POLITIQUE DE PROTECTION DES DONNEES

DATE	REDACTION	VALIDATION	VERSION
18/09/2020	FRANCESCA SERIO	MARINE LACREUSE (DPO)	V1

TABLE DES MATIERES

1. PRESENTATION GENERALE

1.1 Cadre réglementaire

Le Conseil et Parlement Européen ont adopté le 27 avril 2016 un règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, généralement nommé « Règlement Général sur la Protection des Données » (ci-après RGPD). Ce Règlement définit les règles à respecter dans la manipulation de données à caractère personnel (DCP).

L'Assemblée Nationale a adopté la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles modifiant ainsi la loi n°78-17 du 6 janvier 1978 dite « Loi Informatique et Libertés ».

La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité publique en charge d'assurer la régulation autour des DCP en France.

EALIS, en tant qu'organisme privé, réalise des missions nécessitant le traitement de DCP et doit respecter les exigences imposées par ce texte.

1.2 Contexte d'EALIS

1.2.1 Rappel du projet

« EALIS » s'entend du Groupe EALIS, c'est-à-dire la société EALIS et les sociétés qu'elle contrôle au sens de l'article L. 233-3 du Code de commerce, notamment Garantie Privée et National Electronique Service. EALIS a engagé en 2019 une démarche de mise en conformité au RGPD, conscient de la nécessité de protéger davantage les données à caractère personnel de ses salariés et de ses collaborateurs.

EALIS a ainsi commencé par :

- Identifier ses traitements de données à caractère personnel sur un périmètre métier impliquant les données clients ;
- Hiérarchiser et prioriser les points de non-conformité aux exigences du Règlement ;
- Construire une feuille de route pour renforcer son niveau de conformité de manière progressive.

EALIS dispose aujourd'hui d'une structure pour assurer sa conformité au RGPD et pour la maintenir sur le long terme.

1.2.2 Contexte organisationnel et périmètre des DCP traitées par EALIS_

Dans le cadre de son activité EALIS traite des données à caractère personnel de ses collaborateurs ainsi que de ses clients. Les entités d'EALIS concernées par le traitement de données à caractère personnel sont les suivantes :

- GARANTIE PRVEE : dans la gestion des contrats d'assurance ;
- NES : dans la gestion des contrats de garanties, d'extensions de garantie et des activités de réparation.

1.2.3 Risques et enjeux d'EALIS relatifs à la protection des DCP

Les enjeux d'EALIS relatifs à la protection des DCP sont les suivants :

- Intégrer les exigences règlementaires au sein des processus et activités d'EALIS impliquant le traitement de DCP ;
- Assurer la protection des droits et libertés des personnes dont les données sont traitées ;
- Déployer une organisation adaptée permettant de maintenir le respect de ces exigences.

Les principaux risques d'EALIS relatifs à la protection des DCP sont les suivants :

- Un risque de dégradation de l'image d'EALIS au sein de l'opinion publique en cas :
  - De publication par la CNIL d'un avertissement ou d'une sanction adressée à EALIS ;
  - D'une violation de données à caractère personnel générant des impacts sur la vie privée des personnes ;
  - De la constatation par le grand public d'un défaut de conformité d'EALIS sur ses traitements de données ;
- Un risque d'impact sur EALIS en cas de défaut de conformité d'un traitement de DCP du fait de l'impossibilité d'exploiter les données ;
- Un risque financier lié à une sanction financière par la CNIL ;
- Une perte de maîtrise des actions effectuées par les sous-traitants d'EALIS sur les DCP.

1.2.4 Ambitions et engagements d'EALIS pour la protection des DCP

Les ambitions d'EALIS pour la protection des DCP qu'elle traite sont les suivantes :

- Assurer la protection de la vie privée et des libertés fondamentales des personnes dont EALIS traite les données ;
- Maintenir sa conformité avec les exigences règlementaires issues de la règlementation sur la protection des données, ainsi que des bonnes pratiques publiées par la CNIL.

Pour porter ces ambitions, EALIS adopte les engagements suivants :

- Déployer une organisation adaptée s'appuyant sur des processus structurés par les exigences règlementaires ;
- Impliquer et responsabiliser l'ensemble de ses partenaires dans cette démarche, et notamment les sous-traitants intervenant dans les opérations de traitement de DCP ;
- Maintenir une démarche d'amélioration continue de ces processus.

