DiotSiaci

RGPD

Politique relative à la Protection des Données à Caractère Personnel

INFORMATIONS GENERALES

Date	28/03/2018
Libellé	Politique de Protection des Données à Caractère Personnel (PPDCP)
Direction émettrice	Direction Juridique Risques et Conformité Equipe Data Privacy
Validation	Direction Juridique Risques et Conformité
Responsable(s) du document	Santiago VALLS DPO – Juriste Valérie ANTOINE Adjointe DPO Groupe – Cheffe de projet Conformités
Diffusion	Information Publique

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

Versions	1ère version : 28/03/2018 2ème version : 29/10/2018 3ème version : 08/03/2019 4ème version : 24/06/2019 5ème version : 03/03/2020 6ème version : 30/03/2021 7ème version :25/08/2022 (révisée 6-9-2023)

Table des matières

Glossaire

CNIL Commission Nationale de l'Informatique et des Libertés.

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

Donnée de santé Donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne (Article 4.15 du RGPD).

Donnée sensible Au sens du RGPD, la Donnée sensible est une Donnée qui à trait :

- aux origines raciales ou ethniques ;
- aux opinions politiques, philosophiques ou religieuses ou à l'appartenance syndicale des personnes ;
- à la santé, à la vie sexuelle ou à l'orientation sexuelle ;
- aux Données génétiques ;
- aux Données biométriques aux fins d'identifier une personne physique de manière unique.

(Article 9 du RGPD)

DPO Data Protection Officer ou Délégué à la Protection des Données (Article 37 du RGPD)

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

Responsable de traitement Le responsable de traitement est la 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 (Article 4.7 du RGPD).

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 il est intégré à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Sous-traitant Le sous-traitant est la 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 (Article 4.8 du RGPD).

Utilisateur Toute personne qui est amenée à manipuler des Données à caractère personnel informatisées ou non ainsi que toute personne qui procède à des traitements automatisés ou non de ce type de Données et ce, quel que soit le statut de cet Utilisateur.

1. Contexte

1.1 Contexte réglementaire

En France, la législation applicable à la protection des Données à caractère personnel est issue de la loi « Informatique et Libertés » du 6 janvier 1978[1]. La protection des Données à caractère personnel est un enjeu tant au niveau européen, avec la Directive du 24 octobre 1995[2], qu'au niveau national puisque cette Directive a été transposée en France par la loi du 6 août 2004[3] (qui modifia la Loi « Informatique et Libertés ») et modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des Données personnelles.[4]

Le Règlement Général sur la Protection des Données à caractère personnel (ci-après désigné par le RGPD)[5], aussi connu sous le nom de General Data Protection Régulation (GDPR), entré en vigueur le 24 mai 2016 et entré en application le 25 mai 2018 dans tous les Etats membres de l'Union Européenne, remplace la Directive européenne sur la protection des Données personnelles (Directive 95/46/CE).

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

Ce sont 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.

Les risques suivants peuvent être encourus dans le cadre de procédures de protection déficientes :

- risques d'image, de réputation ;
- risques légaux, sanctions du marché, du régulateur, responsabilité en cas d'usurpation d'identité ;
- décrédibilisation de l'entreprise vis-à-vis de ses clients ou de ses salariés ;
- perte d'affaires et ses conséquences sur la réduction des profits et la part de marché.

Les impacts sont également conséquents en cas d'amende administrative prononcée par une autorité de contrôle telle que la Commission de l'Informatique et des Libertés (ci-après-désigné par CNIL) pouvant aller, pour une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent[6].

1.2 Contexte interne

Diot Siaci est l'un des tous premiers acteurs en France de conseil et de courtage en assurance de biens et de personnes notamment pour les entreprises.

Le Groupe peut, dans certaines situations, être responsable de traitement ou co-responsable de traitement indépendant et dans d'autres, sous-traitant. Conscient des enjeux que soulèvent ces différentes qualifications, le Groupe a mis en place la présente Politique de Protection des Données à Caractère Personnel (ci-après désignée par PPDCP) reprenant l'ensemble des principes applicables aux Données à caractère personnel collectées et traitées dans le cadre de ses activités.

2. Domaine d'application

2.1 Définitions

Donnée à caractère personnel

Selon le RGPD, une Donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable »[7].

Dans le cadre de ses activités, notamment de santé et de prévoyance, mais aussi en cas de gestion d'un dossier d'assurance « sinistre corporel », le Groupe est amené à collecter et manipuler des Données à caractère personnel telles que le nom, le prénom, l'âge ou encore l'adresse ou le NIR - Numéro d'Inscription du Registre National (connu sous la dénomination « numéro de sécurité sociale ») mais également des Données dites « sensibles[8] ».

---

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[3] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[4] Article 83 RGPD.
[5] Règlement UE 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard des du traitement des données à caractère personnel à la libre circulation de ces données
[6] Article 83 RGPD
[7] Article 5 RGPD
[8] Article 9 du RGPD

Donnée sensibles

Au sens du RGPD Article 9, la Donnée sensible est une Donnée qui à trait :

- aux origines raciales ou ethniques ;
- aux opinions politiques, philosophiques ou religieuses ou à l'appartenance syndicale des personnes ;
- à la santé[9], à la vie sexuelle ou à l'orientation sexuelle ;
- aux Données génétiques ;
- aux Données biométriques aux fins d'identifier une personne physique de manière unique.

2.2 Etendue de la Politique

La présente PPDCP s'applique à l'ensemble des Utilisateurs de Données à caractère personnel au sein du Groupe. L'Utilisateur est toute personne amenée à manipuler des Données à caractère personnel informatisées ou non ainsi que toute personne qui procède à des traitements automatisés ou non de ce type de Données et ce, quel que soit le statut de cet Utilisateur.
De manière contractuelle, la présente PPDCP s'applique donc également aux partenaires et fournisseurs de prestations de services ainsi qu'à l'ensemble des sous-traitants qui sont ou seront amenés à collecter et/ou traiter des Données à caractère personnel pour le compte et sur instructions du Groupe.
Toute utilisation des Données à caractère personnel est réalisée dans un cadre professionnel et responsable, c'est-à-dire dans le cadre exclusif des attributions de l'Utilisateur et de ses fonctions définies par le Groupe. Les instructions du responsable de traitement doivent être respectées et ce respect doit être contrôlé. A ce titre, l'Utilisateur est responsable de l'usage qu'il fait des ressources du Groupe dans l'exercice de ses fonctions.

