates, pertinentes et limitées par rapport aux finalités pour lesquelles elles sont traitées et qui ont été communiquées aux personnes concernées. La Carac doit ainsi démontrer pourquoi les données personnelles sont traitées et en quoi elles sont non excessives au regard des finalités.

Le principe de minimisation devant être pris en compte dès le début de chaque projet, cette minimisation devra être vérifiée par le DPO lors de l'analyse susmentionnée. Ce principe de minimisation s'applique d'ailleurs également dans le cadre des transferts de données hors UE. Une attention particulière est portée aux modalités de collecte des données (directe, indirecte, auprès de tiers, etc.)

Exactitude des données et mise à jour

La Carac s'assure que les données traitées soient exactes et tenues à jour. A ce titre, la Carac pourra effectuer des audits réguliers et mettre en place des processus opérationnels pour vérifier que les données personnelles traitées restent exactes et à jour et rectifie toute inexactitude ou efface toute donnée personnelle périmée.

Durée de conservation limitée

La Carac s'assure de ne pas conserver les données personnelles au-delà de la durée nécessaire au regard des finalités pour lesquelles elles sont traitées, dans le respect de la législation française et européenne applicable.

La Carac prend appui sur un référentiel des données de conservation devant être suivi. Ce référentiel indique les durées de conservation en base active ainsi qu'en base intermédiaire devant être en principe appliquées. En cas de doute sur la durée de conservation applicable, qui se détermine au cas par cas en tenant compte de la finalité du traitement mais aussi de la réglementation applicable, ou si un département au sein de la Carac s'écarte de ce référentiel, le DPO doit être saisi afin d'émettre un avis. En cas de non-respect du référentiel, le DPO rédige une note à destination du Département concerné afin que ce dernier puisse prendre une décision en connaissance des risques.

Une fois la période de conservation atteinte, la Carac s'engage à supprimer de manière irréversible toutes les copies des données personnelles (y compris des sauvegardes) ou les anonymise.

Référentiel des durées de conservation 

Confidentialité, intégrité et disponibilité : sécurité appropriée des données

La Carac traite les données personnelles de façon à garantir leur sécurité appropriée, y compris contre les traitements non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle.

Pour cela, la Carac met en place des mesures techniques et organisationnelles appropriées permettant de garantir la confidentialité, l'intégrité et la disponibilité des données personnelles, compte tenu

notamment de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques. La Carac prend également en compte les résultats des analyses des risques réalisées dans le cadre des Analyse d'Impact relative à la Protection des Données personnelles (AIPD) et, le cas échéant, des exigences légales spécifiques en matière de sécurité devant être respectées en fonction des données personnelles traitées (par exemple, les données de santé, le numéro de sécurité sociale, etc.).

La Carac évalue et teste régulièrement l'efficacité de ces mesures pour assurer la sécurité de ses traitements.

Politique de sécurité du système d'information 

Loyauté et transparence : droit à l'information

La Carac veille à informer les personnes concernées des traitements de données personnelles réalisés, y compris les collaborateurs, les adhérents, les élus, les visiteurs de son site web, les partenaires commerciaux, etc.

La Carac s'assure que les informations communiquées aux personnes concernées sont concises, transparentes, compréhensibles, intelligibles, adaptées au public, en des termes clairs et simples, et mises à disposition par des moyens aisément accessibles et adaptés aux modalités de collecte. La Carac s'assure également que les mises à jour de ces informations respectent les mêmes exigences.

La Carac met en place une information destinée aux personnes dans la politique de protection des données, dans les formulaires, le bandeau cookies et tout autre support le cas échéant, en conformité avec les exigences de la réglementation applicable.

Les collaborateurs ont l'obligation de respecter cette procédure. En cas de doute, ils ont l'obligation de saisir le DPO.

Droit des personnes concernées

La Carac s'assure du respect des droits des personnes concernées, à savoir : le droit d'accès, le droit de rectification, le droit d'effacement, le droit à la limitation du traitement, le droit à la portabilité, le droit d'opposition y compris

au profilage, les droits spécifiques en matière de décisions individuelles automatisées, le droit au retrait du consentement, ainsi que le droit de donner des directives après son décès.

La Carac a notamment mis en place des moyens permettant aux personnes concernées d'exercer leurs droits de manière simple et appropriée. Les personnes concernées sont informées de ces modalités au sein des formulaires, contrats, de la politique de protection des données mises à leur disposition et peuvent exercer ces droits à tout moment.