1.2.5 Modalités de conformité mises en place

Les modalités de conformité aux exigences de la protection des DCP mises en place par EALIS sont les suivantes :

- La définition d'un corpus documentaire (politique, procédures et outils) encadrant les processus internes liés à la protection des données pour EALIS ;
- La mise en place et la nomination auprès de la CNIL d'un **Délégué à la Protection des Données** (ou « DPO » - « *Data Protection Officer* ») depuis le 25 mai 2018, réalisant le pilotage et la gouvernance de la protection des données ;

- La mise en place d'une filière impliquant des acteurs internes pour assurer la protection des données ;
- La mise en place d'instances de gouvernance pour assurer le pilotage de la protection des DCP.

1.3 Objectifs, destinataires et périmètres de la politique de protection des données

1.3.1 Objectifs de la politique

La présente politique a pour objectif de définir les principes généraux de protection des DCP et de gestion de traitements de DCP d'EALIS pour :

- **Piloter le projet de la conformité au RGPD** : identifier l'ensemble des procédures et outils, les acteurs, les interactions et instances de gouvernances pour la protection des DCP ;
- **Encadrer les nouveaux projets en structurant le processus de Privacy by Design** : cadrage de tout nouveau traitement, la licéité et finalité des traitements, la gestion des durées de conservation, la sécurité des données à assurer, la gestion des sous-traitants, l'information des personnes concernées, les analyses d'impact relatives à la protection des données, et la revue globale de ces principes avant déploiement ;
- **Assurer la protection des données au quotidien** : maintien des registres, la sensibilisation des collaborateurs, la gestion des droits des personnes, la gestion des violations de leurs données, la coopération avec l'autorité de contrôle, le contrôle interne par les métiers et le rôle du DPO ;
- **Réaliser les opérations de contrôles du respect des exigences RGPD** : les opérations de contrôle des exigences de la présente politique et le contrôle des tiers intervenant sur des traitements.

Ces différents principes alimentent un tableau de bord permettant de piloter la conformité d'EALIS. Ces éléments seront détaillés dans des documents spécifiques.

1.3.2 Destinataires de la politique de protection des données

Les destinataires de la présente politique sont l'ensemble des collaborateurs d'EALIS, à savoir notamment :

- Les instances de gouvernance d'EALIS ;
- Les collaborateurs internes d'EALIS ;
- L'ensemble des prestataires et partenaires d'EALIS susceptibles de traiter des DCP en lien avec EALIS.

La présente politique est communiquée à ces destinataires sur demande.

1.3.3 Périmètre de la politique de protection des données pour EALIS

La présente politique porte sur trois catégories de traitements de DCP :

- Ceux mis en place par EALIS pour ses fonctions internes, et pour lesquels elle est « responsable de traitement » au sens du RGPD, sans implication de sous-traitant ;

- Ceux mis en place par EALIS pour ses fonctions internes, et pour lesquels elle est « responsable de traitement » au sens du RGPD, avec l'implication de sous-traitant réalisant des opérations pour le compte d'EALIS ;
- Ceux pour lesquels EALIS est « sous-traitante » au sens du RGPD, et effectués pour le compte d'un « responsable de traitement ».

Les principes à respecter seront applicables pour les trois catégories de traitements, sauf indication spécifique mentionnée dans la présente politique.

1.4 Rappel des définitions et notions

Sont indiquées dans le glossaire (Annexe 1), les principales définitions des termes utilisés dans la présente politique. Ces définitions sont des simplifications des définitions juridiques définies dans le RGPD (notamment à l'article 4 du RGPD[1]) ainsi que la loi dite « Informatique et libertés »[2].
Toute partie prenante impliquée dans des opérations de traitement de DCP effectuées par EALIS est invitée à se référer au RGPD et à la loi Informatique et Libertés pour obtenir des informations détaillées sur ce texte.

1.5 Corpus documentaire liés à la protection des DCP

La politique de protection des données définit un ensemble de principes à respecter pour assurer la protection des DCP.

