POLITIQUE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

1. PRÉAMBULE

Le règlement n°2016/679 nommé, « Règlement Général sur la Protection des Données » (ci-après « RGPD ») est, depuis le 25 mai 2018, le nouveau cadre juridique européen, unique et commun à tous les états membres, en matière de traitement automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel.

Ce règlement dispose également d'un cadre extraterritorial qui permet, sous certaines conditions, d'étendre son périmètre d'application hors UE.

La Compagnie OPTORG a toujours inscrit la protection des données à caractère personnel comme un des éléments clés de sa gouvernance et de celle de ses processus et procédures, aussi bien opérationnels, de support comme de pilotage.

2. CONTEXTE INTERNE

Selon les situations, le Groupe Optorg porte le rôle de Responsable de Traitement ou celui de Sous-Traitant.

Ces différentes qualifications engendrant des obligations et des enjeux distincts, la présente Politique de Protection des Données à Caractère Personnel (ci-après désignée par « PPDCP ») reflète la volonté du Groupe OPTORG de mettre en place l'ensemble des principes applicables aux données à caractère personnel collectées et traitées dans le cadre de ses activités.

Le Groupe OPTORG veille à son alignement permanent, à la fois :

- Avec les orientations et directives de la Loi Informatique et Libertés du 6 janvier 1978 et ses versions modifiées (la dernière modification est formalisée par la loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018 afin d'exercer certaines des « marges de manœuvre nationales » autorisées par le RGPD et de transposer en droit français la Directive « police-justice ») ;
- Avec les orientations et directives des lois relatives à la protection des données à caractère personnel des pays où se situent ses différentes filiales.

3. DÉFINITIONS

- **Données à caractère personnel (ci-après DCP) :** « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres… » ;
- **Traitement :** 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, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;
- **Responsable de Traitement :** désigne la personne physique ou morale qui détermine les finalités et les moyens d'un traitement de données à caractère personnel. En général, le Groupe OPTORG est Responsable de Traitement de ses

propres collectes de données. Il arrive cependant dans certains cas que ce soit ses clients qui soient Responsables de Traitement ;

- **Sous-Traitant :** désigne toute personne physique ou morale qui traite des données à caractère personnel pour le compte du Responsable de Traitement. Le Groupe OPTORG est Sous-Traitant pour les données qu'il traite pour le compte de ses clients ;
- **Sous-Traitant Ultérieur :** désigne les prestataires des Sous-Traitants avec lesquels le Groupe OPTORG travaille et qui interviennent sur les données à caractère personnel que le Groupe OPTORG traite en tant que Responsable de Traitement ;
- **Personnes concernées :** désigne les personnes qui peuvent être identifiées, directement ou indirectement ;
- **Destinataires de Données :** désigne les personnes physiques ou morales qui reçoivent communication des données à caractère personnel. Les destinataires des données peuvent donc être aussi bien des destinataires internes que des organismes extérieurs.

4. CHAMP D'APPLICATION

Le Groupe OPTORG a défini les principes et lignes directrices de la présente PPDCP pour :

1. Encadrer, conformément au RGPD, le traitement de l'ensemble des données collectées, quel que soit leur mode de collecte ou de traitement ;
2. Satisfaire à l'obligation d'informer les personnes concernées sur leurs droits, de manière concise, transparente, compréhensible et aisément accessible ;
3. Formaliser les droits et les obligations du Groupe OPTORG en tant que Responsable de Traitement et en tant que Sous-Traitant.

Le Groupe OPTORG applique cette PPDCP à toutes ses filiales, même établies hors de l'UE, dès l'instant où celles-ci réalisent des traitements de données :

- Relatifs à des personnes qui se trouvent dans l'Union Européenne ;
- Liés à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non.

CRITÈRES D'APPLICATION DU CHAMP EXTRA-TERRITORIAL DU RGPD

Ne constitue pas une offre de biens ou de services à des personnes qui se trouvent dans l'Union Européenne :

1. La simple accessibilité à partir de l'Union Européenne du site internet du Groupe OPTORG, d'une adresse électronique ou d'autres coordonnées ;
2. L'utilisation d'une langue généralement utilisée dans les pays tiers où le Responsable de Traitement est établi.

Sont considérés comme des indices permettant d'identifier une offre de biens ou de services à des personnes qui se trouvent dans l'Union Européenne :

1. L'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs états membres de l'Union Européenne ;
2. La possibilité de commander des biens et des services dans cette autre langue ;
3. La mention de clients ou d'utilisateurs qui se trouvent dans l'Union Européenne.

5. LES ACTEURS DE LA MISE EN ŒUVRE DE LA CONFORMITÉ RGPD

Afin de gérer et dynamiser la conformité de l'ensemble de ses entités vis-à-vis de la réglementation applicable aux données personnelles, le Groupe OPTORG a désigné un Délégué à la Protection des Données ou Data Protection Officer (DPO) et a mis en place un réseau de correspondants appelés les Responsables de Traitement Opérationnels (RTO).

5.1. LE DATA PROTECT OFFICER (DPO)

Le Groupe OPTORG a désigné un DPO auprès de la CNIL (Désignation n° DPO-52428).

Le DPO est rattaché à la Direction Juridique et Fiscale. Pour s'assurer de la bonne gestion de la conformité, il est également en interaction avec les RTO, la Direction des Services Informatiques, la Direction de la Conformité et la Direction des Ressources Humaines.

Ses principales missions sont :

1. Informer et conseiller le Groupe OPTORG (la direction, le personnel participant aux opérations de traitement, etc…) sur les règles à respecter en matière de protection des données personnelles ;
2. Contrôler le respect des règles relatives à la protection des données personnelles, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;
3. Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact sur les DCP et vérifier l'exécution de celle-ci ;
4. Coopérer avec l'Autorité de Contrôle et faire office d'interlocuteur privilégié sur toutes les questions relatives au traitement des DCP ;
5. S'assurer de la bonne tenue de la documentation relative aux traitements des DCP ;
6. Veiller au maintien de ses compétences en se tenant informé des dernières évolutions en matière de protection des données à caractère personnel.

