JUILLET 2025

MIEUX COMPRENDRE LE RGPD

Q&A POUR LES SGP

AFG

SOMMAIRE :

Le présent Q&A vient répondre aux questions posées par des sociétés de gestion (SGP) en complément du *Guide pédagogique RGPD pour les sociétés de gestion*, publié par l'AFG en mars 2019.

L'un des principes fondamentaux du RGPD étant l' « accountability » qui impose à toute entité qui traite des données personnelles de pouvoir démontrer sa conformité au RGPD, il revient à chaque SGP de s'assurer de sa conformité.
Ainsi c'est à vous qu'il revient de vérifier que vous ne collectez pas ou ne traitez pas plus de données que nécessaires, que les personnes sur lesquelles vous détenez des données ont bien été informées de l'existence de traitements, et qu'elles disposent effectivement de la possibilité d'exercer leurs droits et que ces traitements sont sécurisés de manière appropriée.

En se conformant aux règles du RGPD, la SGP va bénéficier positivement d'une vision d'ensemble de ses données lui permettant de les structurer au mieux en fonction de son organisation et d'y intégrer une logique participant à une meilleure anticipation d'éventuelles cyberattaques. Le respect du RGPD apparait également comme une démarche de nature à valoriser les actifs incorporels d'une SGP.

Plus avant la SGP se trouve face à un triple risque d'impact qu'il convient de minimiser : risque d'image en cas de mise en demeure publique (voire de condamnation), risque technique (suspension de la mise en œuvre d'un traitement) et risque financier (amende).

Par ailleurs en toute hypothèse, la CNIL, attentive au respect des données personnelles dispose, dans l'exercice de ses missions, d'une palette de sanctions de la simple mise en demeure, en passant par une limitation temporaire du traitement, et pouvant aller jusqu'à une amende de 20 millions d'euros et 4% du chiffre d'affaires annuel en cas de violation des principes relatifs aux traitement des données personnelles, sans oublier la réparation du préjudice des personnes concernées.

L'assistance de la conformité, d'un DPO, d'un juriste, d'un responsable informatique ou d'un conseil extérieur est souvent nécessaire pour réaliser un audit de conformité, sachant qu'il n'existe pas à ce stade de référentiel de certification. [1]

La démarche de conformité RGPD apparait comme une démarche itérative qui nécessite un suivi régulier des actions mises en œuvre et des actions à mener.

[1] Pour davantage d'informations, se référer aux lignes directrices du CEPD (Comité Européen de la Protection des Données)

Chapitre I - RESPECT DU RGPD

1. UNE SGP EST–ELLE TOUJOURS SOUMISE AU RGPD MEME SI ELLE NE TRAITE QUE DES DONNEES RELATIVES A DES ENTREPRISES ?

Que ce soit en BtoC, ou en BtoB, des données à caractère personnel vont transiter par la SGP et ce notamment :

- Du fait des traitements de données personnelles qu'elle opère sur ses salariés (traitements RH : gestion des paies, des carrières, des formations, etc…)
- Lorsque la SGP traite des données à caractère personnel :

  - de ses clients ou prospects personnes physiques (nom, prénom, adresse électronique, numéro de téléphone …),
  - de personnes morales avec lesquelles elle est en relation (clients, prospects, partenaires contractuels comme des fournisseurs, des prestataires, …). De fait, les personnes concernées par le respect de leurs données personnelles seront non seulement les représentants légaux des sociétés avec laquelle la SGP traite, mais aussi les collaborateurs de ces sociétés.

2. TOUTE SGP DOIT-ELLE AVOIR UN REGISTRE DES TRAITEMENTS ?

L'exonération actuellement en vigueur concernant la mise en place d'un registre des traitements pour les entreprises de moins de 250 salariés (article 30.5 du RGPD) cesse pour les traitements n'ayant pas un caractère « occasionnel », ce qui rend cette exonération moins fréquente.

L'établissement d'un registre des traitements va résulter du traitement par la SGP de données habituelles.
A noter qu'établir un registre permet de faciliter la connaissance par la SGP de ses traitements et, permet donc, de veiller au mieux à leur conformité.

Au sein d'une SGP, la tenue du registre peut être dévolue à la conformité, au responsable informatique, au délégué à la protection des données (« DPO »), etc.

3. DOIS-JE REDIGER ET PUBLIER DES POLITIQUES DE GESTION DES DONNEES PERSONNELLES ?

Le RGPD impose une bonne transparence et une bonne information des personnes sur lesquelles la SGP traite les données.
Votre organisation doit permettre de répondre au droit à l'information préalable des intéressés.
Il peut s'agir de notices d'information qui vous permettent de rendre l'information la plus claire, transparente et accessible possible. Des politiques de gestion des données peuvent aussi contribuer à cette transparence, avec le cas échéant une double politique dédiée l'une aux données externes (client / prospects), et l'autre aux données internes (salariés et candidats).
De façon proportionnelle à leur taille certaines SGP peuvent être amenées à adopter des procédures propres aux fournisseurs, des procédures propres aux partenaires …
En toute hypothèse le site internet de la SGP devrait intégrer les mentions quant à la politique de gestion des données personnelles.

4. COMMENT SE PREPARER A DES FAILLES DE SECURITE (VIOLATION DE DONNEES) TOUCHANT A DES DONNEES PERSONNELLES ?

Pour rappel la SGP doit prévoir en amont une procédure de gestion des failles de sécurité avec une attention particulière sur les données personnelles, celle-ci pouvant inclure 3 phases :

1ère phase – en amont : Etablir un plan d'actions : analyse des risques possibles, mise en place d'un dispositif de détection des incidents, rédaction et diffusion d'une procédure de gestion de crise en cas de violations affectant des données personnelles

2ème phase - Réagir efficacement pendant l'incident : identification du périmètre d'impact, évaluation de la gravité de l'incident pour les personnes concernées, notification à la CNIL et, selon la gravité, information des personnes.
Inscrire l'incident dans le registre des violations de données (document interne à la SGP)

3ème phase - Tirer des enseignements après l'incident : retour d'expérience par rapport aux mesures prévues initialement, plan de progrès pour pallier ce type de vulnérabilité.

