ELIOR GROUP

Politique de protection des données à caractère personnel

Périmètre	Tous périmètres
Version	V1
Rédacteur	Comité opérationnel DCP
Validateur	Comité de pilotage DCP
Date de publication	01/03/2019
Date de mise à jour	

Introduction

La présente politique de protection des données à caractère personnel définit la manière dont le groupe Elior procède lors de la mise en œuvre de traitements de données à caractère personnel pour garantir la protection des libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.

Elle définit les normes que tous les collaborateurs, collaboratrices, partenaires et sous-traitants du Groupe Elior doivent respecter lorsqu'ils traitent des données à caractère personnel.

Il est rappelé que le non-respect des obligations concernant la protection des données à caractère personnel expose le groupe Elior à une sanction de 4 % de son chiffre d'affaires mondial ; à titre indicatif, cela représente près de 268 millions d'euros sur la base des résultats de l'exercice clos au 30 septembre 2018.

Chacune des personnes concernées doit notamment veiller :

- au respect du principe de protection de la vie privée dès la conception de nouveaux projets (*privacy by design*), et notamment à ce que chaque traitement de données (i) corresponde à une finalité délimitée, (ii) prévoie d'informer les personnes du traitement de données mis en œuvre, (iii) détermine des mesures de protection et (iv) fixe une durée de conservation des données à caractère personnel ;
- au respect des délais imposés concernant la réponse aux demandes d'exercice des droits, à savoir un mois, et à la notification de toute fuite de données aux autorités compétentes sous 72 heures ;
- plus généralement, au respect des processus et recommandations mis en place par la présente politique et à la sollicitation, le cas échéant, des ambassadeurs de protection des données à caractère personnel ou de l'équipe GDPR du Groupe Elior via l'adresse gdpr-contact@eliorgroup.com.

Glossaire

« **groupe Elior** » désigne la société Elior Group ainsi que toutes les sociétés qui, au sens de l'article L233-3 du Code de Commerce,

(i) sont sous son contrôle direct ou indirect de la société Elior Group, ou,

(ii) sont, directement ou indirectement, sous contrôle commun avec la société Elior Group ;

« **donnée(s) à caractère personnel** », « **donnée(s) personnelle(s)** » ou encore « **DCP** » désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « **personne concernée** »). Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

« **traitement de données** » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

« **responsable du traitement** » désigne 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 ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union européenne ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union européenne ou par le droit d'un État membre ;

« **sous-traitant** » désigne 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 ;

« **responsable SI du traitement** » désigne le collaborateur au sein du groupe Elior, garant de la connaissance technique relative aux ressources informatiques impliquées dans le traitement, et ce pour chaque traitement de DCP identifié au sein du groupe Elior ;

« **responsable métier du traitement** » désigne le collaborateur au sein du groupe Elior, qui définit le besoin métier et les objectifs (maîtrise d'ouvrage) du traitement, et ce pour chaque traitement de données identifié au sein du groupe Elior ;

« **destinataire** » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, que ce destinataire soit ou non extérieur au groupe Elior (tiers). Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière ne sont pas considérées comme des destinataires ; le traitement de données à caractère personnel par ces autorités est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;

« **consentement [de la personne concernée]** » désigne toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne dont les données à caractère personnel sont traitées accepte, par une déclaration ou par un acte positif clair, que ces données fassent l'objet d'un traitement ;

« **violation de données à caractère personnel** » signifie une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou encore la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

« **règles d'entreprise contraignantes** » ou « **Binding Corporate Rules** » ou « **BCR** » désigne une politique de protection des données intra-Groupe dans le cadre de tout transfert de données personnelles intervenant en tout ou partie hors de l'Espace économique européen. Elles sont juridiquement contraignantes et respectées par les

entités signataires d'un groupe de sociétés, quel que soit leur pays d'implantation, ainsi que par tous les salariés d'une même entité juridique ou d'un même groupe de sociétés. Deux types de BCR existent : (i) les BCR

« responsable de traitement » qui permettent d'encadrer les transferts effectués au sein d'un groupe agissant en qualité de responsable de traitement, et (ii) les BCR « sous-traitant » qui permettent de créer une sphère de sécurité pour les transferts effectués lorsque le groupe agit en qualité de sous-traitant ;

« **analyse d'impact sur la protection des données** » ou « **Data Protection Impact Assessment** » ou « **DPIA** » signifie que le responsable du traitement effectue, avant tout traitement susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, en particulier par le recours à de nouvelles technologies, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Table des matières

1. Contexte

En tant que prestataire de services de restauration, la sécurité des aliments constitue un aspect fondamental de l'activité du groupe Elior. Proposer une alimentation saine, préparée et distribuée conformément à la règlementation en vigueur à ses clients et convives est une préoccupation permanente pour le groupe Elior, et constitue un des fondements de la confiance qu'ils lui accordent. Sur ce même schéma, réaliser des traitements de données à caractère personnel conformes à la législation en vigueur constitue un enjeu fondamental pour le groupe Elior.