En ce sens, la Politique de Sécurité des Systèmes d'Information du Groupe (ci-après désignée PSSI) indique que tout nouvel arrivant prend connaissance de la Charte d'utilisation des ressources informatiques et services Internet dite « Charte Informatique ».
Le Groupe s'engage à traiter les Données de manière confidentielle et pour cela les accès au système d'information sont soumis à habilitation et sont contrôlés[10].
En effet, selon la PSSI du Groupe, quatre (4) types de directives - concernant l'identification, l'authentification, les habilitations, et la responsabilité de la gestion des droits attribués aux profils - ont été mises en place. Le respect de ces principes permet d'attribuer aux utilisateurs, uniquement les droits dont ils ont réellement besoin dans le cadre de leur activité afin d'éviter tout accès inutile et de limiter les conséquences d'une faille des systèmes d'authentification.

3. Objet de la politique

De par sa présence internationale, le Groupe doit être conforme à la Loi française « Informatique & Libertés », au RGPD et aux directives européennes (comme celle relative aux échanges transfrontaliers des Données[11] par exemple), et également aux législations locales applicables.
La PPDCP a donc pour objectif de déterminer une trame globale et commune à l'action concernant la protection des Données personnelles qui sont confiées au Groupe, tout en préservant les particularités de chaque entité, liées aux risques encourus et aux lois et contextes s'y appliquant.

La PSSI prévoit d'ailleurs que le Groupe intègre les contraintes liées :

- Au RGPD ;
- A l'hébergement des Données de santé ;
- Aux informations classifiées défense.

[9] Art. 4, 15° RGPD : une donnée de santé est une « *donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne* ».
[10] Art. 32,4° RGPD
[11] Directive 2011/82/UE du parlement européen et du Conseil du 25 octobre 2011 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière.

4 Organisation détaillée dédiée à la protection des Données à caractère personnel

4.1 Organisation dédiée à la protection des Données personnelles

Le RGPD impose au Groupe Diot Siaci de désigner un Data Protection Officer (DPO) pour les sociétés traitant un volume important de Données personnelles et/ou de Données sensibles.
Afin de gérer au mieux la conformité de l'ensemble de ses sociétés soumises vis-à-vis de la réglementation applicable aux Données personnelles, le Groupe a décidé de désigner un DPO ainsi qu'un réseau de Correspondants à la Protection des Données (ci-après désignés CPD) et un Responsable de la Sécurité du Système d'Information (ci-après désigné RSSI) afin de dynamiser et rendre effective la protection des Données dans l'ensemble du Groupe, un Comité Données Personnelles a également été mis en place.

4.2 Rôles et responsabilités

a. Le DPO

Le RGPD a disposé que la désignation d'un délégué à la protection des Données (DPO) était obligatoire si :

- l'entité est un organisme public ;
- l'entité est une entreprise dont l'activité de base l'amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des Données dites « sensibles » ou relatives à des condamnations pénales et infractions[12].

La CNIL recommande fortement si l'organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des Données, de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des Données et réduire les risques de contentieux.

Le choix du DPO par l'entreprise doit prendre en considération plusieurs critères tels que :
- l'absence de conflit d'intérêts ;
- les compétences professionnelles requises pour exercer les activités de DPO (connaissances juridiques, connaissances techniques, connaissances du secteur de l'assurance, etc.) ;
- l'indépendance ;
- les qualités personnelles indispensables à l'exercice des missions (probité, loyauté, etc.).

Le DPO Groupe est la Directrice Juridique Risques et Conformité du Groupe. Elle est rattachée au Directeur Général Corporate, membre du Comité Exécutif du Groupe Diot Siaci, et directement rattaché à la Présidence.

Le DPO de différentes sociétés de courtage d'assurance du groupe lui est rattaché.
Le DPO Groupe et le DPO susvisés étant appelés ensemble « le DPO ».

Le DPO Groupe (i) coordonne l'action de l'équipe Data Privacy et (ii) dirige le Comité Données Personnelles.
Son rôle est central et compte-tenu de l'importance du sujet et des questions à traiter.
Le périmètre déterminé pour l'implication du DPO et de son équipe est le suivant :
- La DPO est responsable de la mise en conformité au RGPD des sociétés du Groupe pour lesquelles il est déclaré auprès de la CNIL ;
- Il intervient en qualité de DPO Groupe assistant le correspondant local pour les filiales françaises qui ne relèvent pas formellement de l'obligation de désigner un DPO ;
- pour les filiales européennes hors France, Il accompagne les cas échéant le correspondant local.

[12] Article 37.1 c) RGPD

Le DPO maintient un registre des traitements dans lequel figure l'ensemble des traitements de Données personnelles réalisés dans les filiales et les entités du Groupe en France dont il est le DPO déclaré.

(i) Le DPO doit être consulté avant la mise en œuvre de tout nouveau traitement de Données personnelles (formulaire « Nouveau Projet » en ANNEXE 3).

Il veille ainsi au respect de la législation applicable en matière de protection des Données.

Ses avis et recommandations doivent être recherchés avant toute mise en œuvre d'un nouveau projet.

(ii) Le DPO est amené à échanger régulièrement, en fonction des sujets avec les différentes directions « corporate » (Direction des Systèmes d'Information, Direction Financière, Direction des ressources humaines, Direction Communication, etc.) ainsi qu'avec les différents Correspondants à la Protection des Données (CPD) nommés au sein de chaque ligne métier ou département dans les entités du Groupe et le Responsable de la Sécurité des Systèmes d'Information (RSSI) à la Direction des Systèmes d'Informations.

(iii) Le DPO diffuse des instructions aux correspondants dans les entités du Groupe pour lesquelles il n'est pas désigné DPO auprès de la CNIL, en France.

Il est principalement chargé dans le Groupe:

- D'animer et de coordonner le dispositif de protection des Données personnelles ;
- De contribuer à la conformité au RGPD et aux règles internes ;
- D'interagir et de coopérer avec l'autorité de contrôle.

Il est à noter que le DPO n'est pas personnellement responsable en cas de non-conformité de son organisme avec le RGPD.

