GUIDE
PRATIQUE

Le RGPD
POUR LES PR

AGIL'IT
make things simple

Syndicat du Conseil en Relations Publics

Sommaire

Préambule

La protection des données à caractère personnel est à la fois un défi et un enjeu de taille pour les entreprises, notamment pour les agences conseil en relations publics (ci-après les « agences PR »).

Elaboré dans le cadre d'un travail mené conjointement par le Syndicat du Conseil en Relations Publics et le cabinet d'avocats Agil'IT, le présent guide a vocation à permettre aux agences PR d'identifier de manière pédagogique les principes applicables en matière de protection des données à caractère personnel ainsi que les conséquences pratiques en résultant pour ces dernières.

Il n'a pas pour objet de couvrir l'exhaustivité des cas de figure mais de poser les règles générales auxquelles les agences PR doivent se conformer en matière de protection des données à caractère personnel.

Il s'agit ainsi de permettre aux agences PR de prendre conscience des obligations et enjeux résultant de cette réglementation, et d'initier et/ou, le cas échéant, de maintenir une démarche de conformité opérationnelle au regard de la réglementation applicable en matière de protection des données à caractère personnel, dans le cadre d'une bonne gouvernance desdites agences.

A cette fin, le présent guide vise à décrire les **bonnes pratiques attendues** de la part des agences PR pour assurer la protection des données à caractère personnel des personnes physiques dont elles peuvent être amenées à collecter et traiter les données, et ce à l'aide de **diverses illustrations concrètes qui pourront bien entendu nécessiter d'être adaptées et/ou déclinées en fonction du rôle et des responsabilités, et donc de la qualification effective de l'agence PR** (à savoir responsable du traitement, responsable conjoint du traitement ou encore sous-traitant de données à caractère personnel), cette qualification devant être définie par l'agence PR, pour chaque client et/ou mission, au regard des modalités de sa collaboration avec son client et/ou avec ses partenaires.

Le présent guide a été élaboré au regard de la réglementation applicable en la matière, telle que résultant :

- du Règlement européen (UE)2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après désigné le « RGPD ») ;
- de la loi française 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après désignée la « Loi Informatique et libertés ») et de ses décrets d'application, dans leur version en vigueur à la date de publication du présent guide ;

(ci-après désignées ensemble la « réglementation applicable en matière de protection des données à caractère personnel »).

Bonne lecture…

PUBLIC CIBLE : TOUTE L'AGENCE

1.1
LE RGPD : QUOI ET POUR QUI ?

Le RGPD est un règlement communautaire applicable directement (c'est-à-dire sans besoin de transposition par une loi nationale) dans tous les pays de l'Union européenne depuis le 25 mai 2018 qui a vocation à harmoniser le droit de la protection des données à caractère personnel au sein de l'Union européenne.

Le droit de la protection des données à caractère personnel n'est pas nouveau. Le texte de référence en droit français date même de 1978 !

Toutefois, le RGPD, bien que reprenant un certain nombre de règles et de principes d'ores et déjà préexistants dans notre droit national en matière de protection des données à caractère personnel, est venu apporter un changement de paradigme s'agissant de la responsabilité des entités traitant de telles données qui s'en trouve renforcée, voire exacerbée.

Avant de vous présenter ces principes et d'en décliner les conséquences pratiques pour votre agence, un rapide tour d'horizon du périmètre d'application de cette nouvelle réglementation est présenté ci-après.

QUOI ?

La réglementation applicable en matière de protection des données à caractère personnel s'applique dès lors qu'un traitement de données à caractère personnel est mis en œuvre.

A cet égard, il est rappelé que :

- le terme **« données à caractère personnel »** désigne toute information se rapportant à une personne physique identifiée ou identifiable[1] (cette dernière étant dénommé ci-après la « personne concernée »), directement ou indirectement (par exemple, par un numéro identifiant ou un recoupement d'informations).

(EXEMPLES)

Exemples de données à caractère personnel : le nom, le prénom, les coordonnées, le numéro de sécurité sociale, la fonction, les centres d'intérêt, les habitudes de consommation, les données de localisation d'un individu, une adresse IP,...

Il est par ailleurs **indifférent que les données soient relatives à la sphère privée ou professionnelle de la personne concernée** (cf. la personne dont les données à caractère personnel sont traitées) : toute donnée qui permet d'identifier une personne physique est une donnée à caractère personnel.

(ILLUSTRATION)

A titre d'illustration, une adresse de courrier électronique, même professionnelle, est une donnée à caractère personnel à partir du moment où elle permet d'identifier une personne physique. Il en est de même pour le matricule d'un salarié.

- **un traitement de données à caractère personnel** est défini comme 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[2].

(EXEMPLES)

Exemples de traitements : 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 encore la destruction de données à caractère personnel.

Il résulte de ce qui précède que les **agences PR sont susceptibles de mettre en œuvre des traitements de données à caractère personnel,** ne serait-ce que dans le cadre de la gestion administrative des membres de leur personnel, de la tenue et de la mise à jour des fichiers clients et des contacts personnes physiques qui y sont rattachés par exemple ou encore dans le cadre de la gestion et du suivi de leurs relations avec les journalistes, influenceurs, etc.

[1] Cf. article 4 du RGPD.
[2] Cf. article 4 du RGPD.

PUBLIC CIBLE : TOUTE L'AGENCE

LE SAVIEZ-VOUS ?

La réglementation applicable en matière de protection des données à caractère personnel a vocation à s'appliquer à **tous les traitements de données à caractère personnel, quel qu'en soit le support.** Ainsi, outre les traitements dits « automatisés » ou « informatisés », les traitements « non automatisés » ou « manuels » de données à caractère personnel doivent également respecter la réglementation applicable en matière de protection des données à caractère personnel à condition que les données soient contenues ou appelées à figurer dans un fichier[3], défini comme un ensemble structuré de données accessibles selon des critères déterminés (que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique)[4].

En pratique, cela signifie que **sont concernés par cette réglementation les traitements de données à caractère personnel mis en œuvre tant au moyen d'un outil, d'une application ou d'un logiciel métier, que dans un tableau Excel, ou encore sur des documents papiers…**

POUR QUI ?

La réglementation applicable en matière de protection des données à caractère personnel dispose d'un large champ d'application et tout organisme, quels que soient sa taille et son secteur d'activité, est susceptible d'être concerné.

En effet, la réglementation applicable en matière de protection des données à caractère personnel prévoit des obligations à la charge :

- **du responsable de traitement,** à savoir toute entité qui, **seule ou conjointement** avec d'autres, **détermine les finalités et les moyens** d'un (ou plusieurs) traitement(s) de données à caractère personnel ;
- **du sous-traitant,** à savoir toute entité qui traite des données à caractère personnel **pour le compte du responsable de traitement.**

[3] Cf. considérant 15 et article 2 du RGPD et article 2 de la Loi Informatique et libertés.
[4] Cf. article 4 du RGPD.
[5] Pour en savoir plus sur les critères de qualification, voir G29, Avis 1/2010 du 16 février 2010 sur les notions de responsable de traitement et de sous-traitant (WP 169), CEPD, Lignes directrices sur les concepts de responsables de traitement, sous-traitant et responsabilité conjointe, 7 novembre 2019 et la « checklist » proposée par l'autorité de contrôle anglaise (i.e. Information Commissioner's Office).
[6] Cf. article 26 du RGPD.

FOCUS SUR LES CRITÈRES DE QUALIFICATION DU RESPONSABLE DE TRAITEMENT ET DU SOUS-TRAITANT

Afin d'identifier les obligations qui incombent à une entité, il convient de s'interroger sur la qualification que celle-ci doit revêtir en matière de protection des données à caractère personnel, à savoir responsable de traitement ou sous-traitant, et ce pour **chaque traitement mis en œuvre.**

La détermination de la qualification d'une entité en matière de protection des données à caractère personnel, qui doit se faire in *concreto* et en fonction de la finalité poursuivie, est structurante dans la mesure où il en résulte des responsabilités différentes.

Ainsi, **divers critères et indices doivent être pris en compte** afin de déterminer l'entité devant être qualifiée de responsable de traitement[5] : initiative du traitement et définition de la finalité / des objectifs du traitement, influence de droit ou de fait sur le traitement et degré d'influence exercé, autonomie et pouvoir décisionnaire sur le traitement, image donnée aux personnes concernées et attentes raisonnables que cette visibilité peut susciter chez ces dernières, détermination des moyens matériels, humains, techniques et organisationnels du traitement, etc.

Pour un même traitement, **il peut, dans certaines hypothèses, y avoir plusieurs responsables décidant conjointement de la finalité du traitement et des moyens à mettre en œuvre** pour l'effectuer[6]. Ainsi, une responsabilité conjointe naît lorsque plusieurs parties déterminent ensemble la finalité et/ou les éléments essentiels des moyens relatifs à certaines opérations de traitement, étant précisé que la participation des parties à la détermination commune du traitement (cf. finalité / moyens) peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale.

Au contraire, la qualification de sous-traitant renvoie à la notion de délégation : le sous-traitant n'utilise les données que **sur instruction** et **pour le compte du responsable de traitement,** à tout le moins en ce qui concerne la finalité du traitement et les éléments essentiels des moyens.

En tout état de cause, **il convient de se rapprocher du DPO ou, à défaut, du référent en matière de protection des données à caractère personnel pour toute interrogation relative** à la qualification des différents acteurs susceptibles d'intervenir dans le cadre d'un projet impliquant un traitement de données à caractère personnel.

PUBLIC CIBLE : TOUTE L'AGENCE

Il appartient donc à toute agence PR de définir, en fonction des critères de qualification présentés ci-dessus, pour chaque client et/ou mission, si elle agit en qualité de responsable de traitement, de responsable conjoint du traitement, ou encore de sous-traitant, et ce de manière concrète, factuelle, au regard des modalités de sa collaboration avec chaque client et/ou avec chaque partenaire.

La qualification d'une agence PR (cf. responsable de traitement ou sous-traitant) est essentielle dans la mesure où de cette qualification découlent les obligations qui lui sont applicables en termes de protection des données à caractère personnel. Une telle qualification revêt également une importance fondamentale s'agissant des documents contractuels requis au titre de la réglementation applicable en matière de protection des données à caractère personnel.

Le tableau ci-dessous reprend en synthèse lesdites obligations, en fonction de la qualification de l'agence :

OBLIGATIONS DU RESPONSABLE DE TRAITEMENT	OBLIGATIONS DU SOUS-TRAITANT
Licéité, loyauté et transparence du traitement Limitation des finalités Minimisation des données Exactitude des données Proportionnalité des durées de conservation	Traitement des données à caractère personnel sur instructions documentées du responsable de traitement et conformément au contrat conclu avec ce dernier
Réalisation d'une analyse d'impact + consultation de la Cnil le cas échéant	Interdiction du traitement des données à caractère personnel pour d'autres finalités
Mise en œuvre des principes *de privacy by design et de privacy by default*[7]	Coopération avec le responsable de traitement (sécurité, droits des personnes concernées, analyse d'impact, violation de données à caractère personnel,...)
Notification à la Cnil des violations de données à caractère personnel + communication à l'attention des personnes concernées le cas échéant	Accès aux données à caractère personnel limité à ce qui a été autorisé par le responsable de traitement
Encadrement des flux transfrontières de données à caractère personnel	Sous-traitance ultérieure seulement si autorisation préalable et écrite du responsable de traitement
Sécurité des données	Sécurité des données
Registre des traitements « version responsable de traitement »	Registre des traitements « version sous-traitant »
Coopération avec les autorités de contrôle	Coopération avec les autorités de contrôle
Conclusion d'un contrat avec chaque sous-traitant comportant les éléments obligatoires au titre de l'article 28 du RGPD	**CEPD, lignes directrices sur les concepts de responsables de traitement, sous-traitant et responsabilité conjointe au sens du règlement UE 2018/1725 (cf. traitements mis en œuvre par les institutions et organes de l'UE), 7 novembre 2019**
Conclusion d'un contrat avec chaque responsable de traitement conjoint comportant les éléments obligatoires au titre de l'article 26 du RGPD	

[7] Ces principes sont visés à l'article 25 du RGPD.
Le principe de « privacy by design » consiste en la nécessité, dès en amont, avant le déploiement de tout nouveau projet, de procéder à une analyse visant à prévenir toute atteinte à la vie privée des personnes concernées, d'où la nécessité d'adopter une approche proactive pour anticiper les contraintes légales et réglementaires. La protection des données à caractère personnel doit être intégrée dès la conception de tout projet de traitement, qu'il s'agisse d'un nouveau projet, d'une évolution d'un projet déjà existant, du développement d'une nouvelle solution ou encore du recours à un nouveau sous-traitant par exemple. Elle doit donc être assurée lors de la création d'un traitement mais aussi tout au long de son processus et du cycle de vie de la donnée, y compris en ce qui concerne la conservation des données.
Le principe de « privacy by default » consiste en la nécessité de prendre les mesures techniques et organisationnelles appropriées pour garantir que par défaut seules les données qui sont nécessaires au regard de la finalité spécifique du traitement sont collectées et utilisées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.

PUBLIC CIBLE : TOUTE L'AGENCE

D'un point de vue macroscopique, il résulte de ce qui précède, dans les grandes lignes, que le respect des principes fondamentaux en matière de protection des données à caractère personnel et l'assurance de la licéité d'un traitement de données à caractère personnel demeurent principalement à la charge du responsable de traitement.

Toutefois, cette qualification constitue une opportunité pour une agence PR puisqu'elle signifie que lorsque cette dernière se voit qualifiée de responsable de traitement, elle dispose alors d'une maîtrise significative sur le traitement, a minima s'agissant de la détermination de sa finalité et des moyens essentiels du traitement (typologie des données traitées, durée de conservation des données,...).

A l'inverse, la qualification d'une agence PR en qualité de de sous-traitant, par exemple pour l'exercice de certaines missions, induit à sa charge des responsabilités pouvant être considérées comme moindres (tout en étant tout de même tenue notamment à un devoir de coopération, d'alerte ou encore à une obligation de sécurité renforcée s'agissant des données à caractère personnel), mais lui impose de n'agir que sur instructions de son client (cf. le responsable de traitement) et conformément à celles-ci.

En outre, le RGPD s'applique aux traitements de données à caractère personnel mis en œuvre dans le cadre de l'activité d'une **entité située sur le territoire de l'Union européenne,** que l'entité en question dispose de la qualité de responsable de traitement ou de sous-traitant, et **que le traitement ait lieu ou non dans l'Union européenne[8].**

Par ailleurs, si **le responsable de traitement ou le sous-traitant n'est pas établi dans l'Union européenne, alors le RGPD peut tout de même s'appliquer en raison du lieu où se trouvent les personnes concernées par le traitement !** En effet, le RGPD s'applique également si les personnes concernées se trouvent sur le territoire d'un Etat membre de l'Union européenne, et si le traitement est lié :

- soit à une offre de biens ou de services à destination desdites personnes concernées ;
- soit au suivi du comportement de ces personnes dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne[9].

S'agissant des spécificités prévues en la matière par la loi française, la Loi Informatique et libertés est applicable aux traitements de données à caractère personnel effectués dans le cadre des activités d'un responsable de traitement ou d'un sous-traitant sur le territoire français, que le traitement ait lieu ou non en France. En outre, les dispositions françaises prises sur le fondement des dispositions du RGPD s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable de traitement n'est pas établi en France[10].

(EXEMPLES)

Une agence PR est responsable du traitement de données à caractère personnel ayant pour finalité la gestion de ses relations avec ses clients et prospects, ou encore la gestion administrative de son personnel.

S'agissant des fichiers de « relations », de « contacts » ou de « parties prenantes » :

› lorsque ces derniers sont établis par l'agence PR sur instructions et sous le contrôle du client de l'agence PR, pour une finalité déterminée par le client, il sera très probable que l'agence PR agisse en qualité de sous-traitant concernant ces fichiers et ce, même s'ils contiennent des données de « contacts », « relations » ou « parties prenantes » qui ne seraient pas fournies par le client ;

› dans les cas où la finalité et les moyens seraient en revanche déterminés par l'agence PR ayant toute latitude et disposant d'un pouvoir décisionnaire sur le contenu de ces fichiers et sur leur utilisation, l'agence sera vraisemblablement responsable de son propre traitement s'agissant de tels fichiers de « relations », de « contacts » ou de « parties prenantes » en vue de leur utilisation dans le cadre de leur activité d'agence PR.

En tout état de cause, une appréciation au cas par cas doit donc être réalisée par chaque agence PR s'agissant de tels fichiers.

Par exemple, lorsqu'un client demande à son agence PR de réaliser un communiqué ou encore une carte de vœux, et de l'adresser à une liste de contacts que le client lui communique, il peut être considéré que l'agence PR agit en qualité de sous-traitant pour le compte de son client.

[8] Cf. article 3.1 du RGPD.
[9] Cf. article 3.2 du RGPD.
[10] Cf. article 3 de la Loi Informatique et libertés.

PUBLIC CIBLE : TOUTE L'AGENCE

1.2
LE RGPD : ENJEUX ET OPPORTUNITÉS

Le RGPD vise à renforcer la protection des données à caractère personnel et la maîtrise des individus sur leurs données mais également la responsabilité des entités traitant des données à caractère personnel.

L'ensemble des organismes (entreprises, collectivités publiques, associations, organisations professionnelles, syndicats…) doivent donc tenir compte des obligations du RGPD et offrir une protection appropriée des données à caractère personnel qu'ils détiennent (données de leurs salariés ou collaborateurs, de leurs clients, de leurs partenaires ou fournisseurs,…), sous peine de voir leur responsabilité engagée et d'être sanctionnés à ce titre…

En France, le respect de la réglementation applicable en matière de protection des données à caractère personnel est contrôlé par la Commission Nationale de l'Informatique et des Libertés (ci-après la « Cnil »), et le non-respect de ces dispositions peut faire l'objet de sanctions prononcées par la formation restreinte (cf. formation de jugement) de la Cnil.

Or, depuis l'entrée en application du RGPD, les sanctions pouvant être prononcées par la formation restreinte de la Cnil en cas de non-respect de la réglementation applicable en matière de protection des données à caractère personnel peuvent être particulièrement sévères puisque celle-ci peut désormais prononcer des **amendes administratives qui, pour les manquements les plus graves, peuvent atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial,** le montant le plus élevés de ces deux plafonds étant encouru.

(EXEMPLES DE SANCTIONS PRONONCÉES PAR LA CNIL)

- La Cnil a considéré que les traitements de données à caractère personnel mis en œuvre par Google à des fins de **personnalisation de la publicité** sont illicites en l'**absence de recueil valable du consentement** des utilisateurs et du fait du **non-respect par Google de l'obligation d'informer les personnes concernées dont les données sont traitées.** En raison de ces manquements, la Cnil a condamné Google à une **amende de 50 millions d'euros**[11].

- Un défaut de sécurité permettait à un utilisateur d'accéder, depuis son espace personnel en ligne, à des documents enregistrés par d'autres utilisateurs en modifiant légèrement l'URL affichée dans le navigateur. Par conséquent, les documents transmis / uploadés en ligne par des tiers étaient librement accessibles, sans authentification préalable **(cf. manquement à l'obligation d'assurer la sécurité et la confidentialité des données).** En outre, les données collectées via l'espace en ligne étaient conservées de manière illimitée (cf. **manquement à l'obligation de conserver les données pour une durée proportionnée**). En raison de ces manquements, la Cnil a prononcé une **amende de 400 000 euros** à l'encontre de la société mise en cause[12].