Ces processus ont été synthétisés dans un document présentant les principes de gouvernance de la protection des données, les acteurs et les instances (document ***« Gouvernance de la protection des données »*).**

Plusieurs points de la présente politique sont déclinés en procédures ou politiques distinctes :
- Politique de formation au RGPD ;
- Politique de conservation des données personnelles ;
- Procédure de notification des violations de données personnelles ;
- Procédure de gestion des commentaires ;
- Procédure de gestion de la hotline ;
- Procédure de gestion du *Privacy by design* ;
- Procédure de gestion des analyses d'impact (PIA) ;
- Procédure de gestion des audits et contrôles.
- Procédure de gestion des droits des personnes.

Les procédures s'accompagnent d'outils permettant de les mettre en œuvre :
- Registre des traitements de données ;
- Registre des demandes de droits des personnes ;
- Outil de *Privacy by design* ;
- Questionnaire Sous-traitant.

L'objet de ces documents est détaillé en Annexe 4.

[1] Le texte du RGPD est disponible sur le site de la CNIL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[2] Le texte de cette loi est disponible sur le site de la CNIL : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

2. GOUVERNANCE DE LA PROTECTION DES DONNEES

2.1 Maintien de la politique, des procédures et des outils

Une revue annuelle de la politique, des procédures et des outils est effectuée.
De plus, une revue est effectuée à chaque évolution :

- Juridique : toute évolution règlementaire impactant la protection des données, ou toute publication de la CNIL précisant les modalités de gestion des DCP
- Organisationnelle : tout changement majeur de l'organisation d'EALIS.

La politique de protection des données est validée par le DPO et le Direction d'EALIS.

2.2 Animation de la filière DPO

EALIS a défini une organisation de gouvernance de la protection des données, s'appuyant sur plusieurs acteurs, les relais DPO
Ces principes sont définis dans le **document « *Gouvernance de la protection des données* ».**

2.2.1 Organisation de la filière DPO

La filière DPO est composée de la façon suivante :

- Les membres de la Direction d'EALIS
- Les Directions métiers
- Le DPO
- Les relais du DPO intervenant auprès de chaque Direction métier d'EALIS

2.2.2 Rôle et responsabilité des membres de la filière DPO

Les rôles et responsabilités des acteurs de la filière DPO sont les suivants :

- **EALIS** en tant qu'organisme privé, assure la responsabilité des opérations de traitement effectuées dans le cadre de ses activités. Au sens du RGPD, EALIS est donc **« responsable de traitement »** ;
- **La Direction** assure le suivi de la gouvernance de la protection des données et valide la présente politique de Protection des données. Il réalise les arbitrages nécessaires sur les traitements de DCP s'appuyant sur les processus d'EALIS pour traiter les objectifs de conformité au RGPD ;
- **Le DPO** conseille et contrôle le respect des principes de protection des DCP au sein d'EALIS ;
- **Les Directions métiers qui sont « représentantes du responsable de traitement »,** et qui sont responsables de l'application des principes de protection des DCP pour les traitements nécessaires à leurs activités ;
- **Des relais DPO** qui sont identifiés pour chaque direction métier d'EALIS. Ils sont chargés de conseiller les directions métiers dans le déploiement des principes liés aux DCP, et de suivre et contribuer au contrôle du respect de ces principes pour les traitements dont chaque Direction métier a la responsabilité. Ils sont identifiés en considération de leurs fonctions opérationnelles et/ou de leur ancienneté par le DPO et les directeurs métiers ;
- **La Direction Juridique (DJUR)** apporte son expertise juridique et sa connaissance de la règlementation au DPO et métiers ;
- **La Direction des Systèmes d'Information (DSI)** apporte son expertise relative aux systèmes d'information d'EALIS.

N.B :

- **Les direction métiers et les relais sont mobilisés pour les opérations de traitements de données.**
- **Point d'attention relatif à des données utilisées par plusieurs Directions :**
  - Certains traitements de données sont opérés par des Directions métiers en s'appuyant sur des données collectées et traitées en amont par d'autres Directions métiers.
  - Chaque Direction métier est responsable du traitement qu'elle réalise sur son périmètre. En cas de traitement partagé, les relais DPO veilleront à la conformité dans le temps de ces traitements partagés.