(iv) Le DPO analyse la conformité des traitements au regard de la réglementation relative à la protection des Données. Cette analyse porte notamment sur : la finalité, la proportionnalité du traitement, la pertinence des Données au regard de la finalité, la durée de conservation des Données, les destinataires des Données, l'encadrement des relations avec les sous-traitants, les mesures de sécurité, l'information des personnes concernées et les modalités d'exercice de leurs droits et le cas échéant, l'encadrement des flux transfrontières de Données.

Il a également un rôle d'alerte car il informe le Groupe des manquements constatés et le conseille dans la réponse à apporter pour y remédier.

(v) Le DPO et son équipe (Equipe Data Privacy) assurent en lien avec la Direction des Ressources Humaines Service Formation la sensibilisation des salariés du Groupe Diot Siaci et si nécessaire leur formation au travers de sessions ad hoc.

Afin d'assurer l'ensemble de ses missions, le DPO veille au maintien de ses compétences en se tenant informé des dernières évolutions en matière de protection des Données à caractère personnel. Il est ainsi amené à assister régulièrement à des formations ou à des conférences portant sur cette thématique.

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

Ils sont nommés au sein de chaque ligne métier et de chaque entité non soumise à l'obligation de désignation d'un DPO et sont chargés d'être le « référent protection des Données » sur leur périmètre respectif.

Ils sont le point de contact du DPO sur leur périmètre de responsabilité. Ils sont les premiers à être sollicités par les opérationnels sur des questions portant sur la protection des Données.

En sus de leurs activités opérationnelles, leurs principales missions sont :

- D'organiser la remontée des informations relatives à tous nouveaux projets de traitements de Données pour permettre l'échange avec le DPO et la Direction des Systèmes d'Information ;
- De sensibiliser sa Direction à la protection des Données personnelles ;
- De participer aux projets relatifs à la protection des Données personnelles ;
- D'assurer un niveau d'alerte continu sur la conformité à la protection de la data dans sa Direction.
- Ils sont membres du Comité Données Personnelles.

Les Compliance Officer des filiales du Groupe à l'international peuvent être également des interlocuteurs les plus appropriés du DPO Groupe.

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

Le RSSI est en charge au quotidien du respect des obligations de protection des Données au sein du Système d'Information (SI). Il :

- Anime la démarche de protection des Données dans les systèmes d'information (SI) ;
- Dynamise la remontée et la descente d'informations avec le DPO ;
- Participe aux échanges réguliers avec les Correspondants à la Protection des Données (CPD).

Un point d'échange mensuel régulier avec le DPO et l'équipe Data Privacy auquel est invité le DSI (Directeur des Services d'Information) est mis en œuvre pour permettre le partage des informations et la meilleure mise en œuvre de la protection des Données personnelles.

d. La Direction Juridique

La Direction Juridique Groupe (ci-après désignée DJ) apporte son support et son expertise juridique pour la réalisation des missions du DPO. Elle participe notamment à la mise à jour de procédures de contractualisation et de pré-contractualisation ou encore à la rédaction des clauses contractuelles types.
La DJ est également chargée de suivre les évolutions réglementaires et législatives en France en matière de protection des Données.

e. L'équipe Data Privacy

De manière large, L'équipe Data Privacy assiste le DPO dans ses toutes ses missions de protection des Données personnelles dans le Groupe.
Par exemple, l'équipe Data Privacy est chargée de participer à la mise à jour de la documentation interne centrale (Remontées des Business lines pour mises à jour du registre des traitements du Groupe, enregistrement des Analyses d'impacts sur la Protection des Données des traitements anciens et nouveaux réalisées par les Correspondants à la Protection des Données, l'analyse des incidents relatifs à des Données, etc.

g. La Direction des Systèmes d'Information

La Direction des Systèmes d'Information Groupe (ci-après désignée par DSI) assiste le DPO dans la réalisation de ses missions et apporte son expertise au côté du RSSI sur la sécurisation des applicatifs et les principes d'architectures du Système d'Informations (SI).
Les principaux rôles de la DSI en matière de protection des Données sont décrits dans la PSSI du Groupe.
Comme indiqué dans la PSSI du Groupe, différents rôles et responsabilités doivent être clairement définis. La note d'organisation, rédigée en commun avec la DSI, détermine l'organisation de la SSI au sein du Groupe et définissent les rôles et responsabilités de la société en matière de gestion de la sécurité du système d'information.

4.3 Dispositifs de pilotage et de suivi

Le Groupe s'est doté d'un Comité « Données Personnelles » qui :
- Valide les options structurantes et les arbitrages attendus en matière de protection des Données personnelles;
- Fixe les objectifs et les orientations de la conformité réglementaire du Groupe.
- Est informé des incidents constatés et des déficits de conformité le cas échéant ainsi que des plans de remédiation mis en place pour combler lesdits déficits éventuels au mieux de la capacité d'action de l'entreprise (budget, effectifs dédiés, projets à lancer, calendrier de refonte logiciel fixé, etc.)

Ce Comité, dirigé par le DPO Groupe et est formé de :
- Les membres de l'équipe Data Privacy dans son ensemble ;
- Le Directeur des Systèmes d'Information ;
- Le Responsable de la Sécurité du Système d'Information ;
- Le Directeur de la Communication ;
- Le Directeur de département « innovation and Growth » ;
- Les Correspondants à la Protection des Données des lignes métiers et Corporate ;
- Un ou des invités ponctuels selon les thèmes de travail abordés.

Le Comité Données Personnelles se réunit quatre (4) fois par an et garde la possibilité de réunir un Comité d'urgence en cas de problématique devant être résolue rapidement.

Le Groupe Diot Siaci diffuse une culture de protection des Données auprès de l'ensemble de ses collaborateurs.
Pour cela, il veille à ce que l'ensemble de ses salariés soit sensibilisé et respecte les principes applicables à la protection des Données à caractère personnel dans la mise en œuvre de la collecte et du traitement, tant de Données à caractère personnel que de Données dites « sensibles ».

La formation de l'ensemble des collaborateurs est organisée initialement via un module de e-learning à suivi obligatoire inclus dans le parcours de formation du nouvel entrant dans le Groupe et ensuite régulièrement actualisé avec des communications régulières sur l'intranet Groupe, des newsletters dédiées, ou des rappels importants selon les besoins via emails Groupe et des communications ciblées aux Correspondants à la Protection des Données dans les lignes métiers.