- En raison de plusieurs manquements à la réglementation applicable en matière de protection de données à caractère personnel **(non-respect du droit d'opposition à la prospection par téléphone et du droit à l'information des personnes concernées, excessivité des commentaires** saisis dans le logiciel de gestion de la clientèle (commentaires injurieux ou relatifs à l'état de santé des clients), **absence de garanties encadrant les transferts** de données à caractère personnel **hors Union européenne** et **manquement à l'obligation de coopération** avec la Cnil), la Cnil prononcé une **amende de 500 000 euros** ainsi qu'**une injonction de mettre en conformité** le traitement mis en œuvre à des fins de prospection par téléphone avec la réglementation applicable en matière de protection des données à caractère personnel, **injonction assortie d'une astreinte de 500 euros par jour de retard** à l'issue d'un délai d'un mois suivant la notification de la délibération de la Cnil, les justificatifs de la mise en conformité devant être adressés à la cette dernière dans ce délai[13].

[11] Cnil, Délibération n°SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC
[12] Cnil, Délibération n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC
[13] Cnil, Délibération n°SAN-2019-010 du 21 novembre 2019 concernant la société FUTURA INTERNATIONALE

PUBLIC CIBLE : TOUTE L'AGENCE

ET DANS LE RESTE DE L'EUROPE ?

Voir le site :
https://www.enforcementtracker.com/

DUTCH SUPERVISORY AUTHORITY FOR DATA PROTECTION - 3 MARS 2020 (SOCIÉTÉ ROYAL DUTCH TENNIS ASSOCIATION)

› Vente de données à caractère personnel (identité, sexe et coordonnées) de ses membres à des sponsors pour une utilisation par ces derniers à des fins de prospection, sans avoir recueilli le consentement des personnes concernées, ce dont il résulte que la revente de telles données est dépourvu de fondement juridique

› Amende de 525 000 euros

DATA PROTECTION AUTHORITY OF BERLIN - 30 OCTOBRE 2019 (SOCIÉTÉ DEUTSCHE WOHNEN SE)

› Non-respect des principes généraux applicables en matière de protection des données à caractère personnel (notamment non-respect du principe de limitation de la durée de conservation, portant sur des données présentant une particulière « sensibilité », et non-respect du principe de « privacy by design & by default »)

› Amende de 14,5 millions d'euros

ITALIAN DATA PROTECTION AUTHORITY - 15 JANVIER 2020 (SOCIÉTÉ TIM)

› Non-respect de plusieurs dispositions de la réglementation applicable en matière de protection des données à caractère personnel (notamment traitement de données à caractère personnel à des fins de prospection à l'attention de personnes s'y étant opposé ou sans recueil préalable du consentement des personnes concernées, manquement à l'obligation d'information des personnes concernées, défaut de sécurité et absence de clarté des durées de conservation des données)

› Amende de 27,8 millions d'euros + injonction de déployer des mesures correctives

AUSTRIAN DATA PROTECTION AUTHORITY - 23 OCTOBRE 2019 (SOCIÉTÉ AUSTRIAN POST)

› Création de profils de plus de trois millions d'autrichiens, qui incluaient des informations sur leur adresse personnelle, leurs préférences personnelles, leurs habitudes et leurs affinités possibles avec des partis politiques, informations qui ont été revendues, par exemple à des partis politiques et des entreprises

› Amende de 18 millions d'euros + jugement également rendu par un tribunal civil (800 euros d'indemnisation - cf. dommages et intérêts - par victime)

PUBLIC CIBLE : TOUTE L'AGENCE

Outre des amendes administratives, la Cnil peut, en cas de manquement à la réglementation applicable en matière de protection des données à caractère personnel, **prononcer notamment les mesures suivantes[14]:**

- un rappel à l'ordre ;
- une injonction de mette en conformité le traitement, le cas échéant sous astreinte[15] ;
- la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application de la réglementation précitée ;
- le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;
- la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;
- la suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes.

Dans la mesure où **les décisions et sanctions précitées peuvent être rendues publiques,** il peut également en résulter un **préjudice d'image et de réputation** (cf. atteinte à la notoriété) pour l'agence PR qui serait concernée, voire une perte de confiance de la part des clients, partenaires, journalistes,...

Au vu de ces enjeux, il appartient dans un premier temps à chaque agence PR d'entreprendre une **démarche de mise en conformité** de ses traitements de données à caractère personnel.

Une telle démarche est particulièrement opportune pour les agences PR dans la mesure où leur mise en conformité avec les obligations issues de la réglementation applicable en matière de protection des données à caractère personnel, outre le fait qu'elle s'impose, peut constituer pour celles-ci :

- un **gage de confiance** pour leur écosystème (notamment à l'égard des partenaires commerciaux, des clients, des membres du personnel, des prestataires, des journalistes ou encore des Key Opinion Leaders) ;
- mais également un **avantage compétitif** en termes de différenciation vis-à-vis de la concurrence.

En tout état de cause, la protection des données à caractère personnel est un moyen pour l'entreprise de renforcer la confiance qui la lie à ses clients, partenaires, prestataires et membres de son personnel, dans un contexte où les personnes concernées sont de plus en plus sensibilisées à cet égard et accordent une attention particulière et une importance croissante à la protection de leurs données. Il est donc important que les agences PR ne passent pas à côté de cette réglementation.

LE SAVIEZ-VOUS ?

Le non-respect de la réglementation applicable en matière de protection des données à caractère personnel peut également donner lieu à la mise en œuvre de la **responsabilité civile** du responsable de traitement, voire du sous-traitant de données à caractère personnel. A titre d'exemple, une personne concernée a le droit de demander devant les juridictions compétentes des **dommages et intérêts en réparation du préjudice** qu'elle a subi du fait d'un traitement de ses données à caractère personnel qui serait mis en œuvre de manière non-conforme aux dispositions applicables. A cet égard, il convient en outre de noter que le non-respect de ces dispositions peut également faire l'objet **d'actions de groupe** pouvant être exercées en vue (i) de faire cesser le manquement à la réglementation constaté et/ou (ii) d'engager la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis.

Une agence PR, voire le dirigeant ou un collaborateur de l'agence PR concernée dans certaines hypothèses et sous certaines conditions, pourra(ont) également voir **leur responsabilité pénale** engagée au titre d'infractions commises en violation de la réglementation applicable en matière de protection des données à caractère personnel[16]. Dans une telle hypothèse, les sanctions pénales encourues sont de 5 ans d'emprisonnement et de 300 000 € d'amende (le montant maximum de l'amende étant multiplié par 5 lorsque la responsabilité de la personne morale est retenue).

[14] Cf. article 20 de la Loi Informatique et libertés.
[15] Cnil, Délibération n°SAN-2019-010 précitée.
[16] Cf. articles 226-16 et suivants du Code pénal.

PUBLIC CIBLE : TOUTE L'AGENCE

SCHÉMA RÉCAPITULATIF DES ENJEUX ET OPPORTUNITÉS D'UNE MISE EN CONFORMITÉ

AMÉLIORER SON EFFICACITÉ

Identifier ses traitements, ses données et éventuellement ses vulnérabilités pour y remédier

MAINTENIR LA CONFIANCE

Répondre aux demandes des clients, partenaires, etc. : gage de confiance

RESPECTER LA LOI

Eviter des sanctions en constante augmentation

SE DÉMARQUER DE LA CONCURRENCE

Bénéficier d'un facteur de compétitivité au sein de son écosystème

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.1
DOIS-JE DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES ? QUI, QUOI ET COMMENT ?

2.1.1 Présentation des hypothèses de désignation obligatoire

Toute agence PR, qu'elle agisse en qualité de responsable de traitement ou de sous-traitant, est tenue de désigner un délégué à la protection des données (ou « data protection officer », ci-après désigné « DPO ») dès lors que l'un des critères suivants est rempli[17], étant précisé que ces critères sont alternatifs, c'est-à-dire lorsque l'agence PR se retrouve dans au moins une des situations suivantes :

- **les activités de base de l'agence PR consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;**

Les activités de base d'un responsable de traitement « ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire[18]» . Les « activités de base » peuvent être considérées comme les opérations essentielles nécessaires pour atteindre les objectifs du responsable de traitement ou du sous-traitant.

(EXEMPLES)

› Exemple d'activité de base : l'activité de base d'une agence PR est de définir et mettre en œuvre tout ou partie d'une politique de communication. Les agences PR structurent le fonctionnement des organisations avec les « parties prenantes », internes et externes.

› Exemple d'activité venant en soutien de l'activité de base (et donc non considérée comme activité de base) : fonctions dites « support » de type RH ou comptabilité.

La notion de suivi régulier et systématique des personnes concernées n'est pas définie par les textes, mais inclut toutes les formes de suivi et de profilage sur internet, y compris à des fins de publicité comportementale. La notion de suivi ne se limite toutefois pas à l'environnement en ligne.

Le G29[19] interprète le terme « régulier » comme recouvrant une ou plusieurs des significations suivantes :

› continu ou se produisant à intervalles réguliers au cours d'une période donnée ;
› récurrent ou se répétant à des moments fixes ;
› ayant lieu de manière constante ou périodique.

Le G29 interprète le terme « systématique » comme recouvrant une ou plusieurs des significations suivantes :

› se produisant conformément à un système ;
› préétabli, organisé ou méthodique ;
› ayant lieu dans le cadre d'un programme général de collecte de données ;
› effectué dans le cadre d'une stratégie.

(EXEMPLES)

Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées : reciblage (retargeting) par courrier électronique, activités de marketing fondées sur les données et notamment sur des opérations de profilage ou de segmentation, publicité comportementale,...

[17] Cf. article 37 du RGPD. Les exemples et illustrations présentés dans le présent paragraphe « Présentation des hypothèses de désignation obligatoire » sont issus de la doctrine du G29 en la matière (cf. G29, Lignes directrices concernant les délégués à la protection des données, 5 avril 2017 (WP. 243 rev.01) et G29, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE)2016/679, 4 octobre 2017 (WP. 248 rev.01).
[18] Cf. considérant 97 du RGPD.
[19] G29 = groupe de travail européen regroupant des représentants de chaque autorité de contrôle des pays de l'Union européenne. Ce groupe de travail a été remplacé, depuis l'entrée en application du RGPD, par le Comité européen de la protection des données (ou CEPD).

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

Pour ce qui concerne la notion de **« traitement à grande échelle »**, il n'existe pas de jurisprudence en la matière et le G29 précise d'ailleurs qu'il n'est « *pas possible de donner un chiffre précis, que ce soit pour la quantité de données traitées ou le nombre d'individus concernés, qui soit applicable dans toutes les situations. Cela n'exclut toutefois pas la possibilité qu'au fil du temps, une pratique courante puisse émerger, permettant de déterminer en des termes plus spécifiques ou quantitatifs ce qui constitue un traitement «à grande échelle» pour certains types d'activités de traitement courantes. Le G29 prévoit également de contribuer à cette évolution, en partageant et faisant connaître des exemples de seuils pertinents pour la désignation d'un [DPO]* ».

Si des seuils permettant de déterminer ce qu'est un traitement à grande échelle ont été évoqués dans la proposition initiale du RGPD en 2012 (cf. traitement réalisé par une entreprise employant 250 personnes ou plus) puis dans la position arrêtée en première lecture par le Parlement européen en 2014 (cf. traitement effectué par une personne morale et qui porte sur plus de 5000 personnes concernées sur toute période de douze mois consécutifs), cette logique de seuil a été expressément abandonnée dans le RGPD.

En tout état de cause, le G29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement est mis en œuvre « à grande échelle » :

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée ;
- le volume de données et/ou le spectre des données traitées ;
- la durée, ou la permanence, des activités de traitement des données ;
- l'étendue géographique de l'activité de traitement.

[20] C'est-à-dire au cas par cas, *in concreto*.

(EXEMPLES)

Exemples de traitements **« à grande échelle »** : traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités, traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités, traitement des données à caractère personnel par un moteur de recherche à des fins de publicité, collecte de données sur les réseaux sociaux publics dans le but de générer des profils, utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés son digest générique quotidien.

L'exemple suivant du G29, concernant l'activité d'un sous-traitant, pourrait également apporter un éclairage pertinent pour les agences PR et leur permet éventuellement d'en déduire si leur activité est « à grande échelle » ou non : une petite entreprise familiale active dans le secteur de la distribution d'appareils électroménagers dans une seule ville recourt aux services d'un prestataire dont l'activité de base consiste à fournir des services d'analyse de sites internet et d'assistance à la publicité et au marketing ciblés. Selon le G29, les activités de l'entreprise familiale et ses clients n'entraînent pas de traitement de données à « grande échelle », compte tenu du faible nombre de clients et des activités relativement limitées. **Toutefois, prises globalement, les activités du prestataire, qui dispose d'un grand nombre de clients comme cette petite entreprise, consistent en un traitement à grande échelle.**

Cet exemple, transposé aux activités d'une agence PR - et bien que l'expertise de ces dernières permettent justement pour chaque client de cibler les contacts appropriés et non d'adresser des communications à des listings de contacts qui pourraient être qualifiés de contacts « à grande échelle » - pourrait être un argument en faveur de l'existence de traitements de données à caractère personnel « à grande échelle » si l'on tient compte de l'ensemble des contacts de l'agence, pour l'ensemble de ses clients.

Aussi, il convient de réaliser une analyse casuistique[20] des traitements mis en œuvre, en fonction du volume de données pouvant être traité par une agence PR dans le cadre de ses activités de base, afin de déterminer si un traitement « à grande échelle » peut être caractérisé, ce qui pourrait toutefois bien être le cas au regard de l'activité de son activité « cœur de métier ».

- les activités de base du responsable de traitement ou du sous-traitant consistent en un traitement à grande échelle de données dites « particulières » ou « sensibles » ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Voir ci-dessus s'agissant de la notion d'« activité de base » et de « traitement à grande échelle ».

S'agissant de la notion de données « particulières » ou « sensibles », leur traitement fait l'objet d'un régime particulier. Est ainsi visé le traitement des données à caractère personnel qui révèle l'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[21] de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ainsi que le traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions[22].

L'obligation de désigner un DPO peut donc se traduire schématiquement comme suit :

(EXEMPLES)

Exemples de données pouvant être qualifiées de données « particulières » ou « sensibles » : données relatives à l'existence d'une maladie, d'un handicap, … (même sans que le détail de la maladie ou du handicap soit mentionné), appartenance à ou sympathisant d'un parti politique, régime alimentaire,…

DÉSIGNATION D'UN DPO PAR LE RESPONSABLE DE TRAITEMENT / LE SOUS-TRAITANT

OBLIGATION DE DÉSIGNER UN DPO

› si autorité publique ou organisme public ; ou

› si son activité principale consiste en des opérations de traitement qui exigent un suivi régulier et systématique des personnes à grande échelle ; ou

› si son activité principale consiste en un traitement à grande échelle des données dites « particulières » / « sensibles » ou relatives à des condamnations pénales ou à des infractions.

Ainsi, **toute agence PR qui se trouve dans l'une des situations précitées devra désigner un DPO.** A cet égard, s'il n'est pas certain que toutes les agences PR traitent à grande échelle des données dites « particulières » ou « sensibles », **il semble probable qu'elles puissent être considérées comme mettant en œuvre des traitements de données à caractère personnel qui induisent un suivi régulier et systématique à grande échelle des personnes concernées.**

En outre, en dehors des hypothèses obligatoires, la désignation d'un DPO est **facultative** mais reste fortement recommandée.

La recommandation du SCRP

Il est recommandé à toutes les agences PR de désigner un DPO si elles considèrent réunir les critères exposés plus haut. A défaut, si l'agence considère ne pas être tenue par une telle obligation, alors il est fortement recommandé de **désigner un référent** « données à caractère personnel », qui sera en charge de piloter le sujet au sein de l'agence, et ainsi de suivre l'évolution de l'agence et les pratiques déployées en vue de sa mise et de son maintien en conformité au regard de la réglementation applicable en matière de protection des données à caractère personnel, ou encore de donner ses conseils en matière de protection des données à caractère personnel et de répondre aux éventuelles interrogations sur cette thématique qui émaneraient des collaborateurs, des clients, voire des « parties prenantes » par exemple.

[21] Cf. article 9 du RGPD.
[22] Cf. article 10 du RGPD.

2.1.2 Prérequis à la désignation d'un DPO

2.1.2.1 Ce qu'on lui demande d'être

Il résulte des textes applicables que le DPO doit disposer de certaines qualités personnelles et professionnelles.

QUALITÉS PERSONNELLES

Le DPO :

PROBITÉ

› agit en toute circonstance de façon diligente, loyale, responsable et honnête, en fonction de ses connaissances et de son degré d'expertise, au service de l'organisme auprès duquel il exerce sa mission
› respecte l'éthique et n'emploie pas de méthodes illicites

OBJECTIVITÉ

› garde un haut niveau d'objectivité s'agissant de l'analyse, de l'évaluation et de toute communication en ce qui concerne le niveau de conformité de l'organisme auprès duquel il exerce sa mission et résiste au stress
› est impartial, juste et sans parti pris dans toutes ses actions
› procède à une évaluation équilibrée des informations et documentations reçues et n'est pas influencé par ses propres intérêts ou par celui de tiers, ou encore par les préjugés

INDÉPENDANCE

› doit refuser toute intégence ou intrusion dans ses actions
› peut interagir directement et en toute indépendance avec le niveau le plus élevé de la direction
› n'a aucun compte à rendre à un supérieur hiérarchique, dispose d'une liberté organisationnelle et décisionnelle dans le cadre de sa mission, est libre de consulter toute personne, y compris la Cnil, pour prendre ses décisions
› si temps partiel, ne doit pas subir de préjudice du fait de cette mission notamment dans le cadre de l'évaluation de ses performances au titre de ses autres responsabilités

CONFIDENTIALITÉ

› respecte une stricte confidentialité et discrétion s'agissant des informations, procédures, usages, plaintes et litiges dont il a connaissance dans le cadre de son activité

QUALITÉS PROFESSIONNELLES

Le DPO :

COMMUNICATION ET ACCESSIBILITÉ

› doit être un communiquant : il doit convaincre plutôt que de contraindre
› doit être joignable par les personnes en charge du traitement des données, par les personnes concernées et par la Cnil

RESSOURCES

› doit exiger l'accès aux ressources nécessaires (humaines, budgétaires, en temps, en outils,...)
› doit exiger l'accès aux données et opérations de traitement

CONNAISSANCES

› doit disposer de connaissances spécialisées du droit et des pratiques en matière de protection des données
› doit connaître le secteur / domaine d'activité dans lequel il exerce ses fonctions et la réglementation spécifique le cas échéant
› doit avoir des connaissances en technologies de l'information
› le niveau de connaissance requis dépend de la sensibilité et de la complexité des traitements mis en œuvre par le donneur d'ordre
› formation initiale et continue / veille juridique, technologique et sociétale
› la pratique de la langue anglaise est un plus, afin d'être en mesure d'exploiter les nombreux documents et travaux uniquement rédigés dans cette langue.

2.1.2.2 Ce qu'on lui demande de ne pas être

Le RGPD autorise le DPO à « *exécuter d'autres missions et tâches* ». Il exige toutefois que l'organisme qui l'a désigné veille à ce que « *ces missions et tâches n'entraînent* ***pas de conflit d'intérêts*** ».

Aussi, bien que le DPO soit autorisé à exercer d'autres fonctions, il ne peut se voir confier d'autres missions et tâches qu'à condition que celles-ci ne donnent pas lieu à un conflit d'intérêts. Cela signifie en particulier que le DPO ne peut exercer au sein de l'agence PR une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel.

Il résulte de ce qui précède que :

- si le DPO exerce cette fonction à temps partiel, ses autres missions et tâches ne doivent pas conduire à ce qu'il prenne des décisions sur les traitements de données à caractère personnel mis en œuvre par l'agence PR ;
- le DPO se doit d'informer l'organisme qui l'a désigné de tous les intérêts qui pourraient influencer son jugement, altérer son indépendance ou compromettre l'équité dont il doit faire preuve.