2.2.3 Comitologie

Des instances de gouvernance sont organisées afin d'assurer le pilotage de la protection des données. L'organisation de ces instances est décrite dans le support « ***Gouvernance de la protection des données*** **».**

2.3 Veille sur la gestion des DCP

Une veille juridique sur les principes relatifs à la protection des données est réalisée via le dispositif de veille déployé par la DJUR. Ces sujets sont notamment :

- Suivi de l'évolution règlementaire liée à la protection des DCP ;
- Suivi des publications assurées par la CNIL ou tout organisme public compétent pour définir des principes généraux à respecter sur la protection des données.

Le DPO s'appuie sur cette veille juridique.

2.4 Plan de sensibilisation des collaborateurs

EALIS établi chaque année un plan de sensibilisation des DCP des collaborateurs internes. Ce plan intègre tout moyen d'assurer la sensibilisation des collaborateurs d'EALIS aux principes de gestion et de protection des DCP.

Le plan de sensibilisation est destiné aux acteurs mentionnés au point 1.3.2 relatif aux destinataires de la présente politique.

Ce plan est mis à jour chaque année.

3. CADRAGE DE LA MISE EN PLACE DE TRAITEMENTS DE DCP

Les principes définis dans le présent chapitre ont pour objectif d'assurer un cadrage de tout projet de mise en place de traitement de DCP.

La **Procédure de gestion du *Privacy by design*** décrit la démarche à suivre pour s'assurer de l'intégration de ces principes dans les projets de mise en place de traitements de DCP. Cette procédure est applicable aux différents paragraphes du présent chapitre.

3.1 Principe général du « Privacy by design / by default »

Le « Privacy by design » *est un concept ayant pour objectif de garantir que la protection de la vie privée soit intégrée dans tout projet ou application dès leur conception.*
Le « Privacy by default » *est le fait de garantir que par défaut, le plus haut niveau de protection des DCP est appliqué.*

Avant tout déploiement d'un traitement de DCP, EALIS s'assure de :

- Pour le respect du principe de « Privacy by Design » :
  - Que les informations relatives au projet de traitement et que l'ensemble des mesures techniques et organisationnelles nécessaires pour la conformité du traitement et la protection des données ont été définies ;
  - Que ces informations ont été documentées dans le respect de la **Procédure de gestion du *Privacy by design,*** via l'**Outil de *Privacy by Design.***

- Pour le respect du principe de « Privacy by Default » :
  - Qu'un principe de minimisation des données collectées soit appliqué au projet (seules les DCP nécessaires à la finalité sont collectées, conservées durant le temps de l'objectif poursuivi, rendues accessibles à des destinataires dont l'accès est justifié par les besoins du traitement, et les commentaires sont encadrés selon la **Procédure de gestion des zones de commentaire**).
  - Que les moyens nécessaires au maintien de ce principe de minimisation tout au long du cycle de vie du projet sont maintenus, notamment par la suppression des données non nécessaires au traitement qui auraient pu être collectées ou communiquées à EALIS.

3.2 Principes relatifs à la licéité des traitements de DCP

Avant tout déploiement d'un traitement de DCP, EALIS s'assure que le traitement de DCP repose sur l'une des bases légales suivantes :

- Les personnes concernées ont donné leur consentement à ce que leurs DCP soient traitées pour une ou plusieurs finalités spécifiques, et la preuve de ce consentement a été tracée ;
- Les personnes concernées sont parties à des mesures précontractuelles ou un contrat passé avec EALIS qui nécessitent le traitement de leurs DCP ;
- Le traitement est nécessaire au respect d'une obligation légale d'EALIS ;
- Le traitement est nécessaire pour les intérêts légitimes d'EALIS : qui ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées, notamment si la personne

concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ;

- Le traitement est nécessaire pour l'intérêt vital d'une personne concernée (protection d'un intérêt essentiel à la vie de la personne dont les données sont traitées, etc.).

3.3 Principe relatif à la finalité du traitement

Avant tout déploiement d'un traitement de DCP, EALIS s'assure que celui-ci est effectué selon une finalité définie, et qui sera respectée durant tout le cycle de vie de ce traitement.