Les SGP sont invitées à se référer aux publications de l'AFG en matière de cybersécurité.

5. FAUT-IL EFFECTUER UNE COMMUNICATION DE TOUTE VIOLATION DE DONNEES AUX PERSONNES CONCERNEES ?

En cas de violation de données personnelles, la SGP devra réaliser une notification auprès de la CNIL dans les meilleurs délais après avoir pris connaissance de la violation, et au plus tard dans les 72 heures. L'information des personnes concernées va dépendre de l'impact de la violation :

- 1er cas : La violation ne fait pas porter de risques élevés pour les personnes concernées. Il n'existe pas d'obligation légale d'informer les personnes. Cependant la SGP peut choisir pour diverses autres raisons (image, réputation, relation client etc.) de communiquer l'information auprès des personnes concernées.

- 2ème cas : La violation fait porter un risque élevé pour la liberté et les droits des personnes (accès à des données particulières au sens de l'art. 9 du RGPD, accès à des données sensible notamment des données bancaires, risque d'usurpation d'identité, risque de Phishing ciblé, etc.). Dans ce cas, l'information, qui doit être communiquée à la personne dans les meilleurs délais, prendra principalement la forme d'un mail, SMS, courrier aux personnes concernées. Si cette communication individuelle apparait impossible ou disproportionnée, de manière exceptionnelle la communication pourrait être réalisée de manière publique (essentiellement communication sur le site Web).

6. EN CAS DE FAILLE DE SECURITE DANS UNE FILIALE, A QUELLE AUTORITE DE CONTROLE LA NOTIFIER ?

Il existe différentes hypothèses :

-1er cas : la SGP, qui a son siège en France et dispose d'une ou plusieurs filiales en Europe, connait une violation de sécurité qui est globale impactant la maison mère et ses filiales. Dans ce cas, la notification doit être faite auprès de la CNIL, qui relaiera cette notification aux autres autorités compétentes. Rien n'interdit à chaque filiale de réaliser une notification à l'autorité locale tout en informant que l'autorité chef de file (CNIL) a été notifiée.

-2ème cas : la SGP, qui a son siège en France et dispose d'une ou plusieurs filiales en Europe, se trouve face à une violation de sécurité ne touchant qu'une la filiale locale. Dans ce cas, la notification doit être faite par la filiale à son autorité de contrôle locale. Il appartient à la filiale d'informer la maison mère.

-3ème cas : la SGP est située dans un pays de l'Union Européenne autre que la France et la filiale française est touchée par une violation globale. La notification sera faite par la maison mère auprès de l'autorité de contrôle locale. La filiale française pourra, si elle le souhaite, notifier la CNIL en l'informant du fait que la maison mère a réalisé une notification auprès de son autorité chef de file naturelle.

Chapitre II - LICEITE DU TRAITEMENT

1. LES FONDEMENTS POSSIBLES D'UN TRAITEMENT

Pour une SGP, un traitement de données personnelles peut avoir l'un des 4 fondements légaux suivant (alors même qu'il existe 6 bases légales dans le RGPD :

- L'exécution d'un contrat
- La satisfaction d'une obligation légale
- Le consentement de l'utilisateur
- L'intérêt légitime du responsable de traitement

➢ Dans le cadre de ses missions, les traitements mis en œuvre par une SGP reposeront principalement sur **l'exécution du contrat** comme base légale (ex : convention de gestion).

➢ Pour d'autres traitements, comme les traitements liés aux opérations KYC, la base légale sera celle de **l'obligation légale.**

➢ Pour les opérations liées à la recherche de nouveaux clients, la base légale pourra être **l'intérêt légitime** (sauf dans les cas où le consentement s'impose).
Dans ce cas particulier de l'intérêt légitime comme base légale, la SGP devra réaliser ce qu'il convenu d'appeler la « balance des intérêts » qui se décline comme suit :

1/Existence de l'intérêt légitime
- La SGP responsable de traitement a-t-elle un intérêt à traiter ces données ?
- Cet intérêt est-il réel et présent ?
- Cet intérêt est-il légal ?

2/Evaluation de la nécessité
- Le traitement va-t-il véritablement aider la SGP responsable de traitement à atteindre son objectif ?
- Le traitement envisagé est-il proportionné par rapport à l'objectif poursuivi ? Peut-on atteindre cet objectif sans traiter de données, en utilisant moins de données, ou en mettant en œuvre un traitement moins intrusif ?

3/Mise en balance
Pour cette mise en balance, la SGP responsable de traitement doit prendre en compte a minima :
- La nature des données traitées (peu sensibles/à caractère hautement personnel/ sensibles)
- Les attentes raisonnables des personnes concernées : Vous devez montrer, d'une manière objective, qu'une personne raisonnable s'attendrait au traitement de ses

données au regard des circonstances particulières du traitement (ex : existence d'une relation directe entre la personne concernée et le RT, collecte directe des données, etc.)

- L'impact du traitement sur les personnes concernées (le traitement est intrinsèquement susceptible d'être à haut risque pour les personnes concernées (cf. critères du DPIA), est susceptible de constituer un frein à l'exercice des droits et libertés des personnes ou à l'accès à des services ou opportunités, ou peut causer aux personnes concernées un préjudice (quel qu'en soit la nature). La SGP doit prendre en compte la gravité et la vraisemblance de cet impact.
- Les garanties éventuelles pouvant être mises en place pour protéger les droits et intérêts des personnes concernées (ex : pseudo anonymisation des données, restriction des accès, etc.)

L'ensemble de ces facteurs devant être pondéré par la SGP responsable de traitement, celle-ci doit s'efforcer d'être objective dans l'évaluation de ces facteurs.

Les conclusions résultant de cette évaluation permettront à la SGP de déterminer si elle peut effectivement utiliser l'intérêt légitime comme base légale. La réalisation d'une analyse d'impact peut participer à cette évaluation, pour autant que celle-ci soit requise.

2. LA SGP DOIT-ELLE SYSTEMATIQUEMENT RECUEILLIR UN CONSENTEMENT ?

En dehors des bases légales mentionnées au paragraphe précédent, il existe trois cas pour lesquels le consentement est requis :

-1er cas : la prospection commerciale par voie électronique,

-2ème cas : la mise en œuvre de cookies de nature publicitaire sur le site Web (généralement à travers une CMP -Consent Managing Platform -),

-3ème cas : les décisions individuelles entièrement automatisées (hors validation humaine).