A titre d'exemple, le G29 relève ce qui suit :

- « *En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les* ***fonctions d'encadrement supérieur*** *(par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement* »[23].

En raison de la structure organisationnelle spécifique de chaque agence PR, cet aspect doit être étudié au cas par cas : recensement des fonctions potentiellement incompatibles avec la fonction de DPO, mise en œuvre de règles internes destinées à éviter tout éventuel conflit d'intérêts,...

[23] Cf. G29, Lignes directrices concernant les délégués à la protection des données, préc.

2.1.2.3 Ce qu'on lui demande de faire

Par ailleurs, le DPO doit disposer des capacités à accomplir les missions liées à sa désignation.

Ses missions sont multiples et nécessitent en pratique que le DPO regroupe toutes les qualités précitées. En particulier, l'accomplissement de ses missions supposent un bon niveau de connaissances en droit de la protection des données à caractère personnel.

Les missions du DPO sont les suivantes :

- **informer et sensibiliser, diffuser une culture « protection des données à caractère personnel » au sein de l'agence PR,** ce qui implique notamment de :
  - › mener ou piloter des actions visant à sensibiliser la direction et les collaborateurs, dont ceux participants aux opérations de traitement, aux règles à respecter en matière de protection des données à caractère personnel ;
  - › développer son réseau et les synergies entre les membres de l'agence PR ;

(EXEMPLES D'ACTIONS DU DPO)

Supports et séances de formation, communications internes (newsletter du DPO, quizz, modules d'e-learning, FAQ, ...), code de bonne conduite en matière de protection des données à caractère personnel,...

- **veiller au respect de la réglementation applicable en matière de protection des données à caractère personnel,** ce qui implique notamment de :
  - › conseiller la direction et les opérationnels. En tout état de cause, le DPO doit être obligatoirement consulté avant toute mise en œuvre d'un nouveau traitement ou toute modification substantielle d'un traitement existant ;

(EXEMPLES D'ACTIONS DU DPO)

Analyse de la conformité d'un traitement, avis et recommandations motivés et documentés, ajustement des documents contractuels et des mentions d'information des personnes concernées, mise en place d'une démarche « privacy by design » pour tout projet impliquant un traitement de données à caractère personnel,...

  - › s'assurer que les personnes concernées sont informées des traitements opérés impliquant leurs données à caractère personnel, ainsi que de leurs droits ;

(EXEMPLES D'ACTIONS DU DPO)

Vérification et mise à jour des mentions d'information à l'attention des personnes concernées, pour chaque nouveau traitement notamment.

  - › alerter sans délai la direction sur tout risque que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l'agence et/ou à ses dirigeants ;

(EXEMPLES D'ACTIONS DU DPO)

Recommandations / demandes d'arbitrage au niveau le plus élevé de la direction

  - › dispenser des conseils, sur demande, en cas de réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution ;

(EXEMPLES D'ACTIONS DU DPO)

Avis et recommandations sur la nécessité de réaliser une analyse d'impact, conseils méthodologiques, mesures techniques et organisationnelles recommandées, avis sur les conclusions de l'analyse d'impact et sur la nécessité de consulter la Cnil, contrôles réguliers,...

  - › être informé de toute violation de données et être associé aux décisions en matière de notification à la Cnil et de communication aux personnes concernées ;

(EXEMPLES D'ACTIONS DU DPO)

Avis sur la nécessité de notifier / communiquer, participation à la rédaction ou, a minima, revue des notifications / communications avant envoi, échanges ultérieurs avec la Cnil,...

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

- **établir et maintenir une documentation au titre de « l'accountability »,** quelle que soit la qualification de l'agence PR (cf. responsable de traitement ou sous-traitant), ce qui implique notamment d'élaborer des procédures et politiques internes ainsi que de maintenir et mettre à jour le(s) registre(s) des traitements et assurer son accessibilité à la Cnil[24];

FOCUS SUR LA MISE EN ŒUVRE DU PRINCIPE D'ACCOUNTABILITY

Pour en savoir plus, voir le paragraphe « Elaborer les procédures et politiques internes indispensables » ci-après.

FOCUS SUR LE(S) REGISTRE(S) DES TRAITEMENTS

Pour en savoir plus, voir le paragraphe « Recenser mes traitements et réaliser mon(mes) registre(s) des traitements » ci-après.

- **assurer la médiation avec les personnes concernées,** ce qui implique notamment de :
  - recevoir les réclamations des personnes concernées ;
  - veiller au respect des droits des personnes concernées ;
  - traiter ou piloter les réponses aux réclamations, demandes, plaintes (et en tout état de cause s'assurer de leur bon traitement) ;
- **interagir avec la Cnil,** ce qui implique notamment d'être le point de contact privilégié de la Cnil et d'interagir avec cette dernière dans le cadre de toute consultation (rédaction des consultations et des demandes d'avis ou d'autorisations, réponses aux demandes d'informations,...) ;
- **analyser, investiguer, auditer et contrôler,** ce qui implique notamment de mener ou de piloter toute action permettant de juger du degré de conformité de l'agence PR, de mettre en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.), ou encore de vérifier le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données à caractère personnel ;
- **présenter un rapport annuel à la direction,** lequel a vocation à rendre compte de son action au cours de l'année écoulée et des éventuelles difficultés rencontrées ;
- **assister l'agence PR dans le cadre d'un contrôle de la Cnil ou d'une procédure contentieuse / précontentieuse** le cas échéant.

(EXEMPLES D'ACTIONS DU DPO)

Insertion des coordonnées du DPO dans les mentions d'information, analyse de la recevabilité des demandes, déploiement des actions / recherche des éléments nécessaires pour traiter les demandes, élaboration des réponses, ...

[24] A cet égard, il est précisé que le respect du principe d'accountability ainsi que les la tenue du(des) registre(s) des traitements ne sont pas des missions dévolues au DPO mais relèvent de la responsabilité du responsable de traitement (voire du sous-traitant, a minima pour ce qui concerne le registre devant être élaboré par celui-ci). Toutefois, en pratique, et bien que devant demeurer sous la responsabilité de ce dernier, elles sont souvent confiées au DPO.

(EXEMPLES D'ACTIONS DU DPO)

Accompagnement de la Cnil et des opérationnels dans le cadre de contrôles sur place, coopération avec la Cnil, analyse du procès-verbal de constat, identification des actions correctrices, réponses aux demandes complémentaires de la Cnil, réponses à une demande d'informations de la Cnil, à une mise en demeure, à une proposition de sanction,...

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

LE SAVIEZ-VOUS ?

Il résulte de ce qui précède que l**a désignation d'un DPO nécessite d'identifier une personne qui dispose :**

› **des qualités personnelles et professionnelles requises ;**

› **de la capacité à accomplir ses missions en qualité** de DPO ;

› **et dont les autres missions et tâches habituelles ne présentent pas de conflit d'intérêts** avec la fonction de DPO.

Il est donc parfois difficile de trouver en interne une telle personne, notamment en fonction de la taille de l'agence ou en raison de son mode de fonctionnement ou d'organisation (ex : plusieurs fonctions exercées par une même personne). Or, de manière opportune, le RGPD laisse une certaine latitude aux organismes s'agissant des modalités de désignation et d'organisation.

Ainsi, **le DPO peut être :**

› **interne à l'organisme ou externalisé.** En effet, le RGPD prévoit que *« Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service »*. Par ailleurs, lorsque le DPO est externalisé, il peut s'agir d'une personne physique ou morale ;

› **mutualisé entre plusieurs entreprises.** En effet, le RGPD précise que *« Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement »*, étant précisé que la notion de groupe d'entreprises est définie comme suit : *« une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle*[25]*»* , c'est-à-dire un ensemble d'entreprises unies par des liens capitalistiques.

Si de nombreuses combinaisons stratégiques sont envisageables, il existe tout de même une contrainte : une même agence PR ne peut désigner qu'un seul DPO. Toutefois, celui-ci peut (doit) s'entourer des personnes et interlocuteurs en interne aptes à l'aider dans sa mission et à lui apporter le soutien nécessaire.

Pour en savoir plus, voir le paragraphe « Modalités de désignation du DPO et gouvernance interne » ci-après.

[25] Cf. article 4 du RGPD.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.1.3 Modalités de désignation du DPO et gouvernance interne

La désignation d'un DPO nécessite :

- la **mise à disposition de ce dernier par l'agence des ressources nécessaires** pour accomplir sa mission (ressources humaines, ressources budgétaires, ressources en temps de travail dédié à l'accomplissement de sa mission de DPO, ...) ;
- l'élaboration d'**une fiche de poste ou lettre de mission** comportant le descriptif des missions du DPO, une définition claire du rôle et des responsabilités du DPO, ainsi que des ressources mises à sa disposition.

La désignation d'un DPO se fait **en ligne sur le site internet de la Cnil.** A cet égard, un formulaire en ligne dédié est accessible sur le site internet de la Cnil à l'adresse url suivante : https://www.cnil.fr/fr/designation-dpo.

En cas de désignation multiple, lorsqu'il est fait le choix d'un DPO mutualisé au sein d'un groupe, un formulaire de désignation par entité doit en principe être complété. Toutefois, une procédure spécifique est proposée par la Cnil afin de faciliter une telle désignation multiple. Il convient pour en bénéficier de contacter la Cnil qui pourra fournir aux agences PR concernées les explications et documents adaptés à cette démarche (servicedpo@cnil.fr).

Par ailleurs, la désignation du DPO doit s'inscrire dans une démarche de gouvernance interne, nécessitant a minima le déploiement des actions suivantes par ce dernier :

Création d'un « Comité DPO » (composé d'interlocuteurs de différentes directions disposant de compétences et de connaissances complémentaires sur les activités de traitement de données à caractère personnel) :

› **pilotage**

› **réponses aux questions en séance**

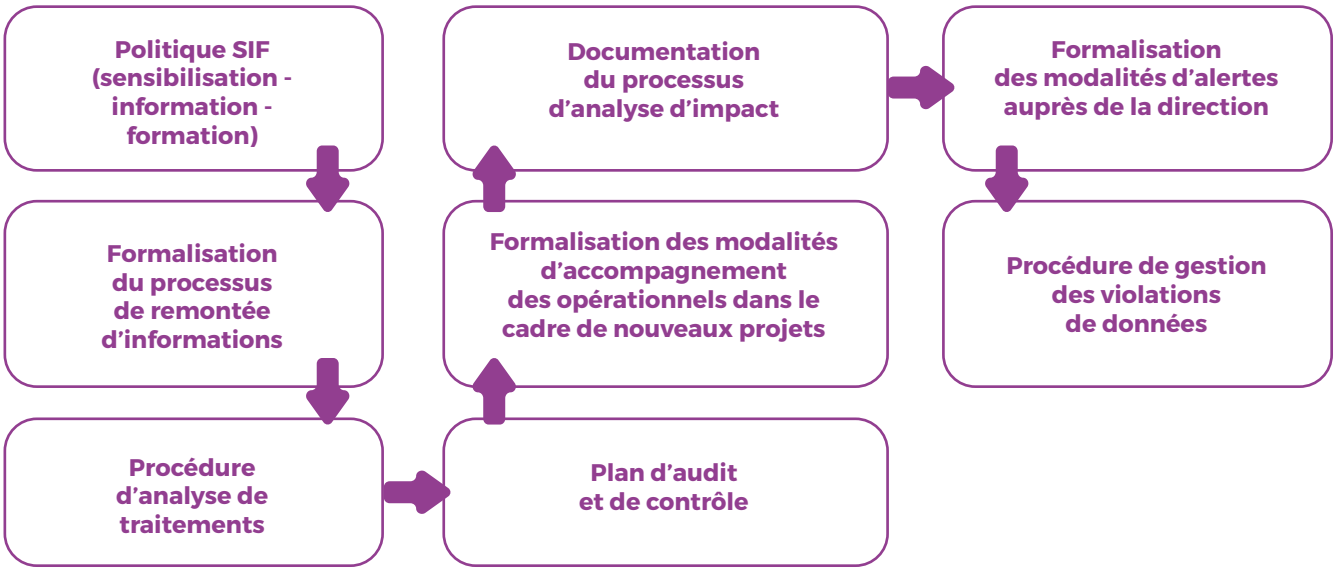
› **compte rendu**

Désignation de relais au sein des équipes :

› **remontée d'informations**

› **diffusion de la sensibilisation**

› **délégation de certaines tâches**



PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.2
RECENSER MES TRAITEMENTS ET RÉALISER MON(MES) REGISTRE(S) DES TRAITEMENTS

2.2.1 Obligation de tenue des registres

L'entrée en application du RGPD a fait disparaître l'obligation de réaliser des formalités préalables auprès de la Cnil dans la quasi-totalité des situations. La logique des formalités préalables laisse la place à celle de la responsabilisation des acteurs. Ainsi, en contrepartie de la suppression de certaines formalités, les responsables de traitement et sous-traitants doivent être en mesure de démontrer, à tout moment, leur conformité à la réglementation applicable en matière de protection des données à caractère personnel en traçant toutes les démarches entreprises (cf. principe d'« accountability »).

Dans le cadre de cette logique, chaque organisme se voit désormais imposer de tenir :

- **un registre de ses activités de traitement de données à caractère personnel effectuées en qualité de responsable de traitement ;**
- **un registre des catégories d'activités de traitement de données à caractère personnel effectuées en qualité de sous-traitant pour le compte de responsables de traitement[26].**

Ces registres ont vocation à recenser l'ensemble des traitements mis en œuvre par un organisme, en tant que responsable de traitement ou sous-traitant.

Les registres doivent être élaborés et tenus sous forme écrite, y compris sous forme électronique.

Des logiciels de registre des traitements ont été développés ; de même, il est possible de créer le(s) registre(s) dans un document Excel ou Word.

Ils doivent être **mis à jour régulièrement, au fur et à mesure de la mise en œuvre de nouveaux traitements ou de la modification de traitements existants.**

Les obligations en matière de tenue des registres des traitements peuvent ainsi se définir schématiquement comme suit :

La tenue des registres est, par principe, **obligatoire.**

Les registres doivent être **mis à jour régulièrement et être tenus sous forme écrite** (possible sous format électronique).

Les registres doivent être **mis à disposition de l'autorité de contrôle** en cas de demande de cette dernière.

[26] Cf. article 30 du RGPD.

2.2.2 Contenu des registres

Les informations devant être contenues dans les registres diffèrent en fonction qu'il s'agit du registre « version responsable de traitement » ou « version sous-traitant[27] » .

En pratique, chaque registre comporte le détail de **chaque traitement mis en œuvre sous forme de fiches. Pour chaque traitement, et donc pour chaque fiche, les informations obligatoires à faire figurer dans les registres sont les suivantes :**

REGISTRE « RESPONSABLE DE TRAITEMENT »	REGISTRE « SOUS-TRAITANT »
Identité et coordonnées du responsable de traitement et de son représentant et du délégué à la protection des données	Identité et coordonnées du sous-traitant et de son représentant, de chaque responsable de traitement et de leur représentant, et du délégué à la protection des données
Finalités du traitement	Catégories de traitements
Catégories de personnes concernées	
Catégories de données traitées	
Catégories de destinataires des données	
Existence de transferts de données hors Union européenne et référence aux garanties associées	
Durée de conservation des données	
Description générale des mesures de sécurité techniques et organisationnelles mises en œuvre	

FOCUS SUR LES REGISTRES DES TRAITEMENTS

A toutes fins utiles, la Cnil a publié son propre registre des traitements qu'elle met en œuvre en qualité de responsable de traitement.

La Cnil a également publié un modèle de registre des traitements à destination des responsables de traitement. Ce modèle peut bien entendu être décliné pour les activités mises en œuvre en tant que sous-traitant, en ne conservant que les éléments identifiés dans le tableau ci-dessus comme devant y figurer.

La Cnil recommande de tenir des registres distincts en fonction de la qualification de l'organisme[28]. Il convient toutefois de noter que le RGPD n'impose pas, en tant que tel, aux organismes agissant à la fois en tant que responsable de traitement (pour certains des traitements qu'ils mettent en œuvre) et en tant que sous-traitant (pour les autres traitements opérés), de tenir deux registres distincts (i.e. : un pour les traitements de données à caractère personnel mis en œuvre par l'organisme en tant que responsable de traitement et un autre pour les traitements opérés par l'organisme en tant que sous-traitant). Si l'organisme décide de n'établir qu'un seul registre des activités de traitement, celui-ci devra alors en tout état de cause clairement distinguer les deux catégories d'activités (cf. distinguer les traitements mis en œuvre en qualité de responsable de traitement de ceux mis en œuvre en qualité de sous-traitant).

[27] Cf. article 30 du RGPD. [28] «Voir la page de la Cnil : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.2.3 Elaboration des registres

L'élaboration des registres des traitements nécessite pour chaque agence de recenser les traitements de données à caractère personnel qu'elle met en œuvre.

Une telle démarche de recensement doit suivre le processus suivant :

- **ÉTAPE 1 : se faire communiquer et étudier les documents d'ores et déjà existants,** telles que les formalités (déclarations, autorisations, ...) antérieurement réalisées auprès de la Cnil ou encore les listes de traitements déjà établies (en cas de désignation antérieure d'un Correspondant à la protection des données ou Correspondant Informatique et libertés, ou « Cil »). Ces premiers éléments pourront servir d'indices pour identifier les traitements mis en œuvre au sein de l'agence ;
- **ÉTAPE 2 : élaborer un questionnaire** reprenant l'ensemble des éléments devant figurer dans les registres, un tel questionnaire ayant vocation à être complété par chaque direction / département / pôle / service, pour chacun des traitements de données à caractère personnel mis en œuvre au sein de l'agence ;

(MODÈLE / EXEMPLE DE QUESTIONNAIRE)

Questions à poser pour identifier un traitement mis en œuvre par le service concerné :

› quelles sont les finalités du traitement ?

› quels sont les outils / applications utilisés en vue de la réalisation de ce traitement ?

› quelles sont les données (sensibles ou non) collectées, traitées, utilisées dans le cadre de ce traitement ?

› des extractions ou requêtes dans les outils / applications utilisés peuvent-elles être réalisées ? dans quel objectif, pour quelles finalités ?

› existe-t-il des zones de commentaires libres (de type champs « commentaires », « observations », « remarques », « autres »,...) ?

› d'où les données traitées proviennent-elles ? comment sont-elles recueillies ?

› qui sont les personnes concernées, c'est-à-dire les personnes dont les données sont collectées et traitées dans le cadre du traitement ?

› quel est le fondement du traitement concerné (cf. suite à un contrat conclu avec la personne concernée, en vue de la conclusion d'un contrat avec cette dernière, du fait d'une obligation légale,...) ?

› qui sont les destinataires des données en interne (c'est-à-dire qui peut y avoir accès ou en avoir communication) ? des tiers peuvent-ils accéder à / recevoir communication de ces données ? quelle est la politique de gestion des habilitations à l'outil/l'application (en interne mais également depuis l'externe le cas échéant) ?

› quels sont les prestataires auxquels il est fait recours dans le cadre du traitement (par exemple, éditeur de l'outil/l'application ? prestataires informatiques ? autres ?) ? est-ce qu'un contrat a été conclu avec ces derniers ? est-ce que ce contrat fait références aux obligations respectives des parties en matière de protection des données à caractère personnel ? (+ demande de communication du contrat pour en vérifier les termes)

› les outils / applications utilisés sont-ils interconnectés avec d'autres outils ou applications ? si oui, lesquels ?

› pendant combien de temps les données traitées dans ce cadre sont-elles conservées ? où ? comment ?

› où les données sont-elles stockées, hébergées ?

› les données sont-elles transférées vers un Etat hors Union européenne ?

› quelles sont les mesures mises en œuvre pour assurer la sécurité et la confidentialité des données ?