Des présentations de sensibilisation au RGPD dans les réunions de département ou d'équipe ont été réalisées dès janvier 2018 et sont toujours réalisées selon les besoins.

En effet, selon la PSSI, la formation et la sensibilisation du personnel à la Sécurité des Systèmes d'Information (ci-après désignée « SSI ») sont des activités prioritaires de SSI et doivent permettre de réduire les risques encourus.
Les Directions des Systèmes d'Information et des Ressources Humaines s'assurent que :

- Les documents relatifs à la sécurité ont été diffusés et présentés à l'ensemble du personnel.
- La Charte Informatique qui constitue une annexe du règlement intérieur de l'UES (Union Economique et Sociale) est diffusée à tous les collaborateurs qui s'engagent à la respecter en la validant par signature.
- Le personnel a, et connaît, les moyens d'accéder en cas de doute ou de question aux documents relatifs à la sécurité.
- Les formations nécessaires sont disponibles.

5. Les principes fondamentaux de la protection des Données à caractère personnel

5.1 Collecte

La collecte, le traitement, la conservation et l'enregistrement de Données à caractère personnel ne peuvent être effectués au sein du Groupe Siaci Saint Honoré, que dans le cadre des instructions reçues par l'Utilisateur.
Cet Utilisateur se doit, dans son activité, de mettre en œuvre notamment les principes fondamentaux décrits ci-dessous.
Tout Utilisateur, dans le cadre de son activité professionnelle et/ou de sa fonction au sein du Groupe Diot Siaci, doit impérativement, lorsqu'il procède à une collecte de Données à caractère personnel, respecter les principes de loyauté, licéité et de légalité édictés par la réglementation applicable à la protection des Données à caractère personnel.
Pour que la collecte soit loyale, licite et légale, la personne concernée par la collecte et le traitement de ses Données doit recevoir une information concise, transparente, compréhensible, facilement accessible et en des termes clairs et simples, de la part de la personne qui recueille de telles Données.
Dans le cadre d'une collecte directe (ex : formulaire d'inscription), les informations suivantes doivent être Données au moment de la collecte :

- L'identité et les coordonnées du responsable de traitement et, le cas échéant, du représentant du responsable de traitement ;
- Les coordonnées du DPO ;
- La / les finalité(s) du traitement ;
- La / les base(s) juridique(s) du traitement (ANNEXE 1). Si le traitement repose sur les intérêts légitimes du responsable du traitement, il est alors nécessaire de préciser quels sont-ils. Dans le cas présent, il sera aussi nécessaire d'informer la personne concernée qu'elle peut retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- Le / les destinataire(s) ou catégorie(s) de destinataire(s) des Données ;
- L'intention d'effectuer un transfert de Données vers un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- La durée de conservation des Données ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée ;
- Les droits d'accès, de rectification ou d'effacement ou de limitation ou d'opposition, et de portabilité ;
- La possibilité d'organiser des directives après sa mort [13];
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Pour chaque Donnée, le caractère obligatoire ou facultatif ainsi que les conséquences éventuelles de la non-fourniture de ces Données (si l'exigence de fourniture de Données à un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat) ;
- L'existence d'une prise de décision automatisée, y compris un profilage ainsi que des informations concernant la logique sous-jacente et l'importance et les conséquences prévues du traitement sur la personne concernée.

Dans le cadre d'une collecte indirecte (ex : achat d'un fichier de prospection), il est nécessaire de fournir l'ensemble des informations précitées ainsi que la source des Données. Ces informations doivent être communiquées à la personne concernée :

- Sous un mois maximum, après obtention des Données ;

[13] Article 85 loi Informatique et Libertés modifiée par la loi pour une république numérique

- Au plus tard au moment de la première communication à ladite personne, si les Données doivent être utilisées aux fins de communication avec la personne concernée ;
- Au plus tard lorsque les Données sont communiquées pour la première fois, si les Données doivent être communiquées à un autre destinataire.

5.2 Déclarations des traitements à la CNIL

Le RGPD a supprimé le régime antérieur de déclaration préalable des traitements auprès de la CNIL.

Il appartient désormais au Groupe de mener une Analyse d'Impact sur la Vie Privée des personnes concernées afin de mesurer le risque que présente la mise en œuvre des nouveaux traitements envisagés.
Si, à l'issue de l'analyse, le risque est élevé pour la vie privée des personnes concernées, le Groupe doit consulter la CNIL pour une demande d'avis ou d'autorisation (uniquement dans le cas où la prise de mesures techniques et/ou organisationnelles nécessaires ne serait pas suffisante à atténuer le risque initialement mesuré par l'analyse d'impact).

5.3 Etude d'Impact sur la Vie Privée

En l'absence de déclaration préalable, le Groupe Diot Siaci évalue le niveau de risque que présente un traitement à l'aide des critères énumérés par le G29 :
- Evaluation ou notation y compris profilage et prédiction : il s'agit de traitements portant sur le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêts, sa fiabilité ou son comportement, ou sa localisation et ses déplacements
- Prise de décision automatisée avec effet juridique ou effet similaire significatif : traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative de façon similaire.
- Surveillance systématique : traitement utilisé pour observer, surveiller ou contrôler les personnes concernées.
- Données sensibles ou Données à caractère hautement personnel : traitements portant sur les catégories de Données visées aux articles 9 et 10 du RGPD. Il peut également s'agir de traitements portant sur des Données pouvant être considérées comme augmentant le risque possible pour les droits et les libertés des personnes (communications électroniques, coordonnées bancaires, …)
- Données traitées à grande échelle : pour cela il faut prendre en compte plusieurs critères tels sur : le nombre de personnes concernées, le volume de donnés, l'éventail des différentes Données traitées, la durée ou permanence de l'activité de traitement, l'étendue géographique de l'activité de traitement.
- Croisement ou combinaison d'ensembles de Données : issus de deux opérations de traitements par exemple ou effectuées à des fins différentes et/ou par différents responsables de traitement, de manière qui outrepasserait les attentes raisonnables de la personne concernée.
- Données concernant des personnes vulnérables : il faut prendre en compte le déséquilibre des pouvoirs existants entre les personnes concernées et le responsable de traitement : enfants, employés, personnes souffrant de maladie mentale, demandeurs d'asile, personnes âgées, patients, etc.
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles : utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques.
- Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat : il s'agit notamment des traitements qui incluent les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat.