En effet, l'évolution rapide des technologies et la mondialisation ont conduit à une augmentation substantielle des flux d'échanges de données à caractère personnel entre acteurs, ce qui se traduit par de nouveaux enjeux pour la protection des DCP. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante, ce qui favorise une utilisation et une valorisation de ces données sans précédent. Le groupe Elior, avec pour ambition de se différencier par l'innovation technologique dans le domaine du numérique et par une capacité croissante à collecter et exploiter des données, s'inscrit pleinement dans cette tendance. Les données sont omniprésentes et désormais positionnées au cœur de la chaîne de création de valeur. Bien gérées et sécurisées, elles permettent de gagner en efficacité et en compétitivité, de personnaliser et de conforter la relation avec les clients et les convives, de conquérir de nouveaux marchés, d'améliorer les produits et services, et de faciliter la collaboration et la mobilité.

Cela ne peut se faire sans établir la confiance qui permettra au positionnement numérique du groupe Elior de se développer, en garantissant aux équipes, aux clients, aux convives et plus généralement à tous les interlocuteurs du groupe Elior le contrôle des données à caractère personnel les concernant.

Devant l'émergence de cadres législatifs nationaux et supranationaux, le groupe Elior veille constamment à s'adapter aux enjeux du numérique et construit une démarche d'amélioration continue et de mise en conformité de la gestion des données à caractère personnel.

2. Périmètre

Le groupe Elior traite en permanence des données à caractère personnel dans le cadre de ses activités, par exemple :

- lors de la capture d'images à l'aide de caméras de vidéosurveillance ;
- lors du traitement de demandes formulées par les clients ;
- lors de la collecte des régimes alimentaires des convives afin de leur servir des repas appropriés ;
- ou encore, lors de la collecte d'informations sur les équipes dans le cadre de la gestion de leurs carrières.

La présente politique s'applique à tous les collaborateurs, collaboratrices, partenaires et sous-traitants du groupe Elior à chaque fois que sont recueillies, utilisées, rendues accessibles ou partagées des données à caractère personnel relatives aux clients, convives, équipes, fournisseurs ou autres personnes physiques.

Étant donnée la localisation du siège social du groupe Elior en France, cette politique vise notamment à répondre aux obligations mises en place par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, ci-après, « Règlement général sur la protection des données », « Règlement » ou « RGPD ».

Cette démarche s'inscrit dans une volonté d'harmoniser par le haut les pratiques au sein du groupe Elior, de simplifier le suivi et le maintien dans le temps de la conformité et de garantir un niveau élevé de protection des données à caractère personnel. Afin de parvenir à cet objectif, la présente politique se doit de prendre en compte dans la mesure du possible les spécificités nationales :

- au sein de l'Espace économique européen, parallèlement au Règlement général sur la protection des données, par le respect des dispositions législatives nationales spécifiques précisant les conditions dans lesquelles le traitement de données à caractère personnel est licite ;
- en dehors de l'Espace économique européen, par la prise en compte dans l'ensemble des États au sein desquels le groupe Elior est présent d'une législation nationale dédiée à la protection des données à caractère personnel, voire d'une autorité spécifiquement compétente pour son application.

Il convient de préciser que le droit à la protection des données à caractère personnel n'est pas un droit absolu, il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité, notamment le respect de la vie privée et familiale, du domicile et des communications, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information ou encore la liberté d'entreprendre. Cette politique ne vise pas à définir l'équilibre entre ces droits, qui devra être étudié au cas par cas par les services juridiques du groupe Elior au regard de l'évolution de la jurisprudence et des recommandations des autorités.

3. Gouvernance

A. Cadre général

La démarche de maîtrise de la gestion des données est pilotée par une **équipe Groupe** composée de :

- Un **Group Chief Compliance Officer** : directement rattaché au directeur général, il est chargé de la mise en œuvre des règles de conformité. Il est le garant de la prise en compte à un niveau optimal de la protection des données à caractère personnel au sein du groupe Elior ;

- Un **Group Data Protection Officer** (DPO) : il est le garant de la mise en œuvre du programme de protection des données à caractère personnel et du respect de la législation associée pour l'ensemble du groupe Elior. Il dispose d'une bonne connaissance des métiers et de l'organisation du groupe Elior, en particulier des opérations de traitement, des systèmes d'information et des besoins du groupe Elior en matière de protection et de sécurité des données. Il exerce ses fonctions et missions en toute indépendance et peut s'appuyer sur un **Group IT Security Compliance Manager**.