La Carac a mis en place une procédure de gestion des demandes d'exercice des droits décrivant les modalités mises en œuvre pour faciliter l'exercice des droits avec les processus à suivre en cas de réception d'une demande, y compris des modèles de réponses. Les collaborateurs doivent notamment remonter toute demande qui n'aurait pas été réceptionnée par le DPO afin d'assurer le suivi conforme de la procédure.

Procédure de gestion des demandes d'exercice de droit 

La Carac maintient enfin un registre de suivi des demandes d'exercice des droits.

Registre de suivi des demandes d'exercice de droits 

Protection des données dès la conception et par défaut

La Carac s'assure que la protection des données est intégrée dans la gestion des projets ainsi que dans la conception des produits et ce dès leur conception et par défaut.

En particulier, chaque collaborateur est chargé de s'assurer que son projet est conforme au RGPD pendant les phases de conception, de construction et d'exécution.

Les Départements de la Carac doivent remonter chaque projet en amont de la phase de conception au DPO ainsi qu'au RSSI et toute autre partie prenante pertinente, le cas échéant comme le service juridique en cas de recours à un nouveau prestataire, afin d'assurer la conformité à la réglementation applicable.

Analyse d'impact relative à la protection des données personnelles

Une analyse d'impact sur la protection des données est réalisée par la Carac pour tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Cette analyse permet notamment d'identifier l'ensemble des risques que peut comporter le traitement, de les évaluer, y compris leurs impacts, et d'implémenter les mesures d'atténuation du risque.

Cartographie permettant l'identification des AIPD 

Relation avec les tiers

Les collaborateurs doivent automatiquement et obligatoirement saisir le DPO en cas de recours à un nouveau prestataire. Le DPO pourra émettre un avis sur la qualification de la relation (responsable de traitement, sous-traitant, responsables de traitement conjoints). Le DPO pourra également évaluer les garanties offertes par le tiers au regard de la présente Politique et de la réglementation applicable.

Tous les tiers doivent être évalués par le DPO : aucune contractualisation ne doit être initiée sans évaluation qui devra être effectuée le plus tôt possible.

Une fois le tiers évalué et validé par la Direction en connaissance des risques exposés le cas échéant par le DPO. Dans tous les cas, le DPO doit être associé à la négociation des contrats impliquant un traitement de données personnelles.

Transferts des données personnelles en dehors de l'UE

La Carac s'assure d'identifier et d'encadrer tout transfert ou transfert potentiel en dehors de l'UE conformément à la réglementation applicable, c'est-à-dire toute transmission, envoi, consultation ou accès aux données personnelles vers, dans, ou depuis un pays hors UE.

A noter : un simple accès à des données personnelles depuis un autre pays est, d'un point de vue juridique, un transfert hors UE : ainsi la simple possibilité d'accès, qu'elle soit voulue ou non, par les autorités d'un pays hors UE à des serveurs situés au sein de l'UE sera considéré comme un transfert potentiel.

En cas de transferts en dehors de l'UE, la Carac s'assure de pouvoir justifier de l'une des dérogations édictées par la réglementation applicable, notamment, par ordre de priorité :

- Une décision d'adéquation dans le respect des conditions fixées par la Commission Européenne
- L'utilisation de garanties appropriées (clauses contractuelles types adoptées par la Commission Européenne pour autant que les conditions d'utilisation de ces clauses soient remplies et que les obligations y figurant soient respectées, ou règles d'entreprise contraignantes approuvées par une autorité de contrôle)
- Une des dérogations de l'Article 49 du RGPD sous réserve que les conditions limitatives de ces dérogations soient respectées.

Tous les transferts doivent être évalués par le DPO ainsi que par le RSSI : aucun transfert ne doit être initié sans consultation. Cette évaluation doit être effectuée le plus tôt possible.

Gestion des incidents de sécurité et des violations de données

La Carac a mis en place une procédure de gestion des incidents de sécurité et de violation des données personnelles décrivant le processus à suivre en matière d'identification, de traitement, d'analyse, de remédiation, et de notification des incidents et violations de données personnelles à la CNIL et, le cas échéant, aux personnes concernées, ainsi que les démarches à entreprendre.

