RGPD

Politique relative à la Protection des Données à Caractère Personnel

Libellé	Politique de Protection des Données à Caractère Personnel (« la Politique »)
Direction émettrice	Direction Juridique Groupe – DPO Groupe - Equipe Data Privacy
Validation	DG Corporate Finance
Responsable(s) du document	DPO Groupe Adjointe DPO Groupe
Diffusion	**Publique**

Version	8e version : 02/10/2025

Ce document est diffusé à l'ensemble des collaborateurs du Groupe Diot Siaci et peut être diffusé dans le cadre de relations commerciales (clients, porteurs de risques, sous-traitants).

GLOSSAIRE

CNIL : Commission Nationale de l'Informatique et des Libertés.

Donnée à caractère personnel ou Donnée(s) : Toute information se rapportant à une personne physique identifiée ou identifiable (article 4.1 du RGPD).

Donnée sensible : Donnée à caractère personnel se rapportant notamment à l'origine raciale ou ethnique, aux convictions politiques, philosophiques ou religieuses, à l'appartenance syndicale, à l'état de santé, à la vie sexuelle ou à l'orientation sexuelle d'une personne. Sont également considérées comme sensibles les données génétiques ainsi que les données biométriques utilisées pour identifier un individu.

Donnée de santé : Donnée à caractère personnel concernant l'état physique ou mental d'une personne, y compris les informations liées à la prestation de soins, et permettant de révéler des éléments relatifs à son état de santé (article 4.15 du RGPD).

DPO : Data Protection Officer ou Délégué à la Protection des Données.

Entité : toute société faisant partie du Groupe Diot Siaci.

Groupe Diot-Siaci ou **Groupe** : désigne la société la Diot-Siaci Symphony TopCo, société par actions simplifiée de droit luxembourgeois dont le siège social est situé au 4 rue du Fort Wallis, L-2714 Luxembourg, Grand-Duché de Luxembourg, immatriculée au Registre du commerce et des sociétés, Luxembourg sous le numéro B298362, et toute entité qui est contrôlée, directement ou indirectement, par cette dernière, au sens de l'article L.233-3 du Code de commerce.

NIR : Numéro d'Inscription au Répertoire national, également nommé « numéro de sécurité sociale ».

Loi Informatique et Libertés : Loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée notamment par l'ordonnance n° 2018-1125 du 12 décembre 2018 et par la loi n° 2018-493 du 20 juin 2018, et consolidée dans sa version en vigueur.

Responsable de traitement : Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

RGPD : Règlement Général sur la Protection des Données à caractère Personnel. S'agissant d'un Règlement européen, il est d'application directe dans l'ordre juridique des pays membres de l'Union européenne. En France, le RGPD est intégré à la Loi Informatique et Libertés.

Sous-traitant : Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel pour le compte du Responsable du traitement.

SOMMAIRE

GLOSSAIRE 3
1. CONTEXTE 5
1.1. CONTEXTE REGLEMENTAIRE 5
1.2. CONTEXTE INTERNE 5
2. DOMAINE D'APPLICATION 6
3. OBJET DE LA POLITIQUE 6
4. ORGANISATION DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DU GROUPE DIOT SIACI 7
4.1. GOUVERNANCE DE LA PROTECTION DES DONNEES 7
4.1.1. Le DPO 7
4.1.2. L'équipe Data Privacy 8
4.1.3. Les Correspondants à la « Protection des Données » (CPD) 8
4.1.4. Les Compliance Officers des filiales à l'international 9
4.1.5. Le Directeur de la Sécurité des Systèmes d'Information (DSSI) 9
4.2. ROLES ET RESPONSABILITES DES ACTEURS 10
4.3. DISPOSITIFS DE PILOTAGE ET DE SUIVI 12
4.4. DISPOSITIFS DE FORMATION 13
4.5. DISPOSITIFS DE CONTROLE 13
4.5.1. Contrôles de conformité 13
4.5.1.1. Audits internes 13
4.5.1.2. Contrôles internes 14
4.5.1.3. Audits des systèmes d'information 14
4.5.1.4. Contrôles et audits des Sous-traitants 14
4.5.1.5. Audits réalisés par des tiers 14
5. PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL 15
5.1. LICEITE, LOYAUTE ET TRANSPARENCE 15
5.2. ORGANISATION ET SUPERVISION DES TRAITEMENTS 16
5.2.1. Registre des traitements 16
5.2.2. Responsabilisation - "Accountability" 16
5.2.3. Analyse d'impact relative à la protection des Données 17
5.2.4. Privacy by design et privacy by default 17
5.2.5. Contractualisation avec les Tiers 18
5.2.6. Gestion des contrôles CNIL 18
5.3. SECURITE ET INTEGRITE DES DONNEES 18
5.3.1. Gouvernance de la sécurité des systèmes d'information 18
5.3.2. Gestion des incidents et des violations de Données à caractère personnel 19
5.4. DROITS DES PERSONNES CONCERNEES 19
5.4.1. Garanties offertes par le Groupe en matière de droits des personnes 19
5.4.2. Traitement des demandes d'exercice de droits 20
5.4.3. Modalités de contact pour l'exercice des droits 20
5.5. TRANSFERTS DE DONNEES 20
5.6. CONSERVATION ET SORT DES DONNEES 21
5.6.1. Le Groupe en qualité de Responsable du traitement 21

5.6.2. Le Groupe agissant en qualité de Sous-traitant 22

1. CONTEXTE

1.1. CONTEXTE REGLEMENTAIRE

La Loi Informatique et Libertés puis le RGPD, entré en application le 25 mai 2018, ont mis en place un cadre règlementaire fort visant à la protection des Données à caractère personnel au sein de l'Union européenne. Dans cette lignée, la plupart des Etats ont adopté des réglementations relatives à la protection des données.

Les personnes sont aujourd'hui très attentives à leurs Données (notamment les Données financières ou de santé) et à leur protection afin d'en préserver la confidentialité. Elles attendent que leur vie privée soit respectée et que les entreprises auxquelles elles confient leurs Données soient en mesure de les protéger.

C'est pour ces raisons que le Groupe Diot Siaci (ci-après désigné par le « Groupe ») travaille à garantir la sécurité des Données qui lui sont confiées. Au-delà du respect de la réglementation en la matière, il s'agit de l'essence même des activités qui lui sont confiées.