Le Groupe Diot Siaci met et mettra en œuvre une Etude d'Impact sur la Vie Privée dès lors que deux critères, a minima, seront remplis. Cependant, le DPO pourra décider qu'une telle étude soit réalisée alors qu'un seul critère est rempli et cela pour des raisons telles que, par exemple, la présence d'une chaine de sous-traitance ou d'un transfert hors UE difficilement encadrés, etc.

5.4 Sécurité des traitements

Comme indiqué dans la PSSI du Groupe, la sécurité d'un système d'information est l'état de protection face aux risques identifiés, résultant de l'ensemble des mesures générales et particulières prises pour assurer : la confidentialité, la disponibilité et l'intégrité des Données à caractère personnel.

Le Groupe s'engage à traiter les Données à caractère personnel de façon à garantir une sécurité appropriée des Données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

En ce sens, la PSSI du Groupe détermine les mesures générales applicables au Système d'Information.

L'ensemble des traitements de Données à caractère personnel réalisés au sein du Groupe doit respecter des règles de protection visant leurs :

- Sécurité physique : mesures destinées à limiter, contrôler l'accès aux endroits où sont stockées les Données aux seules personnes habilitées ainsi que prévenir et protéger les Données à caractère personnel contre les agressions accidentelles ou volontaires telles incendie, dégâts des eaux, etc.
- Sécurité logique : mesures destinées à limiter et contrôler l'accès aux Systèmes d'Information, y compris de télécommunications, aux seules personnes habilitées.

La PSSI du Groupe indique que l'utilisation de techniques de chiffrement ou de procédés cryptologiques n'est pas envisagé sans l'aval du RSSI. Ce document détaille également les mesures de sécurité appliquées au Système d'Information Siaci Saint Honoré.
L'utilisateur est d'ailleurs informé de l'existence d'une traçabilité mise en place afin de sécuriser l'activité et les Systèmes d'Information du Groupe. En effet, l'ensemble des bases de Données du Groupe Diot Siaci dispose d'une solution permettant la journalisation et la traçabilité des accès. Cela permet de déterminer quel collaborateur a eu accès à la base de Données, les actions réalisées et à quel moment.
La PSSI du Groupe indique que les Directives, d'une part, relative à la Journalisation et analyse des journaux des équipements réseaux et télécoms et d'autre part, relative à l'analyse des logs et journaux systèmes, encadrent la traçabilité des accès aux Données.
Les employés en télétravail accèdent à l'entreprise via la plateforme sécurisée CITRIX qui embarque toutes les protections décrites dans la Politique de Protection des Données à Caractère Personnel (PPDCP) ou par l'intermédiaire d'un VPN.
La PSSI DU Groupe prévoit l'accès nomade dans les conditions suivantes :

- Seuls les moyens d'accès nomades validés par la DSI doivent être utilisés.
- Non simultanéité : Pendant l'accès nomade au SI de l'établissement, toute autre communication doit être rendue impossible.
- Authentification de l'accès nomade : Tout accès nomade au SI de l'établissement doit être soumis à une authentification forte.
- Confidentialité et intégrité des flux : Tout accès nomade doit garantir la confidentialité et l'intégrité des flux échangés entre l'équipement nomade et le SI accédé.
- Trace de l'utilisation : Toute utilisation doit être tracée (accès nomade à préciser)
- Sécurisation du poste : Les postes doivent être équipés d'un antivirus et d'un pare-feu. Les mises à jour ne doivent pas être bloquées.
- Sensibiliser les salariés : Les collaborateurs doivent être sensibilisés aux meilleurs usages et aux risques que représentent par exemple l'absence de mise à jour d'un antivirus, le mélange des messageries personnelles et professionnelles, ou le stockage de Données de l'entreprise sur des plates-formes publiques.
- Encadrer les usages : La mise en place d'une Charte au sein de l'entreprise doit ainsi permettre de détailler les bonnes pratiques, d'expliciter les restrictions et de donner les procédures à respecter.

5.5 Le cas particulier du NIR et des Données de santé

Pour les activités de gestion de frais de santé, retraite et prévoyance, les articles R115-1 et R115-2 du code de la Sécurité Sociale autorisent le Groupe à collecter et à utiliser le NIR. Toutefois, cette autorisation ne vaut que pour les traitements effectués dans l'exercice des activités d'assurance maladie, maternité, invalidité et assurance vieillesse complémentaire menées par le Groupe.
Le NIR est collecté pour tous les assurés qui bénéficient d'une complémentaire santé pour permettre la mise en place d'un lien automatique entre les différentes Caisses Primaires d'Assurance Maladie (CPAM) de France et les services du Groupe. Le but est de structurer et d'automatiser le circuit des remboursements de santé dans un souci d'efficacité et de rapidité.
Concernant les Données de santé, le Groupe s'est organisé de manière à préserver la confidentialité de ces Données et à respecter les recommandations des conventions Belorgey et AERAS. L'organisation et les principes applicables en la matière sont disponibles en interne auprès des départements médicaux dans les lignes métiers. De plus, l'hébergeur choisi par le Groupe est certifié « Hébergement Données de Santé ».

5.6 Les droits des personnes concernées

Toute personne physique concernée par les traitements de Données du Groupe dispose de différents droits octroyés par le droit national et le droit de l'Union européenne. Ceux-ci doivent être respectés et leur mise en œuvre doit être effective. Ainsi, ces personnes physiques disposent d'un droit d'accès et d'un droit de rectification afin d'obtenir du responsable du traitement : la confirmation que des Données la concernant sont ou ne sont pas traitées ou bien la rectification des Données personnelles la concernant qui seraient inexactes. Les personnes concernées peuvent également donner des directives relatives à la conservation, à l'effacement et à la communication de leurs Données après leur décès. Il s'agit de la possibilité d'organiser le sort de ses Données personnelles après la mort.

Toute personne physique dispose du droit à l'effacement qui est le droit d'obtenir l'effacement, dans certaines conditions, de Données personnelles la concernant.

Toute personne physique dispose aussi d'un droit à la limitation et d'opposition au traitement.

Les personnes sont titulaires du droit à la portabilité qui est le droit pour la personne concernée de recevoir, dans certaines conditions « dans un format structuré, couramment utilisé et lisible par machine », l'intégralité de ses Données pour qu'elle puisse les transférer à un autre prestataire.