3.4 Principes relatifs aux durées de conservation

Avant tout déploiement d'un traitement de DCP, EALIS s'assure de déterminer la durée de conservation des DCP traitées, selon deux principes :

- La durée déterminée doit dans tous les cas être alignée avec les recommandations définies par la réglementation, la CNIL et, le cas échéant, la jurisprudence
- La durée déterminée doit être alignée avec les besoins d'EALIS sur la base de la finalité du traitement de DCP

La **Politique de conservation des données** décrit la démarche à suivre dans la détermination des durées de conservation des DCP ainsi que les rôles et responsabilités des acteurs au processus.

3.5 Principes relatifs à la gestion des DCP sensibles et aux condamnations pénales / infractions

Avant tout déploiement d'un traitement de DCP, EALIS s'assure qu'aucune donnée dite sensible n'est collectée. Le détail de ces données est présenté en **Annexe 3 – Données sensibles.**

Ces données peuvent être utilisées dans l'un des cas suivants :

- La personne concernée a donné son consentement libre et éclairé au traitement de ces données ;
- Le traitement est nécessaire pour l'exécution d'obligation ou des droits d'EALIS ou de la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;
- Le traitement porte sur des données qui ont été rendues manifestement publiques par la personne concernée ;
- Le traitement est nécessaire à la constatation de l'exercice d'un droit en justice ;
- Le traitement est nécessaire pour des motifs d'intérêt public ;
- Le traitement est nécessaire aux fins de la médecine du travail.

EALIS s'assure également qu'elle ne traite pas de données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté que dans des cas autorisés par la loi.

3.6 Principes relatifs au choix des sous-traitants

Dans le choix des sous-traitants, EALIS s'assure que les sous-traitants garantissent les mesures adéquates pour assurer la protection des DCP. Cette vérification doit se faire selon les modalités suivantes :

- L'analyse des réponses apportées par le sous-traitant au **Questionnaire sous-traitant** permettant d'évaluer les garanties qu'il apporte pour la protection des données ;
- L'analyse des engagements donnés par le sous-traitant, via les clauses contractuelles adaptées permettent de s'assurer de :
    - La protection des DCP ;
    - Le respect des exigences règlementaires ;
    - La contribution au maintien de la conformité d'EALIS, notamment par l'apport de toute information nécessaire pour le traitement (informations nécessaires pour le maintien et la mise à jour du registre des traitements d'EALIS, gestion des violations de données, gestion des demandes d'exercice des droits des personnes, etc.)
    - La possibilité d'auditer le sous-traitant pour s'assurer du respect de ses engagements.

Les garanties et engagements pris par le sous-traitant sont un critère de choix dans l'attribution des marchés.

3.7 Principes relatifs à la transparence et l'information des personnes concernées

Avant tout déploiement d'un traitement de DCP, EALIS s'assure de la transparence du traitement auprès des personnes concernées. Cette transparence est assurée par :

- La production, à l'encontre des personnes concernées, de mentions d'information respectant les exigences du RGPD ;
- La possibilité donnée aux personnes concernées d'exercer leurs droits (cf. **Annexe 2 – Définition des droits des personnes concernées**).

3.8 Principes relatifs à l'analyse d'impact sur la protection des données privée

EALIS s'assure avant toute mise en place d'un traitement de DCP :

- Que la nécessité ou non de mener une analyse d'impact a été déterminée ;
- S'il apparaît qu'une analyse d'impact sur la vie privée est nécessaire, qu'une analyse d'impact sur la protection des données a été formalisée conformément ;
- Que les mesures techniques et organisationnelles adaptées ont été déployées.

La **Procédure de Gestion des Analyses d'Impact (PIA)** décrit la démarche à suivre dans la réalisation des PIA ainsi que les rôles et responsabilités des acteurs au processus.

3.9 Principe de revue de la bonne application des mesures

Avant tout déploiement d'un traitement de DCP, EALIS s'assure de vérifier l'application des différentes mesures énoncées dans le présent paragraphe.
Cette vérification est effectuée via une revue du bon déploiement des principes documentés dans l'**Outil de Privacy by Design** pour chaque traitement.

4. PROTECTION DES DONNEES AU QUOTIDIEN

4.1 Registres d'EALIS

EALIS s'assure de documenter toute évolution ou tout nouveau traitement dans les fiches de registre des traitements (outil « **Registre des traitements de données** »).