La présente Politique de protection des Données à caractère personnel s'appuie donc principalement sur le Règlement Général sur la Protection des Données (RGPD), qui constitue le cadre juridique de référence pour le traitement des Données à caractère personnel au sein de l'Union européenne.

Les Entités du Groupe Diot Siaci, situées en dehors de l'Union européenne, doivent mettre en œuvre, en complément des mesures stipulées dans la présente Politique, les mesures nécessaires à leur conformité aux réglementations locales qui leur sont applicables en matière de protection des Données à caractère personnel.

Pour garantir une conformité rigoureuse, la présente Politique intègre les pratiques et recommandations définies au sein des corpus documentaires suivants :

- Les recommandations de la CNIL : en particulier, les bonnes pratiques définies au sein du Pack de conformité Assurance spécifiquement conçu pour les activités et besoins des acteurs du secteur de l'assurance.
- Les publications du Comité Européen de la Protection des Données (« CEPD », ou *European Data Protection Board*).
- La Politique de Sécurité de l'Information du Groupe (« PSI Groupe »), qui énonce et définit les objectifs de sécurité de l'information ainsi que les moyens techniques et organisationnels mis en œuvre pour les atteindre.

1.2. CONTEXTE INTERNE

Le Groupe Diot Siaci est un leader européen du conseil et de courtage en assurance de biens et de personnes notamment pour les entreprises.

Dans le cadre de ses activités, le Groupe Diot Siaci est amené à collecter et traiter des Données à caractère personnel y compris des Données sensibles, pour son propre compte (en qualité de Responsable de traitement), en association avec d'autres Responsables de traitement (en qualité de Responsable conjoint de traitement) ou pour le compte de Responsables de traitements (en qualité de Sous-traitant).

Son activité est exercée en France, dans l'Union Européenne et dans le monde entier.

Le Groupe Diot Siaci est organisé en Business Unit (« BU ») (regroupant les activités similaires de plusieurs Entités du Groupe) et Directions (*pour plus d'information :* https://www.diot-siaci.com/fr/notre-groupe/) :

- Diot Siaci Corporate Solutions (« DSCS ») (y compris l'activité PRRA et Mid Market) ;
- Protection Sociale France et Internationale (« PSFI ») ;
- Mobilité Internationale (« MSH ») ;
- Conseil RH et Epargne Retraite (« Conseil ») ;
- Diot Siaci Trade Finance (« DSTF ») ;
- International ;
- Corporate (incluant la DSI, les fonctions Juridique, Risques et Conformité et DPO) ;
- Ressources Humaines (« RH »).

Grâce à la mise en œuvre rigoureuse de cette Politique et aux mesures mises en place à cet effet, le Groupe Diot Siaci maitrise pleinement les risques liés à la gestion des Données. Cette démarche proactive permet de préserver l'image et la réputation du Groupe Diot Siaci, de garantir la confiance des clients et des collaborateurs, et de sécuriser sa position sur le marché.

En assurant la conformité avec les exigences réglementaires et les bonnes pratiques et en appliquant ces principes à ses activités quotidiennes, le Groupe Diot Siaci minimise significativement les risques juridiques et financiers, tout en renforçant sa crédibilité et sa pérennité ainsi que le respect de la vie privée des personnes.

2. DOMAINE D'APPLICATION

Il est précisé que la présente Politique couvre l'ensemble des traitements de Données à caractère personnel réalisés par les Entités du Groupe.

Des procédures spécifiques à chaque Entité peuvent compléter les principes définis dans la présente Politique.

La présente Politique s'applique à l'ensemble des collaborateurs du Groupe Diot Siaci.

En outre, le Groupe Diot Siaci s'engage à ce que l'ensemble des principes exposés au sein de la présente Politique soient rigoureusement respectés par ses Sous-traitants, partenaires et fournisseurs de prestations de services. Ces derniers s'engagent à appliquer ces principes conformément aux instructions du Groupe, agissant en qualité de Responsable de traitement, garantissant ainsi une gestion conforme et sécurisée des Données à caractère personnel traitées.

3. OBJET DE LA POLITIQUE

La présente Politique vise à établir un cadre global et harmonisé de règles et d'actions en matière de protection des Données à caractère personnel, applicable à l'ensemble des Entités du Groupe.

Elle intègre également l'organisation des spécificités propres à chaque Business Unit, tenant compte des risques inhérents ainsi que des lois et contextes locaux qui leur sont applicables.

La présente Politique vise à respecter les grands principes de la protection des Données, définis à l'Article 5 du RGPD, à savoir :

- La **licéité** des traitements ;

- La **loyauté** dans la collecte des Données ;
- Un usage des Données collectées uniquement pour des **finalités déterminées ;**
- Le traitement de Données **exactes, complètes et adéquates** ;
- Une **durée de conservation limitée** dans le temps en fonction des exigences légales ;
- La **sécurité** des Données grâce à un niveau de sécurité adapté au risque ;
- Une démarche de responsabilisation « **Accountability »** visant à démontrer la conformité de l'ensemble des mesures techniques et organisationnelles mises en œuvre ;
- Le respect des principes de protection des Données dès la conception (« **Privacy by design »)** et par défaut **(« Privacy by default »)** ;
- Le respect des **droits des personnes** dont les Données sont collectées.

4. ORGANISATION DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL DU GROUPE DIOT SIACI

L'organisation de la protection des Données à caractère personnel au sein du Groupe repose sur une gouvernance clairement définie.

Le Délégué à la Protection des Données (DPO) est chargé de veiller au respect du cadre légal et réglementaire applicable et d'assurer la cohérence des actions menées à l'échelle du Groupe.

Pour exercer ses missions, il s'appuie sur un réseau de Correspondants à la Protection des Données (CPD), présents au sein des différentes Business Units (BU), et sur un réseau de Compliance Officers pour les Entités à l'international, lesquels constituent des relais opérationnels de la conformité aux réglementations en vigueur en matière de protection des Données à caractère personnel.

La sécurité des systèmes d'information est, quant à elle, placée sous la responsabilité du Directeur de la Sécurité des Systèmes d'Information (DSSI), en lien étroit avec le DPO, afin de garantir la mise en œuvre de mesures techniques et opérationnelles adaptées conformément à l'article 32 du RGPD.