› comment les personnes concernées sont-elles informées du traitement de leurs données (cf. moyens et supports d'information) ?

› existe-t-il un process ou une procédure spécifique pour répondre aux demandes d'exercice de leurs droits qui seraient adressées par les personnes concernées ?

› est-ce que le traitement doit faire l'objet d'une analyse d'impact relative à la protection des données (cf. passer en revue les critères sur la base desquels une telle analyse d'impact doit être réalisée tels que rappelés ci-dessous au paragraphe « Analyse d'impact relative à la protection des données en cas de risque élevé ») ?

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

- **ÉTAPE 3 : organiser avec chaque direction / département / pôle / service un entretien, sur la base du questionnaire précité,** en vue d'identifier avec ces derniers :
  - les traitements de données à caractère personnel mis en œuvre et leurs finalités respectives (à titre d'illustration, cf. finalité et sous finalités génériques proposées par la Cnil dans l'exemple de « fiche » intégrée à son modèle de registre de traitements et portant sur la gestion de la paie, ou encore le registre des traitements mis en œuvre par la Cnil, tels que visés au paragraphe « Contenu des registres ») ;
  - les outils utilisés (applications, fichiers, ...) ;
  - les caractéristiques détaillées de ces traitements, c'est-à-dire les éléments permettant de compléter les registres (cf. données collectées et traitées, durées de conservation des données, destinataires et personnes pouvant avoir accès aux données, en ce incluant les sous-traitants, existence de flux de données vers des Etats non membres de l'Union européenne, mesures techniques et organisationnelles mises en œuvre pour assurer la sécurité des données traitées, ...) ;
- **ÉTAPE 4 : identifier pour chaque traitement (cf. chaque finalité de traitement de données à caractère personnel) si l'agence agit en qualité de responsable de traitement ou de sous-traitant** puis élaborer une liste des traitements mis en œuvre en qualité de responsable de traitement, et une liste des traitements mis en œuvre en qualité de sous-traitant.

Une fois ce recensement effectué, il conviendra **d'alimenter les registres en reportant les informations recueillies dans le cadre du recensement dans le registre approprié.** Ainsi, chaque traitement recensé fera l'objet d'une description (cf. une « fiche ») associée dans le registre des traitements concerné.

Ces actions pourront être opportunément réalisées **par le DPO ou, à défaut, le référent** en matière de protection des données à caractère personnel **le cas échéant assisté par les différents relais** désignés au sein de l'agence, chacun pour ce qui les concerne, **mais également par ou en collaboration avec un tiers externe** disposant d'une expertise en droit et pratique de la protection des données à caractère personnel, missionné à cette fin.

Toutefois, l'élaboration et la tenue des registres des traitements relevant de la responsabilité du responsable de traitement ou du sous-traitant (chacun pour la « version » ou « partie » de registre qui le concerne), ces registres devront en tout état de cause être validés par ce dernier.

LE SAVIEZ-VOUS ?

Les registres des traitements doivent obligatoirement être mis à disposition de la Cnil en cas de demande de cette dernière.

Par ailleurs, les registres des traitements peuvent également faire l'objet :

- d'une demande de consultation initiée par un membre du personnel ;
- d'une demande de communication, par une personne concernée ou client, fournisseur, prospect, partenaire, ..., seulement pour la(les) fiche(s) qui le(la) concerne.

En tout état de cause, de telles demandes doivent être adressées ou communiquées au DPO ou, à défaut, au référent en matière de protection des données à caractère personnel, seul habilité à y répondre.

N.B : en cas de demande de communication du registre par une personne autre que la Cnil, il n'existe pas d'obligation de mise à disposition du(des) registre(s). En cas de demande émanant d'un cocontractant (client, fournisseur, ...), il conviendra alors de vérifier s'il est prévu contractuellement que l'agence PR doit ou non communiquer une copie de son(ses) registre(s) des traitements ou permettre à son cocontractant de le(s) consulter.

2.2.4 Mises à jour des registres

Une fois les registres des traitements élaborés dans leur version initiale, leur mise à jour est essentielle. En effet, **les registres doivent refléter les traitements réellement mis en œuvre au sein de l'agence.**

En pratique, une mise à jour du(des) registre(s) est nécessaire pour toute modification qui interviendrait s'agissant des traitements de données à caractère personnel mis en œuvre, à savoir :

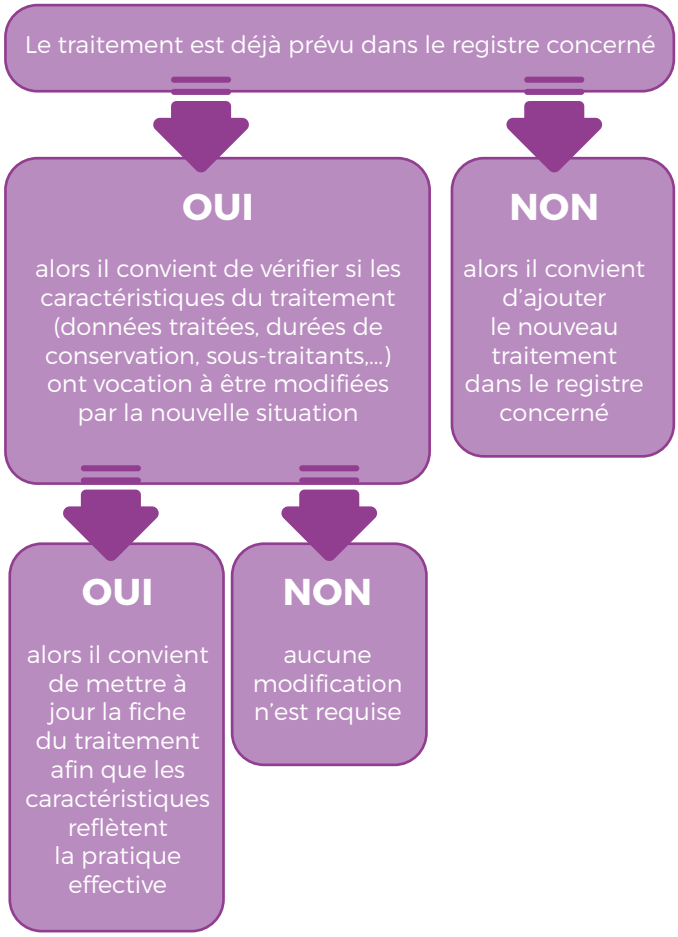
- les nouveaux traitements mis en œuvre ;
- les traitements supprimés ;
- les traitements dont les caractéristiques sont modifiées.

Ainsi, sont concernées, dès lors que des données à caractère personnel ont vocation à être traitées, les situations suivantes :

- tout recours à une nouvelle solution (par exemple, nouvel outil de routage d'emailings ou nouvelle plateforme de mise en relation avec des influenceurs) ;
- tout nouveau service proposé aux clients (par exemple, mise en place de sessions de formation dispensées par l'agence PR à l'attention de ses clients) ;
- tout recours à un nouveau sous-traitant en charge de prestations impliquant un traitement de données à caractère personnel (par exemple, recours à un nouveau prestataire informatique ou à un nouvel hébergeur) ;
- et plus généralement tout nouveau projet au sens large (par exemple, développement d'un nouvel outil impliquant le traitement de données à caractère personnel tel qu'un nouveau système de veille sur les réseaux sociaux) ; ou toute modification apportée dans le cadre des solutions utilisées par l'agence PR, des services qu'elle propose, ou encore des projets qu'elle déploie (par exemple, nouvelle catégorie de données collectées, modification des durées de conservation des données, nouvelle typologie de destinataires des données,...).

Aussi, **pour chaque situation identifiée ci-dessus, il convient de déterminer si ces situations impliquent le traitement de données à caractère personnel et de vérifier si ce traitement est déjà prévu dans le registre concerné** (ou dans la « partie » de registre concernée en cas de registre unique regroupant les activités de l'agence PR en qualité de responsable de traitement et de sous-traitant).

La démarche à suivre est ensuite la suivante :



Les registres devant être régulièrement mis à jour, il est indispensable de définir et de formaliser en interne un processus de remontée d'informations afin que le DPO, ou à défaut le référent en matière de protection des données à caractère personnel, soit informé sans délai des situations listées ci-dessus pouvant nécessiter à une mise à jour du(des) registre(s).

2.3
ANALYSER LA CONFORMITÉ DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Le recensement des traitements de données à caractère personnel permet de réaliser le(s) registre(s) des traitements (voir le paragraphe « Recenser mes traitements et réaliser mon(mes) registre(s) des traitements » ci-avant).

Toutefois, ce n'est pas parce que les traitements de données à caractère personnel ont été recensés et intégrés dans les registres qu'ils sont mis en œuvre conformément à la réglementation applicable en matière de protection des données à caractère personnel !!

Aussi, le fait de cartographier les traitements de données à caractère personnel mis en œuvre au sein de l'agence a également vocation à permettre à cette dernière d'identifier les traitements mis en œuvre et d'en connaître les caractéristiques pour en analyser la conformité au regard des principes applicables[29].

Cette analyse a vocation à effectuer les constatations appropriées quant au niveau de conformité des traitements de données à caractère personnel mis en œuvre, en particulier s'agissant des écarts de conformité, afin d'élaborer un plan d'actions à déployer en vue de remédier auxdits écarts et de s'assurer de la mise et du maintien en conformité de l'ensemble des traitements concernés.

FOCUS SUR LES PRINCIPES GÉNÉRAUX APPLICABLES EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La réglementation applicable en matière de protection des données à caractère personnel se décline en plusieurs grands principes qu'il appartient à chaque organisme qui met en œuvre des traitements de données à caractère personnel de respecter.

Ces principes peuvent être synthétisés de la manière suivante[30]:

› Légitimité/limitation des finalités poursuivies par un traitement de données à caractère personnel ;
› Licéité de la collecte et du traitement de données à caractère personnel ;
› Loyauté/transparence de la collecte et du traitement de données à caractère personnel ;
› Minimisation des données à caractère personnel collectées ;
› Exactitude/qualité des données à caractère personnel traitées ;
› Proportionnalité de la conservation des données à caractère personnel ;
› Limitation/justification des destinataires des données ;
› Encadrement des flux transfrontières de données ;
› Sécurité des données à caractère personnel ;
› Encadrement des relations avec les tiers (sous-traitants, responsables conjoints, destinataires, ...) ;
› Respect des droits des personnes concernées sur leurs données à caractère personnel.

Ces divers principes seront développés et explicités tout au long du présent guide.

A titre liminaire, il est rappelé qu'il convient de respecter ces principes pour tous les traitements de données à caractère personnel d'ores et déjà mis en œuvre mais également pour tous les projets menant à des traitements de telles données, depuis leur origine et leur conception, et de s'assurer de la conformité desdits traitements aux dispositions applicables en matière de protection des données à caractère personnel tout au long de leur cycle de vie et/ou du projet (cf. principe de « privacy by design »).

[29] Cf. article 5 du RGPD et article 4 de la Loi Informatique et libertés.
[30] Cf. article 5 du RGPD et article 4 de la Loi Informatique et libertés.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

LE SAVIEZ-VOUS ?

Pour mémoire, il est précisé que **le respect de l'ensemble des principes susvisés incombe par principe au responsable de traitement** (cf. tableau de synthèse des obligations, en fonction de la qualification de l'agence PR, proposé au paragraphe « Le RGPD : quoi et pour qui ? » ci-dessus).

Aussi, lorsque l'agence PR agit en qualité de responsable de traitement, il lui incombe de s'assurer de la conformité de ses traitements de données à caractère personnel.

En revanche, lorsque l'agence PR agit en qualité de sous-traitant, il appartient au responsable de traitement de s'assurer de la conformité de ses traitements de données à caractère personnel, et de communiquer l'ensemble de ses instructions à l'agence PR visant à permettre à cette dernière de mettre en œuvre le traitement concerné (à titre d'exemple, le responsable de traitement doit indiquer à l'agence PR les catégories de données qu'il convient de collecter / traiter, ou encore si l'agence PR est tenue de collecter les données à caractère personnel pour le compte du responsable de traitement, il appartient à ce dernier de communiquer l'ensemble des mentions d'information, voire de recueil du consentement, à l'attention des personnes concernées).

Néanmoins, **l'agence PR agissant en qualité de sous-traitant** pour le compte d'un responsable de traitement n'est pas exonérée de toute obligation en matière de protection des données à caractère personnel dans la mesure où elle **doit notamment alerter immédiatement ledit responsable de traitement dans l'hypothèse où une instruction de ce dernier constituerait, selon l'agence, une non-conformité au regard de la réglementation applicable en matière de protection des données à caractère personnel,** et notamment des principes susvisés dans le Focus ci-dessus.

2.3.1 Limitation et légitimité des finalités

Il convient de s'assurer que chaque traitement de données à caractère personnel mis en œuvre poursuit une finalité déterminée, explicite et légitime.

Cela signifie que l'agence ne doit collecter des données à caractère personnel que pour **des finalités/des objectifs clairement défini(e)s et légitimes, et qu'il n'est pas possible de réutiliser ces données pour des finalités ultérieures incompatibles** avec les finalités initiales (cf. risque de détournement de finalité).

(ILLUSTRATIONS)

A titre d'illustrations, les utilisations suivantes peuvent être considérées comme non compatibles avec la finalité initiale de la collecte des données : envoi d'une newsletter à un candidat à un emploi en l'absence de demande expresse de sa part, utilisation des images prises par une caméra de vidéosurveillance au sein de l'agence pour calculer le temps de travail effectif d'un salarié, revente par un collaborateur de données de contacts chez les clients de l'agence, ayant initialement vocation à être utilisées dans le cadre de l'exécution d'une prestation, à des fins de mise à jour de bases de données tierces de publipostage,...

Ainsi, ce principe :

› impose de s'assurer que chaque donnée à caractère personnel traitée au sein de l'agence est traitée pour la(les) finalité(s) pour laquelle(lesquelles) elle a été collectée ;

› interdit de réutiliser les données pour des finalités différentes de la finalité pour laquelle elles ont été collectées, et donc notamment de procéder à des extractions des applications utilisées au sein de l'agence dans le cadre de son activité professionnelle pour élaborer des tableaux, reportings,... (par exemple, tableurs Excel) pour des finalités différentes de celles identifiées initialement s'agissant de l'utilisation de l'application d'origine (c'est-à-dire des finalités différentes de celles dont les personnes concernées ont été informées).

2.3.2 Licéité du traitement et hypothèses de consentement obligatoire

Il convient de veiller à ce que les données soient collectées et traitées de manière licite, conformément aux dispositions applicables.

En pratique, il convient de s'assurer que chaque traitement de données à caractère personnel mis en œuvre est fondé sur **une justification prévue par la réglementation applicable en matière de protection des données à caractère personnel.**

A titre liminaire, il est rappelé qu'il est interdit de réaliser un traitement de données à caractère personnel à partir de données collectées de manière illicite.

En tout état de cause, pour chaque traitement de données à caractère personnel mis en œuvre, mais également avant la mise en œuvre d'un nouveau traitement de données à caractère personnel ou la modification d'un traitement existant, il convient de s'assurer, en coopération avec le DPO ou, à défaut, le référent en matière de protection des données à caractère personnel, que ledit traitement repose sur un fondement licite.

A cet égard, il est rappelé qu'un traitement ne peut être réalisé que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

- 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**[31]**;**
- le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable de traitement serait soumis ;
- le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique ;
- le traitement est nécessaire à **l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique** dont serait investie le responsable de traitement ;
- le traitement est nécessaire aux fins des **intérêts légitimes poursuivis par le responsable de traitement ou par un tiers,** à condition que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

L'existence d'un intérêt légitime doit faire l'objet d'une **évaluation attentive,** notamment afin de vérifier que les intérêts et droits fondamentaux de la personne concernée ne prévalent pas sur l'intérêt légitime du responsable de traitement à traiter ses données.

L'utilisation de ce fondement nécessite en tout état de cause de systématiquement procéder à une **balance des intérêts en présence,** au regard notamment des critères suivants :

- typologie et volume de données à caractère personnel traitées ;
- nombre de personnes concernées ;
- attentes raisonnables de la personne concernée ;
- incidences négatives (exclusion) ou positives (évolution) du traitement de données à caractère personnel pour la personne concernée ;
- existence d'un déséquilibre (ou non) dans les relations entre le responsable de traitement et la personne concernée (au regard du statut de la personne concernée) ;
- garanties offertes aux personnes concernées (transparence accrue, consultation des instances représentatives du personnel, pseudonymisation, anonymisation à bref délai si possible ...).

En pratique, plus le traitement présente des risques pour les personnes concernées (c'est-à-dire plus le traitement est attentatoire à la vie privée), plus les intérêts de ces personnes concernées risquent de prévaloir sur ceux du responsable de traitement, et donc plus il existe un risque que les intérêts légitimes du responsable de traitement ne puissent pas permettre de justifier le traitement des données à caractère personnel.

FOCUS SUR LA DÉTERMINATION DU FONDEMENT D'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Voir les chapitres « Le RGPD et le conseil en relations publics » et « Le RGPD et les ressources humaines » ci-après pour des illustrations concrètes par métier.

[31] Pour un approfondissement sur ce sujet, voir EDPB, Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées, 8 octobre 2019.

Pour les traitements qui ne peuvent pas être fondés sur une des hypothèses précitées, alors le consentement de la personne concernée devra être obtenu. Contrairement à une idée reçue, le consentement de la personne concernée n'a donc pas à être recueilli dans tous les cas mais uniquement dans des cas bien particuliers, en fonction de l'analyse spécifique du traitement envisagé.

Certaines opérations spécifiques nécessitent en tout état de cause le consentement des personnes concernées. A cet égard, il convient d'identifier les situations dans lesquelles le consentement des personnes concernées est requis.

- Les hypothèses de recueil du consentement

Ainsi que cela est précisé ci-dessus, un traitement de données à caractère personnel, pour être mis en œuvre, doit reposer sur un fondement juridique précis.

Parmi ces fondements juridiques, figurent les hypothèses dans lesquelles la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques. Aussi, **lorsqu'aucun autre fondement juridique ne peut être invoqué** (voir ci-dessus - ex : respect d'une obligation légale ou réglementaire, exécution d'un contrat, intérêts légitimes du responsable de traitement, ...), **alors le consentement de la personne concernée doit être recueilli.**

Par ailleurs, **dans certaines hypothèses, un traitement de données à caractère personnel qui serait par principe « interdit » peut être autorisé car fondé sur le consentement des personnes concernées.**

Il s'agit donc de circonstances bien différentes dans lesquelles le consentement de la personne devra être collecté. Dans certaines hypothèses, le consentement de la personne concernée devra être recueilli car il n'existe pas d'autre fondement juridique pour pouvoir traiter les données de cette personne. Dans d'autres hypothèses, le consentement explicite devra être recueilli pour, par exemple, pouvoir traiter des données dites « sensibles » de la personne concernée s'il n'est pas possible d'invoquer un autre fondement juridique pour y procéder ou encore pour transférer des données à caractère personnel en dehors de l'Union Européenne.

NB. Des conditions bien spécifiques sont prévues pour que le recueil de ce consentement soit valable (voir le paragraphe « Les modalités de recueil du consentement » ci-dessous).

- Le cas particulier de la prospection par courrier électronique, télécopie ou système automatisé de communications électroniques

(EXEMPLES)

Exemples d'hypothèses pour lequel le traitement peut être autorisé car fondé sur le consentement :

- **le traitement porte entre autres sur des données dites « sensibles »** (par exemple : données de santé, données révélant l'origine raciale ou ethnique des personnes, ou encore les opinions politiques ou religieuses, etc.). Le traitement de telles données étant par principe interdit, le recueil du consentement explicite des personnes concernées est un des fondements pouvant être invoqué pour autoriser le traitement de telles données ;
- **le traitement met en œuvre des flux transfrontières de données à caractère personnel,** c'est-à-dire des flux de données vers des Etats non membres de l'Union européenne. De tels flux étant par principe interdits, le recueil du consentement explicite des personnes concernées est un des fondements pouvant être invoqué pour autoriser de tels flux transfrontières de données, à condition toutefois qu'il ne s'agisse que de flux ponctuels et non de flux structurels et massifs, et que la personne concernée ait été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées encadrant ces flux transfrontières.