Tout collaborateur doit automatiquement remonter chaque incident au DPO ainsi qu'au RSSI en suivant le processus défini au sein de la procédure. Les collaborateurs doivent conserver toutes les preuves relatives à l'incident. La notification déclenche la mise en place d'une cellule de gestion de crise afin d'enquêter sur la violation, de regrouper les éléments et documents nécessaires, de proposer des mesures de remédiation et de statuer sur les notifications à effectuer.

Une forte collaboration entre le DPO et le RSSI est nécessaire. Il est toutefois important de noter que certains incidents sont purement des incidents de sécurité qui n'ont pas d'impact sur les données personnelles. Ces incidents ne sont pas gérés par le DPO mais uniquement par le RSSI. Inversement, certains incidents sont des violations de données personnelles sans impact sur la sécurité des données. Dans ce cas, elles seront gérées uniquement par le DPO.

Le DPO formule des recommandations concernant la décision de notifier la violation à la CNIL et, si nécessaire, aux personnes concernées. La décision définitive revient à la direction de la Carac. En cas de décision positive, le DPO reste compétent pour communiquer la violation à la CNIL dans les 72h. La notification sera accompagnée de tous les éléments requis par la réglementation applicable.

Procédure de gestion des violations des données personnelles 

Le DPO tient à jour un registre des violations recensant et décrivant l'ensemble des violations de données personnelles ainsi que les mesures prises en conséquence.

Registre de suivi des violations de données personnelles 

Sensibilisation et formation

Le DPO s'assure que les collaborateurs de la Carac ont les connaissances suffisantes pour remplir leurs obligations au titre de la réglementation applicable, en fonction de leur degré d'implication dans les traitements de données personnelles. Pour cela, le DPO déploie un plan de formation et s'appuie sur un support de sensibilisation qui peut être adapté selon les publics.

Plan de formation RGPD 

Pour s'assurer également du respect de la réglementation applicable par les collaborateurs, la Carac leur fait signer à leur arrivée un engagement de confidentialité, inséré au sein du contrat de travail, ainsi qu'une Charte IT contraignante.

Le RSSI s'assure également que les collaborateurs de la Carac ont les connaissances suffisantes en matière de sécurité pour remplir leurs obligations au titre de la réglementation applicable, en fonction de leur rôle et responsabilité.

Contrôles de l'autorité de protection des données (CNIL)

Tout ordre formel de se conformer à la réglementation applicable doit être immédiatement remonté au DPO. En fonction du risque, de la portée, et de la gravité de l'injonction, le DPO doit soit approuver les actions prévues, soit faire des recommandations, soit participer à l'exécution des mesures citées ou à la réponse à l'autorité.

Toute investigation diligentée par une autorité de contrôle doit être immédiatement remontée au DPO suivant le processus décrit au sein de la procédure de gestion d'un contrôle CNIL.

Procédure de contrôle CNIL 

Sanctions

Des collaborateurs

La présente Politique s'applique à tous les collaborateurs, même occasionnels. En particulier, tous les collaborateurs sont individuellement responsables du respect de cette Politique, y compris du respect des politiques, procédures ou autres documents annexes auxquels elle renvoie.

Le respect est obligatoire : toute violation peut donner lieu à des mesures disciplinaires dans les conditions prévues par la loi.

De la Carac

En cas de non-respect de cette Politique, y compris des politiques, procédures ou autres documents annexes auxquels elle renvoie, la Carac s'expose aux risques suivants :

- Des sanctions administratives pouvant aller jusqu'à 10 millions d'euros ou 20 millions d'euros ou bien jusqu'à 2% ou 4% du CA annuel mondial selon les manquements.

- Des sanctions civiles puisque les personnes concernées peuvent demander réparation du dommage causé, et même constituer une action de groupe impliquant une obligation de dédommager toutes les parties prenantes.
- Des sanctions pénales pouvant aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.
- Des risques contractuels puisqu'une non-conformité peut impliquer des sanctions contractuelles de la part des clients pour non-respect des obligations contractuelles.
- Des risques opérationnels puisqu'une mise en demeure de la CNIL ou une sanction peut impliquer l'arrêt du traitement jusqu'à mise en conformité et le retrait des produits et solutions du marché et ainsi engendrer une perte en avantage concurrentiel.
- Des risques réputationnel puisqu'une mise en demeure de la CNIL ou une sanction peut porter atteinte à la réputation de la Carac, les délibérations de la CNIL pouvant être publiées, et ainsi engendrer une perte de confiance des clients