Afin d'assurer une coordination efficace et un suivi régulier, un comité Données Personnelles se réunit chaque trimestre. Il constitue l'instance de pilotage et de supervision des actions menées en matière de protection des Données.

4.1. GOUVERNANCE DE LA PROTECTION DES DONNEES

4.1.1. Le DPO

Le pilotage de la conformité au Règlement Général sur la Protection des Données (RGPD) est assuré par le Délégué à la Protection des Données (DPO) du Groupe (ci-après "DPO" ou "DPO Groupe").

Conformément à l'article 37 du RGPD, le DPO a été désigné en raison de la nature des activités du Groupe Diot Siaci, qui impliquent un suivi régulier et systématique des personnes à grande échelle ainsi que le traitement à grande échelle de Données sensibles.

Le Groupe s'est assuré que la désignation de ce DPO respecte pleinement les critères définis par le RGPD, notamment :

- L'absence de conflit d'intérêts dans l'exercice de ses missions ;
- Les compétences professionnelles nécessaires pour exercer les missions de DPO, incluant des connaissances juridiques, techniques et une bonne compréhension du secteur de l'assurance ;
- L'indépendance dans l'exercice de ses fonctions ;
- Les qualités personnelles indispensables, telles que la probité et la loyauté.

Le DPO est rattaché au Directeur Juridique Groupe et placé sous l'autorité du Directeur Général Corporate, membre du Comité Exécutif du Groupe Diot Siaci, garantissant ainsi son autonomie et son accès aux plus hauts niveaux de gouvernance.

La Direction du Groupe Diot Siaci doit s'assurer que les moyens mis à la disposition du DPO, des CPD et des Compliance Officers permettent d'assurer les missions qui leur sont assignées.

Il est à noter que le DPO, conformément aux dispositions légales en vigueur, notamment l'article 38.3 du RGPD, n'est pas personnellement responsable en cas de non-conformité de son organisme avec le RGPD.

4.1.2. L'équipe Data Privacy

De manière générale, l'équipe Data Privacy, rattachée à la Direction Juridique Groupe, assiste le DPO dans l'ensemble de ses missions relatives à la protection des Données à caractère personnel au sein du Groupe.

Cette équipe a notamment pour mission de contribuer à la mise à jour de la documentation interne centrale et de fournir son expertise, au besoin, aux Correspondants à la Protection des Données afin de garantir l'actualisation rigoureuse de chaque registre des traitements au sein du Groupe.

Elle étudie les analyses d'impact sur la protection des Données (AIPD), relatives aux traitements existants et nouveaux, réalisées par les Correspondants à la Protection des Données.

Par ailleurs, l'équipe Data Privacy prend en charge l'analyse des incidents liés aux Données à caractère personnel ainsi que le traitement des demandes d'exercice des droits des personnes concernées.

De manière générale, l'équipe Data Privacy apporte son support et son expertise juridique pour la réalisation des missions du DPO. Elle participe notamment à la mise à jour des procédures de contractualisation et de pré-contractualisation ou encore à la rédaction des clauses contractuelles relatives à la protection des Données.

Enfin, l'équipe Data Privacy a la charge de suivre les évolutions réglementaires et législatives en France en matière de protection des Données.
Dans les Entités à l'international, cette veille réglementaire doit être organisée par les Compliance Officers.

4.1.3. Les Correspondants à la « Protection des Données » (CPD)

Les Correspondants à la Protection des Données sont nommés au sein de chaque Business Unit. Leur nombre peut être adapté en fonction de la taille, de l'organisation ou des enjeux spécifiques de certaines activités.

Leur mission principale est d'animer la démarche de protection des Données à caractère personnel au sein de leur Business Unit ou de leur périmètre d'activité. Ainsi, ils jouent un rôle essentiel dans le déploiement et l'animation de la Politique au sein de leur Business Unit.

À ce titre, les CPD constituent le point de contact privilégié du DPO sur leur périmètre de responsabilité et sont les premiers interlocuteurs sollicités par les équipes opérationnelles en matière de protection des Données notamment pour les questions liées au traitement de Données, aux analyses d'impact ou à la gestion des droits des personnes.

Ces derniers contribuent activement à la sensibilisation, à la remontée des incidents potentiels, au suivi des actions de conformité, et à la mise en œuvre des bonnes pratiques en matière de protection des Données à caractère personnel.

Les CPD sont également membres du Comité Données Personnelles du Groupe.

4.1.4. Les Compliance Officers des filiales à l'international

Les Compliance Officers sont responsables de la conformité des filiales internationales sous leur responsabilité à toute législation locale relative à la protection des Données à caractère personnel.

À ce titre, ils constituent le point de contact privilégié du DPO Groupe sur leur périmètre de responsabilité et sont les interlocuteurs sollicités par les équipes opérationnelles des filiales de leurs périmètre en matière de protection des données.

Ils sont également responsables des remontées d'information au DPO Groupe de tout évènement significatif en matière de protection des Données à caractère personnel.

4.1.5. Le Directeur de la Sécurité des Systèmes d'Information (DSSI)

Le DSSI pilote la sécurité de l'information et des systèmes d'information du Groupe. Il est hiérarchiquement rattaché au Directeur des Systèmes d'Information (DSI) qui reporte au Directeur Général des fonctions Corporate ainsi qu'au Directeur Général du Groupe Diot Siaci.

Un point d'échange mensuel régulier avec le DPO et l'équipe Data Privacy est mis en œuvre pour permettre le partage des informations et la meilleure mise en œuvre de la protection des Données à caractère personnel.