3. UNE SGP PEUT-ELLE IMPOSER A SES CLIENTS UNE FINALITE CONNEXE ?

Il est possible lors de la collecte des données à caractère personnel que l'ensemble des finalités n'ait pas été totalement stabilisé et qu'apparaissent de nouveaux besoins. Faut-il dans ce cas réinformer les personnes et/ou obtenir leur consentement pour ces nouvelles finalités ?

Tout dépend de la nature de ces finalités :

- S'il s'agit de finalités totalement nouvelles, il faudra effectivement informer les personnes concernées.

- S'il s'agit de ce que l'on appelle « des finalités connexes » la SGP pourra utiliser ces données sans formalité additionnelle. Toute la question est d'identifier une finalité connexe d'une finalité qui ne le serait pas.

Pour se déterminer, une attention devrait être accordée aux points suivants :

- Le lien entre la finalité initiale et la nouvelle finalité ;
- Le contexte dans lequel les données ont été collectées (quelle est la relation entre la SGP et la personne concernée ?) ;
- Le type et la nature des données (s'agit-il de données sensibles ?) ;
- Les conséquences du traitement ultérieur envisagé (impact sur la personne concernée) ;
- L'existence de garanties appropriées (par exemple, chiffrement ou pseudo anonymisation).

Chapitre III - RESPONSABLE DE TRAITEMENT / SOUS-TRAITANT

1. COMMENT UNE SGP PEUT-ELLE S'ASSURER DU RESPECT DU RGPD PAR SES SOUS-TRAITANTS ?

Le RGPD prévoit des dispositions particulières dans le cadre d'une relation entre le responsable du traitement (une SGP) et son, ou ses, sous-traitant(s).

La notion de sous-traitance, définie de manière spécifique dans le RGPD, ne doit pas être confondue avec la notion de sous-traitance générale (dans le cadre du Droit des affaires).

Au sens du RGPD, un sous-traitant est un prestataire qui procède à des opérations sur les données du responsable du traitement et pour le responsable du traitement. La CNIL a publié différentes documentions et recommandations sur la notion de sous-traitance. Elle indique par exemple qu'en matière RH, la paie externalisée constitue un cas de sous-traitance, qu'en matière de communication passée par un prestataire pour envoyer des newsletters est un cas de sous-traitance, ou encore, que les prestations assurées par les ESN (entreprises de service numérique) sont aussi des cas de sous-traitance.

La relation entre la SGP responsable du traitement et un sous-traitant repose sur trois grandes règles :

-Règle numéro 1 : la SGP doit s'assurer avant tout contrat que le sous-traitant respecte le RGPD et permet ainsi à la SGP de le respecter elle-même.

-Règle numéro 2 : le RGPD impose l'existence d'un contrat en plus du contrat principal destiné à fixer les droits et obligations du sous-traitant et du responsable du traitement. Ce document est communément appelé « DPA pour Data Privacy Agreement ». Il convient d'être attentif à la rédaction de ce DPA, car il doit répondre aux exigences posées par l'art 28 du RGPD. Cet article

impose la présence de huit dispositions contractuelles, qu'il s'agit de la collaboration du sous-traitant pour l'application du RGPD, du sort des données à la fin du contrat ou encore, des conditions d'audit du sous-traitant par le responsable du traitement

-Règle numéro 3 : même s'il ne s'agit pas d'une obligation formelle (il n'existe pas de disposition dans le RGPD qui l'impose), le responsable du traitement pourrait auditer et contrôler le respect du RGPD et du DPA par son sous-traitant. Cet audit peut prendre différentes formes. Il peut s'agir d'un simple audit documentaire, mais la SGP pourrait dans certains cas (pour les traitements sensibles) réaliser des audits par inspection (visite sur place). Ces audits peuvent être réalisés par la SGP ou par un prestataire mandaté.

Enfin, il convient de rappeler les règles de responsabilité entre le responsable et le sous-traitant fixées à l'article 82 du RGPD qui précisent que : « Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci. ». Autrement dit, la SGP reste le plus souvent responsable des agissements de sous-traitant vis-à-vis de la CNIL.

Il convient de rappeler que si le sous-traitant est établi en dehors de l'UE, en plus du DPA les parties devront traiter le cas particulier des flux transfrontières. (Cf. Chapitre XI du FAQ).

2. UNE SGP A-T-ELLE QUALITE DE RESPONSABLE DE TRAITEMENT S'AGISSANT DE SA RELATION AVEC SES FONDS (SICAV, FCP, FCPE…) ?

Les FCP, FCPE n'ayant pas de personnalité morale, la SGP est de fait responsable de traitement.

S'agissant des SICAV, du fait que la SGP détermine les finalités et les moyens du traitement, celle-ci se trouve en pratique être responsable de traitement.

Il est souhaitable de formaliser dans le registre de traitement de la SGP les traitements de données réalisés en relation avec la gestion des fonds.

3. COMMENT S'ANALYSENT LES RELATIONS DE LA SGP AVEC SES DISTRIBUTEURS ?

Les distributeurs de la SGP collectant des données personnelles de clients finaux pour des finalités qui leur sont propres, ces distributeurs sont responsables de traitement.

Le groupe de travail RGPD de l'AFG a rédigé une clause type qui définit les responsabilités respectives des parties au regard du traitement des données personnelles qui a été intégré au modèle de contrat de distribution de l'AFG.

Chapitre IV - DPO

1. SUIS-JE TENU DE DESIGNER UN DPO ?

Le délégué à la protection des données (DPO) a pour fonction principale de conseiller le responsable du traitement, de contrôler l'application du RGPD, et d'être l'interface entre la SGP, la CNIL, et les personnes concernées. La désignation d'un DPO n'est obligatoire que dans trois cas :

- 1er cas : les acteurs publics.
- 2ème cas : Les responsables du traitement qui opèrent un traitement à grande échelle des données particulières au sens de l'article 9 du RGPD (ex : appartenance religieuse, syndicale, données de sante etc.), et l'article 10 du RGPD (ex : condamnation pénale).
- 3ème : les responsables du traitement qui opèrent des traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées.