- Un **Group Senior Legal Counsel** : il accompagne et conseille le DPO dans la compréhension et l'interprétation des textes juridiques et dans la relation avec les autorités de protection des données à caractère personnel. Il est également le garant de la prise en compte de problématiques de protection des données à caractère personnel au sein des relations contractuelles.

L'équipe Groupe s'appuie sur des acteurs décentralisés dans le groupe Elior : les **ambassadeurs DCP**. Ces ambassadeurs DCP sont les relais du DPO au sein de leur périmètre et contribuent notamment :

- à la construction des politiques et procédures associées ;
- à la garantie de la conformité avec la politique Groupe, notamment vis-à-vis de l'exercice des droits et la tenue du registre des traitements ;
- à être les points de contact privilégiés vis-à-vis de l'équipe RGPD Groupe et de leur périmètre pour toute question relative aux DCP.

La présente politique est révisée sur une base annuelle, à l'initiative de l'équipe RGPD Groupe afin de prendre en compte toute évolution de la législation ou des pratiques internes au sein du groupe Elior. Il relève de la liberté de chacune des filiales du groupe Elior de s'organiser en interne et de décliner la présente politique afin d'en faciliter la diffusion et l'application.

B. Outil de la conformité

Le groupe Elior s'est doté récemment d'un logiciel de gestion de la conformité, permettant de répondre aux obligations relatives à la protection des données à caractère personnel et de piloter les démarches associées ou encore d'accompagner ses équipes dans le respect des règles de conformité dans le cadre de leurs activités.

L'ensemble des collaborateurs du groupe Elior appelés à avoir des responsabilités en matière de traitements de données à caractère personnel (à savoir les responsables SI et métier ainsi que les ambassadeurs DCP) disposent d'un accès à cet environnement. Cet outil permet notamment de :

- maintenir à jour les registres de traitement (responsable de traitement/sous-traitants) ;
- accompagner les responsables de projet dans l'application des exigences relatives à la protection des données ;
- générer des formulaires de contacts pour l'exercice des droits des personnes et piloter leur traitement ;
- maintenir un registre des sous-traitants ;
- gérer les notifications d'incidents ;
- plus généralement permettre le respect de la législation au sein du groupe Elior conformément au principe de responsabilisation.

Il est toutefois de la responsabilité :

- des chefs de projet (responsable SI et responsable métier) de renseigner tout nouveau traitement de données au sein de cet environnement et aux ambassadeurs DCP d'accompagner et de valider les informations renseignées ;
- des ambassadeurs DCP de veiller au bon traitement des demandes d'exercice des droits avec le soutien des responsables SI et métier.

C. Comité de pilotage DCP (CP DCP)

Animé par le DPO et sous la présidence du Group Chief Compliance Officer, le comité de pilotage des données à caractère personnel est l'instance décisionnelle.

Il a notamment les attributions suivantes relatives à la protection des données à caractère personnel au sein du groupe Elior :

- valider la politique et ses évolutions ;
- dresser le bilan annuel des actions ;
- prendre acte du niveau de conformité ;
- valider et arbitrer la priorité des actions.

En complément de l'équipe Groupe, le CP DCP est composé des membres suivants :

- le directeur des systèmes d'information Groupe ;
- le directeur juridique Groupe ;
- le directeur de l'audit interne Groupe ;
- le directeur assurances et prévention des risques Groupe ;
- les directeurs des systèmes d'information des opérations ;
- les directeurs juridiques opérations.

Un recueil des décisions du CP DCP sera formalisé par le DPO à l'issue des comités. Les comptes-rendus seront accessibles à l'ensemble des parties prenantes.

Le CP DCP se réunit sur une base annuelle. Il peut se réunir extraordinairement à l'occasion d'un évènement jugé significatif, sur proposition du DPO (incident majeur, arbitrage important, contrôle des autorités…).

D. Groupe de travail relatif à la protection des données à caractère personnel (GT)

Animé par le IT Security Compliance Manager et le Group Senior Legal Counsel sous la présidence du DPO, le comité opérationnel DCP est l'instance de planification et suivi des préconisations émises par le CP DCP.