4.2. ROLES ET RESPONSABILITES DES ACTEURS

ACTEURS	MISSIONS
DPO Groupe (Délégué à la protection des Données)	○ Pilotage de la stratégie de mise en conformité au RGPD des Entités du Groupe ; ○ Assistance aux CPD et Compliance Officers et diffusion des instructions visant à l'harmonisation de la conformité au sein du Groupe ; ○ Supervision de la tenue et la mise à jour des registres des traitements et des analyses d'impact relatives à la protection des Données réalisées par les CPD et les Compliance Officers ; ○ Conseil ou validation, à la demande des CPD et des Compliance Officers, sur tout nouveau traitement de Données à caractère personnel ; ○ Validation des AIPD ; ○ Supervision de la gestion et des réponses aux demandes d'exercice de droits dans le respect des délais réglementaires ; ○ Remontée à la Direction Générale des alertes et manquements à la règlementation en vigueur ; ○ Organisation et participation aux travaux de sensibilisation et de formation des collaborateurs du Groupe ; ○ Assure les échanges et la coopération avec l'autorité en charge du contrôle relatif à la protection des Données ; ○ Organisation des réunions du Comité Données personnelles ; ○ Supervision des activités et travaux de l'Equipe Data Privacy.
CPD (Correspondants à la protection des Données)	○ Tenue des registres de traitements (Article 30.1 RGPD) et registres Sous-traitants (Article 30.2 RGPD) ; ○ Rédaction et mise à jour des analyses d'impact relatives à la protection des Données (Article 35 RGPD) : ○ Remontée au DPO de tout nouveau projet complexe nécessitant l'avis ou la validation de ce dernier ; ○ Participation active aux projets impliquant des traitements de Données à caractère personnel et analyse de leur conformité au RGPD ; ○ Participation aux Appels d'offres et audits avec le suivi des recommandations éventuellement formulées ; ○ Vérification de la conformité des engagements contractuels au RGPD ; ○ Remontée au DSSI de tout nouveau projet ; ○ Veiller sur l'évolution des traitements et la mise en œuvre d'un niveau d'alerte constant sur la conformité de ces derniers au RGPD ; ○ L'application des durées de conservation définies dans la charte Groupe ou la détermination de durées spécifiques aux activités de la BU ; Veiller au respect des règles de conservation définies dans les traitements mis en œuvre au sein de la BU.

	○ Sensibilisation et formation des équipes opérationnelles aux bonnes pratiques, spécifiques aux activités de la Business Unit, en matière de protection des données ; ○ Assistance dans la gestion des violations de données et des demandes d'exercices de droits.
COMPLIANCE OFFICERS	○ Responsables de la conformité des Entités sous leur responsabilité aux réglementations applicables et à leurs évolutions ; ○ Gestion de la mise en œuvre des Politiques et Procédures du Groupe ; ○ Gestion des reportings périodiques définis par le Groupe ; ○ Obligation de remonter, toute violation de données ou tout contrôle d'une autorité, à l'équipe Data Privacy sans délai (cf. Procedure for reporting information and alerts to the Group) ; ○ Information du DPO Groupe de tout événement majeur en lien avec la conformité à la règlementation en vigueur ; ○ Organisation de la sensibilisation et formations des collaborateurs des filiales internationales à la règlementation.
DSSI (Directeur de la sécurité des systèmes d'information)	Les missions de l'équipe Cybersécurité dirigée par le DSSI sont les suivantes : • Gouvernance sécurité - Politiques et standards de sécurité ; - Avis sécurité sur les évolutions et nouveaux projets ; - Sensibilisation et formation des collaborateurs du Groupe. • Risques, Contrôles et Conformité - Anomalies et non conformités ; - Gestion des risques ; - Contrôles internes ; - Threat Intelligence - Définition du threat model. • Sécurité opérationnelle - Détections, investigations (CSIRT) ; - Incidents & crises (CSIRT) ; - Remédiations ; - Traitement des demandes de dérogation ; - Traitement des escalades du Help Desk ; • Tests de sécurité - Pentesting (tests d'intrusion) ; - Audits de sécurité (filiales, fournisseurs, etc.) ; - Audit de code ; - Tests de phishing.

- Solutions sécurité
  - Définition, pilotage et application des mesures de sécurité préventive ;
  - Sécurité dans les projets (security & privacy by design) ;
  - Définition et mise en place des outils de sécurité en lien avec les opérations ;
- Audits et appels d'offre
  - Réponses aux questionnaires de sécurité des prospects, des clients et des partenaires.
- International
  - Coordination de la sécurité des filiales.

4.3. DISPOSITIFS DE PILOTAGE ET DE SUIVI

Le Groupe Diot Siaci a instauré un **Comité Données Personnelles (ci-après le « Comité »)** pour garantir une gouvernance forte et une responsabilité (« Accountability ») effective en matière de protection des Données. Cette instance traduit l'engagement du Groupe à assurer une gestion rigoureuse, sécurisée et conforme des traitements de Données à caractère personnel.

Sous la direction du DPO Groupe, le Comité remplit plusieurs missions essentielles :

- **Piloter et coordonner la conformité** : il organise la gouvernance RGPD du Groupe, en s'appuyant sur les Correspondants à la Protection des Données (CPD) pour relayer les actions et bonnes pratiques au sein de chaque Entité.
- **Définir les orientations stratégiques** : il fixe les objectifs de conformité, établit les priorités et oriente les actions nécessaires pour assurer la sécurité et la licéité des traitements.
- **Superviser les mesures de protection** : il veille à la mise en œuvre et au suivi des mesures techniques et organisationnelles permettant de garantir la confidentialité, l'intégrité et la disponibilité des Données.
- **Valider les décisions structurantes** : il statue sur les choix majeurs liés à la protection des Données (nouveaux projets sensibles, transferts internationaux, traitements à risque élevé, etc.) et arbitre les situations complexes.
- **Contribuer à l'amélioration continue** : il identifie les difficultés rencontrées, hiérarchise les pistes d'amélioration et impulse des plans d'action adaptés. Il promeut activement la sensibilisation et l'acculturation au RGPD par des actions ciblées.
- **Assurer la traçabilité et la démonstration de la conformité** : il permet au Groupe de justifier, à tout moment, de sa conformité vis-à-vis des autorités de contrôle, des clients et des partenaires.

Le Comité est composé du DPO et de l'équipe Data Privacy, du DSI (ou de son représentant), du DSSI (ou de son représentant), des Correspondants à la Protection des Données, ainsi que d'invités ponctuels en fonction des sujets traités.

Il se réunit **au moins quatre (4) fois par an**, avec la possibilité de convoquer un comité extraordinaire en cas de situation urgente. Chaque réunion fait l'objet d'un compte rendu diffusé aux membres, qui sont responsables de relayer les décisions et informations auprès de leurs Business Units respectives.

4.4. DISPOSITIFS DE FORMATION

Le Groupe Diot Siaci diffuse une culture de la protection des Données auprès de l'ensemble de ses collaborateurs.