Pour mémoire, la définition juridique de la prospection est très large puisque constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services[32] ou l'image d'une personne vendant des biens ou fournissant des services . Les appels et messages ayant pour objet d'inciter une personne à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent également de la prospection directe.

(EXEMPLES)

Une newsletter ou la prise de contact avec un journaliste pour diffusion d'un communiqué est une prospection directe au sens de la réglementation applicable.

[32] Cf. article L.34-5, alinéa 3 du Code des postes et des communications électroniques.

Si par principe la prospection par courrier postal ou par télémarketing n'est pas soumise au consentement préalable du destinataire des sollicitations, en revanche un tel consentement est requis pour les traitements de données à caractère personnel **ayant pour finalité la prospection directe par courrier électronique, télécopie ou système automatisé de communications électroniques (ex : automate d'appels)[33].**

LE SAVIEZ-VOUS ?

Au sens de cette réglementation, **la notion de courrier électronique regroupe les emails mais également les sms, mms, pushs ou notification adressées par l'intermédiaire d'applications ou d'une technologie bluetooth,...**

Il existe toutefois **deux exceptions pour lesquelles le recueil du consentement préalable pour adresser des courriers électroniques de prospection n'est pas requis[34]:**

EXCEPTION 1 (exception dite des « produits et services analogues »[35]) - la prospection directe du consentement par courrier électronique est autorisée, sans recueil préalable de consentement, lorsque les conditions suivantes sont cumulativement réunies :

- les coordonnées de la personne concernée ont été recueillies directement auprès d'elle, à l'occasion d'une vente ou d'une prestation de services ;
- la prospection directe concerne des produits ou services analogues fournis par la même personne physique ou morale que celle à l'origine de la collecte des données ;
- le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, et de manière simple, à l'utilisation de ses coordonnées lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.

[33] Cf. article L.34-5, alinéa 1 du Code des postes et des communications électroniques.
[34] Voir la page de la Cnil, la prospection commerciale par courrier électronique, 28 décembre 2018.
[35] Cf. article L.34-5, alinéa 4 du Code des postes et des communications électroniques.

EXCEPTION 2 (exception dite « B to B ») – la Cnil a élaboré une exception doctrinale aux termes de laquelle la prospection directe du consentement par courrier électronique entre professionnels (B to B) est autorisée, sans recueil préalable de consentement, à condition que la sollicitation soit adressée sur une adresse de courrier électronique professionnelle et que l'objet de la sollicitation soit en rapport avec la profession de la personne sollicitée (par exemple : message présentant les mérites d'un logiciel à l'attention de paul.toto@nomdelasociété.fr, directeur informatique ou encore message présentant un nouveau catalogue de formation à l'attention de pierre.toto@nomdelasociete.com, responsable de la formation).

(EXEMPLES)

Exemples de traitements mis en œuvre à des fins de prospection par courrier électronique entre professionnels (cf. exception 2 ci-contre) appliqués à l'activité des agences PR : envoi par un email d'un communiqué de presse concernant une certaine thématique (l'environnement par exemple) à un journaliste ayant pour habitude d'écrire sur cette thématique si cet envoi est réalisé vers son adresse email utilisée notamment à des fins professionnelles (il n'est pas rare que les journalistes utilisent une adresse email tant à des fins professionnelles qu'à des fins personnelles), contact par email de la directrice de la communication d'une société pour l'inviter à un évènement ou une conférence de presse ou encore dans le cadre de la mise en œuvre d'une stratégie presse ou médias si cet envoi est réalisé vers son adresse email professionnelle,...

Pour en savoir plus, il est renvoyé aux « Bonnes pratiques en matière de collectes des données » présentées ci-après au chapitre 3.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

En dehors de ces hypothèses qui doivent être interprétées strictement, tout traitement de données à caractère personnel ayant pour finalité la prospection directe par courrier électronique (email, sms, mms, bluetooth, ...), télécopie ou système automatisé de communications électroniques **doit impérativement reposer sur le consentement des personnes concernées.**

En pratique, il convient de vérifier si la collecte et le traitement des données à caractère personnel mis en œuvre par l'agence PR nécessitent le consentement des personnes concernées conformément à la réglementation applicable en matière de protection des données à caractère personnel et, dans l'affirmative, de s'assurer que le consentement a été recueilli ou, à défaut, de procéder au recueil dudit consentement, étant rappelé que (i) le recueil de ce consentement incombe à l'agence PR lorsqu'elle agit en qualité de responsable de traitement et que (ii) lorsqu'elle agit en qualité de sous-traitant, il lui incombe tout de même d'alerter immédiatement le responsable de traitement pour le compte duquel elle intervient en vue du recueil de ce consentement.

- Les modalités de recueil du consentement

L'expression « consentement de la personne concernée » désigne toute manifestation de volonté, libre, spécifique, éclairée et univoque 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[36].

En conséquence :

- le consentement ne peut pas être recueilli de manière tacite ou implicite. A titre d'exemple, il ne saurait y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité de la personne concernée ;
- le consentement doit être recueilli de manière distincte d'autres déclarations ou acceptations (le recueil du consentement à un traitement de données à caractère personnel, lorsqu'il est requis, ne peut être recueilli au moyen de l'acceptation de conditions générales par exemple) ;
- lorsque le traitement poursuit plusieurs finalités soumises au consentement, alors le consentement de la personne concernée doit être donné pour chacune de ces finalités ;
- la personne concernée doit avoir reçu une information claire et complète sur le traitement envisagé (voir le paragraphe « Loyauté et transparence du traitement » ci-après) ;
- la personne concernée doit disposer d'une liberté de choix et pouvoir refuser de donner son consentement ;
- la personne concernée doit avoir le droit de retirer librement et à tout moment son consentement. Il convient de s'assurer qu'elle a été dûment informée de l'existence du droit de retirer son consentement à tout moment.

En tout état de cause, il convient, lorsque le consentement est requis, de **se prémunir la preuve du recueil de ce consentement.**

En outre, bien qu'aucun formalisme ne soit imposé en la matière, il est rappelé que le consentement doit être donné par un acte positif clair ; un consentement tacite ou implicite ne serait pas considéré comme valable.

Aussi, il est recommandé de recueillir le consentement, lorsqu'il est requis, par écrit, y compris par voie électronique (online ou par échange d'emails).

De manière synthétique, **pour tout traitement de données à caractère personnel, qu'il s'agisse d'un traitement existant ou encore d'un nouveau traitement ayant vocation à être mis en œuvre, il convient de procéder de la manière suivante pour déterminer si le consentement des personnes concernées est requis** et, dans l'affirmative, les modalités devant accompagner son recueil :

ÉTAPE 1	**Déterminer si le consentement des personnes concernées est requis,** le recours au consentement des personnes concernées ne devant pas être privilégié s'il existe d'autres fondements légitimant le traitement
ÉTAPE 2	**Identifier de manière exhaustive les sources / modalités de collecte** des données
ÉTAPE 3	**Déterminer selon quelles modalités et sur quels supports** le consentement pourra être recueilli, quelles que soient les sources / modalités de collecte des données
ÉTAPE 4	**Formaliser une mention + case à cocher (ou tout autre processus valable)** pour recueillir le consentement de la personne concernée
ÉTAPE 5	**Anticiper les conséquences effectives d'un refus ou d'un retrait** de consentement et s'assurer qu'il pourra en être effectivement tenu compte
ÉTAPE 6	**Déterminer les modalités de conservation de la preuve** du recueil du consentement

[36] Pour en savoir plus sur la validité du consentement : cf. EDPB, Lignes directrices 05/2020 sur le consentement, 4 mai 2020

LE SAVIEZ-VOUS ?

Certains articles du RGPD imposent le recueil d'un **consentement « explicite » des personnes concernées,** dans des situations où un risque sérieux lié à la protection des données survient, et où un niveau élevé de contrôle sur les données à caractère personnel par la personne concernée est de ce fait approprié (ce qui est le cas par exemple dans les hypothèses où le consentement est nécessaire (i) pour le traitement de données dites « sensibles » ou encore (ii) pour la mise en œuvre de flux transfrontières de données à caractère personnel).

Dans une telle hypothèse, il convient alors de porter une attention particulière à la manière de recueillir le consentement des personnes concernées dans la mesure où un consentement « explicite », **pour être valablement recueilli, doit répondre à un niveau d'exigence supérieur** (ex : formulation d'une déclaration de consentement exprès, par exemple au moyen d'une déclaration écrite confirmant expressément le consentement ou encore vérification du consentement « en deux étapes »[37]).

2.3.3 Loyauté et transparence

Il convient d'informer les personnes concernées s'agissant du traitement de leurs données à caractère personnel et des caractéristiques de ce traitement.

2.3.3.1 Obligation d'information des personnes concernées

Les principes de transparence et de loyauté du traitement de données à caractère personnel se traduisent par une **obligation d'information des personnes concernées, cette information devant être délivrée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.**

En pratique, il convient de vérifier que les personnes concernées sont informées de la collecte et du traitement de leurs données conformément à la réglementation applicable en matière de protection des données à caractère personnel ou, à défaut, de procéder à leur information (sauf s'il est possible de se fonder, le cas échéant, sur l'une des exceptions à l'obligation d'information prévues par le RGPD et détaillées au paragraphe « Informations générales à fournir » ci-dessous), étant rappelé que (i) l'information des personnes concernées incombe à l'agence PR lorsqu'elle agit en qualité de responsable de traitement et que (ii) lorsqu'elle agit en qualité de sous-traitant, il lui incombe tout de même d'alerter immédiatement le responsable de traitement pour le compte duquel elle intervient en vue de cette information des personnes concernées.

Lorsque l'agence PR se procure des données à caractère personnel auprès de tiers, et sous la même réserve que ce qui précède concernant le rôle qui lui est imparti en fonction de sa qualité de responsable de traitement ou de sous-traitant, il convient de s'assurer au préalable que ces tiers :

- disposent des droits nécessaires à la collecte et à la communication à l'agence PR de telles données ;
- garantissent que les personnes concernées en ont été informées, voire que leur consentement a le cas échéant été obtenu lorsqu'un tel consentement est requis pour le traitement de données à caractère personnel ayant vocation à être mis en œuvre.

Toutefois, même dans l'hypothèse du recueil de données à caractère personnel par l'intermédiaire de tiers, une information doit en principe être fournie aux personnes concernées une fois que les données sont « récupérées » par l'agence PR (sauf s'il est possible de se fonder sur l'une des exceptions à l'obligation d'information prévues par le RGPD et détaillées au paragraphe « Informations générales à fournir » ci-dessous).

[37] Pour en savoir plus : cf. EDPB, Lignes directrices 05/2020 sur le consentement, 4 mai 2020

2.3.3.2 Informations générales à fournir

Le tableau ci-après a vocation à présenter les informations devant être fournies aux personnes concernées, en distinguant selon qu'il s'agit :

- **d'une collecte directe** (les données sont obtenues directement auprès de la personne concernée, telle que par la complétion d'un formulaire, par exemple sur papier ou sur le site internet de l'agence PR ou lors d'un échange avec la personne concernée) ; ou
- **d'une collecte indirecte** (les données de la personne concernée sont obtenues auprès d'un tiers, dans le cadre d'un achat de fichiers clients par exemple ou dans le cadre d'opérations de recrutement via des sites internet tiers spécialisés).

COLLECTE DIRECTE	COLLECTE INDIRECTE
L'identité et les coordonnées du responsable de traitement et, le cas échéant, de son représentant.	
Les coordonnées du délégué à la protection des données	
Les finalités du traitement ainsi que le fondement juridique du traitement	
N/A	Les catégories de données à caractère personnel concernées
Le cas échéant, les intérêts légitimes poursuivis par le responsable de traitement ou par un tiers	
Les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent	
Le cas échéant, le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays situé en dehors de l'Union Européenne ou à une organisation internationale + l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne ou la référence aux garanties appropriées ou adaptées encadrant ces flux de données et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition	
La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	
L'existence du droit d'interrogation, du droit d'accès, du droit à la rectification, du droit d'opposition, du droit à l'effacement, de limitation, du droit à la portabilité des données et du droit de définir des directives post-mortem	
Lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment	
Le droit d'introduire une réclamation auprès d'une autorité de contrôle	
N/A	La source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public
Le caractère obligatoire ou facultatif des réponses, ainsi que les conséquences d'un défaut de réponse. Des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données.	Le caractère obligatoire ou facultatif des réponses / des données, ainsi que les conséquences d'un défaut de réponse.
L'existence d'une prise de décision automatisée, y compris un profilage + des informations utiles concernant la logique sous-jacente de cette prise de décision + les conséquences possibles de ce traitement pour la personne concernée	
Le cas échéant, l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées.	

Cette information doit être fournie aux personnes concernées de manière concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples[38].

FOCUS : QUAND FAUT-IL INFORMER LES PERSONNES CONCERNÉES ?

Les informations obligatoires doivent être fournies :

- **dans le cas d'une collecte directe**, au moment où les données sont obtenues ;

- **dans le cas d'une collecte indirecte :**
› dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas 1 mois ;
› si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ;
› s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Attention, en cas de modification affectant les caractéristiques du traitement mis en œuvre (par exemple, modification affectant les modalités d'hébergement d'un outil / d'une application utilisé(e) et impliquant un nouveau transfert de données en dehors de l'Union européenne, nouveaux destinataires des données,...), une nouvelle information complète doit être portée à la connaissance des personnes concernées selon les modalités prévues ci-dessus.

Par exception à ce qui précède, l'obligation d'information n'est pas requise dans les situations suivantes :

COLLECTE DIRECTE	COLLECTE INDIRECTE
- la personne concernée dispose déjà de ces informations.	- la personne concernée dispose déjà de ces informations ; - la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés (en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties imposées pour ce type de traitement), ou dans la mesure où l'obligation d'information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement (en pareils cas, l'agence PR doit en tout état de cause prendre des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées, y compris en rendant les informations publiquement disponibles par exemple) ; - l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel l'agence PR est soumise et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ; - les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

[38] Pour en savoir plus, voir la page dédiée sur le site internet de la Cnil « Conformité RGPD : comment informer les personnes et assurer la transparence ? » et G29, Lignes directrices sur la transparence, 11 avril 2018 (WP.260 rev.01)

Les exceptions à l'obligation d'information présentées ci-dessus sont toutefois résiduelles et doivent être interprétées de manière stricte. A titre d'illustration, **dès lors que le responsable de traitement dispose des coordonnées des personnes concernées** (postales, téléphoniques, électroniques,...) **ou d'un moyen de les contacter, il pourrait être considéré que l'information desdites personnes concernées ne peut pas être qualifiée d'impossible[39].**

Aussi, **ces exceptions permettant de ne pas informer les personnes concernées ne doivent être utilisées qu'avec beaucoup de prudence** et dans des cas ou circonstances exceptionnel(le)s correspondant strictement aux hypothèses visées par les textes.

(EXEMPLES)

Exemple : une agence PR (ou son client lorsque l'agence agit en tant que sous-traitant) pourrait éventuellement justifier le fait de ne pas informer individuellement les personnes concernées (à supposer que leurs coordonnées soient connues), dont elle(il) collecterait les données au moyen de différentes sources publiques (données rendues publiques par les personnes concernées sur différents sites par exemple) dans le cadre de l'élaboration de fichiers de « parties prenantes » sur un thème donné (par exemple : avis de professionnels d'un secteur particulier sur un produit alimentaire), lorsque le nombre de personnes concernées est très élevé et que leur information engendrerait un coût excessif pour l'agence ou son client le cas échéant (du fait du grand nombre de personnes concernées notamment et/ou de la multiplicité des sources sur lesquelles ces données publiques ont été collectées), constituant par là des efforts qui seraient considérés comme disproportionnés. Néanmoins, pour chaque hypothèse dans laquelle il serait envisagé de bénéficier de cette exception à l'obligation d'information, la mise en balance entre d'une part les efforts qui seraient nécessaires pour informer les personnes concernées et d'autre part l'incidence et les effets sur celles-ci d'une absence d'information individuelle doit être documentée par le responsable de traitement et le recours à cette exception strictement justifié. En outre, dans une telle hypothèse, le responsable de traitement doit tout de même prendre des mesures appropriées pour protéger les droits, les libertés et les intérêts légitimes des personnes concernées, a minima en rendant accessible au public une information générale relative au traitement concerné, notamment sur le site internet de l'agence PR ou de son client, voire sur d'autres supports opportuns et/ou appropriés le cas échéant, qu'il convient de déterminer au cas par cas. En tout état de cause, toute décision relative à l'application d'une exception à l'obligation d'information au traitement d'une agence PR ou d'un client doit être soumise à l'appréciation du DPO ou, à défaut, du référent en matière de protection des données à caractère personnel du responsable de traitement.

[39] Pour en savoir plus, voir G29, Lignes directrices sur la transparence, 11 avril 2018 (WP260 rev.01)

2.3.3.3 Modalités d'information des personnes concernées

De manière synthétique, pour tout traitement de données à caractère personnel, qu'il s'agisse (i) d'un traitement existant pour lequel il existe un doute quant à l'existence ou la validité d'une information des personnes concernées, ou encore (ii) d'un nouveau traitement ayant vocation à être mis en œuvre, le respect des obligations en matière de fourniture d'informations à l'attention des personnes concernées suppose la réalisation des actions identifiées dans le cadre des étapes suivantes :

ÉTAPE 1 — **Identifier de manière exhaustive les sources / modalités de collecte** des données (directe / indirecte, supports / absence de support,...)

ÉTAPE 2 — **Déterminer selon quelles modalités et sur quels supports** la mention d'information pourrait être insérée, et ce pour toutes les sources / modalités de collecte (sauf si l'agence PR peut valablement se fonder sur l'une des exceptions à l'obligation d'information, et ce sous les réserves / précautions précitées)

ÉTAPE 3 — **Formaliser une mention d'information** pour chacune des hypothèses précitées

ÉTAPE 4 — **Déterminer les modalités de conservation de la preuve** de la communication de l'information

FOCUS SUR L'INFORMATION DES PERSONNES CONCERNÉES DANS LE CADRE DES ACTIVITÉS DE CONSEIL EN RELATIONS PUBLICS ET EN MATIÈRE DE RESSOURCES HUMAINES

Voir les chapitres « Le RGPD et le conseil en relations publics » et « Le RGPD et les ressources humaines » ci-après pour des illustrations concrètes par métier.

2.3.4 Minimisation des données

Il convient de s'assurer que les données à caractère personnel collectées et traitées ne sont pas excessives.

Seules peuvent être collectées et traitées les données à caractère personnel **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies** pour un traitement. La collecte de données non strictement indispensables à la finalité du traitement doit rester facultative pour la personne concernée, étant précisé que toute collecte de données sans rapport avec la finalité du traitement est strictement interdite.