En complément de l'équipe Groupe, sont également présents les ambassadeurs DCP des zones (restauration collective, restauration de concession et services) et, suivant opportunité, des ambassadeurs DCP à l'international.

Le CO DCP se réunit sur opportunité.

E. Animation transverse

L' IT Security Compliance Manager est responsable de l'animation des travaux relatifs à la protection des données à caractère personnel en France et à l'international. Il a également pour mission d'identifier et de diffuser les bonnes pratiques associées au sein du groupe Elior.

4. Nos obligations

La présente section décrit les diverses obligations liées à la protection des données à caractère personnel qui incombent au groupe Elior.

A. Responsabilité et inventaires des traitements

Le Règlement général sur la protection des données introduit le principe de responsabilisation, ou *accountability*, dans le cadre du traitement de données. Depuis son entrée en vigueur, le groupe Elior doit être capable de démontrer sa conformité vis-à-vis du règlement ; cela passe notamment par la réalisation de l'inventaire des traitements de données mis en œuvre.

Ainsi, deux types de registres sont à maintenir au sein du groupe Elior ; le premier concerne les traitements pour lesquels toute entité du groupe Elior est responsable de traitement, le second concerne les traitements pour lesquels toute entité du groupe Elior agit en qualité de sous-traitant.

Pour chacun des traitements pour lesquels le groupe Elior agit en tant que responsable de traitement, les informations suivantes doivent être contenues dans le registre :

- l'identité du responsable de traitement et des sous-traitants ;
- l'identité et les coordonnées des responsables SI et métier ;
- la finalité (l'objectif poursuivi par la collecte et le traitement de données) ;
- la base légale du traitement ;

- la liste des données collectées, leur durée de conservation et les personnes concernées ;
- les catégories de personnes ayant accès aux données (administrateur, ressources humaines, sous-traitants…) ;
- la présence de transfert vers un pays tiers ;
- la manière dont l'information des personnes est réalisée ;
- les mesures de sécurité mises en place ;
- éventuellement, les résultats de la DPIA.

Pour chacun des traitements pour lesquels le groupe Elior agit en tant que sous-traitant, les informations suivantes doivent être contenues dans le registre :

- le nom et coordonnées de chaque client pour le compte duquel sont traitées les données ;
- le nom et coordonnées de chaque sous-traitant ultérieur, le cas échéant ;
- les catégories des traitements effectués pour le compte de chaque client ;
- les transferts de données hors UE effectués pour le compte du client ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en place.

Il incombe aux responsables SI et métier de renseigner ce registre en s'appuyant sur leurs ambassadeurs DCP.

B. Transparence et loyauté

Transparence

Il est du devoir du groupe Elior et de ses équipes d'être clairs et transparents sur les traitements de données à caractère personnel. Les données qui sont collectées ne doivent pas être utilisées d'une manière et dans un objectif qui ne serait pas raisonnablement attendu et prévu au regard de la finalité poursuivie.

Par conséquent, avant de recueillir des données à caractère personnel, il convient de communiquer en langage clair et simple sur :

- qui nous sommes ;
- quelles sont les données à caractère personnel collectées et quelle en est la source ;
- les opérations qui vont être réalisées avec ces données à caractère personnel et la base légale ;
- si les données à caractère personnel sont ou vont être partagées avec d'autres destinataires ;
- la durée de conservation des données à caractère personnel ;
- si les données à caractère personnel vont être transférées en dehors de l'Espace économique européen ;
- les droits garantis aux personnes relatifs au traitement de données à caractère personnel.

Licéité du traitement

Afin qu'un traitement de données à caractère personnel soit licite, il est nécessaire d'avoir des raisons légitimes ou de justifier d'obligations légales ou encore d'avoir obtenu le consentement de la personne concernée. Ainsi, préalablement à tout traitement de données à caractère personnel, en complément de l'information des personnes, il convient de s'assurer que ce dernier repose sur l'une des bases suivantes :

- **Obligation légale** : le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (droit national ou droit de l'Union européenne) ; par exemple la communication à la sécurité sociale et à l'administration fiscale des données relatives à la rémunération des salariés.

- **Nécessité contractuelle** : 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.
  Cette situation doit uniquement couvrir les services essentiels à la réalisation du contrat et notamment exclure tout démarchage commercial ; par exemple, la collecte des coordonnées d'un convive pour l'édition et l'envoi de factures ou encore le traitement des données des salariés pour la mise en oeuvre de la paie.

- **Intérêts légitimes** : le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. L'intérêt légitime du responsable de traitement doit alors systématiquement être mis en balance avec les droits et libertés fondamentaux des personnes concernées; par exemple, la communication d'éléments liés à la corruption à une autorité hors Union européenne ou l'analyse du trafic internet pour prévenir l'accès à des systèmes malveillants dans un but de sécurité du réseau informatique.