Enfin, toute personne physique a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Le responsable de traitement doit répondre à la demande de la personne concernée d'exercer les droits que lui confèrent le RGPD et la Loi « Informatique et Libertés ». Le responsable de traitement doit fournir à la personne concernée les informations dans les meilleurs délais et en tout état de cause dans un délai d'un (1) mois à compter de la réception de la demande. Ce délai peut être porté à deux (2) mois si la demande est complexe. Dans ce dernier cas, il sera essentiel de démontrer la complexité de la demande.

Le Groupe a mis en place une Procédure de gestion des demandes d'exercice des droits des personnes concernées ainsi qu'un Mode opératoire dédié. La Procédure de gestion des Données personnelles, quant à elle, décrit en détail les conditions générales applicables dès réception de toute demande et les conditions spécifiques applicables à un type déterminé de demande. Le Mode opératoire a vocation à déterminer rapidement comment mettre en œuvre concrètement la demande de la personne concernée dans les délais légaux.

L'ensemble de ces documents est disponible en interne auprès du DPO du Groupe et l'ensemble des salariés y a accès via l'intranet personnel. Une diffusion régulière est également réalisée.

Le DPO tient et met à jour régulièrement un tableau des demandes permettant d'historiser les demandes d'exercice des droits des personnes et les réponses qui y sont apportées.

L'ensemble des demandes réalisées par les personnes concernées doit impérativement être transmis au DPO du Groupe et traitée par ce dernier et ses collaborateurs. Pour permettre cela, le DPO est joignable par mail (à l'adresse suivante : **dpo@s2hgroup.com**). La procédure d'information du DPO décrit en détail « quand et comment » informer le DPO Groupe.

Un formulaire de transmission des demandes d'exercice des droits par les personnes concernées (ANNEXE 4 et ANNEXE 5) est mis à disposition des opérationnels pour faciliter la transmission des demandes. Ce formulaire, une fois transmis au DPO, permettra d'adapter sa réponse à la personne concernée.

5.7 Transferts de Données à caractère personnel

Le Groupe Diot Siaci réalise son activité sur deux types de zones géographiques :

- Sur le territoire de l'Union européenne ;
- En dehors du territoire de l'Union européenne.

Le transfert, l'importation ou l'exportation de Données à caractère personnel, en dehors des traitements gérés dans le Système d'Information Groupe, ne peuvent être réalisés que dans le cadre d'une instruction préalable, expresse et écrite du supérieur hiérarchique de l'utilisateur et en conformité avec les déclarations ou autorisations et l'information des personnes concernées décidés par le Groupe.

Un transfert de Données à caractère personnel est possible à condition que :

- Le pays vers lequel le transfert a lieu assure un niveau de protection adéquat reconnu par la Commission Européenne par le biais d'une décision d'adéquation ;
- Le responsable de traitement ait prévu des garanties appropriées et informé les personnes concernées du transfert, lesquelles disposent de droits opposables et de voies de droit effectives. Les garanties appropriées peuvent être, entre autres, la mise en place de règles d'entreprises contraignantes (ou Binding. Corporate. Rules (B.C.R.), des clauses types adoptées par la Commission Européenne, les clauses types adoptées par une autorité de contrôle et approuvées par la Commission Européenne ou encore un mécanisme de certification approuvé. Avec autorisation de la CNIL, il est également possible de mettre en place des clauses contractuelles entre le responsable de traitement ou le sous-traitant et le responsable de traitement, le sous-traitant ou le destinataire des Données.

Le Groupe Diot Siaci accorde une vigilance importante à l'ensemble de ses transferts de Données à caractère personnel en dehors de l'Union européenne.

La PSSI indique que les échanges des informations sont encadrés par les Directives relatives à l'envoi de supports informatiques et aux échanges d'informations par messagerie électronique.

5.8 Sous-traitance

Le RGPD apporte une vigilance particulière concernant le recours à la sous-traitance.
Le Groupe Diot Siaci, dans le cadre de contrats conclus avec ses sous-traitants amenés à traiter des Données à caractère personnel pour son compte (ou d'une entité du Groupe), veille à ce que soit précisé dans le contrat :

- Que le sous-traitant est informé du fait que ces Données et fichiers sont soumis au respect de la législation applicable à la protection des Données et relève de la vie privée et du secret professionnel ;
- Et qu'il s'engage à mettre en place toutes les procédures ou mesures nécessaires pour en assurer la sécurité et la confidentialité.

Le Groupe veille à ce que le sous-traitant présente des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité et l'ensemble des contrats de sous-traitance, contient une clause relative à la protection des Données personnelles déterminant la responsabilité de chacun des acteurs.
Les contrats de prestation des sous-traitants sont assortis d'une annexe RGPD travaillées par la Direction Juridique pour garantir la répercussion sur le prestataire ou le fournisseur sous-traitant de toutes les exigences issues du règlement européen.
Selon la PSSI du Groupe, une convention de service est établie entre Siaci Saint Honoré et ses hébergeurs. Cette convention précise les engagements de l'exploitation vis-à-vis des besoins et exigences exprimés par la maîtrise d'ouvrage lors de la mise en production. Elle décrit donc le niveau de secours, la sécurité physique et logique, les tâches d'exploitation prévues et les plages d'astreinte, la disponibilité requise et les mesures conservatoires.

5.9 Contrôle

Outre les contrôles de conformité qui peuvent être menés en interne, la CNIL peut avoir accès, de 6 heures à 21 heures, pour l'exercice de ses missions, aux lieux et locaux servant à la mise en œuvre des traitements de Données à caractère personnel.
Elle peut demander la communication de tous les documents nécessaires à l'accomplissement de sa mission, quel qu'en soit le support, en prendre copie, accéder aux programmes informatiques et aux Données.
Toutefois, seul un médecin peut requérir la communication de Données de santé.
Le Groupe Diot Siaci s'engage, en cas de contrôle de la CNIL, à coopérer avec cette dernière.

5.10 Protection des Données dès la conception des projets et au plus haut niveau de protection

Afin de pouvoir assurer la conformité du Groupe Diot Siaci en matière de protection des Données, le DPO doit impérativement être consulté dès l'initialisation de tout projet impliquant des traitements de Données à caractère personnel.
Il convient donc pour tout utilisateur, en charge d'un nouveau projet entrant dans ce périmètre, de consulter le DPO. Pour cela, le Groupe a mis en place un formulaire « Nouveau Projet » (en ANNEXE 3) permettant aux équipes en charges des nouveaux projets de faire prendre connaissance au DPO du projet en question pour que ce dernier puisse les conseiller.