Pour s'assurer du respect de ce principe de minimisation des données, les bonnes pratiques suivantes doivent être encouragées :

- s'abstenir de collecter des données à caractère personnel « qui pourraient s'avérer utiles » / « au cas où » / « parce qu'on ne sait jamais » / ... mais qui en définitive ne sont pas indispensables ;
- éviter de collecter des données autres que celles provenant des questionnaires de collecte de l'agence PR ou autres que celles strictement nécessaires telles que prédéfinies dans le cadre des processus de l'agence PR (à titre d'exemple, en cas d'achat de fichiers, ne traiter -et donc ne conserver- que les données nécessaires au regard de la finalité poursuivie telles que définies par l'agence en fonction de ses besoins ou, pour une autre illustration, ne collecter parmi les données à caractère personnel publiquement disponibles que les données nécessaires telles que définies par l'agence en fonction de ses besoins) ;
- pour toute création d'un nouveau support de collecte de données à caractère personnel, identifier sur celui-ci (par exemple au moyen de l'insertion d'un astérisque accompagné d'une légende qui permette de distinguer clairement les champs obligatoires et champs facultatifs), les champs à remplir obligatoirement pour que la finalité principale du traitement soit atteinte, afin de les distinguer de ceux qui sont facultatifs (c'est-à-dire de ceux qui sont nécessaires uniquement pour des finalités secondaires).

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

ATTENTION : ces principes s'appliquent quelles que soient les modalités de collecte, de saisie et de traitement des données dans les applications, fichiers, etc. utilisés. **Les « champs de commentaires libres » ou « zones de saisie libre »** (de type champs « commentaires », « observations », « remarques », « autres », ...) **doivent notamment être utilisés avec prudence** (minimisation et proportionnalité des données, objectivité, ...).

Par ailleurs, certaines données particulièrement sensibles ne doivent pas être collectées. En effet, **sont par principe interdits la collecte et le traitement des données suivantes :**

- **les données dites « particulières » ou « sensibles »,** à savoir les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée, les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne concernée[40].
- **les informations relatives à des infractions, condamnations ou mesures de sûreté associées.**

Il existe des exceptions à ces interdictions. A titre d'exemple, les données dites « particulières » ou « sensibles » peuvent être traitées si elles sont nécessaires à la finalité poursuivie par le traitement dans les hypothèses suivantes :

- consentement explicite de la personne concernée ;
- données manifestement rendues publiques par la personne concernée.

Toutefois, ces exceptions doivent être interprétées de manière stricte.

(EXEMPLES)

Exemples de données pouvant être qualifiées de données « particulières » ou « sensibles » : données relatives à l'existence d'une maladie, d'un handicap, ... (même sans que le détail de la maladie ou du handicap soit mentionné), appartenance à ou sympathisant d'un parti politique, régime alimentaire,...

(EXEMPLE)

Exemple : information sur une condamnation pénale.

FOCUS SUR LA MINIMISATION DES DONNÉES ET LA COLLECTE DE DONNÉES DITES « PARTICULIÈRES » DANS LE CADRE DES ACTIVITÉS DE CONSEIL EN RELATIONS PUBLICS

Voir le chapitre « Le RGPD et le conseil en relations publics » ci-après pour des illustrations concrètes propres au métier de relations publics.

[40] Cf. article 9 du RGPD.

2.3.5 Exactitude et qualité des données

Il convient de s'assurer que les fichiers et bases de données utilisés par l'agence PR sont tenus à jour.

En effet, il convient de s'assurer que les données traitées dans les fichiers et bases de données adossées aux applications et outils utilisés au sein de l'agence sont exactes et tenues à jour : toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes ou périmées par exemple, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

(EXEMPLES)

Exemples : changement de fonctions d'un journaliste, changement d'adresse de courrier électronique d'un influenceur,...

Pour ce faire, il convient que **chaque membre du personnel de l'agence s'engage à mettre à jour régulièrement les données à caractère personnel qu'il est amené à collecter et à traiter** dans le cadre de son activité.

De même, lorsque les données sont collectées auprès de tiers, **il convient d'encadrer contractuellement les relations avec ces tiers afin que ces derniers garantissent la mise à jour des données en temps réel.**

(EXEMPLES)

Exemples : prise en compte effective et sans délai des demandes de rectification ou d'effacement, mise en place de processus permettant d'effectuer une revue régulière des données afin de déterminer si elles sont encore pertinentes ou au contraire devenues obsolètes, etc.

2.3.6 Proportionnalité de la conservation des données à caractère personnel

Il convient de définir la durée pendant laquelle l'agence a besoin de conserver les données, traitement par traitement, au regard de la finalité de chacun de ces traitements.

Les données à caractère personnel ne doivent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

La conservation illimitée des données à caractère personnel n'est pas autorisée.

Il convient donc de s'assurer (i) que des durées de conservation maximum sont définies pour chaque traitement de données à caractère personnel, (ii) que ces durées sont strictement proportionnées par rapport aux finalités poursuivies par le traitement et (iii) que ces durées sont respectées.

Pour mémoire, la Cnil distingue deux phases dans le cycle de conservation des données à caractère personnel, à savoir[41] :

CONSERVATION EN BASE ACTIVE

Il s'agit de la durée d'utilisation courante des données (cf. durée nécessaire au regard de la finalité poursuivie par le traitement)

CONSERVATION EN ARCHIVES

Il peut être justifié que des données soient conservées pour des durées plus longues sous forme d'archives, si obligation légale de conservation pendant une durée déterminée ou intérêt administratif (par exemple, en vue d'un éventuel contentieux, conservation pendant la durée des délais de prescription / forclusion). Attention, les données ne peuvent donc pas continuer à être utilisées par les opérationnels (cf. accès restreint et utilisation limitée aux finalités précitées)

[41] Pour en savoir plus, voir la page de la Cnil relative à la conservation des données ainsi que sa délibération n°2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

EXEMPLES DE DURÉES DE CONSERVATION ISSUES DES RECOMMANDATIONS DE LA CNIL[42]:

Gestion et suivi des opérations de recrutement [43]

› base active : deux ans maximum après le dernier contact avec la personne concernée
› archives le cas échéant : délais de prescription et durées obligatoires de conservation

A titre d'illustration, pour ce qui concerne les candidatures reçues par email par les collaborateurs d'une agence PR, il pourrait être envisagé de les classer dans un dossier commun dédié et de les archiver une fois le recrutement réalisé pour un poste donné (et en tout état de cause dans un délai de deux ans maximum après réception des candidatures). Ces candidatures pourront alors ensuite être conservées sous forme d'archives par exemple pendant six ans (cf. délai couvrant les délais de prescription pouvant trouver à s'appliquer en droit du travail en matière de recrutement et correspondant au délai de prescription de droit commun de l'action publique pour les délits en droit pénal, par exemple le délit de discrimination).

Gestion administrative du personnel[44]

› base active : les informations relatives à un salarié figurant dans le registre unique du personnel peuvent être conservés pendant la durée pendant laquelle le salarié fait partie des effectifs
› archives : cinq ans à compter du départ du salarié de l'organisme

S'agissant des données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à crédit d'heures de délégation (ex: exercice d'un mandat électif ou représentatif syndical) :

› base active : le temps de la période de sujétion de l'employé concerné
› archives : pendant six ans (cf. prescription pénale en matière de délits)

Gestion de la paie[45] :

› base active : les bulletins de salaires peuvent être conservés pendant un mois
› archives : cinq ans par principe et cinquante ans en version dématérialisée

Pour plus d'exemples s'agissant des durées de conservation des données à caractère personnel des salariés, voir le référentiel de la Cnil

Gestion de la relation clients/ prospects[46]

› base active : durée strictement nécessaire à la gestion de la relation commerciale + trois ans maximum pour une finalité de prospection / sollicitation commerciale à compter de la fin de la relation commerciale ou du dernier contact émanant du client / prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un email ; en revanche, l'ouverture d'un email ne peut être considérée comme un contact émanant du prospect)
› archives le cas échéant : délais de prescription et durées obligatoires de conservation

Gestion de la relation avec les fournisseurs[47]

› base active : durée de la relation avec le fournisseur
› archives le cas échéant : délais de prescription et durées obligatoires de conservation

Gestion et suivi des précontentieux et contentieux[48]:

› suppression des données traitées pour gérer un précontentieux dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante
› suppression des données traitées pour gérer un contentieux lorsque les recours ne sont plus possibles contre la décision rendue pour la faire exécuter

En tout état de cause, la durée de conservation des données doit être limitée au strict minimum. **Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais doivent notamment être fixés pour leur effacement ou leur examen périodique.** Des aménagements peuvent être prévus pour certaines données ou pour certaines finalités. D'un point de vue pragmatique, une véritable politique de conservation, d'archivage et de purge des données doit être formalisée.

[42] Les normes simplifiées adoptées par la Cnil n'ont plus de valeur depuis le 25 mai 2018 mais donnent un aperçu de la doctrine de la Cnil en la matière. En effet, dans l'attente de la production de référentiels, la Cnil indique sur son site internet qu'elle a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité. A toutes fins utiles, certains référentiels sont à ce jour en projet (cf. projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales ou encore projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestions des impayés).
[43] Cnil. Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.
[44] Cnil. référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel. 21 novembre 2019.
[45] Cnil. référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel. 21 novembre 2019.
[46] Cnil. Délibération n° 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects. NS-048.
[47] Cnil. Délibération n°2005-005 du 18/01/2005 décidant de la dispense de déclaration des traitements relatifs à la gestion des fichiers de fournisseurs comportant des personnes physiques. DI-004.
[48] Cnil. Délibération n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues. AU-046.

2.3.7 Justification des destinataires

Il convient de s'assurer que les données à caractère personnel traitées ne sont accessibles qu'aux personnes dont les fonctions / missions justifient l'accès à ces données.

Ainsi, des niveaux d'habilitation différenciés doivent être mis en place en fonction des besoins et devraient opportunément être formalisés dans une politique de gestion des habilitations.

De manière générale, **il convient de vérifier que les collaborateurs de l'agence PR n'ont accès qu'aux données strictement nécessaires à l'exercice de leurs activités et fonctions (s'agissant des répertoires réseau par exemple) et que les droits d'accès octroyés aux prestataires sont strictement** justifiés par leur activité de sous-traitance des données à caractère personnel intégrées dans les outils et applications concernés. A défaut, il convient de déployer ou faire déployer les mesures techniques et organisationnelles à cette fin.

En tout état de cause, il convient de **s'assurer que tout destinataire des données et que toute personne pouvant avoir accès aux données peuvent être justifiés !**

(EXEMPLES)

S'assurer que les candidatures à un emploi proposé au sein de l'agence PR ne sont traitées que par cette dernière et qu'elles ne sont pas transmises à d'autres agences PR, s'assurer que les outils de reportings / requêtes / extractions ne permettent pas de passer outre / de contourner les habilitations éventuellement définies dans le cadre de l'accès aux données via les applications métiers, formaliser et déployer des processus de revue des habilitations des membres du personnel,...

2.3.8 Encadrement des flux transfrontières de données

Il convient de maîtriser les flux de données à caractère personnel lorsque ces dernières « sortent » de l'Union européenne.

Il existe un flux transfrontière de données lorsque des données sont transférées depuis un Etat membre de l'Union européenne vers un Etat non membre de l'Union européenne. Un tel transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex : d'un disque dur d'ordinateur à un serveur).

Les transferts de données à caractère personnel à destination de pays hors Union européenne ou d'organisations internationales, ou flux transfrontières de données, doivent être identifiés dans la mesure où ils sont par principe interdits.

De tels transferts sont toutefois autorisés si le pays ou l'entreprise destinataire assure un niveau de protection suffisant aux données transférées. En effet, il importe que lorsque des données font l'objet de tels transferts, le niveau de protection des données des personnes physiques ne soit pas compromis.

(EXEMPLES)

Communication de données à caractère personnel à une personne hors Union européenne ; hébergement d'un outil / d'une application informatique métier, et donc des données à caractère personnel qui y sont contenues, dans un pays situé hors Union européenne ; accès par des personnes hors Union européenne à des données stockées sur des serveurs en Union européenne.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

En premier lieu, un tel transfert de données à caractère personnel peut avoir lieu si le pays tiers ou l'organisation internationale a été reconnu(e) par la Commission européenne comme assurant un **niveau adéquat de protection** des données. Dans cette hypothèse, aucune autorisation n'est nécessaire pour mettre en œuvre le transfert.

A ce jour, les pays reconnus par une décision d'adéquation comme offrant un niveau suffisant de protection des données à caractère personnel sont les suivants[49] :

- la Suisse[50];
- le Canada[51]
- l'Argentine[52] ;
- Guernesey[53] ;
- l'Ile de Man[54] ;
- Jersey[55] ;
- Andorre[56] ;
- les Iles Féroé[57] ;
- Israël[58] ;
- l'Uruguay[59]
- la Nouvelle-Zélande[60] ;
- le Japon[61] .

Les Etats de l'Espace économique européen non membres de l'Union européenne (la Norvège, l'Islande et le Lichtenstein) sont également considérés comme disposant d'un niveau de protection adéquat.

Il en était de même jusqu'à présent lorsque le destinataire des données était établi aux Etats-Unis et adhérent au Privacy Shield. Néanmoins, la Cour de justice de l'Union européenne (CJUE) vient d'invalider la décision d'adéquation de la Commission européenne relative à ce mécanisme, ce dont il résulte que l'adhésion au Privacy Shield de l'organisme destinataire n'est plus valable pour encadrer les flux transfrontières de données vers les Etats-Unis[62].

FOCUS SUR LES CONSÉQUENCES DU BREXIT

Dans le cadre de l'accord de retrait conclu entre l'Union européenne et le Royaume-Uni, une période transitoire allant jusqu'au 31 décembre 2020 à minuit a été convenue, durant laquelle le droit de l'Union continuera de s'appliquer au Royaume-Uni (étant précisé que cette période transitoire pourra être prolongée une fois pour une durée maximale d'un à deux ans).

Jusqu'à la fin de la période transitoire, le RGPD continuera donc de s'appliquer au Royaume-Uni. Il en résulte qu'il n'est pas nécessaire d'encadrer les flux de données à caractère personnel vers le Royaume-Uni au moyen de garanties appropriées prévues par le RGPD pour les transferts vers les pays tiers.

Toutefois, à l'issue de cette période transitoire, les transferts de données à caractère personnel vers le Royaume-Uni devront être encadrés par un mécanisme assurant des garanties appropriées (voir ci-après), **à moins qu'une décision prise par la Commission européenne ne reconnaisse d'ici là que le Royaume Uni garantit un niveau de protection adéquat[63] .**

En deuxième lieu, le transfert peut être fondé sur un **mécanisme assurant des garanties appropriées.** En fonction du mécanisme retenu, une autorisation de l'autorité de contrôle peut devoir être obtenue.

Ces mécanismes sont listés dans le tableau infra, selon qu'une autorisation de l'autorité de contrôle est nécessaire ou non[64] :

ABSENCE DE NÉCESSITÉ D'UNE AUTORISATION PARTICULIÈRE	NÉCESSITÉ D'UNE AUTORISATION DE L'AUTORITÉ DE CONTRÔLE
Instrument juridique contraignant et exécutoire entre les autorités ou organismes publics concernés.	Dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits effectifs et opposables pour les personnes concernées
Règles d'entreprise contraignantes (couramment désignées sous le terme anglais « binding corporate rules » ou « BCR »). *Précision : les BCR concernent un groupe d'entreprises, leur contenu est régi par le RGPD et ce document doit être validé par l'autorité de contrôle avant de pouvoir constituer un fondement valable pour les transferts de données.*	Clauses contractuelles ad hoc entre d'une part le responsable de traitement ou le sous-traitant, et d'autre part l'organisme situé dans un pays tiers ou l'organisation internationale.
Clause contractuelles types adoptées par la Commission européenne ou par l'autorité de contrôle et approuvées par la Commission européenne.	
Code de conduite / mécanisme de certification approuvé, dans les conditions du RGPD, assorti de l'engagement contraignant et exécutoire pris par le destinataire des données dans le pays tiers d'appliquer les garanties appropriées, y compris pour ce qui concerne les droits des personnes concernées.	

[49] Cf. article 45 du RGPD. Pour en savoir plus, voir notamment la carte de la Cnil permettant de visualiser les différents niveaux de protection des données dans les différents pays.
[50] Décision 2000/518/CE du 26-07-2000.
[51] Décision 2002/2/CE du 20-12-2001.
[52] Décision 2003/490/CE du 30-06-2003.
[53] Décision 2003/821/CE du 21-11-2003.
[54] Décision 2004/411/CE du 28-04-2004.
[55] Décision 2008/393/CE du 08-05-2008.
[56] Décision 2010/625/UE du 19-10-2010.
[57] Décision 2010/146/UE du 5-3-2010.
[58] Décision 2011/61/UE du 31-1-2011.
[59] Décision 2012/484/UE du 21-8-2012.
[60] Décision 2013/65/UE du 19-12-2012.
[61] Décision (UE)2019/419 du 23-1-2019.
[62] Décision (UE)2016/1250 du 17-7-2016, invalidée par la décision de la CJUE, n°C-311/18, du 16-7-2020.
[63] Pour en savoir plus, voir la page de la Cnil relative aux conséquences du Brexit.
[64] Cf. articles 46 et 37 du RGPD. Pour savoir plus, voir notamment la page de la Cnil relative aux clauses contractuelles types et celle relative aux règles d'entreprises contraignantes.

En troisième lieu, des **dérogations pour des situations particulières** sont également prévues par la réglementation applicable en matière de protection des données à caractère personnel en l'absence de décision d'adéquation ou de garanties appropriées[65] .

Ainsi, des transferts de données vers des Etats hors Union européenne ou une organisation internationale peuvent être mis en œuvre à condition de répondre **à une des conditions suivantes :**

- la personne concernée a consenti explicitement au transfert ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement, ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et un tiers ;
- le transfert est nécessaire pour des motifs importants d'intérêt public reconnus par le droit de l'Union européenne ou le droit de l'Etat membre auquel le responsable de traitement est soumis ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité de donner son consentement ;
- le transfert a lieu au départ d'un registre qui est destiné à fournir des informations au public et est ouvert à la consultation du public en général, ou de toute personne justifiant d'un intérêt légitime (uniquement conformément aux conditions prévues dans le droit de l'Union européenne ou de l'Etat membre concerné).

En tout état de cause, **de tels transferts doivent faire l'objet, avant d'être éventuellement mis en œuvre, d'une analyse spécifique visant à déterminer (i) leur faisabilité ainsi que (ii) les mesures et garanties particulières devant être déployées.** Aussi, il convient de ne transférer des données à caractère personnel vers un pays hors Union européenne qu'après avoir vérifié que les mesures et garanties adéquates sont mises en œuvre.

[65] 63 Cf. article 49 du RGPD.

(ATTENTION)

Ces dérogations ou exceptions risquent de faire l'objet d'une interprétation restrictive par les autorités de contrôle et ne doivent donc être utilisées pour fonder un transfert de données qu'avec prudence, après une analyse approfondie préalable du respect des conditions posées par le RGPD. Par ailleurs, en l'absence de décision d'adéquation, le droit de l'Union européenne ou d'un Etat membre peut venir fixer des limites au transfert de certaines catégories spécifiques vers des Etats non membres ou des organisations internationales, ce dont il résulte qu'une vérification de ces hypothèses au cas par cas s'impose, en sus des dérogations précitées stricto sensu.

FOCUS SUR L'ENCADREMENT CONTRACTUEL DES FLUX TRANSFRONTIÈRES DE DONNÉES

Par principe, hors les cas où les données sont communiquées à des destinataires (responsable de traitement ou sous-traitant) établis dans un pays considéré comme disposant d'un niveau adéquat de protection des données, **il est nécessaire d'encadrer contractuellement les flux et échanges de données à caractère personnel vers un Etat non membre de l'Union européenne, à savoir des règles d'entreprise contraignantes si les flux sont mis en œuvre au sein d'un groupe d'entreprises, ou des clauses contractuelles types dans les autres situations.**

Pour mémoire, la Commission européenne a élaboré des clauses contractuelles types qu'il convient de conclure avec les destinataires de données à caractère personnel hors Union européenne. Il s'agit des documents suivants :

- pour les flux depuis un responsable de traitement en Union européenne vers un responsable de traitement hors Union européenne, voir le modèle de 2001 et le modèle de 2004 ;
- pour les flux depuis un responsable de traitement en Union européenne vers un sous-traitant hors Union européenne, voir le modèle de 2010.