L'ensemble des collaborateurs est sensibilisé dès son intégration grâce à un module de e-learning obligatoire inclus dans le parcours de formation des nouveaux arrivants. Cette sensibilisation est régulièrement renforcée par des communications sur l'intranet Groupe, des newsletters dédiées, des rappels ponctuels via courriel, ainsi qu'une formation spécifique au respect du secret médical, en particulier dans le cadre du traitement des Données sensibles. Des exercices de simulation de cyberattaques sont également organisés pour tester la vigilance des équipes ; ils donnent lieu à des rapports d'analyse et, si nécessaire, à des rappels individualisés ou collectifs visant à renforcer les bons réflexes en matière de cybersécurité.

En cohérence avec les exigences de la Politique de Sécurité de l'Information (PSI), **la formation et la sensibilisation du personnel à la sécurité des systèmes d'information sont considérées comme des activités prioritaires**, visant à réduire les risques liés à la sécurité de l'information.

À ce titre, les Directions des Systèmes d'Information et des Ressources Humaines s'assurent que :

- Les documents relatifs à la sécurité sont diffusés et présentés à l'ensemble du personnel ;
- La Charte Informatique, annexée au règlement intérieur de l'UES, est remise à tous les collaborateurs, qui s'engagent à la respecter en la signant ;
- Les collaborateurs savent comment accéder aux documents de référence en matière de sécurité, en cas de doute ou de question ;
- Les formations nécessaires sont accessibles et disponibles.

Les CPD bénéficient, dès leur prise de fonction, d'une formation spécifique leur permettant de maîtriser leur rôle et d'accompagner efficacement les équipes métiers dans le respect des exigences en matière de protection des Données. Ils reçoivent également des communications ciblées pour assurer une veille active sur les évolutions réglementaires et les bonnes pratiques à appliquer.

Enfin, des conférences sont organisées à destination du comité managérial, afin de renforcer leur compréhension des enjeux stratégiques liés à la protection des Données et de soutenir leur rôle de relais actif de la culture de conformité au sein des équipes.

Les compétences du DPO et de certains CPD sont certifiées par leur obtention de la Certification AFNOR « Délégué à la protection des données (DPO) ».

4.5. DISPOSITIFS DE CONTROLE

Le Groupe Diot Siaci a mis en place un dispositif de contrôle et d'audit destiné à garantir le respect des exigences légales et contractuelles en matière de protection des Données à caractère personnel. Ces actions participent à une démarche d'amélioration continue de la conformité et de maîtrise des risques.

4.5.1. Contrôles de conformité

4.5.1.1. Audits internes

Une fonction d'Audit interne, indépendante et objective, exerce ses missions dans le cadre d'un plan pluriannuel formalisé par la Charte d'audit interne Diot Siaci de juillet 2025.

Cette fonction évalue, de manière systématique et méthodique, les dispositifs de gouvernance, de gestion des risques et de contrôle, et formule des recommandations destinées à améliorer leur efficacité et à renforcer la valeur ajoutée pour l'organisation.

4.5.1.2. Contrôles internes

Dans le cadre de la conformité au RGPD, la Direction Risques, Contrôle interne et Conformité du Groupe met en œuvre un dispositif de contrôle régulier visant à garantir le respect des exigences réglementaires.

Ces contrôles, définis dans le cadre d'un plan annuel de contrôle, portent notamment sur :

- La bonne tenue de la documentation légale applicable
- Le respect des durées de conservation ;
- La sécurité et la confidentialité des Données ;
- L'effectivité de l'exercice des droits des personnes concernées.

Ces contrôles peuvent donner lieu, le cas échéant, à la définition et au suivi de plans d'actions correctifs.

4.5.1.3. Audits des systèmes d'information

Des audits spécifiques du système d'information sont réalisés conformément à la Politique de Sécurité de l'Information (PSI).

Ces audits sont planifiés et approuvés de façon à limiter tout risque de perturbation des activités métiers, et leur mise en œuvre est strictement encadrée afin de garantir la confidentialité et la sécurité des environnements audités.

4.5.1.4. Contrôles et audits des Sous-traitants

Le Groupe Diot Siaci s'assure que ses Sous-traitants respectent les obligations qui leur incombent en matière de protection des Données à caractère personnel, conformément aux dispositions contractuelles et réglementaires applicables.

À ce titre, le Groupe met en œuvre :

- **Un audit pré-contractuel** réalisé en amont de la signature du contrat avec le Sous-traitant conformément à la Politique Achats Groupe, incluant notamment des audits de sécurité, ainsi que des questionnaires cybersécurité.

- **Des contrôles réguliers**, destinés à vérifier notamment la mise en œuvre effective des mesures de sécurité, la confidentialité des Données traitées, la gestion des habilitations, le respect des durées de conservation et la capacité du Sous-traitant à assister le Groupe dans la gestion des droits des personnes concernées ;

- **Des audits documentaires ou sur site**, conduits lorsque cela est nécessaire, afin d'évaluer plus en détail le niveau de conformité du Sous-traitant et de définir, le cas échéant, des actions correctives adaptées.

Ces contrôles et audits sont réalisés dans le respect des dispositions contractuelles, et dans des conditions garantissant la confidentialité, la sécurité des informations échangées ainsi que la continuité des activités du Sous-traitant.

4.5.1.5. Audits réalisés par des tiers

Le Groupe met à la disposition des Tiers (assureurs, co-courtiers, partenaires, etc…) les informations nécessaires pour attester du respect de ses obligations en matière de protection des Données à caractère personnel.

Sous réserve des stipulations contractuelles, le Groupe autorise la réalisation d'un audit par client et par année civile, effectué par le client lui-même ou par un auditeur tiers dûment mandaté par celui-ci.

Toute demande d'audit doit être notifiée au Groupe par lettre recommandée avec accusé de réception au moins trente (30) jours avant la date prévue. La réalisation de l'audit s'effectue dans le respect des conditions convenues contractuellement, notamment en matière de sécurité, de confidentialité et de limitation de la portée des investigations.

5. PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

5.1. LICEITE, LOYAUTE ET TRANSPARENCE

Le Groupe Diot Siaci s'engage à ce que l'ensemble des traitements de Données à caractère personnel mis en œuvre dans le cadre de ses activités reposent sur une base légale conforme au Règlement Général sur la Protection des Données (RGPD). Les bases juridiques sont déterminées, au cas par cas, conformément à l'article 6 du RGPD, et documentées dans le registre des traitements.