Le Groupe OPTORG veille à ce que le DPO soit inscrit dans la PSSI (telle que définie ci-après) et soit associé, d'une manière appropriée et en temps utile, à toutes les problématiques relatives à la protection des données personnelles telles que :

1. Le Privacy by Design, c'est-à-dire la prise en compte des impacts sur la vie privée dès la conception du traitement de DCP ;
2. Le Privacy by Default, c'est- à-dire la prise en compte des impacts sur la vie privée par défaut ;
3. L'analyse d'impact sur la vie privée ou DPIA ;
4. La notification des violations de données personnelles à l'Autorité de Contrôle et la communication aux personnes concernées si nécessaire ;
5. La relation et la coopération avec le DPO des Clients Responsables de Traitement et le DPO des sous-Traitants pour assurer le respect des règles du RGPD.

Afin de renforcer l'indépendance du DPO et l'absence de tout conflit d'intérêts, le Groupe OPTORG lui garantit :

1. De ne recevoir aucune instruction en ce qui concerne l'exercice de ses missions ;
2. De ne pas être relevé de ses fonctions ou pénalisé pour l'exercice de ses missions ;
3. De rapporter directement au niveau le plus élevé de la Direction.

5.2. LE RESPONSABLE DE TRAITEMENT

Le Responsable de Traitement mentionné dans la présente Politique de Confidentialité des Données à Caractère personnel est la Compagnie OPTORG, Société Anonyme à Directoire et Conseil de Surveillance, au capital de 38 952 240 euros, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le n°552 126 385, dont le siège social est situé au 49-51, Quai de Dion Bouton - 92800 Puteaux – France et dont Monsieur Tarafa MAROUANE Président, est le représentant légal.

La Compagnie OPTORG détermine les finalités et les moyens de tous les traitements dont elle est responsable.

5.3. LES RESPONSABLES DE TRAITEMENT OPERATIONNELS (RTO)

Les RTO sont nommés au sein de chaque ligne métier et opération. Ils sont le point de contact du DPO sur leur périmètre de responsabilité. Leurs principales missions sont de/d' :

1. Organiser la remontée des informations relatives à tous nouveaux projets de traitements de données pour permettre l'échange avec le DPO ;
2. S'assurer de la réalisation et de la mise à jour du registre des activités de traitement de leur périmètre ;
3. Remonter dans les meilleurs délais toute suspicion de violation de données à caractère personnel.

6. STOCKAGE DES DONNÉES

Tous les Data Centers du Groupe OPTORG dans lesquels sont susceptibles d'être hébergées des DCP sont situés en France ou dans un ou des pays de l'UE.

7. LES ENGAGEMENTS DU GROUPE OPTORG EN TANT QUE RESPONSABLE DE TRAITEMENT

Le Groupe OPTORG est Responsable de Traitement lorsqu'il détermine les finalités et les moyens de ses traitements de données à caractère personnel.

7.1. LE RESPECT DES OBLIGATIONS DU RGPD

En tant que Responsable de Traitement, le Groupe OPTORG respecte les principes suivants :

1. La désignation d'un DPO ;
2. L'utilisation des données à caractère personnel pour des finalités explicites, légitimes et déterminées, en lien avec les métiers du Groupe OPTORG ;
3. La collecte et traitement des DCP strictement utiles : Le Groupe OPTORG applique ainsi le concept de Privacy by Default qui protège les personnes concernées de toute collecte excessive de données ;
4. Une conservation des DCP collectées ne dépassant pas la durée nécessaire et proportionnelle à l'accomplissement des finalités. Au terme de ce délai et des délais prévus par les normes et autorisations de la CNIL ou par la loi, les DCP sont supprimées sur tous les supports et sauvegardes ;

5. Une communication des DCP uniquement aux destinataires autorisés, dans le cadre strict des finalités définies au préalable ;
6. Un choix de Sous-Traitants en fonction de leurs garanties techniques et organisationnelles assurant la protection des données qui leur sont confiées ;
7. Aucun transfert des données collectées effectué à des tiers autres que les sociétés apparentées au Groupe OPTORG intervenant dans le cadre de l'exécution du contrat ;
8. Une politique d'encadrement des transferts de données personnelles hors UE dans le cas de transferts intra-Groupe ou autres (CCT 2010/87/UE, 2016/2295 et 2016/2297) ;
9. L'information préalable, claire et transparente des personnes concernées sur la finalité d'utilisation de leurs données, sur le caractère facultatif ou obligatoire de leurs réponses dans les formulaires, sur les droits dont ils disposent et des modalités d'exercice effectif de ces droits ;
10. Le recueil d'un consentement explicite, éclairé, actif et non équivoque de la personne concernée pour le traitement de ses DCP ;
11. La réalisation d'Analyses d'Impact pour les traitements susceptibles d'entraîner un risque élevé pour les droits et libertés des personnes physiques ;
12. La conception d'outils et de systèmes intégrant au cœur de leurs fonctionnalités et de leur développement le respect du RGPD et de la protection de la vie privée des personnes concernées. La Compagnie OPTORG applique ainsi le concept de Privacy by Design qui permet le développement d'outils et de systèmes responsables ;
13. Une politique de sécurité veillant à prendre toutes les mesures contre les violations de données personnelles, en informant la CNIL dans les 72h et le cas échéant, les personnes concernées, ainsi qu'une documentation des corrections consécutives à une violation ;
14. Une adhésion à des codes de conduite ou le recours à un mécanisme de certification.

7.2. LE RESPECT DES OBLIGATIONS DE SÉCURITÉ DES TRAITEMENTS DES DONNÉES À CARACTÈRE PERSONNEL

Le Groupe OPTORG a élaboré une PSSI (Politique de Sécurité des Systèmes d'Information) pour assurer la sécurité des infrastructures, des ressources et des systèmes d'applications.