- **Intérêts vitaux** : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; par exemple, le recueil d'un numéro de téléphone personnel pour l'envoi de SMS d'alerte en cas d'évènements graves sur le lieu de travail ou la collecte de données relatives à un régime alimentaire spécifique pour prévenir tout risque pour la santé d'une personne.

- **Intérêt public** : cette base juridique concerne la situation dans laquelle le responsable du traitement est investi d'une autorité publique ou d'une mission d'intérêt public, pour laquelle le traitement est nécessaire. Dans le cas où cette situation pourrait se présenter, cette base juridique doit être utilisée au cas par cas après validation par un ambassadeur DCP.

- **Recueil du consentement** : la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques :
    - Son consentement doit être libre (choix réel, sans conséquences négatives), spécifique (un consentement spécifique pour chaque finalité), éclairé (présence, au moment de l'expression du consentement, d'informations appropriées et suffisantes) et univoque (logique d' « opt-in », aucune ambigüité et absence de consentement par défaut ou lié à une inaction) ;
    - le recueil du consentement doit pouvoir être démontrable, (ex. : case à cocher, formulaire à remplir, procédures ou mécanismes systématiques) et donner à la personne la possibilité de le retirer.

Minimisation des données

En outre, les informations collectées et enregistrées doivent être pertinentes et strictement nécessaires à l'objectif poursuivi. Ainsi, des mesures doivent être prises pour réduire au minimum le volume de données à caractère personnel collectées et s'assurer que ces dernières sont adéquates au regard de la réalisation des finalités du traitement.

C. Maintenir des données exactes et les conserver durant une durée limitée

Détenir des informations erronées ou inexactes sur une personne peut être source de préjudices. Par exemple, une personne pourrait ainsi être exclue d'avantages ou de bénéfices liés à son statut. Par conséquent, il convient d'être particulièrement vigilant lorsqu'une décision est prise en se fondant sur des données à caractère personnel.

Exactitude des données

Les collaborateurs du groupe Elior doivent s'assurer que les informations détenues sont exactes, cela est notamment garanti par la mise en place des mécanismes suivants :

- vérifier l'exactitude de l'information au moment de la collecte lorsque c'est possible ;
- dans la mesure du possible, donner la possibilité aux personnes concernées d'actualiser les données les concernant ;
- examiner périodiquement les données à caractère personnel conservées pour s'assurer qu'elles demeurent à jour ;
- corriger ou supprimer les données inexactes.

Risques inhérents aux zones de libres commentaires (ZLC)

Les champs texte et les zones de commentaire doivent faire l'objet de précautions particulières. Ces champs de texte libre sont utiles pour assurer le suivi d'un dossier ou pour personnaliser une relation. S'il n'est pas interdit d'y recourir, des actions de sensibilisation et des règles de gestion doivent encadrer leur utilisation pour éviter que les commentaires saisis puissent porter atteinte aux droits des personnes concernées.

Certains commentaires pourraient s'avérer être désobligeants, discriminants, voire injurieux, ou encore faire apparaître des données dites sensibles, telles que des données relatives à la santé. Les commentaires doivent donc être appropriés, objectifs et respectueux.

La meilleure des précautions est de garder à l'esprit que les personnes concernées (clients, convives, salariés…) peuvent, à tout moment et sur simple demande, accéder au contenu de ces zones commentaires en exerçant leur droit d'accès.

Durée de conservation

Les données à caractère personnel ne peuvent être conservées de façon indéfinie, une durée de conservation doit donc être déterminée en fonction de l'objectif ayant conduit à la collecte de ces données. Une fois cet objectif atteint, ces données doivent être, selon le cas, archivées, supprimées ou anonymisées (afin notamment de produire des statistiques).

Il est important de noter que dans l'intérêt légitime du groupe Elior et la défense de ses intérêts, ces données pourront cependant être conservées pour des durées plus longues, justifiées par un contexte spécifique, dans le cadre de contentieux par exemple, et dans tous les cas après notification auprès du DPO.

D. Assurer la sécurité des données

La sécurité des données est un sujet primordial pour le groupe Elior. Le fait de ne pas assurer la sécurité des données sur l'ensemble de leur cycle de vie, de leur collecte à leur destruction, peut entraîner des préjudices importants pour les individus. Une vigilance accrue doit être apportée à la sécurité des prestataires externes lorsque ces derniers sont parties prenantes d'un traitement de données à caractère personnel.