Les principaux fondements juridiques applicables aux activités du Groupe sont :

- **L'exécution d'un contrat**, notamment lors de la conclusion et de la gestion d'un contrat d'assurance ;
- **Le respect d'obligations légales**, par exemple dans le cadre des contrôles relevant du Code des assurances ;
- **L'intérêt légitime du Groupe**, lorsque celui-ci est conforme aux droits et libertés fondamentaux des personnes concernées ;
- **Le consentement** des personnes concernées, notamment lors de la collecte de certaines Données sensibles lorsqu'aucune autre base légale ne peut être mobilisée.

Conformément aux recommandations de la CNIL et du Pack conformité Assurances, les traitements de Données relatifs à la prospection commerciale font l'objet d'un encadrement spécifique, illustré ci-après :

Type de prospection	Base légale	Modalités	Droit des personnes
BtoC	Consentement préalable, libre et éclairé	Opt-in obligatoire, et possibilité de retrait à tout moment via un mécanisme dédié.	Droit de retrait du consentement exercé via l'adresse dpo@s2hgroup.com
BtoB	Intérêt légitime du Groupe	Données limitées aux contacts professionnels communication proportionnée	Droit d'opposition au traitement

En outre, dans le cadre de l'ensemble de ses activités en BtoB, le Groupe est amené à traiter des Données à des fins de communication et d'organisation d'événements. A ce titre, le Groupe pourra collecter et traiter des Données d'identification de Tiers (incluant les noms, prénoms et courriels professionnelles) et s'engage à respecter l'ensemble de ses obligations au titre du RGPD et de la présente Politique.

Le Groupe Diot Siaci veille également à la loyauté et à la transparence de ses traitements. Les Données à caractère personnel sont collectées et traitées de manière licite, conformément aux finalités annoncées, et dans le respect des attentes légitimes des personnes concernées.

Afin de garantir la transparence, toute personne est informée, au moment de la collecte, au moyen d'un document clair, concis et compréhensible, des éléments essentiels suivants :

- **L'identité du Responsable du traitement,**
- **Les finalités poursuivies et la base légale applicable,**
- **Les destinataires des Données,**
- **Les droits dont elle dispose et les modalités pour les exercer.**

Ces informations sont également mises à disposition, de façon permanente et accessible, sur les différents espaces numériques du Groupe.

5.2. ORGANISATION ET SUPERVISION DES TRAITEMENTS

5.2.1. Registre des traitements

Conformément à l'article 30.1 du RGPD, les Entités du Groupe tiennent à jour les registres des activités de traitement, qui constituent un élément central de la démarche de conformité et de responsabilisation ("Accountability").

La tenue et la mise à jour de ces registres sont assurés par les CPD au sein de chaque Business Unit du Groupe, et par les Compliance Officers pour les Entités à l'international, en lien direct avec les opérationnels concernés. Les CPD et les Compliance Officers veillent à ce que l'ensemble des informations requises soient correctement renseignées, notamment les finalités poursuivies, les catégories de Données traitées, les destinataires, les durées de conservation ainsi que les mesures de sécurité mise en place.

Le DPO supervise la tenue de ces registres. A ce titre, il s'assure de leur cohérence et de leur conformité au cadre légal et réglementaire. Le DPO peut également accompagner les CPD et les Compliance Officers dans l'identification des traitements, formuler des recommandations et organiser des contrôles de cohérence périodiques.

5.2.2. Responsabilisation – « Accountability »

Le Groupe Diot Siaci applique le principe de responsabilisation (« Accountability ») tel que prévu par le Règlement Général sur la Protection des Données. Ce principe implique non seulement de mettre en œuvre des traitements conformes aux exigences légales, mais également d'être en mesure d'en démontrer à tout moment la conformité.

A ce titre, le Groupe déploie et maintient un ensemble de dispositifs et procédures documentés. Le Délégué à la Protection des Données, assisté par l'équipe Data Privacy, rédige et supervise l'ensemble de cette documentation afin d'en garantir l'exhaustivité, la mise à jour régulière et la disponibilité au sein du Groupe.

Cette documentation atteste du respect par le Groupe de ses obligations en matière de protection des Données et peut être mobilisée en cas de contrôle par une autorité ou de sollicitation d'un partenaire contractuel.

5.2.3. Analyse d'impact relative à la protection des Données

Conformément à l'Article 35 du RGPD, une analyse d'impact relative à la protection des Données (AIPD) est réalisée lorsque les traitements envisagés sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Au sein du Groupe Diot Siaci, la conduite opérationnelle des AIPD relève des Correspondants à la Protection des Données rattachés aux différentes Business Units. Les CPD et les Compliance Officers sont chargés de piloter l'exercice en lien avec les équipes métiers concernées, ainsi que la Direction de la sécurité des systèmes d'information, afin d'identifier les risques et de proposer les mesures de protection et de sécurité appropriées.

L'équipe Data Privacy assure un rôle de supervision et d'accompagnement méthodologique. Elle apporte son expertise pour garantir la qualité des analyses menées, ainsi que leur homogénéité au sein du Groupe.

La validation finale de l'analyse de risque et de sa conformité aux exigences de l'article 35 du RGPD, relève de la responsabilité du DPO, qui veille à ce que les analyses soient correctement documentées, complètes et intégrées dans la démarche globale de gestion des risques en matière de protection des Données.

L'approbation définitive de l'AIPD est ensuite formalisée par la validation et la signature du responsable du traitement.

5.2.4. Privacy by design et privacy by default

Le Groupe Diot Siaci applique le principe de protection des Données, dès la conception et par défaut, tel que prévu par l'article 25 du RGPD. Ce principe implique l'intégration systématique des exigences de protection des Données à caractère personnel tout au long du cycle de vie des projets, dès leur phase de conception et jusqu'à leur mise en œuvre opérationnelle.

Afin de garantir une approche homogène, le Groupe s'est doté d'une **matrice "Privacy by design**". Cet outil méthodologique permet de vérifier, par thématique, le respect des principales obligations en matière de conformité, notamment :

- La sécurisation des Données dès la conception des traitements ;
- L'identification des risques et la détermination des AIPD à réaliser ;
- L'analyse de la conformité contractuelle applicable aux Sous-traitants ;
- La transparence et l'information des personnes concernées ;
- La protection des Données par défaut, incluant la minimisation, la limitation de la conservation et le paramétrage adéquat des outils.