Elle a mis en œuvre les mesures de sécurité ci-dessous afin de garantir un niveau de sécurité adapté aux risques liés aux traitements :

1. Sensibiliser et authentifier les utilisateurs ;
2. Gérer les habilitations ;
3. Tracer les accès et gérer les incidents ;
4. Sécuriser les postes de travail et l'informatique mobile ;
5. Protéger le réseau informatique interne ;
6. Sécuriser les serveurs et les sites web ;
7. Sauvegarder et prévoir la continuité d'activité ;
8. Archiver de manière sécurisée ;
9. Encadrer la maintenance et la destruction des données ;
10. Gérer la sous-traitance ;
11. Sécuriser les échanges avec d'autres organismes ;
12. Protéger les locaux ;
13. Encadrer les développements informatiques ;

14. Chiffrer et garantir l'intégrité.

7.3. LE RESPECT DES EXIGENCES DU PRIVACY BY DESIGN ET PRIVACY BY DEFAULT

Les concepts de Privacy by Design et de Privacy by Default permettent la mise en œuvre du principe de « minimisation des données », en garantissant que les données collectées sont, tant qualitativement que quantitativement, strictement nécessaires au traitement.

7.3.1. MESURES TECHNIQUES ET ORGANISATIONNELLES AU TITRE DU PRIVACY BY DESIGN

Pour répondre aux exigences du RGPD, le Groupe OPTORG a mis en place les mesures suivantes concernant les DCP :

- Réduction de leur traitement à un minimum ;
- Pseudonymisation dès que possible ;
- Garantie de la transparence quant aux finalités et aux traitements ;
- Possibilité donnée à la personne concernée de contrôler le traitement de ses DCP ;
- Mise en place de dispositifs de sécurité.

7.3.2. MESURES TECHNIQUES ET ORGANISATIONNELLES AU TITRE DU PRIVACY BY DEFAULT

Le Groupe OPTORG met en œuvre des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les DCP nécessaires sont traitées.
Cela concerne :

- La quantité de DCP collectées ;
- L'étendue de leur traitement ;
- Leur durée de conservation ;
- Leur accessibilité.

Les mesures décrites ci-dessus garantissent par défaut que les données personnelles ne sont pas rendues accessibles à un nombre indéterminé de personnes, sans l'accord de la personne concernée.

8. LES ENGAGEMENTS DE LA COMPAGNIE OPTORG EN TANT QUE SOUS-TRAITANT

Le Groupe OPTORG intervient en qualité de Sous-Traitant lorsque le Client a la qualité de Responsable de Traitement des données à caractère personnel.

Concernant les activités de sous-traitance associées aux contrats européens, le Groupe OPTORG s'appuie, dans ses mises en œuvre, en plus des différents dispositifs légaux, sur les préconisations du **Guide du Sous-Traitant** [1], édité par la CNIL en Septembre 2017, résumées comme suit :

1. Désignation d'un DPO (Data Protection Officer) qui jouera notamment le rôle de représentant dans l'UE pour les contrats établis directement entre un Client donneur d'ordre européen et une filiale du Groupe établie en dehors de l'Union Européenne ;
2. Définition des responsabilités du Client donneur d'ordre et du Groupe OPTORG relativement aux rôles de :
    a) Sous-traitant ;

[1] https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

b) Responsable de Traitement ;

3. Encadrement contractuel détaillé des relations de sous-traitance afin de prendre en compte les dispositions du RGPD ;
4. Interdiction des transferts des données à caractère personnel hors de l'Union Européenne ou dans un pays non-reconnu par la Commission Européenne comme disposant d'un niveau de protection suffisant, sauf si ce transfert est fondé sur :
   - Des Clauses Contractuelles Types (CCT 2010/87/UE) adoptées par la Commission Européenne et règlementant les transferts de données personnelles hors de l'UE ;
   - Une décision d'adéquation ;
5. Respect des finalités des activités de traitement sous-traités et traçabilité des instructions du Client ;
6. Information et obtention du consentement du Client donneur d'ordre en cas de recours à un ou plusieurs Sous-Traitant(s) Ultérieur(s) ;
7. Mise à disposition du Client des documents pouvant l'aider à respecter ses obligations réglementaires en tant que Responsable de traitement ;
8. Traçabilité des actions d'accès ou de manipulations des DCP ;
9. Tenue d'un registre des activités des traitement sous-traitées par le Client donneur d'ordre ;
10. Information immédiate pour tout cas détecté de violation des règles de protection des données à caractère personnel ;
11. Assistance pour la réalisation des études d'impact sur la vie privée chaque fois que possible et souhaité par le Client donneur d'ordre ;
12. Formation et sensibilisation récurrente du personnel du Groupe OPTORG aux principes de confidentialité et aux obligations liées à règlementation sur la protection des données à caractère personnel ;
13. Capacité de démonstration permanente du respect des obligations incluant les garanties de :
    a) Privacy by Design ;
    b) Privacy by Default ;
    c) Sécurisation organisationnelle et technique des DCP.

Afin de préserver la sécurité et la confidentialité des données à caractère personnel traitées, le Groupe OPTORG s'engage sur :

1. Des mesures de sécurité physique afin d'empêcher les personnes non autorisées d'accéder à ses infrastructures ;
2. Un système de gestion des permissions permettant de limiter l'accès aux locaux et aux données aux seules personnes habilitées, dans le cadre de leurs fonctions et de leurs périmètres d'activité ;
3. Un système d'isolation physique et/ou logique de ses différents Clients ;
4. Une politique stricte de gestion des mots de passe permettant une authentification forte des utilisateurs et des administrateurs ;
5. Le fait de s'assurer qu'au cours du traitement, pendant le transfert et après le stockage, les données à caractère personnel ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation ;
6. Un dispositif permettant de tracer l'ensemble des actions réalisées sur notre système d'information et d'effectuer, conformément à la réglementation en vigueur, des rapports en cas d'incident affectant les données du Client.