A priori, les SGP ne sont pas visées par les cas trois cas ci-dessus.

Même si la désignation d'un DPO ne s'avère pas obligatoire, elle reste fortement conseillée. Cette désignation permet notamment :

-de favoriser une culture RGPD au sein de la SGP ;
-de s'assurer du maintien dans le temps des documents et procédures liés à l'application du RGPD au sein de la SGP ;
-de disposer d'un référent unique permettant de conseiller et de répondre aux questions de opérationnels ;
-de rassurer dans certains les clients et les partenaires commerciaux ;
-et enfin d'être un interlocuteur privilégié de la CNIL en cas de demande et / ou de contrôle.

Le DPO peut être désigné en interne ou en dehors de l'entreprise, la condition requise est que le DPO dispose des compétences et des moyens pour mener à bien sa mission. Le DPO peut être mutualisé, c'est-à-dire partagé entre plusieurs responsables du traitement distincts (plusieurs SGP désignent un même DPO), ou être un DPO Groupe (un DPO unique pour une maison mère et ses filiales).

4. COMMENT NOTIFIER AUX AUTORITES UN « DPO GROUPE » ?

Pour ce qui est des groupes, dans le cas où un seul DPO est désigné pour l'ensemble du groupe, la désignation du DPO se fait là où se trouve le responsable du traitement :

- Si la société mère pilote les traitements elle pourra avoir un DPO pour l'ensemble,
- Si les filiales sont autonomes dans tout ou partie de leurs traitements, elles désigneront chacune un DPO.

Chaque entité responsable de traitement (filiales et holding) désigne un DPO qui peut être mutualisé au sein du groupe. La désignation s'effectue auprès de l'autorité nationale auprès de laquelle le responsable de traitement dépend.

Chapitre V - EXERCICE DES DROITS DES PERSONNES

1. UN CLIENT DE LA SGP PEUT-IL DEMANDER A ACCEDER AUX DONNEES LE CONCERNANT ?

L'exercice du droit d'accès et de copie, régi par l'article 15 du RGPD, permet au client de prendre connaissance des données le concernant qui font l'objet d'un traitement et d'en obtenir la communication dans un format compréhensible, d'en contrôler l'exactitude, et si nécessaire, de les faire rectifier ou de les effacer.

Dès lors qu'un client exerce son droit d'accès, la SGP responsable du traitement doit être en mesure de lui adresser une copie des données qu'elle détient et de le renseigner, notamment sur la finalité d'utilisation des données, les catégories de données collectées, la durée de conservation, la possibilité de saisir la CNIL, etc.

A noter des limites à ce droit d'accès et de copie, si ces données concernent la police ou intéressent la sureté de l'Etat/ si la demande est jugée excessive et infondée par l'entreprise (celle-ci doit en apporter la preuve) /ou si la demande porte atteinte aux droits et libertés d'autrui.

En tout état de cause la SGP dispose d'un délai d'un mois pour satisfaire aux demandes légitimes des personnes concernées.

2. UN CLIENT DE LA SGP PEUT-IL DEMANDER LA RECTIFICATION DES DONNEES LE CONCERNANT ?

Le droit de rectification (articles 16 RGPD) permet à toute personne d'obtenir du responsable de traitement qu'il rectifie, complète, actualise les informations qui la concernent (telles que l'âge, l'adresse ou le nom) dès lors que des erreurs, des inexactitudes ou un traitement illicite apparaissent.,

Les SGP étant par ailleurs soumises à des obligations règlementaires en matière de connaissance client (KYC, know your customer), il conviendra aux SGP de s'assurer que l'exercice du droit de rectification s'articule avec les processus et procédures existants de mise à jour d'informations de KYC lorsqu'applicable.

Chapitre VI - CONSERVATION/SUPRESSION DES DONNEES

1. COMBIEN DE TEMPS UNE SGP PEUT-ELLE CONSERVER DES DONNEES PERSONNELLES ?

Dans la perspective d'une mise en conformité avec les règles applicables en matière de durée de conservation des données personnelles, la SGP doit déterminer dans quel cas cette conservation se situe :

1er cas - Une disposition légale ou réglementaire précise la durée de conservation de ce type de données.
Par exemple, le Code du travail impose à l'employeur de conserver un double de bulletin de paie du salarié pendant 5 ans.

2ème cas - Des règles émanant de la CNIL constituent un point de repère pour les responsables de traitements, qu'il s'agisse de durées imposées ou de recommandations.
Par exemple, la CNIL propose des référentiels sectoriels de durées dans le cadre des dispositifs d'alertes professionnelles, de la gestion de la prospection commerciale etc.

3ème cas - En l'absence de prescription concernant la durée de conservation par la loi ou la CNIL, les SGP doivent se référer au principe de proportionnalité.
En se fondant sur la finalité pour laquelle le traitement des données personnelles est mis en œuvre. Par la suite, la SGP devra identifier et évaluer ses besoins opérationnels afin d'appliquer une durée.

2. FACE A UNE DEMANDE DE SUPPRESSION LA SGP A-T- ELLE L'OBLIGATION DE SUPPRIMER LES DONNEES ?

Il faut ici distinguer droit à l'effacement et demande de suppression. Si les deux conduisent à une suppression, la règle du jeu n'est pas la même.

Le droit à l'effacement, tel que prévu par le RGPD (article 17.1), intègre six cas dans lesquels une personne concernée peut exiger l'effacement de ses données :

- Les données ne sont plus nécessaires à la poursuite des finalités
- Le retrait du consentement
- L'exercice du droit d'opposition reconnu valable
- Traitement illicite
- Le respect d'une obligation légale
- Les données collectées en ligne auprès de mineurs

En dehors de ces cas la demande de suppression peut être refusée dans différentes hypothèses :

1) Lorsque la SGP est tenue de conserver les données pour respecter la loi

2) Lorsque la SGP est tenue de conserver les données à des fins probatoires notamment en cas de contentieux.

3. QUELLES SONT LES INCIDENCES DE L'ANONYMISATION SUR LA DUREE DE CONSERVATION ?

L'anonymisation est différente de la pseudonymisation.