Pour les traitements pour lesquels EALIS fait appel à des sous-traitants, il est nécessaire de maintenir la liste de sous-traitance, détaillant les informations suivantes :

- L'ensemble des sous-traitants EALIS ;
- Les mesures permettant de s'assurer que les tiers fournissent un niveau de protection adéquat.

4.2 Assurer l'exercice des droits des personnes concernées

EALIS s'assure de traiter les demandes d'exercice d'un droit par une personne concernée. L'ensemble de ces droits est défini en **Annexe 2 – Définition des droits des personnes**.

La **Procédure de Gestion des droits des personnes** décrit la démarche à suivre dans le traitement des demandes d'exercice d'un droit ainsi que les rôles et responsabilités des acteurs au processus.

4.3 Gestion des violations de DCP

EALIS s'assure que toute violation de donnée fait l'objet des actions suivantes :

- Notification auprès de la CNIL ;
- Communication auprès des personnes concernées, si applicable.

La **Procédure de Notification des violations de données personnelles** décrit la démarche à suivre dans la gestion des violations de DCP ainsi que les rôles et responsabilités des acteurs au processus.

4.4 Point de contact avec l'autorité de contrôle

Pour toute sollicitation effectuée par la CNIL, EALIS s'assure que son DPO est son point de contact unique :

- Toute demande émise par la CNIL à EALIS est remise au DPO ainsi qu'à la partie prenante / métier concerné par la demande, dans les plus brefs délais ;
- Le DPO coopère avec la CNIL et lui fournit la documentation nécessaire conformément aux Procédures de **Gestion des audits et contrôles** et de **Gestion des violations de données**.

4.5 Autocontrôle des opérations de traitement

EALIS s'assure que des opérations d'autocontrôles sont réalisées et tracées tout au long du cycle de vie du traitement de DCP par les parties prenantes intervenant sur les DCP.

La **Procédure de Gestion des audits et contrôles** décrit les principes à suivre dans l'application des autocontrôles et les rôles et responsabilités des acteurs au processus.

4.6 Conseil et sensibilisation des collaborateurs d'EALIS

EALIS s'assure que toute demande de conseil par l'un des destinataires de la présente politique est suivie et traitée, notamment par l'intermédiaire des relais DPO et de son DPO.

EALIS s'assure de la sensibilisation de l'ensemble de ses collaborateurs à la gestion et la manipulation des DCP conformément aux exigences du RGPD déclinées dans la présente politique.

5. PRINCIPES A RESPECTER DANS LE CONTROLE DU RESPECT DE LA CONFORMITE

5.1 Contrôle interne

EALIS s'assure que le DPO définit un plan de contrôle permettant de vérifier le respect de l'application des principes de protection des données.

La **Procédure de Gestion des audits et contrôles** décrit la démarche à suivre dans l'application des contrôles internes et les rôles et responsabilités des acteurs au processus.

5.2 Contrôles des tiers

EALIS peut réaliser des opérations d'audits réguliers de ses sous-traitants.

Annexe 1 : Définition des notions de base - Glossaire

Définitions des notions de bases		
Nom	**Définition**	**Articles du RGPD**
Données personnelles (Données à caractère personnel)	Toute information se rapportant à une personne physique identifiée ou identifiable	Article 4 – 1)
Personnes concernées	Personnes dont les DCP font l'objet d'un traitement	Article 4 – 1)
Traitement de DCP	Toute opération réalisée sur des DCP	Article 4 – 2)
Responsable de traitement	Acteur définissant pourquoi et comment va être mis en place un traitement de données	Article 4 – 7)
Délégué à la protection des données	Acteur chargé d'accompagner les organisations pour conseiller et suivre le respect du RGPD	Article 39
Sous-traitant	Acteur réalisant un ou plusieurs traitements de DCP pour le compte du responsable de traitement	Article 4 – 8)
Violation de DCP	Tout incident de sécurité créant une perte de confidentialité ou destruction de DCP	Article 4 – 12)
« Privacy by design »	Le *Privacy by design* est un concept ayant pour objectif de garantir que les principes de protection des DCP soient intégrés dans tous projets ou applications dès leur conception	Article 24
« Privacy by default »	Le *Privacy by default* est le fait de garantir que, par défaut, le plus haut niveau de protection des DCP est appliqué	Article 25