N.B. Des informations complémentaires doivent être fournies à la personne concernée lors de la collecte de ses données à caractère personnel en présence de tels flux transfrontières. Sur ce point, voir le tableau « Informations générales à fournir » dans le paragraphe « Loyauté et transparence » ci-dessus.

2.4

SÉCURITÉ ET CONFIDENTIALITÉ DES DONNÉES

2.4.1 Obligation générale de sécurité

Chaque agence PR, et ce quelle que soit sa qualification (responsable de traitement ou sous-traitant), est tenue d'assurer la sécurité des données à caractère personnel qu'elle collecte, traite, utilise, conserve, stocke,… et demeure responsable de toute faille de sécurité, violation de données à caractère personnel, fuite de données,… due à un manquement à son obligation de sécurité.

L'assurance que les données à caractère personnel sont traitées dans des conditions appropriées de sécurité et de confidentialité constitue en outre un facteur important de confiance pour les personnes dont l'agence PR traite les données ainsi que pour ses cocontractants (clients, prestataires, partenaires,…).

Ainsi, chaque agence PR, qu'elle agisse en qualité de responsable de traitement ou de sous-traitant, doit, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, mettre en œuvre les mesures techniques et organisationnelles appropriées afin de **garantir un niveau de sécurité adapté au risque,** y compris entre autres, selon les besoins :

- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- la pseudonymisation et le chiffrement des données à caractère personnel le cas échéant en fonction des caractéristiques du traitement[66].

Pour y parvenir, il convient de définir en interne les principes appliqués et mesures techniques et organisationnelles déployées en matière de sécurité des données à caractère personnel, dont le détail pourrait opportunément figurer dans une **politique de sécurité des données à caractère personnel dédiée.**

[66] Cf. article 32 du RGPD.

En pratique

Si une politique générale de sécurité des systèmes d'information existe habituellement au sein de tout organisme, il est recommandé de formaliser également une politique de sécurité dédiée à la protection des données à caractère personnel dans la mesure où les éléments devant y être prévus présentent une certaine spécificité.

A titre d'exemple, les mesures suivantes doivent être prévues dans la politique de sécurité « données à caractère personnel » et faire l'objet d'une attention particulière : méthode d'identification et d'authentification des utilisateurs, gestion des habilitations, sensibilisation et formation des utilisateurs (cf. risque d'ingénierie sociale), traçabilité et journalisation des accès et actions sur les données, sécurisation des postes de travail et de l'informatique mobile et nomade, plans de continuation / de reprise d'activité et/ou plan de secours informatique, gestion des incidents, sécurisation des locaux, du réseau interne, des serveurs et des applications, sécurisation des échanges avec les tiers, chiffrement, anonymisation ou pseudonymisation des données le cas échéant, archivage et sauvegarde sécurisés, lutte contre la vulnérabilité des canaux informatiques (surveillance de l'activité du réseau, interdiction de toute communication directe entre des postes internes et l'extérieur, cloisonnement des réseaux en sous-réseaux, interdiction de raccordement d'équipements informatiques non maîtrisés, etc.), mais également des canaux « papier », mise à jour des logiciels et anti-virus, etc.

Par ailleurs, l'application d'un code de conduite ou d'un mécanisme de certification approuvé peut servir d'élément attestant du respect des exigences de sécurité.

Enfin, une procédure visant à tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles prises pour la sécurité des traitements doit également être déployée. Elle doit être réalisée au terme d'un travail de coopération et de concertation entre des auditeurs techniques et juridiques. Une telle procédure d'audit de sécurité doit également être déployée auprès des sous-traitants par les responsables de traitement (voir sur ce point les développements ci-dessous dans le paragraphe « Encadrer les relations avec les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel »).

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

Il convient également de garder à l'esprit que, outre la sécurisation du système d'information d'un organisme, **la sécurité est l'affaire de tous** et doit être une préoccupation de chaque instant. Tous les collaborateurs ont un rôle à jouer, notamment s'agissant des composantes ci-dessous :

A cette fin, il est par exemple recommandé de déployer les mesures de sécurité suivantes, et de s'assurer de leur respect :

- **mesures de sécurisation des postes de travail, matériels et logiciels :** par exemple, protection contre le vol des postes peu volumineux (antivol, dispositif de géolocalisation,...), obligation d'extinction du poste de travail en cas d'absence et a minima de verrouillage dudit poste en cas d'absence temporaire, verrouillage automatique de session au bout de quelques minutes, interdiction de l'exécution d'applications téléchargées ne provenant pas de sources sûres, récupération et effacement sécurisés des données avant réaffectation d'un poste de travail d'un collaborateur à un autre, interdiction pour les collaborateurs de contourner les mesures de protection ou de rechercher les vulnérabilités des outils métier utilisés, interdiction pour les collaborateurs d'installer sur leurs terminaux personnels des applications ou outils mis à disposition par l'agence dans le cadre de leur activité professionnelle (notamment les outils de messagerie électronique ou les accès aux serveurs par exemple), interdiction d'installer sur les terminaux professionnels ou d'utiliser à des fins professionnelles des outils ou applications non validés ou autorisés par l'agence,... ;
- **mesures de sécurisation de l'informatique mobile ou nomade[67] :** par exemple, limitation du stockage sur le matériel nomade au strict minimum et interdiction en cas de déplacements à l'étranger, filtre de confidentialité sur les écrans, chiffrement des communications entre le poste nomade et le système d'information interne, limitation de l'usage des supports amovibles à ceux fournis par l'agence, verrouillage à distance du poste nomade et/ou du téléphone mobile en cas de perte ou de vol, interdiction pour les collaborateurs de laisser les équipements informatiques mis à disposition par l'agence PR sans surveillance (ex : dans sa voiture, dans un lieu de restauration, au stand d'un événement,...) ;
- **mesures d'authentification des collaborateurs :** mise en place d'identifiants individuels uniques et exclusifs (comptes nominatifs), interdiction des comptes partagés / génériques (cf. interdiction de l'utilisation par plusieurs utilisateurs d'un même identifiant individuel), interdiction de divulguer un moyen d'authentification à un tiers, même à un collègue au sein d'un même service, élaboration et mise en œuvre d'une politique de gestion des mots de passe respectant les recommandations de la Cnil[68],...
- **gestion des habilitations :** identification des rôles et responsabilités, définition de profils d'habilitation en séparant les tâches et les domaines de responsabilité, gestion des habilitations sur les messageries électroniques, dossiers et répertoires partagés, suppression des comptes obsolètes, interdiction pour les collaborateurs d'utiliser des données auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions, interdiction de divulgation des données à des tiers non autorisés,... ;
- **sécurisation des échanges de données à caractère personnel avec des tiers :** identification des tiers pouvant légitimement accéder au système d'information interne et aux données, utilisation privilégiée, en lieu et place de la messagerie électronique, d'un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers comportant des données à caractère personnel (protocole SFTP ou HTTPS dans leur version la plus récente), chiffrement et sauvegarde des données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur amovible), envoi de fichiers compressés dans un dossier ZIP protégé par un mot de passe ou en utilisant un outil dédié aux entreprises et validé par la direction informatique ou par le prestataire informatique de l'agence,...
- **protection des locaux :** système de détection des intrusions / interventions (cf. alarmes et vérifications périodiques de leur bon fonctionnement), définition d'horaires d'accès, portes extérieures verrouillées en dehors des heures normales d'accès par les visiteurs, interdiction d'utiliser des moyens d'accès aux locaux d'une autre personne autorisée (clé, badge,...), mesures pour protéger le matériel (inventaire des équipements / des matériels / du parc / des ressources informatiques, effacement, destruction ou démantèlement sécurisé des ressources informatiques et matérielles mises au rebut, redondance des matériels,...), mesures pour protéger les documents papier (contrôle par code d'accès personnel pour l'impression des documents, limitation de la diffusion des documents papier aux personnes ayant besoin d'en disposer dans le cadre de leur activité et envoi de documents papier uniquement si nécessaire, destruction par broyeur approprié,...),...

[67] Voir également les bonnes pratiques à l'usage des professionnels en déplacement recommandées par l'Agence nationale de la sécurité des systèmes d'information (« Anssi »).
[68] Pour en savoir plus sur les mesures d'authentification par mot de passe, voir les recommandations de la Cnil à ce sujet.

FOCUS SUR LES PRÉCAUTIONS ÉLÉMENTAIRES À PRENDRE EN MATIÈRE DE SÉCURITÉ

Pour en savoir plus sur, voir le guide de la sécurité des données personnelles publié par la Cnil.

En tout état de cause, il convient de sensibiliser les collaborateurs aux bonnes pratiques en matière de sécurité des systèmes d'information, et plus particulièrement en matière de sécurité des données à caractère personnel. **Une charte ou un code de bonne conduite à cet effet est une pratique opportune qu'il convient de déployer et de rendre opposable à l'ensemble des collaborateurs de l'agence, voire aux prestataires extérieurs pouvant intervenir dans le traitement des données à caractère personnel (ex : freelances)** – voir le paragraphe « Comprendre l'accountability et élaborer les procédures et politiques internes indispensables » et la référence à la Charte de bonne conduite en matière de sécurité des données, de type « les 10 règles indispensables en matière de sécurité des données ».

***NB :** cette charte ou ce code de bonne conduite **doit inclure, ou être complété par, un engagement de confidentialité** à la charge de toute personne autorisée à traiter les données à caractère personnel, qu'il s'agisse par exemple des membres du personnel de l'agence PR ou encore de ses prestataires extérieurs, cet engagement de confidentialité devant également leur être en tout état de cause opposable.*

La liste de mesures de sécurité proposée ci-dessus n'est pas exhaustive et doit être adaptée au regard de la pratique effective de chaque agence PR. Ainsi, chaque agence doit procéder, pour chaque traitement de données à caractère personnel mis en œuvre, à une **évaluation des risques** d'atteinte aux données, en fonction de leur vraisemblance et de leur gravité, afin d'identifier les mesures de sécurité à déployer. Ainsi, **plus le risque identifié sera élevé, plus les mesures de sécurité envisagées devront être renforcées.**

Ainsi, **pour apprécier les risques engendrés par chaque traitement,** il convient de procéder aux actions suivantes :

Identifier les impacts potentiels du traitement sur les droits et libertés des personnes concernées, les sources de risques (qui ou quoi pourrait être à l'origine de chaque évènement redouté ?) et les menaces réalisables (qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?)

↓

Déterminer les mesures existantes ou prévues qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation)

↓

Estimer la gravité et la vraisemblance des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale)

C'est au regard d'une telle analyse que **les mesures techniques et organisationnelles de sécurité à déployer doivent être déterminées.**

2.4.2 Analyse d'impact relative à la protection des données en cas de risque élevé

Lorsqu'un traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, **est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées,** alors le responsable de traitement est tenu d'effectuer, avant ledit traitement, **une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel[69].**

La réalisation d'une telle analyse est requise en particulier dans les cas suivants :

- évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- traitement à grande échelle de données sensibles ou données relatives à des condamnations pénales et à des infractions ;
- surveillance systématique à grande échelle d'une zone accessible au public.

[69] Cf. article 35 du RGPD.

Cette liste de traitements n'est pas exhaustive et **les neuf critères suivants permettent de caractériser un traitement susceptible d'engendrer un risque élevé et donc soumis à la réalisation d'une analyse d'impact[70] :**

- données traitées à grande échelle ;
- données sensibles ;
- données concernant des personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- croisement ou combinaison de données ;
- évaluation/scoring (y compris le profilage) ;
- prise de décision automatisée avec un effet juridique ou similaire ;
- surveillance systématique de personnes ;
- traitement pouvant exclure du bénéfice d'un droit, d'un service ou d'un contrat ;
- utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles.

Dès lors qu'un traitement de données à caractère personnel répond à 2 des 9 critères précités (ce qui en principe doit être identifié dans le cadre des opérations précitées de recensement des traitements mis en œuvre), alors une analyse d'impact sur la protection des données doit être réalisée.

A toutes fins utiles, la Cnil a publié une liste des traitements pour lesquels une analyse d'impact est requise[71] ainsi qu'une liste pour lesquels elle n'est au contraire pas requise[72], étant précisé qu'**en toute hypothèse, le responsable de traitement reste bien entendu soumis à l'ensemble des autres obligations qui lui incombent en matière de protection des données à caractère personnel, et notamment en matière de sécurité des données à caractère personnel.**

Une analyse d'impact doit contenir :

- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le résultat d'une telle analyse a vocation à permettre au responsable de traitement de déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte la réglementation applicable en matière de protection des données à caractère personnel. **Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées** compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, **la Cnil doit être consultée avant que le traitement n'ait lieu[73].**

FOCUS SUR LES MODALITÉS DE RÉALISATION D'UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Le présent guide n'a pas vocation à présenter de manière précise et détaillée les modalités de réalisation d'une analyse d'impact en raison de la complexité et de la technicité de celle-ci.

Aussi, en cas de nécessité de procéder à une telle analyse, **il est fortement recommandé de se faire assister d'un conseil externe à l'agence spécialisé en la matière.**

Pour en savoir plus, voir les pages de la Cnil dédiées à l'analyse d'impact (modèle de dossier d'analyse d'impact, exemples d'analyses d'impact fictives, application / logiciel d'accompagnement pour la réalisation d'une analyse d'impact,...).

A noter que la réalisation d'une analyse d'impact relative à la protection des données est à la charge du responsable de traitement. Si une agence PR agit en qualité de sous-traitant de son client pour la réalisation d'une activité donnée, elle peut néanmoins procéder à la réalisation d'une analyse d'impact pour ce qui concerne les opérations de traitement qui lui sont confiées, et en tout état de cause a minima réunir tous les éléments utiles à cette fin, ce qui lui permettra très utilement d'aider son client dans la réalisation de sa propre analyse (cf. obligation de coopération qui incombe en tout état de cause au sous-traitant). Il n'est pas rare en effet que les clients demandent à leur agence de les assister dans la réalisation de cette analyse (et l'agence est dès lors dans l'obligation d'assister son client à cet égard) et il est toujours préférable qu'une telle demande du responsable de traitement soit anticipée.

[70] Cnil, Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données prévues par le règlement général sur la protection des données. **Pour en savoir plus,** voir G29, lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, 4 octobre 2017 (WP 248, rev.01).

[71] Cnil, Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

[72] Cnil, Délibération n° 2019-118 du 12 septembre 2019 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise.

[73] Cf. article 36 du RGPD.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.4.3 Violation de données à caractère personnel

En cas de violation de données à caractère personnel, c'est-à-dire de violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, 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[74], une obligation de notification à la Cnil et, le cas échéant, de communication à l'attention des personnes concernées incombe à l'agence PR concernée[75].

Ainsi, en cas de violation de données à caractère personnel, le responsable de traitement doit :

- **notifier à la Cnil toute violation de données à caractère personnel, à moins qu'elle ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées,** et ce dans les meilleurs délais et, si possible, dans un délai de 72h au plus tard après en avoir eu connaissance. Une telle notification à la Cnil doit, à tout le moins, :

› décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

› préciser le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (le cas échéant) ;

› décrire les conséquences probables de la violation de données à caractère personnel ;

› décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;

[74] Cf. article 4 du RGPD.
[75] Cf. considérants 85 à 88 et articles 33 et 34 du RGPD.

(ILLUSTRATIONS)

A titre d'illustration, peut constituer une violation de données à caractère personnel la perte ou le vol d'un ordinateur ou d'une clé USB comportant des données à caractère personnel, l'accès frauduleux par une personne non autorisée dans un système d'information et de communication, l'installation d'un ransomware (ou rançongiciel) cryptant les données à caractère personnel, l'envoi même par erreur ou négligence d'un email comportant des données à caractère personnel à l'attention de destinataires n'ayant pas à en connaître,...

LE SAVIEZ-VOUS ?

La notification à la Cnil d'une violation de données à caractère personnel peut être effectuée via le téléservice dédié accessible à l'adresse url suivante : https://notifications.cnil.fr/notifications/index.

La notification doit être transmise à la Cnil dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

- **une notification initiale** dans un délai de 72 heures si possible à la suite de la constatation de la violation (si le délai de 72 heures est dépassé, vous devrez expliquer, lors de votre notification, les motifs du retard) ;
- **une notification complémentaire** dès lors que les informations complémentaires sont disponibles.

- **communiquer aux personnes concernées la violation de données à caractère personnel les concernant si celle-ci est susceptible d'engendrer un risque élevé pour leurs droits et libertés.** Une telle communication doit :

› décrire en des termes clairs et simples la nature de la violation ;

› préciser le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (le cas échéant) ;

› décrire les conséquences probables de la violation de données à caractère personnel ;

› décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

En revanche, une telle communication aux personnes concernées n'est pas nécessaire[76] si :

› le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

› le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;

› elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

En tout état de cause, il convient de garder à l'esprit qu'à la suite d'une notification à la Cnil, celle-ci peut exiger du responsable du traitement qu'il procède à une telle communication à l'attention des personnes concernées.

Compte-tenu des conséquences attachées aux violations de données à caractère personnel, il est fortement recommandé de **mettre en place une procédure de gestion des violations de données à caractère personnel en plusieurs étapes,** comme suit :

Identification et correction technique de la violation (processus de détection et de remédiation des incidents)

Organisation de la remontée d'informations (signalement au supérieur hiérarchique, au DPO, à défaut, au référent en matière de protection des données à caractère personnel / si sous-traitant, au responsable du traitement)

Constitution d'un dossier de preuves et qualification juridique des faits (origine / sources de la violation, rapport d'incident, audit technique,...), le cas échéant en coopération avec le(s) sous-traitant(s) intervenant dans le traitement

Dépôt d'une plainte (escroquerie, maintien frauduleux dans un STAD, vol d'informations,...) + déclaration aux assurances

Notification à la Cnil dans un délai de 72h (sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes)

Communication à la personne concernée de la violation si la violation est susceptible d'engendrer un risque élevé pour ses droits et libertés

Mise en place d'un plan de communication (communication interne + externe)

Documentation de la faille (faits et effets) + mesures prises pour y remédier (cf. registre des violations de données)

[76] Attention, ces exceptions doivent faire l'objet d'une interprétation stricte.

Aussi, en cas de survenance d'une telle violation de données à caractère personnel, il appartient à tout collaborateur de coopérer avec l'agence PR afin de déployer le processus ci-dessus formalisé.

En pratique, chacun doit :

- **informer immédiatement la Direction des systèmes d'information en cas de suspicion d'une faille de sécurité** ou violation de données à caractère personnel, et lui communiquer les éléments à l'appui de cette suspicion ;
- **coopérer** avec la Direction des systèmes d'information dans le cadre de la limitation des impacts et de la résolution de la violation ;
- **déployer les mesures** demandées dans ce cadre et dans le cadre des améliorations à envisager.

Enfin, compte tenu de la complexité dans certains cas de l'analyse de risques à mener en vue de la détermination des actions tant juridiques qu'opérationnelles à déployer, mais également du processus à mettre en œuvre dans l'hypothèse de la survenance d'une violation de données à caractère personnel, **il est fortement recommandé de se faire assister, si une telle situation se présente, de conseils externes à l'agence spécialisés en la matière.**

LE SAVIEZ-VOUS ?

La procédure de gestion des violations de données à caractère personnel est en principe à la charge du responsable de traitement et n'incombe pas au sous-traitant. Toutefois, les textes applicables imposent à ce dernier, en vertu de son devoir de coopération, d'informer le responsable d'un traitement concerné par une telle violation dans les meilleurs délais après que le sous-traitant en a pris connaissance. En tout état de cause, une telle coopération doit être prévue contractuellement (à cet égard, voir le paragraphe « Encadrer les relations entre les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel » ci-dessous).