Avec l'anonymisation, la SGP va altérer la donnée de manière irréversible rendant impossible l'identification d'une personne.

En revanche, l'utilisation de la pseudonymisation revient à remplacer les données directement identifiantes par des données indirectement identifiantes.

Concernant la conservation des données, l'anonymisation permet de les conserver au-delà de leur durée de conservation : les données réellement anonymisées sortent du champ d'application du RGPD.

4. UN EXTRAIT DU CASIER JUDICIAIRE POURRAIT-IL ETRE DEMANDE LORS D'UN RECRUTEMENT PUIS CONSERVEE PAR LA SGP ?

La CNIL offre des précisions à ce sujet (cf. site CNIL). Si la demande d'extrait du casier judiciaire B3 peut être admise au moment de la signature du contrat de travail, en revanche il est interdit à la SGP d'en conserver la copie, seule la mention oui (l'extrait du casier judiciaire a été communiqué) / non (l'extrait du casier judiciaire n'a pas été communiqué) peut être conservée.

Chapitre VII - ANALYSE D'IMPACT

L'analyse d'impact, appelée aussi DPIA (Digital Privacy Impact Assessment), constitue un outil qui permet non seulement de construire des traitements de données respectueux de la vie privée, mais aussi de démontrer sa conformité au RGPD (en lien avec le principe d'accountability prôné par le RGPD.

1. DANS QUEL CAS UNE SGP DOIT METTRE EN ŒUVRE UNE ANALYSE D'IMPACT ?

L'analyse d'impact, qui vise le traitement des données susceptibles de générer un risque élevé pour le droit et liberté des personnes concernées, est obligatoire dans deux cas :

- Si le traitement figure dans la liste des types de traitements pour lesquels la CNIL impose une analyse d'impact
- Lorsque le traitement remplit au moins deux des neuf critères déterminés par les lignes directrices du CEPD**2** .

Une analyse d'impact comporte trois parties :

-une description détaillée du traitement mis en œuvre d'un point de vue technique et opérationnel,

-une évaluation de la nécessité ainsi que de la proportionnalité s'agissant des principes et droits fondamentaux,

-une étude technique des risques sur la sécurité des données ainsi que de leur impact potentiel sur la vie privée.

[2] Les 9 critères sont : l'évaluation ou la notation ; la prise de décisions automatisée avec effet juridique ou effet similaire significatif ; la surveillance systématique ; les données sensibles ou données à caractère hautement personnel ; les données traitées à grande échelle ; le croisement ou la combinaison d'ensembles de données ; les données concernant des personnes vulnérables ; l'utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles et les traitements en eux-mêmes qui «*empêchent [les personnes concernées] d'exercer un droit ou de bénéficier d'un service ou d'un contrat*»

Une **liste des traitements non soumis à analyse d'impact** est accessible sur le site de la CNIL **3** et ces concepts ont été intégrés dans le modèle de registre du traitement de l'AFG.

2. DES TRAITEMENTS EFFECTUES PAR UNE SGP DANS LE CADRE D'UNE OBLIGATION LEGALE SONT-ILS EXEMPTES DE DPIA ?

Le fait pour les SGP d'être tenues de respecter des obligations légales, comme celle de mise en place de KYC (« know your Customer ») ou de mesures de lutte contre le blanchiment et le financement du terrorisme ne les exempte pas de tout DPIA.

Le RGPD (article 35) impose une analyse de l'impact lorsqu'un type de traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques », Les SGP peuvent se référer aux recommandations du CEPD qui suggère une analyse d'impact dès lors que le traitement répond à au moins 2 des 9 critères mentionnés ci-après :

- Evaluation ou notation, y compris les activités de profilage et de prédiction
- Prise de décisions automatisée avec effet juridique, ou effet similaire significatif
- Surveillance systématique
- Données sensibles ou données à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données
- Données concernant des personnes vulnérables
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles
- Traitements qui empêchent les personnes concernées « d'exercer un droit ou de bénéficier d'un service ou d'un contrat ».

Aux SGP de se faire leur appréciation de certains traitements (KYC …).

En toute hypothèse la CNIL a dressé une liste de 14 traitements pour lesquels l'analyse d'impact est obligatoire qui inclut les traitements ayant pour finalité la gestion des alertes et des signalements en matière professionnelle.

[3] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

Chapitre VIII - LUTTE CONTRE LE BLANCHIMENT ET LE FINANCEMENT DU TERRORISME (LCB-FT)

1. LES DONNEES COMMUNIQUEES PAR DES PRESTATAIRES EXTERIEURS EN LCB-FT IMPLIQUENT-ELLES DES ENJEUX PARTICULIERS POUR LES SGP ?

Afin d'accompagner les professionnels, la CNIL a élaboré dans le cadre de ses référentiels, une autorisation unique (AU-003) leur permettant de répondre à leurs obligations légales de lutte contre le blanchiment de capitaux et le financement du terrorisme.
Par ailleurs le Règlement européen LCB-FT 2024/1624 rappelant au considérant 153 les recommandations du GAFI en matière de conservation des informations nécessaires aux mesures de vigilance à l'égard de la clientèle fixe cette durée de conservation à 5 ans après la fin de la relation d'affaires ou après la transaction à titre occasionnel.

Le sujet de la recherche d'antécédents négatifs par des opérateurs extra-européens via des bases de données externes (FACTIVA, WORLDCHECK…) est un sujet d'attention pour les SGP qui doivent s'efforcer d'obtenir de ces opérateurs de s'engager contractuellement à respecter le RGPD. Des travaux sont entrepris par la CNIL à ce sujet.

Par ailleurs, l'article 10 du RGPD apporte des restrictions quant aux traitements des données à caractère personnel relatives aux condamnations pénales et aux infractions qui peuvent être effectués que conformément aux garanties appropriées prévues par le droit national ou européen.

Chapitre IX - QUELS CONTROLES LA CNIL PEUT-ELLE METTRE EN ŒUVRE ?