5.11 Gestion des incidents/failles/violations de Données

En cas d'incident de sécurité Diot Siaci, a mis en place une Procédure de gestion des incidents-failles-violations permettant de détecter, d'évaluer et de répondre à une violation de Données par exemple.
Selon la PSSI du Groupe, la procédure de gestion des incidents permet de réagir à bon escient et de transmettre l'information. Le système de gestion des incidents mis en place, compte :

- Des systèmes de détection des incidents ;
- Des processus de reporting et de traitement après la découverte d'un incident jusqu'à la gestion de crise ;
- Une consolidation d'une base d'information ;
- Un système de suivi et un tableau de bord.

Le Groupe a également mis en place un Plan de Continuité de Service en cas d'indisponibilité critique de tout équipement. Ces solutions sont décrites dans les documents intitulés « Plan de Continuité d'Activité » ou « Plan de Reprise d'Activité » et incluent les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées.

En qualité de Sous-Traitant, le Groupe Diot Siaci s'engage à notifier au Responsable de Traitement, dans les meilleurs délais après en avoir pris connaissance, toute violation de sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des Données à Caractère Personnel.
De manière générale, le Groupe s'engage à aider son Client, dans la mesure du possible et au moyen de mesures techniques et opérationnelles appropriées, dans la gestion de notification des Violations de Données à Caractère Personnel.

Toute détection de Violation fera l'objet par le Groupe d'une évaluation rapide avec la mise en place d'un dispositif adapté à l'identification de la cause racine de la Violation et ce, dans l'optique de prévenir ou atténuer les effets causés par la Violation.
Lorsqu'une Violation est détectée, le Groupe prendra toutes les mesures nécessaires pour empêcher que ces incidents ne se reproduisent.

5.12 Le sort des Données après réalisation de la prestation

En tant que responsable de traitement, le Groupe Diot Siaci met en œuvre ou s'organise en vue de la suppression des Données de manière régulière et selon les exigences légales.
En tant que sous-traitant, le Groupe Diot Siaci s'engage à ne traiter les Données que sur instruction documentée du Client. Selon le choix de ce dernier, le Groupe s'engage également à supprimer toutes les Données ou à les renvoyer au Client au terme de la prestation de services relatifs au traitement ainsi qu'à détruire les copies existantes dans les conditions prévues à l'annexe contractuelle RGPD.

5.13 Examens de conformité périodiques

Le Groupe Diot Siaci est amené à réaliser deux types d'audits :

- En interne dans le cadre du plan d'audit interne pluriannuel. La fonction audit interne du Groupe Diot Siaci est une activité indépendante et objective qui donne à l'organisation une assurance sur le degré de maitrise de ses opérations, lui apporte des conseils pour les améliorer et contribue à créer de la valeur ajoutée. La fonction audit interne aide le Groupe Diot Siaci à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité. La mise en œuvre de l'audit interne est décrite dans la Charte d'audit interne S2H Groupe 2017.

- Chez les sous-traitants dans le cadre de leurs relations contractuelles afin de vérifier que les principes applicables à la protection des Données à caractère personnel sont bien respectés.

Le Groupe met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues par la législation applicable à la protection des Données à caractère personnel. Diot Siaci s'engage également à permettre la réalisation d'audits par le Client ou un autre auditeur qu'il a mandaté, et contribuer à ces audits dans les conditions suivantes : un (1) audit par année calendaire dont la demande aura été exposée par lettre recommandé avec accusé de réception minimum trente (30) jours avant la date de réalisation de l'audit.

Concernant les audits des systèmes d'information, la PSSI du Groupe indique qu'ils sont planifiés et approuvés de façon à minimiser les risques de perturbation des processus professionnels. L'accès aux outils d'audit des systèmes est protégé afin d'empêcher toute compromission ou toute utilisation abusive éventuelle.

ANNEXE 1 : Rappels des bases juridiques d'un traitement de Données personnelles

L'article 6, 1 du RGPD défini les différentes bases légales qui permettent au responsable de traitement de mettre en œuvre un traitement de Données à caractère personnel de manière licite :

1. Le consentement spécifique et éclairé de la personne concernée par le traitement ;

2. Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (ex : Données nécessaires pour réaliser un contrat d'assurance) ;

3. Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis (exemple : obligations de lutte contre le blanchiment et le financement du terrorisme) ;

4. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (ex : la santé de la personne concernée ou d'une autre personne est en jeu) ;

5. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique dont est investi le responsable du traitement ;

6. Le traitement est nécessaire aux fins d'intérêts légitimes poursuivis par le responsable du traitement ou pas un tiers (étude de proportionnalité des intérêts du responsable de traitement et de la personne concernée).

ANNEXE 2 : rappel des grands principes posés par le RGPD pour la protection des Données :

L'ensemble des considérants du RGPD pose les principes qui doivent être respectés pour assurer la protection des Données à caractère personnel et ainsi la vie privée des personnes concernées.

1. La licéité des traitements ;
2. La loyauté dans la collecte des Données ;
3. Un usage des Données collectées uniquement pour les finalités déterminées ;
4. Le traitement de Données exactes, complètes et adéquates ;
5. Une durée de conservation limitée dans le temps en fonction des exigences légales ;
6. La sécurité des Données grâce à un niveau de sécurité adapté au risque ;
7. Une démarche d'Accountability visant à démontrer la politique mise en œuvre et notamment le respect des principes de Privacy by design et Privacy by default ;
8. Le respect des droits des personnes dont les Données sont collectées.