Il existe de nombreuses façons de protéger les données à caractère personnel, qu'elles soient conservées sous un format électronique ou papier. Afin d'accompagner ses équipes, le groupe Elior maintient à leur disposition un corpus documentaire conforme à l'état de l'art, dont l'application est obligatoire :

- une politique de sécurité des systèmes d'information et des directives associées détaillant les exigences applicables aux systèmes d'information du groupe Elior ;
- des exigences de sécurité qui sont un prérequis à tout contrat avec un prestataire de services informatiques.

Les recommandations présentées ci-dessous doivent être adaptées au cas par cas et en fonction des risques induits par les traitements de données sur les libertés et la vie privée des personnes concernées :

- les applications doivent être protégées par des systèmes d'authentification (identifiant et mot de passe) conformément à la politique de sécurité de l'information ;
- l'accès aux données à caractère personnel n'est autorisé qu'aux seules personnes habilitées à avoir accès aux données en question, il s'agit du droit d'en connaître ;
- quel que soit le type de support physique, numérique ou sous format papier, ces derniers doivent être sécurisés. Il convient d'être particulièrement vigilant concernant les équipements mobiles, et de ne pas laisser sans surveillance ou protection ces équipements.

Pour toute question, il convient de prendre contact avec le responsable de la sécurité des systèmes d'information du groupe Elior.

E. Sous-traitance et transfert de données à caractère personnel

En cas de transfert de données à caractère personnel, le groupe Elior doit s'assurer au préalable que ce dernier est légalement possible et sécurisé. Le transfert de données à caractère personnel doit s'interpréter au sens large ; il peut par exemple s'agir :

- de transferts de données entre entités juridiques au sein même du groupe Elior ;
- d'une administration ou maintenance externalisée d'une ressource informatique ;
- de l'hébergement d'un service dans le cloud.

Obligations du sous-traitant

Conformément au RGPD, le sous-traitant est tenu d'accompagner le responsable de traitement dans sa démarche permanente de mise en conformité. Il est de la responsabilité du responsable de traitement de s'assurer que le sous-traitant remplit cette mission. Il doit être attendu du sous-traitant une obligation de :

- **transparence** : rendue possible par la rédaction d'un acte juridique (i) définissant clairement les obligations de chacune des parties, (ii) précisant que le sous-traitant agit uniquement sur instruction du responsable de traitement. Cette transparence est également garantie par le maintien d'un registre à jour des activités effectuées pour le compte du responsable de traitement et par la mise à disposition de toutes les informations nécessaires pour démontrer le respect de ces obligations ;
- **conseil et d'assistance** : le sous-traitant doit accompagner le responsable de traitement dans la détermination des données strictement nécessaires, dans le traitement des demandes d'exercice des droits et plus généralement pour l'ensemble de ses obligations ;
- **sécurité** : le sous-traitant doit s'assurer que ses employés sont soumis à une obligation de confidentialité et doit prendre toute mesure pour garantir un niveau de sécurité adapté aux risques et une conservation des données pour la stricte durée prévue ;

- **notification** : le sous-traitant doit notifier au responsable de traitement toute violation de données dans un délai raisonnable (idéalement 24 ou 36 heures).

Le groupe Elior et ses équipes s'engagent à s'assurer du respect de ces exigences pour chaque recours à des sous-traitants et lorsque le groupe Elior agit en qualité de sous-traitant.

Lorsque le groupe Elior agit en tant que responsable de traitement et fait appel à un ou plusieurs sous-traitants, ce(s) dernier(s) doi(ven)t respecter les exigences du groupe Elior en matière de protection des données à caractère personnel. Le transfert de données vers des sous-traitants doit s'effectuer de manière sécurisée. Il est de la responsabilité du groupe Elior de s'assurer que ses sous-traitants ont mis en place des mesures adéquates pour assurer la sécurité des données à caractère personnel.

Les directions juridiques doivent être systématiquement consultées afin de vérifier que tout contrat prévoit les obligations requises en matière de protection des données à caractère personnel.

Cas particulier des transferts hors de l'Espace économique européen (EEE):

Le transfert de données à caractère personnel hors EEE doit être encadré par des mécanismes appropriés, par exemple :

- la signature des clauses contractuelles type approuvées par la Commission européenne ;
- la rédaction de règles d'entreprise contraignantes : BCR « responsable de traitement » ou BCR « sous-traitant » ;
- la signature d'engagements spécifiques (ex. : Privacy Shield) pour les organismes basés en dehors de l'EEE.