Les différents contrôles de la CNIL :

- Contrôle CNIL sur convocation. Un courrier est adressé à l'entreprise pour que des représentants se présentent dans les locaux de la CNIL, à une date fixée au préalable ;

- Contrôle CNIL en ligne. Les agents de la Commission réalisent des vérifications des données librement accessibles ou rendues accessibles en ligne (exemple : contrôle à distance des sites web pour la gestion des cookies) que ce soit par choix, par imprudence, par négligence ou du fait d'un tiers. Les agents de la CNIL peuvent décider d'utiliser une identité d'emprunt.

- Contrôle CNIL sur place : les agents se rendent dans tout local utilisé pour mettre en œuvre un traitement des données personnelles. Toute visite sur place peut être précédée d'une information au procureur de la république territorialement compétent et d'une autorisation

par le juge de la liberté et de la détention du tribunal dans le ressort duquel sont situés lesdits locaux. Dès lors, les agents de la CNIL peuvent se faire communiquer et obtenir une copie de tous documents, renseignement, audition, programmes informatiques et données qu'ils jugent utiles à leur mission.

Toute entité, et donc toute SGP, peut être soumise à un contrôle de la CNIL. L'une des clés d'un contrôle maitrisé porte sur un très haut niveau de collaboration avec les agents de la CNIL.

Il existe trois types de suites apportées à un contrôle :

- La mise en demeure : La SGP devra justifier de sa mise en conformité accompagnée des justificatifs adéquats. Si ces justificatifs apportent les réponses attendues, la procédure de contrôle prend fin avec un courrier de clôture.
- Le courrier « explicatif ». La CNIL demande des explications sur tel ou tel point, une réponse doit y être apportée par la SGP.
- Un courrier « informatif » : En l'informant d'une situation qu'elle a constatée, la CNIL n'attend pas une réponse, mais une action de la SGP. Dans ce cas il convient de suivre les préconisations de la CNIL. Par ailleurs il est conseillé de répondre à la CNIL, même si elle indique ne pas attendre de réponse.

À l'issu d'un contrôle, la CNIL peut décider soit de clôturer la procédure, soit ordonner des mesures correctrices et sanctions.

Chapitre X - QUELLES SONT LES REGLES EN MATIERE DE PROSPECTION COMMERCIALE ?

1. UN MAIL D'INFORMATION DE LA SGP A SES CLIENTS ET/OU PROSPECTS N'AYANT PAS VOCATION A VENDRE UN PRODUIT OU UN SERVICE EST-IL CONSTITUTIF D'UN MESSAGE DE PROSPECTION ?

Selon l'article L34-5 du Code des postes et des communications électroniques (CPCE), tout message destiné à promouvoir, directement ou indirectement, l'image d'une société relève de la prospection commerciale.

2. QUELLES BASES LEGALES PEUVENT-ETRE UTILISEES DANS LE CADRE DE LA PROSPECTION COMMERCIALE ?

La base légale sur laquelle pourra se fonder la prospection commerciale va dépendre notamment du type de personnes visées par la prospection (prospection BtoB ou BtoC) de la SGP, mais également du canal de prospection utilisé.

Prospection commerciale en BtoC :

Lorsque la prospection commerciale est réalisée par voie non-automatique, c'est-à-dire par voie postale ou téléphonique, le traitement pourra être fondé sur l'intérêt légitime (article 6.1.f du RGPD).

En revanche, lorsque la prospection commerciale est réalisée par voie électronique, le traitement devra, en principe, être fondé sur le consentement (article L. 34-5 du CPCE et 6.1.a du RGPD).

Il existe toutefois une exception à ce principe. En effet, le responsable de traitement pourra se fonder sur son intérêt légitime pour prospecter ses clients pour des produits ou services analogues à ceux déjà acquis ou souscris par ces derniers.

Cette exception ne peut donc pas être utilisée pour de la prospection à destination de purs prospects.

Ensuite, l'appréciation du caractère « analogue » des produits/services concernés doit se faire au cas par cas. Enfin, cette exception n'est valable que pour l'entité qui collecte directement les données auprès des personnes concernées.

Prospection commerciale en BtoB :

Dans un cadre BtoB, la prospection commerciale pourra être fondée sur l'intérêt légitime, quel que soit le canal de prospection utilisé, sous réserve que le message soit bien en lien avec la profession de la personne démarchée.

Dans le cas contraire, il faudra appliquer le régime de la prospection BtoC.

3. COMMENT INFORMER LES PERSONNES CONCERNEES DANS LE CADRE D'UNE PROSPECTION COMMERCIALE ET QUEL DROIT D'OPPOSTION POUR ELLES ?

En cas de collecte directe, la SGP devra informer les personnes concernées préalablement à la collecte des données, par exemple sur le support de collecte.

En cas de collecte indirecte des données, les personnes concernées devront être informées dès que possible. La communication des informations doit donc se faire notamment à l'occasion du premier contact avec la personne concernée, et au plus tard dans un délai d'un mois.

Il est à souligner que le partage de données au sein d'un même groupe peut être assimilé à de la collecte indirecte, notamment lorsqu'il s'agit d'entités juridiques distinctes.

Toute personne concernée dispose du droit absolu de s'opposer au traitement de ses données à des fins de prospection, ou de retirer son consentement lorsqu'il est applicable à tout moment, en BtoC comme en BtoB.

La personne concernée n'a pas alors à justifier sa demande d'exercice de droit d'opposition, ou de retrait de consentement, et la SGP ne peut se prévaloir de l'existence de motifs légitimes et impérieux prévalant sur les intérêts et les droits de la personne concernée pour poursuivre le traitement de ses données.

Afin de faciliter l'exercice du droit d'opposition ou de retrait de consentement, la SGP peut, par exemple, prévoir un lien de désinscription/désabonnement, ou la mention d'une adresse de contact pour en effectuer la demande.

Le responsable de traitement doit permettre l'opposition à la prospection commerciale avant la réception de tout message de prospection et à tout moment, notamment sur le support de collecte des données.

La SGP peut constituer des « listes repoussoirs » afin de prendre en compte de manière effective les demandes d'opposition des personnes concernées. Il est utile de veiller au respect du principe de minimisation lors de la constitution de cette liste repoussoir, et ne conserver que les données nécessaires à la prise en compte de l'opposition, c'est-à-dire les données de contact de la personne concernée **4.**

Les mêmes recommandations s'appliqueront en cas de retrait de consentement.