Le Groupe OPTORG peut être amenée à accéder aux données du client :

1. Dans le cadre d'obligations légales suite à des demandes judiciaires et/ou administratives ;
2. Afin d'assurer le bon fonctionnement des services ;

3. Dans le cadre de prestations de support pouvant impliquer un accès à distance aux données du Client par d'autres entités de la Compagnie OPTORG situées dans des pays non reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant.

Dans tous ces cas de figure, l'accès aux données à caractère personnel est soumis :

1. Aux règles de transfert exposées plus haut ;
2. A des accréditations et habilitations particulières par le client.

8.1. INSTRUCTIONS DU CLIENT

Le Groupe OPTORG s'engage à traiter les données à caractère personnel :

- Dans le cadre du contrat qui le lie avec son Client ;
- Dans le respect des instructions documentées et communiquées par le Client au fur et à mesure de l'exécution de la prestation.

Le Groupe OPTORG informera immédiatement le Client si elle considère qu'une instruction de ce dernier constitue une violation du RGPD, de la présente PPDCP ou d'autres dispositions du droit de l'UE ou du droit français relatives à la protection des données à caractère personnel. Cette information sera adressée par écrit et dans un temps compatible avec sa prise en compte par le Client.

8.2. SORT DES DONNÉES À LA FIN DU CONTRAT DE SOUS-TRAITANCE

En tant que Responsable de Traitement, le Groupe OPTORG met en œuvre la suppression des données de manière régulière et selon les exigences légales.

En tant que Sous-Traitant et au terme de la prestation de service relative au traitement, le Groupe OPTORG s'engage à :

- Traiter les données uniquement sur instruction documentée du Client ;
- Supprimer ou restituer toutes les données selon le choix du Client ;
- Détruire toutes les copies existantes et envoyer au Client une attestation de destruction de toutes les copies existantes de ses données.

9. PERSONNES CONCERNÉES PAR LES TRAITEMENTS DES DCP

Le Groupe OPTORG, en qualité de Responsable de Traitement, effectue des traitements sur les DCP communiquées directement par les catégories de personnes physiques suivantes :

1. Visiteurs des sites internet et extranet (consultation) ;
2. Utilisateurs des sites internet et extranet (dépôt de formulaires de candidature, etc…) ;
3. Prospects ;
4. Clients ;
5. Partenaires commerciaux ;
6. Fournisseurs et Sous-Traitants ;
7. Collaborateurs et dirigeants du Groupe OPTORG ou de l'une de ses filiales ;
8. Candidats/Intérimaires ;
9. Retraités et personnes ayant auparavant occupé des fonctions au sein de la Compagnie ;

10. Famille, personnes à charge ou d'autres personnes en relation avec les collaborateurs liés au Groupe OPTORG par un contrat de travail.

10. DONNÉES À CARACTÈRE PERSONNEL TRAITÉES

La présente PPDCP s'applique au traitement des informations personnelles des candidats et des collaborateurs du Groupe OPTORG, dans le cadre de(s) :

- Activités de recrutement menées à la fois en ligne par le biais de son site web ou de sites web tiers ou hors ligne, lors d'un événement de recrutement, d'un entretien téléphonique ou en face à face ;
- La gestion des ressources humaines et de l'exécution du contrat de travail.

Le Groupe OPTORG traite les catégories d'informations personnelles suivantes selon les conditions énoncées à la section 9 et 14 de la présente PPDCP :

1. **Données d'identification/état civil :** Nom, prénom, civilité, adresse postale ou/et électronique, coordonnées téléphoniques, numéro de sécurité sociale pour la déclaration préalable à l'embauche (DPAE) ou la déclaration sociale nominative (DSN) auprès de l'URSSAF ;
2. **Données de vie professionnelle :** Formation, diplômes, certificats et attestations, langues étrangères pratiquées, compétences, Curriculum vitae, références professionnelles, évaluations professionnelles , suivi des demandes de formation professionnelle et des périodes de formation effectuées, évaluation des connaissances et des formations, dates des entretiens d'évaluation,, compétences professionnelles du salarié, objectifs assignés, résultats obtenus, appréciation des aptitudes professionnelles sur la base de critères objectifs et présentant un lien direct et nécessaire avec l'emploi occupé, observations et souhaits formulés par l'employé, prévisions d'évolution de carrière, documents de suivi de l'activité des salariés, notes de frais, annuaires, élections professionnelles, suivi et maintenance des matériels informatiques mis à disposition, véhicules et cartes de paiement, date et conditions d'embauche ou de recrutement, date, objet et motif des modifications apportées à la situation professionnelle du salarié, simulation de carrière, désirs du salarié en termes d'emploi, sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés, suivi administratif des visites médicales, casier judiciaire (B3) ;
3. **Données de vie personnelle :** Situation matrimoniale et nombre d'enfants, nationalité, statut d'immigration et de visa, hobbies, loisirs, catégorie de permis de conduire, mobilité géographique, délai de disponibilité ;
4. **Informations d'ordre économique et financière :** salaire brut, prétentions salariales, coordonnées bancaires pour le versement du salaire, informations de rémunération (variables, primes…) ;
5. **Données de connexion :** adresse IP, connexions et logs de connexion des salariés, gestion des outils informatiques, gestion de la téléphonie (numéros appelés, numéros des appels entrants, identité de l'utilisateur du service téléphonique…), vidéosurveillance (etc..) géolocalisation, contrôles d'accès sur les lieux de travail, données relatives au paiement des repas, contrôle des horaires (éléments d'identification et données utilisées pour le suivi du temps de travail), autorisations d'accès aux applications et aux réseaux.

Le Groupe OPTORG peut avoir besoin de mettre ces DCP à disposition :

- D'autres entités du Groupe ;
- De prestataires de services externes tels que les prestataires de gestion de paie, etc….