F. Exercice des droits

Le groupe Elior veille à ce que les personnes concernées puissent pleinement jouir de leurs droits, notamment :

- d'accéder aux données à caractère personnel les concernant ;
- de demander la rectification des données à caractère personnel les concernant ;
- de demander la portabilité des données à caractère personnel les concernant sous un format structuré ;
- de s'opposer à faire l'objet d'une décision fondée exclusivement sur un traitement automatisé ;
- de demander l'effacement des données à caractère personnel ;
- de demander la limitation du traitement des données à caractère personnel ;
- de s'opposer au traitement des données à caractère personnel.

G. Privacy by design

Il est plus simple et moins coûteux de prendre en compte les considérations sur la vie privée et sur la sécurité au plus tôt dans les projets. C'est pourquoi, dès le démarrage d'un nouveau projet, il incombe au responsable du projet de prendre en compte la problématique de la protection des données à caractère personnel, et de s'assurer du respect de la vie privée des personnes concernées, que ce soit dans la mise en place d'un nouveau service/produit ou lors de sa modification.

Cela signifie notamment que pour tout nouveau projet, le responsable du projet doit :

- identifier les données à caractère personnel susceptibles d'être présentes ;
- le cas échéant :
    - renseigner ce projet au sein de l'outil de gestion de la protection des données personnelles et suivre les indications,
    - identifier les principaux risques liés aux données à caractère personnel qui peuvent survenir dans le cadre d'un projet particulier, notamment les risques juridiques, les risques liés à la réputation et les risques pour les personnes,
    - pour les traitements de données à haut risque, réaliser une analyse d'impact sur la protection des données (« DPIA »). Ces traitements concernent notamment l'utilisation de données à grande échelle, l'usage de nouvelles technologies, le traitement de données sensibles, la surveillance systématique ou la mise en place de traitement visant à la prise de décision automatisée et profiling. Le Comité européen de la protection des données référence sur son site, pays par pays, la liste des traitements pour lesquels un DPIA est obligatoire,
    - s'assurer de la conformité avec la politique Groupe,
    - veiller à la mise en œuvre et au contrôle des mécanismes de protection organisationnels et techniques.

En cas de besoin d'accompagnement ou de précisions, le responsable du projet peut se tourner vers ses ambassadeurs DCP.

H. Communication et sensibilisation

Sur une base annuelle, en fonction des enjeux identifiés et des constats relatifs à la conformité du groupe Elior, un plan de communication et de sensibilisation est initié par l'équipe Groupe avec le soutien des ambassadeurs DCP. Cette démarche doit avoir pour objectif d'instaurer une culture de la protection des données à caractère personnel au sein du groupe Elior.

Les équipes sont invitées à contribuer à l'amélioration de la politique et des processus associés.

I. Catégories particulières de traitements et de données à caractère personnel

Données à caractère personnel sensibles ou assimilées

Il s'agit des informations qui révèlent les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne physique. Les informations relatives aux infractions ou condamnations doivent également être considérées comme telles.

Il est recommandé au sein du groupe Elior de ne pas recueillir ni utiliser ces données du fait des risques élevés portant sur la vie privée des personnes, sauf dans certains cas précis :

- si la personne concernée a donné son consentement exprès (écrit, clair et explicite) ;
- si ces données sont nécessaires dans un but médical ou pour la recherche dans le domaine de la santé ;
- si leur utilisation est autorisée par l'autorité de protection des données personnelles.

Ces cas pouvant varier suivant le droit national du pays, il convient donc de se rapprocher des ambassadeurs DCP ou de l'équipe RGPD Groupe pour ce type de problématiques. Une DPIA devra systématiquement être réalisée.

Données à caractère personnel et droit à l'image relatifs aux enfants

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences ou des garanties qui doivent être apportées et de leurs droits liés au traitement des données à caractère personnel.

Dans le cadre des services de la société de l'information, le traitement des données à caractère personnel relative à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans. Ne pas hésiter à se rapprocher de l'ambassadeur DCP afin d'identifier le seuil d'âge en fonction du traitement envisagé.

Une DPIA devra systématiquement être réalisée avant la mise en œuvre de ces traitements.

Opérations marketing

Les opérations marketing doivent respecter les choix et les droits des personnes concernés. Lors des opérations marketing, par voie électronique notamment, il convient de s'assurer que :

- les personnes concernées ont donné leur consentement exprès (pour les relations BtoC) ;
- les personnes n'ont pas exercé leur droit d'opposition à la prospection ;
- les messages offrent la possibilité de se désabonner facilement (« opt-out ») ;
- aucun destinataire ne peut voir les noms et coordonnées d'un autre destinataire.