4. QUELLES REGLES EN CAS DE TRANSMISSION DE DONNEES A DES PARTENAIRES A DES FINS DE PROSPECTION COMMERCIALE ?

Toute entité souhaitant faire l'acquisition d'une base de données afin de conduire des opérations de prospection commerciale doit s'assurer de la licéité de cette opération.

Licéité de la transmission :

Le vendeur d'une base de données personnelles doit s'assurer que la finalité visée par l'acheteur ne soit pas incompatible avec la finalité pour laquelle les données avaient été collectées initialement. En pratique, selon la CNIL, le vendeur doit s'informer auprès de l'acheteur de la

[4] CNIL, Tables Informatique & Libertés, édition 2024, p. 217

finalité pour laquelle les données seront utilisées et s'assurer contractuellement qu'elles ne le soient que pour cette finalité **5.**

La transmission d'une base de données personnelles, à titre onéreux comme à titre gratuit, est un traitement de données à caractère personnel qui doit être fondée sur une base légale déterminée. En principe, la base légale de cette transmission correspond à la base légale applicable à l'opération de prospection. En conséquence, si l'opération de prospection est fondée sur le consentement, la SGP propriétaire de la base de données devra obtenir le consentement des personnes concernées avant la transmission.

Quelle que soit la base légale retenue pour effectuer la transmission des données, le détenteur initial des données devra informer les personnes.

Lorsque cette transmission est fondée sur le consentement, la liste exhaustive des destinataires **6** devra être communiquée. De plus, la CNIL recommande que chaque nouveau destinataire soit communiqué aux personnes concernées et fasse l'objet d'un consentement conforme aux exigences du RGPD. Dans ce cas, la demande de consentement pourra être obtenue par l'envoi par la SGP d'un mail aux personnes concernées, cette prise de contact pouvant être effectuée sur la base de l'intérêt légitime du responsable de traitement.

En revanche, si la transmission est fondée sur l'intérêt légitime, la communication de la liste détaillée des destinataires n'est pas nécessaire : la SGP responsable de traitement pourra se contenter de la communication du secteur d'activité des partenaires et de leur nombre.

5. UNE SGP PEUT-ELLE UTILISER DES DONNEES PUBLIQUES AFIN DE MENER DES OPERATIONS DE PROSPECTION COMMERCIALE ?

En principe, la réutilisation de données publiques n'est pas libre.

La SGP responsable de traitement doit veiller à fonder le traitement sur une base légale adaptée, notamment en fonction du canal de prospection envisagé (automatisé ou non).

De plus, si la SGP envisage de fonder son traitement sur l'intérêt légitime, elle devra porter une attention toute particulière aux attentes raisonnables des personnes.

[5] CNIL, Tables Informatique et libertés – édition 2024, pp.219-220 (cf. CNIL, P, 27 avril 2023, Rappel aux obligations, Société X, n°RAL231017, non publié)

[6] CNIL, Tables Informatique et libertés – édition 2024, p.218 (cf. CNIL, P, 1er décembre 2021, Mise en demeure, Société X, n° MED-2021-131, non publié)

Si le traitement de prospection est fondé sur le consentement, le responsable de traitement devra solliciter le consentement des personnes concernées avant de procéder à toute opération de prospection commerciale. Le traitement de données mis en œuvre pour la sollicitation de ce consentement pourra être fondé sur l'intérêt légitime du responsable de traitement. Il faudra toutefois que ce premier message corresponde à des attentes raisonnables des personnes concernées.

La SGP responsable de traitement devra également prêter attention aux conditions légales des sites internet à partir desquels les données sont collectées. En effet, certains interdisent l'aspiration et la réutilisation des données à des fins commerciales.

Enfin, la SGP devra veiller à respecter le principe de minimisation en ne collectant que les données strictement nécessaires à la prospection.

Ces recommandations s'appliqueront, par exemple, dans le cadre de la collecte d'informations d'identité, de contact ou de situation professionnelle par le biais de réseaux sociaux (LinkedIn, etc.), dans le cadre d'activités de prospection commerciale par les sociétés de gestion, ou par leurs prestataires.

6. QUELLE DUREE DE CONSERVATION APPLIQUER AUX DONNEES PERSONNELLES TRAITEES A DES FINS DE PROSPECTION ?

Les durées de conservation à appliquer aux données personnelles traitées à des fins de prospection commerciale vont dépendre du type de personnes concernées (les clients ou les prospects), ainsi que de la base légale retenue pour le traitement.

En principe, les données traitées dans le cadre de la prospection commerciale pourront être conservées trois ans par la SGP (pour les clients à compter de la fin de la relation commerciale, et pour les prospects à compter de la collecte des données ou du dernier contact venant du prospect).

Cette durée pourra être reconduite, par exemple lorsque la personne concernée prend contact avec le responsable de traitement, ou clique sur un lien prévu à cet effet dans un mail de prospection.

Toutefois, la SGP responsable de traitement devra veiller à supprimer les données traitées par suite du retrait du consentement d'une personne concernée lorsque le traitement est fondé sur le consentement, ou encore lorsqu'une personne concernée exerce son droit d'opposition quand le traitement est fondé sur l'intérêt légitime.

Chapitre XI - COMMENT GERER LES FLUX DE DONNEES EN DEHORS DE L'UE?

Le transfert de données vers des entités publiques ou privées qui ne sont pas situées dans l'EU doit respecter les exigences du RGPD. On entend par flux transfrontaliers, la mise à disposition des données à caractère personnel par une SGP vers une autre entité (responsable du traitement ou sous-traitant) située en dehors de l'UE.

Attention : il y a flux transfrontalier lorsque la SGP communique un fichier de données par courrier à une entité en dehors de l'UE, mais le seul fait de donner accès, et en simple consultation par des entités hors UE, à des données personnelles hébergées en France ou en Europe est aussi qualifié de flux transfrontière.