Cette démarche vise à s'assurer que les projets développés ou déployés au sein du Groupe intègrent, de manière anticipée et systématique, les exigences légales et les bonnes pratiques en matière de protection des Données à caractère personnel.

5.2.5. Contractualisation avec les Tiers

Dans le cadre de sa maîtrise des risques liés à ses relations avec les Tiers, le Groupe Diot Siaci intègre les exigences de conformité au RGPD et de sécurité des données dès la phase de pré-contractualisation, soit lors des appels d'offres et des consultations menées par la Direction des achats Groupe, afin de garantir un haut niveau d'exigence dès la sélection de ses partenaires.

Le Groupe Diot Siaci veille ensuite à ce que toute contractualisation avec un Tiers comporte des stipulations précises relatives au respect des obligations issues du RGPD et à la sécurité des systèmes d'information. Les contrats du Groupe intègrent également, lorsque cela est applicable, un Plan d'Assurance Sécurité (PAS) visant à encadrer les obligations relatives à la sécurité et à la confidentialité des données en phase avec la Politique de Sécurité de l'Information (PSI) du Groupe.

Grâce à cette démarche proactive de prévention et de gestion des risques, le Groupe Diot Siaci veille à ce que chacun de ses Tiers co-contractants applique, de manière continue, des standards de conformité et de sécurité équivalents à ceux du Groupe et pleinement alignés sur les obligations légales et réglementaires en vigueur.

5.2.6. Gestion des contrôles CNIL

Toute Entité du Groupe Diot Siaci peut faire l'objet de contrôles de la part des autorités de protection des données.

Ces contrôles peuvent intervenir à distance ou sur place, annoncés ou inopinés, et visent à s'assurer du respect du RGPD et de la législation nationale en vigueur.

En tant que Groupe de sociétés, dont les principales décisions liées au traitement de données à caractère personnel sont prises en France, la CNIL est l'autorité chef de file au sens du RGPD.

Le Groupe Diot Siaci s'engage à coopérer pleinement avec toute autorité de protection des données dans le cadre de ces contrôles. A ce titre, il veille à ce que l'ensemble de la documentation démontrant sa conformité soit disponible, à jour et facilement accessible.

Le Délégué à la Protection des Données est chargé de coordonner les relations avec la CNIL et d'assister les Compliance Officers dans leurs relations avec les autorités de protection des données locales. Il accompagne les équipes concernées durant le déroulement du contrôle, afin de garantir la cohérence et la complétude des informations transmises.

5.3. SECURITE ET INTEGRITE DES DONNEES

5.3.1. Gouvernance de la sécurité des systèmes d'information

La sécurité des traitements de Données à caractère personnel constitue une priorité stratégique pour le Groupe Diot Siaci. La maîtrise des enjeux de sécurité est intégrée dès la phase de conception des projets impliquant des traitements de Données, conformément au principe de Privacy by Design et de Privacy by Default susmentionné.

Une équipe dédiée à la cybersécurité pilote la **Politique de Sécurité de l'Information,** qui définit l'ensemble des mesures techniques et organisationnelles mises en œuvre pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des Données. Cette gouvernance repose sur une approche de gestion des risques, réévaluée régulièrement pour tenir compte de l'évolution des menaces et des réglementations.

Le Groupe a également instauré **un Plan d'Urgence et de Poursuite d'Activité (PUPA)** sous l'autorité de la Direction risques et conformité (DRC). Ce plan garantit la continuité des activités et la disponibilité

des Données en cas d'incident majeur ou de crise, en s'appuyant sur des procédures de sauvegarde et de restauration sécurisées.

Les collaborateurs jouent un rôle essentiel dans la sécurité des systèmes d'information et sont régulièrement formés et sensibilisés aux enjeux de cybersécurité et de protection des Données, notamment au travers de modules de formation, d'une charte informatique annexée au règlement intérieur, ainsi que de campagnes de sensibilisation diffusées via les canaux internes du Groupe.

Enfin, une organisation spécifique encadre la gestion des Données de santé, particulièrement sensibles. Leur traitement s'effectue dans le respect de la réglementation en vigueur, avec un hébergement confié à un prestataire certifié **hébergeur de Données de Santé (HDS).**

5.3.2. Gestion des incidents et des violations de Données à caractère personnel

Le Groupe Diot Siaci a mis en place un dispositif spécifique de détection, gestion et notification des incidents de sécurité et des violations de Données à caractère personnel. Ce dispositif inclut :

- Un processus d'escalade interne permettant de remonter rapidement tout incident de sécurité ;
- Une équipe Data Privacy et des CPD / Compliance Officers dédiés à l'analyse et au traitement des incidents, mobilisables en cas de crise ;
- Des procédures documentées pour évaluer les impacts, limiter les risques et remédier aux incidents de sécurité.

En cas de violation de Données à caractère personnel, avérée ou potentielle, le Groupe applique les obligations prévues par le RGPD :

- Notification à la CNIL ou à l'autorité de protection des données compétente, dans les délais légaux (72 heures), lorsque cela est requis ;
- Information des personnes concernées, lorsqu'un risque élevé pour leurs droits et libertés est identifié ;
- Documentation systématique des incidents dans un registre interne de gestion des Violations de données

Ces mesures assurent un haut niveau de protection et de conformité aux exigences réglementaires.

5.4. DROITS DES PERSONNES CONCERNEES

5.4.1. Garanties offertes par le Groupe en matière de droits des personnes

Le Groupe Diot Siaci garantit, en sa qualité de responsable de traitement, à toute personne identifiable dont les Données à caractère personnel font l'objet d'un traitement, une information claire, accessible et compréhensible, quel que soit le support utilisé : site web institutionnel, formulaires, documentation contractuelle, communications internes, charte informatique, etc.

Lorsque les Données sont collectées directement auprès de la personne concernée, le Groupe fournit toutes les informations prévues à l'article 13 du RGPD, notamment : l'identité et les coordonnées du responsable du traitement, les coordonnées du Délégué à la Protection des Données, les finalités du traitement et sa base légale, les catégories de Données traitées, les destinataires, les durées de conservation, les éventuels transferts en dehors de l'UE, ainsi que les droits dont dispose la personne concernée.