Dans le respect de la présente PPDCP, le Groupe OPTORG s'engage à limiter la collecte des DCP

à leur strict nécessaire.

11. CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL TRAITÉES

Les catégories particulières de DCP sont des Données Sensibles au sens RGPD du terme.
Ce sont des données génétiques ou biométriques permettant d'identifier une personne physique de manière unique, un Numéro d'identification national unique (NIR pour la France) comme le numéro de sécurité sociale ou alors des données concernant :

- L'origine raciale ou ethnique ;
- Les opinions politiques ;
- Les convictions religieuses ou philosophiques ;
- L'appartenance syndicale ;
- La santé ;
- Les condamnations pénales ou infractions ;
- L'orientation sexuelle.

Le traitement de ces catégories particulières de DCP ne peut s'effectuer sans le consentement explicite des personnes concernées, à moins que le traitement ne soit autorisé sur d'autres bases juridiques.
En tout état de cause, le Groupe OPTORG veille à respecter la réglementation en vigueur.

12. FINALITÉS DES TRAITEMENTS ET BASES JURIDIQUES APPLICABLES

Le RGPD exige que tout traitement de données à caractère personnel repose sur un fondement juridique.
Le Groupe OPTORG traitera toutes les données à caractère personnel selon les finalités déterminées et les bases juridiques applicables, telles qu'elles sont définies par le RGPD et exposées ci-après :

1. Le consentement de la personne concernée ;
2. Le respect d'une obligation légale ;
3. L'exécution d'un contrat ou l'exécution de mesures précontractuelles ;
4. La sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
5. L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le Responsable de Traitement ;
6. A des fins d'intérêts légitimes poursuivis par le Responsable de Traitement, sous réserve de ne pas ignorer l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le Groupe OPTORG se réserve le droit d'inclure des finalités spécifiques qui seront communiquées aux personnes concernées sur des supports contractuels spécifiques complétant ou dérogeant à la présente Politique de Protection des Données à Caractère Personnel.

12.1. LE CONSENTEMENT

Conformément au RGPD et à chaque fois que le Groupe OPTORG agira en tant que Responsable de Traitement, il s'attachera à obtenir le consentement des personnes concernées pour les finalités le nécessitant.

12.1.1. FINALITÉS DES TRAITEMENTS BASÉS SUR LE CONSENTEMENT

Les finalités suivantes nécessitent le consentement explicite des personnes concernée :

1. Démarchage portant sur des produits et services ;
2. Prospection commerciale par courrier électronique ;
3. Établissement de statistiques liées au trafic sur les sites internet du Groupe OPTORG ;
4. Établissement de fichiers à des fins de statistiques commerciales ;
5. Participation à des opérations de promotion commerciale ;
6. Amélioration de l'expérience client ;
7. Réalisation d'enquêtes de satisfaction ;
8. Géolocalisation ;
9. Cookies.

12.1.2. FINALITÉS DES TRAITEMENTS NON-BASÉS SUR LE CONSENTEMENT

Lorsqu'elles sont basées sur l'exécution d'un ou plusieurs contrats ou sur l'exécution de mesures précontractuelles, afin de respecter la réglementation en vigueur ou afin de permettre au Groupe OPTORG de protéger ses intérêts légitimes, les finalités suivantes ne nécessitent pas le consentement explicite des personnes concernées :

1. Analyse de risques et détermination des besoins du client ou du prospect ;
2. Exercice du devoir de conseil ;
3. Exécution d'un contrat de travail ;
4. Amélioration de l'expérience client ;
5. Réalisation d'enquêtes de satisfaction ;
6. Participation à des opérations de promotion commerciale ;
7. Exécution de toutes obligations d'ordre public ;
8. Établissement de fichiers à des fins statistiques.

12.1.3. RECUEIL ET TRAÇABILITÉ DU CONSENTEMENT

En tant que Responsable de Traitement, le Groupe OPTORG doit démontrer que le consentement de la personne concernée au traitement de ses DCP a été obtenu de manière libre, éclairée et univoque. Le mécanisme de traçabilité mis en place par le Groupe OPTORG lui permet de répondre à cette exigence majeure du RGPD en :

- Apportant la preuve du consentement ;
- Assurant l'intégrité de ce consentement dans le temps.

CAS PARTICULIER DU PROFILAGE

Le Groupe OPTORG est susceptible d'utiliser et de compiler des DCP à des fins de profilage. Le traitement automatisé sert à évaluer, analyser et prédire les préférences ou les intérêts de la personne concernée mais peut produire des effets juridiques la concernant ou l'affectant de manière significative.

Le Groupe OPTORG s'engage à informer la personne concernée et à obtenir son consentement explicite avant tout traitement de profilage.

13. UTILISATION DES COOKIES

Les visiteurs et utilisateurs des sites internet du Groupe OPTORG peuvent se référer aux mentions légales de ces sites pour prendre connaissance des conditions d'utilisation des cookies.

14. LE RESPECT DU PRINCIPE D'ACCOUNTABILITY PAR LA COMPAGNIE OPTORG

Le Groupe OPTORG a mis en œuvre des mécanismes et des procédures internes permettant de démontrer à tout moment et de manière continue le respect des règles imposées par le RGPD, notamment à travers la mise en place de mesures techniques et organisationnelles et d'une obligation de documentation. Ces mesures sont réexaminées et actualisées si nécessaire.

Le Groupe OPTORG peut ainsi démontrer le respect des principes relatifs au traitement des données personnelles tels que :

1. Licéité, loyauté et transparence des traitements ;
2. Limitation des finalités ;
3. Minimisation ;
4. Exactitude des DCP ;
5. Limitation de la durée de conservation ;
6. Intégrité et confidentialité des DCP.