Pour qu'un flux de données transfrontalier soit légal, il doit répondre à l'un des cadres suivants :

- Le flux est réalisé vers un pays disposant d'un niveau de protection adéquat. La liste de ces pays figure sur le site de la CNIL ;
- Les flux sont justifiés notamment par un consentement ou plus généralement pour une SGP, ce flux est rendu nécessaire pour l'exécution d'un contrat concernant la personne concernée elle-même ;
- Les flux sont encadrés par des contrats particuliers :
    - soit des règles internes (autrement appelé Binding corporate rules) qui sont peu nombreuses et sont généralement l'apanage des grandes entreprises multinationales ;
    - soit dans le cadre de la signature de « clauses contractuelles types » élaborées par la Commission européenne.

En dehors de ces cas, les flux en dehors de l'EU sont purement et simplement interdits.

Concernant les clauses contractuelles à intégrer dans le Data Processing Agreement (DPA), il convient de respecter, lorsque le destinataire est sous-traitant, les règles ci-dessous :

- Si le pays de destination des données personnelles fait partie de l'EEE, il convient d'utiliser les clauses contractuelles types sous-traitants validées par la Commission Européenne et listées dans la décision d'exécution UE 2021/915 (lien web : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0915)

- Si le pays de destination des données personnelles est un pays tiers hors EEE bénéficiant d'une décision d'adéquation de la Commission Européenne, le transfert de données est considéré comme étant réalisé dans des conditions de sécurité équivalentes à celles d'un pays de l'EEE et les clauses contractuelles « EEE » peuvent être utilisées.

En l'absence de décision d'adéquation de la Commission européenne, une analyse d'impact du transfert de données doit être impérativement réalisée en amont.
L'exportateur des données personnelles doit évaluer le niveau de protection du pays de destination et le cas échéant les garanties à apporter. Cette évaluation doit :

- permettre d'évaluer le niveau de protection offert par la législation locale,
- tenir compte des pratiques des autorités dans le pays tiers en matière d'accès aux données transférées,
- permettre de déterminer si nécessaire les mesures supplémentaires permettant de combler les lacunes constatées dans la protection et d'assurer le niveau requis par la législation de l'Union Européenne.

Quant à la mise en conformité contractuelle dans ce contexte, il convient d'imposer si possible au sous-traitant des « garanties appropriées » ; celles-ci peuvent être apportées par des clauses contractuelles types spécifiques « pays tiers » validées par la Commission européenne et listées dans la décision d'exécution UE 2021/914 (ci-après lien web) :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32021D0914

Point d'attention : En l'absence de décision d'adéquation ou de garanties appropriées, le transfert de données personnelles vers un pays tiers ne pourra avoir lieu que si l'une des conditions suivantes est remplie :

- consentement explicite de la personne concernée au transfert envisagé (après avoir été informée sur le transfert de données personnelles),
- transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement,
- transfert nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne.

A noter, pour l'ensemble des pays (EEE ou pays tiers) destinataires du transfert de données personnelles, la SGP responsable de traitement devra s'assurer vis-à-vis du sous-traitant des mesures de conformité suivantes :

- mettre en place un mode de transfert sécurisé des données personnelles (du type FTPS ou équivalent) entre responsable de traitement et sous-traitant,
- informer les personnes physiques concernées par le traitement,
- donner des instructions écrites au sous-traitant, en particulier sur la durée de conservation des données, pendant et à la fin de la prestation (si ces durées ne sont pas déjà précisées contractuellement),
- au cours de la prestation, demander si nécessaire à réaliser des contrôles périodiques sur la conformité du sous-traitant, sous forme d'audits documentaires (informations que celui-ci s'engage contractuellement à mettre à disposition). D'éventuelles inspections sur place pourraient parfois s'avérer nécessaires, le RGPD n'impose pas au responsable de traitement de réaliser ces audits, mais impose au sous-traitant de mettre à la disposition du responsable

du traitement ou des autorités de contrôle toutes les informations nécessaires à la réalisation d'audits (article 28-3-h).

GLOSSAIRE DES PRINCIPALES DEFINITIONS

- **Donnée à caractère personnel** : au sens de l'article 4 du RGPD, toute information relative à une personne physique (ce qui exclut les données relatives aux personnes morales), identifiée ou identifiable, directement ou indirectement par référence à un numéro d'identification ou à plusieurs éléments qui lui sont propres (exemple NIR/RNIPP).

- **Donnée sensible :** Se trouve interdit, sauf exception, de traiter des données suivantes en raison des risques qu'elles présentent par leur caractère sensible : les informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

- **Traitement :** toute opération ou tout ensemble d'opérations relatifs aux données personnelles, et ce quel que soit le procédé utilisé au sens de l'article 4-2 du RGPD (notamment la collecte, l'enregistrement, la conservation, l'adaptation ou la modification, ...)

- **Responsable de traitement :** personne physique ou morale (entreprise, organisme public, commune, etc.) qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser.

- **Sous-traitant :** personne physique ou morale qui traite des données pour le compte d'un autre organisme (« le responsable de traitement »), dans le cadre d'un service ou d'une prestation. Ce dernier est soumis à des obligations dans son contrat de prestation permettant de garantir la protection des données personnelles.

- **Consentement :** toute manifestation de volonté par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement au sens du considérant 32 du RGDP.

- **Analyse d'impact**, aussi appelée DPIA ou AIPD : s'inscrit dans le cas de traitement de données susceptibles de générer un risque élevé pour le droit et liberté des personnes concernées. L'analyse d'impact permet de mettre en œuvre des traitements conformes concernant la vie privée des personnes mais également de démontrer la conformité de ces traitements avec le RGPD.

L’AFG remercie les membres du Groupe de travail RGPD qui ont participé à l’élaboration de ce document, en particulier son président Luc Fouché (Crédit Mutuel Asset Management) et Éric Barbry (Racine).

Le Groupe de travail RGPD est rattaché à la Commission Déontologie et Conformité présidée par Monique Diaz (AXA Investment Managers Paris). Valentine Bonnet, directrice Gouvernement d’entreprise et Conformité (AFG), a coordonné ces travaux.

AFG

Ensemble, s'investir
pour demain

17 square Edouard VII · 75009 Paris · +33 (0)1 44 94 94 00 ■ Avenue des Arts 56 · 1000 Bruxelles ■ www.afg.asso.fr