J. Violations de données

Malgré l'application de standards de haut niveau pour assurer la sécurité des données, le groupe Elior ne peut se prémunir totalement contre le risque de violations de données qui peuvent se définir par :

- Une atteinte à la confidentialité, c'est-à-dire une fuite de données (ex. : perte de clé USB contenant des fichiers clients) ;
- une atteinte à l'intégrité, c'est à dire une modification non prévue (ex. : modification non désirée de la base de données qui indique automatiquement aux autorités l'attributaire d'un véhicule de fonction) ;
- une atteinte à la disponibilité, c'est-à-dire une destruction de données (ex. : logiciel malveillant chiffrant une base de données).

La source de ces violations peut aussi bien être externe (ex. : attaque d'une ressource du groupe Elior ou d'un prestataire exposé à internet) qu'interne. Elle peut également être intentionnelle ou accidentelle (ex. : écran non protégé par un filtre de confidentialité exposé dans les transports en commun).

Il est de la responsabilité de chacun d'être vigilant et de notifier toute violation de données sans délai à l'équipe RGPD Groupe. En cas d'atteinte, avérée ou supposée, à la sécurité, il convient d'agir immédiatement afin de limiter les effets et les dommages. Dans les cas les plus graves, le groupe Elior devra informer l'autorité de protection des données compétente et lui fournir un plan d'action permettant de mitiger les impacts de la violation dans les 72 heures et, dans certains cas, informer également les personnes concernées.

K. Contrôle et relation avec les autorités de protection des données

Impacts potentiels de la non prise en compte de la protection des données à caractère personnel

Les infractions à la législation sur la protection des données à caractère personnel peuvent avoir de graves conséquences, notamment :

- des sanctions financières pouvant aller jusqu'à 4 % du chiffre d'affaires total du groupe Elior ;
- des demandes d'indemnisation des personnes concernées par l'atteinte à la vie privée ;
- la mise en conformité sous astreinte, la limitation d'un traitement ou la suspension des flux de données ;
- une atteinte à la réputation et à l'image du groupe Elior.

Pouvoir des autorités de protection des données

Le groupe Elior est en cours de rédaction de *Binding Corporate Rules*. Ces BCR ont pour objectif de démontrer le respect d'un niveau de protection des données similaire quel que soit le lieu de localisation de l'entité juridique filiale du groupe Elior et d'autoriser les transferts de données personnelles au sein du groupe Elior.

L'autorité de protection des données personnelles dispose du pouvoir de contrôler la conformité au Règlement général sur la protection des données via des contrôles physiques ou à distance et peut notamment :

- obtenir copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des traitements de données à caractère personnel ;
- demander la communication de tous documents nécessaires à l'accomplissement de sa mission ;
- accéder aux programmes informatiques et aux données, et en demander la transcription ;
- demander copie de contrats (ex. : contrats de location de fichiers, contrats de sous-traitance informatique), formulaires, dossiers papiers, bases de données, etc.
- réaliser à distance des scans de vulnérabilité, des audits de sécurité et vérifier la présence des mentions d'information légale.

En France, l'article 51 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés dite « loi Informatique et Libertés » dispose que toute entrave à l'action de la Cnil est punie d'un an d'emprisonnement et de 15 000 € d'amende. L'entrave à l'action de l'autorité de protection des données personnelles est réalisée en cas :

- d'opposition à l'exercice des missions confiées aux membres ou agents habilités lorsque la visite a été autorisée par le juge des libertés et de la détention ;
- de refus de communiquer, dissimulation ou destruction des renseignements et documents utiles à la mission de contrôle ;
- de communication d'informations non conformes au contenu des enregistrements tel qu'il était au moment où la demande de l'autorité de protection des données personnelles a été formulée ou de présentation d'un contenu sous une forme qui n'est pas directement accessible.

Conduite à tenir :

Il est recommandé de contacter sans délai l'équipe Groupe et de coopérer pleinement avec les autorités après vérification de l'identité des personnes (mandat et carte d'identité professionnelle).

L'équipe Groupe est la seule entité habilitée à communiquer avec des autorités de protection des données (ex. : démarche préalable, demande d'information, réponse aux saisines, etc.). Toute sollicitation des autorités doit donc lui être notifiée sans délai.

5. Information complémentaire

Si vous avez des questions au sujet de cette politique ou si vous souhaitez obtenir de plus amples renseignements sur l'un ou l'autre des sujets qui y sont traités, vous pouvez contacter l'équipe Groupe via l'adresse mail suivante : gdpr-contact@eliorgroup.com.