Annexe 2 : Définition des droits des personnes concernées

Exigences relatives aux droits des personnes concernées	
Droits	**Exigences**
Droit d'accès	EALIS s'assure que les personnes concernées ont un droit d'accès à leurs DCP
Droit d'opposition	EALIS s'assure que les personnes concernées sont en mesure de s'opposer à la réalisation d'un traitement de DCP
Droit de rectification	EALIS s'assure que les personnes concernées ont un droit de rectifier les DCP incomplètes ou incorrectes qui font l'objet de traitement de DCP
Droit à l'effacement	EALIS s'assure que les personnes concernées ont un droit à l'effacement de leurs DCP
Droit à la portabilité	EALIS s'assure que les traitements de données qu'il effectue permettent la portabilité des DCP traitées (possibilité d'exporter les données traitées sur un format interopérable)
Droit à la limitation du traitement	EALIS s'assure que les traitements de DCP qu'il effectue peuvent être restreints selon les demandes des personnes concernées
Droit d'opposition au profilage	EALIS s'assure que les personnes concernées ont la possibilité de demander une intervention humaine dans le traitement de leurs données soumis à profilage

Annexe 3 : Données « sensibles »

Les données définies par le RGPD dans son article 9 comme « sensibles » sont les suivantes :

- L'origine raciale ou ethnique ;
- Les opinions politiques ;
- Les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
- Les données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique ;
- Les données concernant la santé ;
- Les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Annexe 4 : Composition du corpus documentaire

Sont listés ci-dessous les documents du corpus documentaire de protection des données :

Document	Objet
Politique de protection des données	Politique cadre définissant les principes généraux de protection des DCP et de gestion de traitements de DCP d'EALIS (présent document).
Politique de formation au RGPD	Politique détaillant les plans de formation et de sensibilisation des collaborateurs d'EALIS en ce qui concerne la protection des données personnelles.
Politique de conservation des données personnelles	Politique détaillant les principes et règles à respecter pour la conservation de DCP, et les rôles des parties prenantes à ce processus.
Procédure de gestion des commentaires	Procédure détaillant les principes et règles à respecter dans l'utilisation de zones de texte / commentaires libres dans des traitements de DCP, et les rôles des parties prenantes à ce processus.
Procédure de gestion de la hotline	Procédure détaillant les principes et règles à respecter en matière de protection des données dans le cadre des processus hotline.
Procédure de gestion des Analyses d'Impact (PIA)	Procédure détaillant les principes et règles à respecter pour identifier les traitements de DCP porteur de risque et définir des mesures permettant de réduire ces risques, et les rôles des parties prenantes à ce processus.
Procédure de gestion des audits et contrôles	Procédure détaillant les principes et règles à respecter en matière de contrôle interne du respect des exigences de la politique de protection des données et des procédures, d'audit des sous-traitant de traitements de DCP, et les rôles des parties prenantes à ces activités.
Procédure de notification des violations de données personnelles	Procédure détaillant les principes, règles et étapes à respecter dans la gestion d'une violation de DCP, et les rôles des parties prenantes à ce processus.

Procédure de gestion du Privacy by Design	Procédure détaillant les principes, règles et étapes à respecter dans la définition d'un traitement de DCP et les rôles des parties prenantes à ce processus.
Procédure de gestion des droits des personnes	Procédure détaillant les principes, règles et étapes à respecter pour traiter les demandes d'exercice de droit des personnes dont EALIS traite les données (détaillé en annexe 2).
Registre des traitements de données	Outil recensant l'ensemble des traitements de DCP réalisé par EALIS en tant que responsable de traitement ou par EALIS en tant que sous-traitant.
Registre des demandes des droits des personnes	Outil recensant l'ensemble des demandes d'exercice de droits des personnes dont EALIS traite les DCP et listant le suivi à date du traitement de ces demandes.
Questionnaire « Privacy By Design »	Outil permettant de documenter lors des phases de projets l'ensemble des mesures prévues, développées et vérifiées permettant de s'assurer que les principes de la présente politique de protection des données est respectée avant tout déploiement.
Questionnaire Sous-traitant	Outil / questionnaire permettant de solliciter les futurs sous-traitant d'EALIS afin d'identifier s'ils respectent les principes de protection des DCP.