14.1. MISE EN PLACE DE MESURES TECHNIQUES

1. Le chiffrement des données confidentielles ;
2. La gestion des droits d'accès ;
3. Les outils de lutte contre les intrusions extérieures dans le réseau (firewall, anti-virus) ;
4. La politique des mots de passe (complexité, changement régulier) ;
5. La protection via des flux sécurisés (TSL/SSL, https, sftp).

14.2. MISE EN PLACE DE MESURES ORGANISATIONNELLES

1. Procédure de cartographie des données ;
2. Revue des contrats (sous-traitants, partenaires, salariés, clients) ;
3. Sensibilisation/formation des équipes métiers et IT ;
4. Tenue du registre des activités de traitement ;
5. Politique de minimisation des données (Privacy by Design/Privacy by Default) ;
6. Analyse de risque (PIA) ;
7. Gestion des droits des personnes.

14.3. DOCUMENTATION DE L'ACCOUNTABILITY

Soucieux de l'importance de la protection des DCP, le Groupe OPTORG a mis en place tous les éléments de documentation permettant de démontrer sa conformité au RGPD.

Cette documentation est mise à jour de façon régulière et inclut :

1. **Les procédures internes relatives au Privacy by Design, au Privacy by Default et aux analyses d'impact sur la vie privée, comprenant :**
    a) La documentation permettant de démontrer la prise en compte de la protection des DCP dans le cadre d'implémentation de nouveaux produits ;
    b) Les modèles d'analyse d'impact ainsi que les analyses d'impact réalisées, y compris leurs mises à jour ;
    c) Les raisons ayant conduit le Responsable de Traitement à ne pas réaliser d'analyse d'impact pour un traitement présentant potentiellement un risque élevé ;
    d) Les règles de revue des analyses d'impact à réaliser en cas de changements relatifs aux traitements ou après une certaine durée (tous les 3 ans).

2. **La désignation d'un DPO**
    a) La lettre de mission du DPO ;
    b) Les motifs de non-désignation d'un DPO si c'est le cas ;
    c) La déclaration du DPO à la CNIL ;
    d) Les éléments permettant d'établir que le DPO fait régulièrement rapport de ses missions au niveau le plus élevé de la direction ;
    e) Les qualifications professionnelles du DPO.

3. **Les relations contractuelles avec les Sous-Traitants**
    a) Les contrats avec les sous-traitants ;
    b) La politique de suivi encadrant les relations de sous-traitance (modèles de questionnaires adressés régulièrement aux sous-traitants et réponses à ces questionnaires) ;
    c) Les modalités d'audit des sous-traitants ;
    d) Les résultats des audits réalisés et les actions prises en conséquence ;
    e) Les accords de coresponsabilité avec d'autres Responsables de Traitement participant au traitement des DCP.

4. **La politique de sécurité**
    a) La politique de sécurité des systèmes d'information et la documentation décrivant les mesures prises pour assurer la sécurité des DCP (pseudonymisation et chiffrement) ;
    b) Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    c) Les moyens permettant de rétablir la disponibilité des DCP et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
    d) Les plans de test visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et les résultats des tests de sécurité réalisés ;
    e) La politique de gestion des habilitations et des accès.

5. **Les violations de données personnelles**
    a) La politique interne relative aux violations de données personnelles et les coordonnées des personnes à contacter ;
    b) Le registre des violations de données personnelles et des notifications aux personnes concernées et à la CNIL ;
    c) Les éléments justifiant la décision du Responsable de Traitement de ne pas envoyer de notification aux personnes concernées en cas de violations de leurs DCP.

6. **Les transferts de données personnelles vers les Pays Tiers et les mécanismes de transfert mis en œuvre :**
    a) Le récapitulatif des transferts de DCP et le mécanisme de transfert retenu pour chacun ;
    b) La documentation relative à la mise en œuvre des transferts en fonction du mécanisme choisi :
        i. Les BCR et leur décision d'approbation par la CNIL ;
        ii. Les Clauses Contractuelles Types de protection des données personnelles signées avec les importateurs et les exportateurs de DCP ;
        iii. Les clauses contractuelles ad hoc approuvées par la CNIL et la décision d'approbation ;
        iv. Les documents relatifs aux transferts effectués sur la base des « exceptions » de l'article 49 du RGPD, comme la preuve du consentement de la personne concernée ou l'analyse relative à la mise en balance des intérêts de la personne concernée et du Responsable de Traitement ;
        v. Les décisions d'adéquation.

7. **La politique de protection des données personnelles**
    a) La politique de confidentialité des données à caractère personnel (PPDCP) ;
    b) La politique de conservation des DCP (durée de conservation et délais de destruction ainsi que les règles d'archivage intermédiaire) ;
    c) Les procédures mises en œuvre pour assurer le respect des droits des personnes concernées ;
    d) Les modèles des principales clauses d'information et de recueil du consentement figurant dans les contrats, sur le site internet et les autres principaux canaux de communication avec les personnes concernées ;
    e) La documentation relative à la gestion des demandes des personnes concernées, comprenant les demandes d'exercice de leurs droits et les réponses apportées ;
    f) Le mécanisme mis en œuvre permettant d'assurer la traçabilité et le suivi des droits exercés par les personnes concernées.

8. **Les codes de conduite et la certification** :
    a) Le document attestant de l'adhésion à un code de conduite et la documentation associée ;
    b) Les certifications.

9. **Le plan de contrôle de conformité**

10. **La correspondance avec la CNIL**
    a) L'historique des correspondances avec la CNIL
        i. Consultation préalable consécutive à une analyse d'impact ;
        ii. Notification de violation de données personnelles ;
        iii. Contrôle ou demande d'information de la part de la CNIL.

11. **La tenue du Registre des Traitements**

Tous les traitements doivent figurer dans le Registre des Traitements.
A ce titre et en fonction de ses rôles, le Groupe OPTORG tient plusieurs registres :

1. Un Registre de traitement en tant que Responsable de Traitement, où les

traitements fondés sur le consentement de la personne concernée sont séparés des traitements fondés sur des bases légales ;
2. Un Registre de Traitement en tant que Sous-Traitant ;
3. Un Registre de Traitement de Notification des violations de DCP.