ANNEXE 3 - Informer le DPO des mises à jour à enregistrer au registre des traitements (Utilisation interne Groupe Diot Siaci)

FORMULAIRE « NOUVEAU PROJET »

1. Informations générales relatives au nouveau projet
- Titre : _____
- Date du nouveau projet : _____
- Personne en charge : _____
- Service / Département : _____
- Date de transmission du DPO : _____

2. Informations spécifiques relatives au nouveau projet :

- Date souhaitée de mise en production : _____/_____/_____

- Types de Données personnelles concernées :
- ☐ Etat-civil identité (nom, prénom, mail, image) : _____
- ☐ Vie personnelle (habitudes de vie, situation familiale) : _____
- ☐ Vie professionnelle (CV, scolarité, formation) : _____
- ☐ Informations d'ordre économique et financier (revenus, situation fiscale) : _____
- ☐ Données de connexion, cookies (adresse IP, logs) : _____
- ☐ Données de localisation (déplacements, Données GPS) : _____
- ☐ Autres : _____

- Présence de Données sensibles ?
- ☐ Non
- ☐ NIR = Numéro de sécurité sociale
- ☐ Données de santé : _____
- ☐ Données concernant la vie sexuelle ou l'orientation sexuelle : _____
- ☐ Données relatives aux condamnations pénales : _____
- ☐ Données biométriques aux fins d'identifier une personne physique de manière unique : _____
- ☐ Données génétiques : _____
- ☐ Données révélant l'appartenance syndicale : _____
- ☐ Données révélant les convictions religieuses ou philosophiques : _____
- ☐ Données révélant les opinions politiques : _____
- ☐ Données révélant l'origine raciale ou ethnique : _____
- Type de collecte :
- ☐ Directement auprès de la personne concernée
- ☐ Indirectement (utilisation d'une autre BDD, achat d'un fichier, …) : _____

- Type de personnes concernées :
- ☐ Salariés
- ☐ Usagers
- ☐ Visiteurs
- ☐ Adhérents
- ☐ Clients (actuels)
- ☐ Prospects (potentiels futurs clients)
- ☐ Autres : _____

- Utilisation d'une technologie particulière :
- ☐ Dispositif sans contact (RFID) : _____
- ☐ Mécanisme d'anonymisation : _____
- ☐ Mécanisme de pseudonymisation : _____
- ☐ Carte à puce : _____
- ☐ Géolocalisation : _____

☐ Vidéo protection : _____
☐ Nanotechnologies : _____
☐ Profilage : _____
☐ Autre : _____

- Durée de conservation prévue :
☐ 1 mois
☐ 2 mois
☐ 3 mois
☐ Pendant la durée de la relation contractuelle
☐ Illimitée
☐ Autre : _____

- Une suppression définitive est-elle possible à l'issue de ce délai ?
☐ Oui : _____
☐ Non : _____

- Un processus d'archivage ou de suppression automatique est-il prévu ?
• Oui : _____
• Non : _____

- Destinataire(s) des Données :
☐ Autre Département / Service de S2H Groupe : _____
☐ Prestataire / Fournisseur : _____
☐ Filiale / Autre entité du Groupe : _____
☐ Personnes concernées par le traitement : _____
☐ Autre : _____

- Sécurité du traitement :
☐ Accès physique au traitement est protégé
☐ Procédé d'authentification des utilisateurs mis en œuvre
☐ Journalisation des connexions
☐ Traitement réalisé sur un réseau interne dédié (non relié à internet)
☐ Autre : _____

- Transferts de Données hors UE :
☐ Oui :
o Vers quel pays ? _____
o Le transfert est-il sécurisé ? Si oui, comment ? _____
☐ Non

- Droit des personnes concernées :
• Les personnes seront-elles informées du traitement ?
☐ Oui. Comment ? _____
☐ Non
• Pourront-elles donner leur consentement ?
☐ Oui. Comment ? _____
☐ Non. Pourquoi ? _____

• La mise en œuvre des droits des personnes concernées est-elle prévue (accès, rectification, portabilité, suppression, …) ?
☐ Oui. Comment ? _____
☐ Non : _____

3. Acteurs de consultation :

☐ DRC _____ le ___/___/_____
☐ DJ : _____le ___/___/_____

- ☐ DSI : _____ le ___/___/_____
- ☐ DG : _____ le ___/___/_____

ANNEXE 4 : Remonter une demande d'exercice de droit d'une personne physique au DPO (Utilisation interne Groupe Diot Siaci)

FORMULAIRE DE TRANSMISSION D'UNE DEMANDE D'EXERCICE DES DROITS PAR UNE PERSONNE CONCERNEE (INTERNE)

Informations sur la personne ayant reçu la demande :

- Demande reçue le : _____/_____/_____, à ____H_____
- Demande reçue par :
- Entité :
- Service :

Informations sur la personne concernée :

- Nom :
- Prénom :
- Adresse postale :
- Téléphone :
- Adresse mail :
- Autre information mentionnée :

Informations sur la demande :

- Type de demande (cochez la demande exercée par la personne – possibilité qu'il y ait plusieurs choix – et indiquer si la personne concernée a précisé sa demande)

□ Demande d'accès :
□ Demande de rectification :
□ Demande de suppression / effacement :
□ Demande de portabilité :
□ Demande de limitation du traitement :
□ Demande d'opposition au traitement :
□ Demande d'organisation de directives après le décès :

- Transmission de la demande au DPO S2H Groupe le : _____/_____/_____, à ____H_____

Nom et signature de la personne ayant reçu la demande

ANNEXE 5 : Adresser une demande de droit d'une personne concernée au Responsable de Traitement lorsque le Groupe Diot Siaci est sous-traitant (Utilisation interne Groupe Diot Siaci)

FORMULAIRE DE TRANSMISSION D'UNE DEMANDE D'EXERCICE DES DROITS PAR UNE PERSONNE CONCERNEE AU RESPONSABLE DE TRAITEMENT : Société X (Responsable de traitement hors Groupe Diot Siaci)

Informations sur la personne ayant reçu la demande :

- Demande reçue le : _____/_____/_____, à ____H_____
- Demande reçue par :
- Entreprise : Société X
- Service :
- Qualité (prestataire de service, fournisseur, développeur, hébergeur, …) :
- Responsable de traitement :

Informations sur la personne concernée :

- Nom :
- Prénom :
- Adresse postale :
- Téléphone :
- Adresse mail :
- Autre information mentionnée :

Informations sur la demande :

- Type de demande (cochez la demande exercée par la personne – possibilité qu'il y ait plusieurs choix – et indiquer si la personne concernée a précisé sa demande)

□ Demande d'accès :
□ Demande de rectification :
□ Demande de suppression / effacement :
□ Demande de portabilité :
□ Demande de limitation du traitement :
□ Demande d'opposition au traitement :
□ Demande d'organisation de directives après le décès :

- Transmission de la demande au DPO S2H Groupe le : _____/_____/_____, à ____H_____

Nom et signature de la personne ayant reçu la demande