Le Groupe garantit également à chaque personne concernée l'exercice effectif des droits prévus par le RGPD et la Loi Informatique et Libertés : droit d'accès, de rectification, d'effacement (« droit à l'oubli »),

de limitation, d'opposition, de portabilité, ainsi que le droit de définir des directives post-mortem relatives à la conservation, à l'effacement et à la communication de ses Données.

Enfin, les personnes bénéficient du droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques ou les affectant de manière significative.

Lorsque le Groupe agit en qualité de Sous-traitant, la responsabilité de l'information incombe au responsable de traitement. Toutefois, le Groupe Diot Siaci facilite cette obligation en mettant à disposition des supports standardisés et en activement avec ses clients dans une logique de conformité partagée.

5.4.2. Traitement des demandes d'exercice de droits

Lorsqu'il agit en tant que responsable de traitement, le Groupe Diot Siaci répond aux demandes d'exercice de droits dans les meilleurs délais et au plus tard dans un délai d'un (1) mois à compter de leur réception. Ce délai peut être porté à deux (2) mois en cas de complexité particulière de la demande, sous réserve d'une justification claire apportée à la personne concernée.

Pour garantir la transparence et la traçabilité, le Groupe a mis en place une procédure interne formalisée de gestion des demandes, prévoyant notamment :

- L'identification et la vérification de l'identité du demandeur, le cas échéant ;
- L'analyse de la demande en fonction du droit exercé (accès, rectification, effacement, opposition, limitation, portabilité, directives post-mortem, etc.) ;
- La coordination avec les équipes internes concernées, incluant les CPD ;
- La réponse documentée et adaptée, dans le respect des délais légaux.

Toutes les demandes sont centralisées par le DPO et l'Equipe Data Privacy, qui tient à jour un registre de suivi des droits. Ce registre assure la traçabilité des échanges, la conformité des réponses et permet d'identifier les améliorations éventuelles du processus.

Pour les Entités à l'international, chaque Compliance Officer est responsable de la mise en œuvre d'une procédure équivalente.

5.4.3. Modalités de contact pour l'exercice des droits

Afin de faciliter l'exercice de leurs droits, les personnes concernées peuvent adresser leur demande :

- Par courriel à l'adresse dédiée : dpo@s2hgroup.com ;
- Par courrier postal à l'attention du Délégué à la Protection des Données, à l'adresse postale du siège du Groupe ;

- Ou, le cas échéant, via les formulaires en ligne mis à disposition sur les sites web du Groupe.

5.5. TRANSFERTS DE DONNEES

Le Groupe Diot Siaci est composé de nombreuses Entités présentes tant en France qu'au sein de l'Union européenne et à l'international. Cette organisation entraine des partages et des transferts de données intra Groupe encadrés contractuellement.

Le Groupe Diot Siaci s'appuie également sur un large réseau de Tiers, présents dans le monde entier. Cet écosystème implique que certaines Données à caractère personnel puissent être communiquées ou transférées vers des pays situés en hors de l'Union européenne, dans des conditions conformes au RGPD.

Le transfert, l'importation ou l'exportation de Données hors du territoire de l'Union européenne ne peut intervenir que si les conditions cumulatives suivantes sont respectées :

- Sur la base d'une instruction préalable, expresse et écrite de la hiérarchie concernée ;
- sous réserve du respect du cadre réglementaire applicable aux transferts de données hors UE c'est-à-dire s'il est réalisé soit :
  - Vers un pays disposant d'une décision d'adéquation de la Commission européenne, garantissant un niveau de protection jugé équivalent à celui de l'UE, ou ;
  - En présence de garanties appropriées, parmi lesquelles :
    - Les clauses contractuelles types (CCT) adoptées par le Commission européenne ou par une autorité de contrôle et approuvées par la Commission ;
    - Les règles d'entreprise contraignantes (*Binding Corporate Rules – BCR*) ;
    - Un mécanisme de certification reconnu ;
    - Des clauses contractuelles spécifiques, approuvées par l'autorité compétente.
- Si les données sont classifiées « Public », « Interne », « Restreint », mais pas « Confidentiel » (les règles de classification sont définies dans la Directive 13-A de la PSI) ;
- Si l'équipe cybersécurité du DSSI a donné son accord concernant les modalités et les systèmes permettant le transfert, l'importation ou l'exportation hors UE.

Dans l'ensemble de ces cas, les personnes concernées sont informées du transfert et disposent de droits opposables et de voies de recours effectives.

5.6. CONSERVATION ET SORT DES DONNEES

5.6.1. Le Groupe en qualité de Responsable du traitement

En tant que responsable de traitement, le Groupe Diot Siaci applique le principe fondamental de limitation de la conservation des Données, conformément à l'article 5 du RGPD. Les données personnelles sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont conservées que pour une durée n'excédant pas celle nécessaire à la réalisation de ces finalités.

Afin d'assurer une application homogène de ce principe, le Groupe a établi une charte interne de durée de conservation des Données, définissant les délais applicables en fonction des différentes catégories de Données et des obligations légales ou réglementaires. Cette charte s'applique à l'ensemble des Entités du Groupe et est régulièrement mise à jour afin d'intégrer les évolutions réglementaires et jurisprudentielles.

En complément, certaines Business Units peuvent fixer des durées de conservation spécifiques, adaptées à leurs activités ou contraintes sectorielles, dès lors qu'elles respectent le cadre général fixé par le Groupe.

À l'issue des durées de conservation :

- Les Données sont **supprimées** de manière sécurisée, ou ;
- Lorsque cela est pertinent, **anonymisées** afin de permettre leur utilisation à des fins statistiques ou d'analyse, sans possibilité de ré-identification des personnes concernées ;
- Et ce, sauf obligation légale, réglementaire ou contractuelle imposant un archivage prolongé.

Le Groupe s'assure également que les opérations de suppression ou d'anonymisation sont **traçables et documentées**, afin de garantir un haut niveau de responsabilité et de transparence.

5.6.2. Le Groupe agissant en qualité de Sous-traitant

En tant que Sous-traitant, le Groupe Diot Siaci s'engage à ne traiter les Données à caractère personnel que sur instruction documentée du client. Au terme de la prestation de services, et conformément à l'article 28 du RGPD ainsi qu'aux annexes contractuelles, le Groupe procède :

- Soit à la **suppression définitive et sécurisée** des Données ;
- Soit à leur **restitution complète** au client, avant de détruire toutes les copies résiduelles, sauf disposition légale contraire.