La tenue des registres est dynamique, avec une mise à jour en fonction de l'évolution des traitements existants (y compris de leur suppression) ainsi que de la création de nouveaux traitements.

15. DURÉE DE CONSERVATION DES DCP

Les DCP des personnes concernées sont conservées dans le cadre des finalités annoncées, en respect des prescriptions légales en vigueur, notamment en matières civile, fiscale, commerciale et pénale.

Les données ayant pour finalité la gestion du recrutement sont conservées, sauf demande contraire, pendant deux ans à compter de leur réception ou du dernier contact avec le candidat.

Les données ayant pour finalité la gestion du personnel sont conservées pendant toute la durée de l'exécution du contrat du salarié. Certaines données peuvent être conservées au-delà, mais toujours dans les délais légaux en vigueur dans la réglementation.

Les données ayant pour finalité la prospection ou le démarchage commercial sont conservées pendant trois ans à compter de leur réception ou du dernier contact avec le client prospect.

Archivage intermédiaire : L'accès aux DCP conservées dans ce cadre est strictement limité. A la fin du délai de conservation, les DCP seront détruites ou anonymisées afin qu'il ne soit plus possible d'identifier les personnes concernées.

16. TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL

Le Groupe OPTORG s'engage à respecter l'ensemble des obligations en matière de transfert de données à caractère personnel vers un pays tiers et notamment à conclure un acte juridique contraignant avec le destinataire des données comme des Clauses Contractuelles Types ou des BCR.

Le Groupe OPTORG s'engage à ne transmettre des données à ses filiales ou à des tiers « Destinataires des Données » que lorsque cela s'avère strictement nécessaire.

Dans ce cas, le Groupe OPTORG s'assurera que le « Destinataire des Données » présente au moins le même niveau de sécurité dans son traitement des données.

Conformément au RGPD, la sous-traitance des données fera l'objet d'un accord écrit entre le Groupe OPTORG et le Sous-Traitant, engageant ce dernier à n'opérer aucun transfert de données sans l'autorisation du Groupe OPTORG.

Si un transfert de données doit être opéré en dehors de l'Union Européenne, le Groupe OPTORG s'engage à n'y procéder que dans ces conditions :

- Le « Destinataire des Données » se trouve dans un État considéré par la

Commission européenne comme assurant un niveau de protection adéquat ;

- Le « Destinataire des Données » présente des Clauses Contractuelles Types de la Commission européenne ;
- Tout Sous-Traitant Ultérieur situé hors UE devra répondre à au moins l'une des conditions énoncées précédemment.

17. DROITS DES PERSONNES

Conformément à la réglementation, les personnes concernées disposent du :

1. Droit d'information avant toute collecte de DCP ;
2. Droit d'obtenir la confirmation que les DCP sont ou ne sont pas traitées ;
3. Droit d'accès permettant d'obtenir les informations suivantes :
   a) Finalités du traitement ;
   b) Catégories de données personnelles concernées ;
   c) Destinataires ou catégories de destinataires auxquels les données personnelles ont été ou seront communiquées ;
   d) Garanties appropriées en cas de transfert des données vers un pays tiers ;
   e) Durée de conservation des données envisagée ou les critères utilisées pour déterminer cette durée ;
   f) Existence du droit de demander au Responsable du Traitement la rectification ou l'effacement des données, la limitation du traitement, ou le droit de s'y opposer ;
   g) Droit d'introduire une réclamation auprès de la CNIL ;
   h) Information sur la source en cas de collecte indirecte de DCP ;
   i) Existence d'une prise de décision automatisée et/ou de profilage et les conséquences sur la personne concernée ;
4. Droit à la rectification ;
5. Droit à la limitation ;
6. Droit à l'oubli ;
7. Droit d'opposition concernant un traitement spécifique pour lequel un consentement explicite a été nécessaire (retrait du consentement) ;
8. Droit à la portabilité des données ;
9. Droit de de ne pas faire l'objet d'une décision fondée sur un procédé automatisé ;
10. Droit de ne pas faire l'objet de profilage ;
11. Droit post mortem.

Toute personne concernée pourra exercer ses droits, accompagnés d'un justificatif d'identité soit :

- Par l'envoi d'un mail à dpo@optorg.com ;
- Par courrier à :

Compagnie OPTORG
Délégué à la Protection des Données
49-51, Quai de Dion Bouton 92800 Puteaux – France

Le Groupe OPTORG :

- Se réserve le droit de réclamer au demandeur des pièces complémentaires justifiant son identité ;
- Informe les personnes concernées qu'en conformité aux règles d'ordre public en vigueur, certaines données ou certaines finalités ne pourront faire l'objet d'une réponse favorable aux demandes.

Si une personne concernée estime ne pas avoir pu exercer ses droits conformément au RGPD

ou à toute disposition légale en vigueur en matière de protection des données, elle pourra formuler une réclamation auprès de la :
Commission nationale de l'informatique et des libertés (CNIL)
3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07.

18. CONFIDENTIALITÉ RENFORCÉE ET ACCÈS AUX DCP

Tous les collaborateurs et intervenants du Groupe OPTORG sont sensibilisés aux principes de protection des données, par des formations régulières adaptées à leur activité et à leurs responsabilités. Ils ont uniquement accès aux informations nécessaires à leur activité.
L'accès aux données sensibles fait l'objet d'habilitations et de contrôles.
Le Groupe OPTORG garantit en outre que ses collaborateurs sont soumis à une stricte obligation de confidentialité et s'engage à faire signer par toutes les personnes susceptibles d'accéder à des données à caractère personnel un engagement individuel de confidentialité.
Le Groupe OPTORG s'engage également à ce que ses Sous-Traitants et ses éventuels Sous-Traitants Ultérieurs soient tenus par cette obligation spécifique.
Cependant, et malgré toute la rigueur et toutes les précautions apportées à la mise en œuvre de la protection des DCP, il n'est pas possible d'en garantir la sécurité absolue, en raison de l'évolution des techniques d'intrusion et des risques inévitables pouvant survenir lors de leur transmission.

19. VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL

Au sens du RGPD, une violation des DCP est une violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou non autorisée de DCP transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

19.1. NOTIFICATION DE VIOLATION DES DCP EN TANT QUE SOUS-TRAITANT

Il appartient au Client, et à lui seul, de notifier les éventuelles violations de sécurité à la CNIL.
Le Groupe OPTORG s'engage à notifier au Client, dans les meilleurs délais et pour permettre à celui-ci de respecter le délai légal de 72h maximum, toute violation de donnée à caractère personnel qu'il aurait subi.

En cas de retard dans la communication de la violation, le Groupe OPTORG accompagnera sa notification des motifs expliquant ce retard.

La violation de données est communiquée à l'interlocuteur désigné par le Client et précisera :

1. La nature de la violation des données, y compris, si possible :
    a) Les catégories et le nombre approximatif de personnes concernées par la violation ;
    b) Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernées ;
2. Le nom et les coordonnées du DPO du Groupe OPTORG ;
3. Les conséquences probables de la violation de données ;
4. Les mesures déjà prises ou celles qui sont proposées pour y remédier.

Si le Groupe OPTORG est dans l'incapacité de fournir l'ensemble de ces informations dans le délai imparti, il procédera en deux temps en envoyant :

1. Une notification initiale immédiate dès le constat de la violation ;
2. Une notification complémentaire dans le délai de 72 heures si possible après la notification initiale.

En cas de violation de données, le Groupe OPTORG prendra, dès que possible, toutes les mesures nécessaires pour remédier et diminuer l'impact de la violation et informera le Client des mesures prises et des résultats attendus et constatés.

Le Groupe OPTORG s'engage à collaborer activement avec le Client pour qu'il soit en mesure de répondre à :

- Ses obligations règlementaires et contractuelles ;
- Aux interrogations de la CNIL.

19.2. NOTIFICATION DE VIOLATION DES DCP EN TANT QUE RESPONSABLE DE TRAITEMENT

En sa qualité de Responsable de Traitement, le Groupe OPTORG s'attache à garantir une sécurité des traitements opérés sur les DCP, afin d'éviter toute violation de celles-ci.

Néanmoins, en cas de violation de données personnelles, le Groupe OPTORG respectera l'obligation de notifier la violation en question à la CNIL, dans les meilleurs délais, et si possible dans les 72 heures suivant sa prise de connaissance, sauf si la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Au-delà des 72 heures, la notification que le Groupe OPTORG communiquera à la CNIL précisera les motifs du retard.

19.3. PROCESSUS DE GESTION ET DE PREVENTION DES RISQUES ET DES INCIDENTS

Afin de prévenir les violations et d'en limiter les incidences, le Groupe OPTORG a défini et mis en place un dispositif de détection des intrusions et une procédure de gestion des incidents.

19.3.1. DÉTERMINATION DE MESURES PRÉVENTIVES

1. La mise en place d'une solution de sauvegarde efficace et sécurisée ;
2. Le recours à des procédés de cryptage ;
3. La limitation de l'accessibilité aux données personnelles ;
4. La traçabilité des comptes disposant d'un « accès global » à une base de données ;
5. Le stockage sécurisé des mots de passe ;
6. Le contrôle permanent des vulnérabilités potentielles des technologies utilisées et la mise à jour des logiciels ;
7. L'information des salariés des conséquences des potentielles violations de données ;
8. L'application du Privacy by Design et du Privacy by Default ;
9. Les dispositions prises dans le cadre des analyses d'impact sur la vie privée.

19.3.2. NOTIFICATION ÉVENTUELLE AUX PERSONNES CONCERNÉES

Lorsqu'une violation de DCP est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée, le Groupe OPTORG en tant que Responsable de Traitement s'engage à **:**

- La tenir informée dans les meilleurs délais ;

- Lui proposer des recommandations et des mesures de protection pour atténuer le préjudice subi.

La notification :

- Sera libellée en termes clairs et simples pour être facilement compréhensible ;
- Contiendra les mêmes informations que celles communiquées à la CNIL.

20. CONTRÔLE DE LA CNIL

Le Groupe OPTORG est tenue de coopérer avec la CNIL, à la demande de celle-ci.
Dans le cas où le contrôle concernerait des traitements mis en œuvre au nom et pour le compte d'un de ses Clients, le Groupe OPTORG s'engage à l'en informer immédiatement et à ne prendre aucun engagement pour lui.

En cas de contrôle de la CNIL auprès d'un Client et portant sur les services délivrés par le Groupe OPTORG en tant que Sous-Traitant, ce dernier s'engage à coopérer avec le Client et à lui fournir toute information dont la CNIL pourrait avoir besoin.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le Groupe OPTORG en tant que Responsable de Traitement, celui-ci s'interdit de communiquer ou de faire état des données à caractère personnel d'un Client dont il serait le Sous-Traitant.

21. AUDIT

Pour s'assurer du respect des obligations du RGPD, les Clients peuvent réaliser une fois par an un audit sous forme de questionnaire ou d'une demande d'information sur le niveau de conformité RGPD du Groupe OPTORG.

Par ailleurs, et dans le même esprit, le Groupe OPTORG, en tant que Responsable de Traitement, exercera son droit d'audit sur ses propres Sous-traitants et procèdera de même avec les Sous-Traitants Ultérieurs si cela se révèle nécessaire.

22. RÉVISION

La présente PPDCP sera révisée chaque fois que nécessaire en cas d'une :

- Évolution de la jurisprudence ;
- Décision de la CNIL ;
- Nouvelle règlementation en matière de protection des données à caractère personnel.