Par conséquent, lorsque l'agence PR est responsable de traitement, il convient, dans les contrats avec les sous-traitants de l'agence, de préciser le périmètre de l'obligation de coopération desdits sous-traitants afin de s'assurer que l'agence pourra obtenir le cas échéant tous les éléments et toutes les informations utiles en vue le cas échéant de procéder à l'analyse de la situation, à une notification à la Cnil si tel est requis et, si nécessaire, à l'information des personnes concernées.

A l'inverse, lorsque l'agence PR est considérée comme agissant en qualité de sous-traitant, il est tout de même particulièrement opportun pour cette dernière de cadrer et de formaliser contractuellement les contours de son obligation de coopération à cet égard avec ses partenaires ou clients qualifiés de responsables de traitement.

2.5
ENCADRER LES RELATIONS AVEC LES DIFFÉRENTS ACTEURS INTERVENANT DANS LE CADRE D'UN TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Plusieurs acteurs sont susceptibles d'intervenir dans la mise en œuvre d'un traitement de données à caractère personnel. **La qualification de chacun d'entre eux[77] est particulièrement structurante** puisqu'il en résulte (i) des obligations spécifiques en matière de protection des données à caractère personnel et (ii) un positionnement différent des acteurs dans le cadre de la négociation des documents contractuels requis pour encadrer les rôles et responsabilités de chacun.

2.5.1 Relations entre responsable de traitement et sous-traitant

Lorsque l'agence PR agit en qualité de responsable de traitement et fait appel à des sous-traitants, elle doit s'assurer que ces derniers présentent des **garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation applicable en matière de protection des données à caractère personnel et garantisse la protection des droits de la personne concernée.

En outre, il convient de conclure un contrat spécifique avec le sous-traitant, lequel doit définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits de l'agence PR[78].

Ainsi, il appartient à chaque agence PR de procéder aux actions suivantes :

› **identifier les sous-traitants intervenant pour le compte de l'agence PR** en matière de traitement de données à caractère personnel ;

(BONNES PRATIQUES)

A cette fin, la rédaction d'un cahier des charges dédié ou d'un questionnaire à remplir par le sous-traitant dans sa réponse à un appel d'offres lancé par l'agence PR par exemple sont des bonnes pratiques qui pourraient être déployées (cf. processus dédié visant à s'assurer que les sous-traitants qu'elle envisage de recruter présentent des garanties suffisantes). Par ailleurs, l'application par le sous-traitant d'un code de conduite ou d'un mécanisme de certification constitue également un bon indice qui pourrait permettre le cas échéant de justifier du choix de l'agence PR dans le recrutement de ses sous-traitants.

(EXEMPLES)

Exemples de prestataires pouvant intervenir en qualité de sous-traitant pour le compte de l'agence PR : prestataire informatique, prestataire de routage d'emailings, freelances, ...

[77] Pour mémoire, voir les critères de qualification présentés au paragraphe « Périmètre conceptuel » ci-dessus.
[78] Cf. article 28 du RGPD.

› **élaborer et conclure un contrat de sous-traitance** avec chaque prestataire (ou si existant, un avenant) **comportant l'ensemble des éléments obligatoires** au titre de la réglementation applicable en matière de protection des données à caractère personnel, à savoir :

Définition du traitement de données à caractère personnel sous-traité (objet, durée, nature, finalité, type de données, catégories de personnes concernées, droits et obligations du responsable de traitement)

Respect par le sous-traitant des exigences de sécurité et de confidentialité des données imposées par le RGPD et par l'agence PR + obligation d'aider le responsable et traitement en vue de garantir le respect par ce dernier de ses obligations à ce titre (notamment sécurité et analyse d'impact)

Obligation pour le sous-traitant d'**aider** le responsable de traitement pour donner suite aux demandes d'exercice de leurs droits par les personnes concernées

Traitement des données par le sous-traitant uniquement sur **instruction documentée** du responsable de traitement + obligation d'alerte de l'agence PR par le sous-traitant en cas d'instruction illicite

Nécessité d'une autorisation écrite préalable, spécifique ou générale du responsable de traitement pour le recrutement d'un autre sous-traitant par le sous-traitant (si autorisation générale, obligation d'information du responsable de traitement de tout changement et possibilité de refus)

Suppression des données par le sous-traitant ou renvoi des données au responsable de traitement et **suppression de copie** au terme de la prestation

Obligation de confidentialité à la charge des personnes autorisées à traiter les données chez le sous-traitant

Obligation pour le sous-traitant de mettre à la charge des sous-traitants ultérieurs les **mêmes obligations** que celles à sa charge telles que prévues au contrat

Mise à disposition du responsable de traitement par le sous-traitant des **informations** nécessaires pour apporter la preuve du respect de ses obligations et permettre la réalisation d'audits

Bien entendu, **dans les hypothèses où l'agence PR agirait en qualité de sous-traitant** pour le compte d'un responsable de traitement, **un contrat comportant ces éléments obligatoires devrait également être conclu entre l'agence PR et le responsable de traitement. Il en va de même avec les cocontractants ayant la qualité de sous-traitants auxquels l'agence PR pourrait avoir recours (cf. les « sous-traitants ultérieurs »)** dans les hypothèses où elle agirait en qualité de sous-traitant pour le compte d'un responsable de traitement, étant précisé que, dans cette hypothèse, il conviendrait de s'assurer que les obligations prévues dans le contrat entre l'agence PR et le sous-traitant ultérieur sont cohérentes avec celles prévues dans le contrat initial conclu entre l'agence PR et le responsable de traitement.

ATTENTION : dans l'hypothèse où l'agence PR agit en qualité de sous-traitant, outre la vérification qu'un contrat conforme à la réglementation applicable en matière de protection des données à caractère personnel a bien été conclu, il convient que cette dernière s'assure de respecter ses obligations en qualité de sous-traitant, notamment s'agissant (i) de l'obligation de ne traiter les données à caractère personnel que sur instruction du responsable de traitement, (ii) de l'obligation de restitution / suppression des données à l'issue de la relation contractuelle avec le responsable de traitement ou encore (iii) de l'obligation d'obtenir l'autorisation (spéciale ou générale, en fonction des précisions visées au contrat) du responsable de traitement pour le recours à un sous-traitant ultérieur.

FOCUS SUR LA CLAUSE À INTÉGRER DANS LES CONTRATS AVEC LES SOUS-TRAITANTS

A toutes fins utiles, il est recommandé d'élaborer des clauses types, lesquelles auraient vocation à permettre à l'agence PR d'être force de proposition et de renforcer sa position dans les négociations.

Voir le modèle de clause-type entre un responsable de traitement et un sous-traitant, orientée « responsable de traitement », proposée par la Cnil.

Attention : ce modèle est un modèle générique proposé à titre informatif. Il ne prend pas en considération les situations spécifiques qui peuvent être rencontrées et devra donc impérativement être adapté en fonction des circonstances de l'espèce, des spécificités de la relation avec tel ou tel sous-traitant, des particularités du projet,... Bien entendu, pour chacun des contrats à conclure, il convient de mener une analyse spécifique permettant de déterminer précisément la qualification ainsi que la répartition des rôles et responsabilités entre l'agence PR et son cocontractant. A cet égard, il peut être opportun de confier la réalisation d'une telle analyse et, le cas échéant, la rédaction ou la validation des clauses à intégrer au contrat en matière de protection des données à caractère personnel au DPO ou, à défaut au référent en matière de protection des données à caractère personnel, voire à un conseil externe à l'agence spécialisé en cette matière.

Par ailleurs, et pour mémoire, **les transferts de données à caractère personnel en dehors de l'Union européenne doivent être encadrés.** Ainsi, pour chaque sous-traitant, il convient de déterminer si des flux transfrontières de données à caractère personnel sont mis en œuvre (en identifiant où est situé le sous-traitant, où sont hébergées les données, ...) et, dans l'affirmative, de déployer les mesures nécessaires pour l'encadrement de tels flux (voir le paragraphe « Encadrement des flux transfrontières de données » ci-dessus).

LE SAVIEZ-VOUS ?

Par principe, toute personne ayant subi un dommage matériel ou moral du fait d'une violation de la réglementation applicable en matière de protection des données à caractère personnel a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi[79].

Tout responsable de traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation de la réglementation applicable en matière de protection des données à caractère personnel. 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 ladite réglementation 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[80]. Ainsi, un responsable du traitement ou un sous-traitant est exonéré de responsabilité, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable[81].

Lorsque le responsable de traitement et le sous-traitant sont responsables d'un dommage causé par le traitement, chacun est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective (cf. mécanisme de solidarité à des fins d'indemnisation de la personne concernée) et celui qui aura réparé intégralement la personne concernée bénéficiera d'une action récursoire à l'encontre des autres acteurs impliqués dans le traitement en cause, afin de répartir en eux la charge de la dette d'indemnisation[82].

[79] Cf. article 82.1 du RGPD.
[80] Cf. article 82.2 du RGPD.
[81] Cf. article 82.3 du RGPD.
[82] Cf. article 1317 du Code civil.
[83] Cf. article 26 du RGPD.
[84] CJUE, 20 juillet 2019, aff. C-40/17, Fashion ID.

2.5.2 Relations entre responsables conjoints du traitement

Lorsque l'agence PR est conjointement responsable d'un traitement de données à caractère personnel avec un autre organisme, il convient de conclure un contrat spécifique avec le responsable conjoint du traitement, lequel doit définir de manière transparente les obligations respectives de ce dernier ainsi que celles de l'agence PR aux fins d'assurer le respect des exigences de la réglementation applicable en matière de protection des données à caractère personnel (notamment en ce qui concerne l'exercice des droits de la personne concernée, l'information des personnes concernées, ...). Ce contrat doit dûment refléter les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées, étant précisé que les grandes lignes d'un tel contrat doivent être mises à la disposition de la personne concernée[83].

(EXEMPLE)

Par exemple, il a pu être considéré que l'éditeur d'un site internet intégrant un plug-in Facebook (cf. bouton « J'aime ») sur ledit site est conjointement responsable avec Facebook, des opérations de collecte et de communication par transmission des données à caractère personnel des visiteurs de son site internet[84].

Ainsi, il en résulte que l'agence PR qui intègre un tel plug-in sur son site internet est conjointement responsable de ce traitement avec Facebook (et ce même dans l'hypothèse où l'agence PR n'aurait accès qu'à des données qui sont constitutives, pour elle, de données « anonymisées », la responsabilité conjointe sur un traitement de données à caractère personnel ne nécessitant pas a priori, en l'état de la jurisprudence, un accès aux données à caractère personnel par tous les responsables conjoints).

Ainsi, il appartient à chaque agence PR de procéder aux actions suivantes :

- **identifier les hypothèses dans lesquelles l'agence PR agit en qualité de responsable conjoint du traitement ;**
- **élaborer un contrat spécifique avec chaque responsable conjoint du traitement** (ou si existant, un avenant) **comportant l'ensemble des éléments obligatoires** au titre de la réglementation applicable en matière de protection des données à caractère personnel, la répartition des rôles et responsabilités devant être cohérente avec la pratique envisagée. De manière générale, certains engagements de l'agence PR pourraient être opportunément limités aux seuls systèmes d'information, outils, applications ou bases de données dont ladite agence PR a exclusivement la maîtrise.

2.6
RÉPONDRE AUX DEMANDES DES PERSONNES CONCERNÉES

2.6.1 Typologie des droits des personnes concernées

Les personnes concernées par les activités de traitement de données à caractère personnel mis en œuvre par une agence PR en qualité de responsable de traitement disposent d'un certain nombre de droits qu'elles peuvent exercer auprès de ladite agence. Il s'agit des droits suivants :

- droit d'interrogation et d'accès ;
- droit de rectification ;
- droit à l'effacement (ou « droit à l'oubli ») ;
- droit à la limitation ;
- droit à la portabilité ;
- droit d'opposition ;
- droit de définir des directives post-mortem.

2.6.1.1 Le droit d'interrogation et d'accès

Toute personne concernée a le droit d'obtenir d'une agence PR agissant en qualité de responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées par ses soins et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes[85]:

- les finalités du traitement ;
- les catégories de données à caractère personnel concernées ;
- les destinataires ou catégories de destinataires auxquels ses données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays hors Union européenne ou les organisations internationales (la personne concernée a également le droit de connaître les garanties appropriées encadrant ces transferts de données vers des destinataires hors Union européenne) ;
- lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable de traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source (c'est-à-dire l'origine de la collecte des données) ;
- l'existence d'une prise de décision automatisée, y compris un profilage, et au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande d'accès à ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Recenser la liste des applications, dossiers, etc.** dans lesquels les données de la personne concernée doivent être recherchées pour une réponse complète, étant rappelé que les réponses à de telles demandes doivent être exhaustives.

2/ Le cas échéant, **se rapprocher des sous-traitants** auxquels l'agence a recours et qui peuvent être amenés à traiter des données à caractère personnel de la personne concernée afin que ces derniers communiquent à l'agence les données de la personne concernées en leur possession.

3/ **Présenter ces données dans un format lisible et compréhensible** en vue de leur communication à la personne concernée. Les sigles et abréviations employées dans les outils métiers de l'agence doivent par exemple être définis et les termes techniques explicités le cas échéant.

4/ **S'assurer que les données extraites ne comportent pas de données à caractère personnel d'autres personnes concernées** que le demandeur (à titre d'exemple, en cas de demande d'accès adressée par Monsieur et Madame X », il convient de communiquer séparément les données de Monsieur X (expurgées des données de Madame X) à celui-ci et les données de Madame X (expurgées des données de Monsieur X) à celle-ci, et non de communiquer l'ensemble des données du couple à ces derniers).

[85] Cf. article 15 du RGPD.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.6.1.2 Le droit à la portabilité

Toute personne concernée a le droit de recevoir les données à caractère personnel la concernant qu'elle a fournies à l'agence PR agissant en qualité de responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine. Elle a en outre le droit d'exiger que l'agence PR les transmette à un autre responsable de traitement, lorsque cela est techniquement possible[86].

L'exercice de ce droit est toutefois limité aux traitements fondés sur le consentement de la personne concernée ou sur l'exécution d'un contrat, et à condition que ces traitements soient effectués à l'aide de procédés automatisés. En outre, la personne concernée ne peut obtenir que les données qu'elle a fournies au responsable de traitement (ex : nom d'utilisateur communiqué via un formulaire en ligne, historique de recherche, etc.), et non celles déduites ou calculées par ce dernier (ex : données créées par un prestataire à partir des données fournies, création d'un profil, etc.).

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande de portabilité de ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Recenser la liste des applications, dossiers, etc.** dans lesquels les données de la personne concernée doivent être recherchées pour une réponse complète, étant rappelé que les réponses à de telles demandes doivent être exhaustives.

2/ Le cas échéant, **se rapprocher des sous-traitants** auxquels l'agence a recours et qui peuvent être amenés à traiter des données à caractère personnel de la personne concernée afin que ces derniers communiquent à l'agence les données de la personne concernées en leur possession.

3/ **Présenter ces données dans un format lisible et compréhensible** en vue de leur communication à la personne concernée. Les sigles et abréviations employées dans les outils métiers de l'agence doivent par exemple être définis et les termes techniques explicités le cas échéant.

3bis / **Retranscrire ces données dans un format structuré, couramment utilisable et lisible par machine.** Selon les autorités de contrôle, à date, un tel format peut être un fichier Excel ou un fichier à plat de type « .csv ». **A cet égard, il convient de préciser qu'il est particulièrement opportun d'anticiper de telles demandes et de se doter (en interne ou par le recours à un tiers) d'un outil dédié (par exemple un outil de type « requêteur »)** qui permettrait, dans chaque cas de figure, d'extraire les données concernées par une telle demande et de les présenter conformément aux textes applicables (cf. format structuré, couramment utilisable et lisible par machine, l'idée sous-jacente étant que ces données doivent pouvoir être facilement réintégrées dans une autre base de données, par exemple la base de données d'un autre responsable de traitement).

4/ **S'assurer que les données extraites ne comportent pas de données à caractère personnel d'autres personnes concernées** que le demandeur (à titre d'exemple, en cas de demande d'accès adressée par « Monsieur et Madame X », il convient de communiquer séparément les données de Monsieur X (expurgées des données de Madame X) à celui-ci et les données de Madame X (expurgées des données de Monsieur X) à celle-ci, et non de communiquer l'ensemble des données du couple à ces derniers).

[86] Cf. article 20 du RGPD. Pour en savoir plus : cf. G29, Lignes directrices relatives au droit à la portabilité des données, 5 avril 2017 (WP.241 rev.01)

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.6.1.3 Le droit de rectification

Toute personne concernée a le droit d'obtenir d'une agence PR agissant en qualité de responsable de traitement, dans les meilleurs délais, que ses données soient rectifiées ou complétées dès lors que ces dernières sont inexactes ou incomplètes[87].

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande de rectification de ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Effectuer les rectifications requises** (cf. dans les conditions prévues par les textes) dans l'ensemble des applications et systèmes d'information de l'agence PR, étant précisé qu'il est particulièrement opportun d'automatiser un tel processus à l'aide d'un outil dédié permettant techniquement d'y procéder.

2/ **Notifier la rectification à chaque destinataire** auquel les données à caractère personnel de la personne concernée ont été communiquées afin que chacun en répercute les conséquences (à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés, étant précisé que ces exceptions sont interprétées de manière très stricte par la Cnil) + communiquer la liste de ces destinataires à la personne concernée en cas de demande de cette dernière.

2.6.1.4 Le droit à l'effacement (ou « droit à l'oubli »)

Toute personne concernée a le droit d'obtenir d'une agence PR agissant en qualité de responsable de traitement, dans les meilleurs délais, l'effacement des données la concernant dans les situations suivantes[88] :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ;
- la personne concernée retire le consentement sur lequel est fondé le traitement et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose au traitement de ses données à caractère personnel ;
- ses données ont fait l'objet d'un traitement illicite ;
- il existe une obligation légale d'effacer les données à laquelle est soumise l'agence PR ;
- les données ont été collectées dans le cadre de l'offre de services de la société de l'information aux enfants.

[87] Cf. article 16 du RGPD.
[88] Cf. article 17 du RGPD.

Toutefois, par exception, le droit à l'effacement ne s'applique pas par exemple pour les traitements qui sont nécessaires :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale à laquelle l'agence PR est soumise ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques dans la mesure où ce droit est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;
- à la constatation, à l'exercice ou à la défense de droits en justice.

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande d'effacement de ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Procéder aux effacements requis** (cf. dans les conditions prévues par les textes) dans l'ensemble des applications et systèmes d'information de l'agence PR, étant précisé qu'il est particulièrement opportun d'automatiser un tel processus à l'aide d'un outil dédié permettant techniquement d'y procéder.

2/ **Notifier l'effacement à chaque destinataire** auquel les données à caractère personnel de la personne concernée ont été communiquées afin que chacun en répercute les conséquences (à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés, étant précisé que ces exceptions sont interprétées de manière très stricte par la Cnil) + communiquer la liste de ces destinataires à la personne concernée en cas de demande de cette dernière.

3/ **Déployer (si l'agence PR a rendu publiques les données à caractère personnel) des mesures raisonnables,** y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, **pour informer les responsables de traitement** qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables de traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

2.6.1.5 Le droit à la limitation

Le droit à la limitation du traitement permet aux personnes concernées de demander à une agence PR agissant en qualité de responsable de traitement le marquage de leurs données, afin de limiter leur traitement futur, dans les situations suivantes[89]:

- la personne concernée conteste l'exactitude des données traitées (cf. limitation pendant une durée permettant à l'agence PR de vérifier l'exactitude des données à caractère personnel concernées) ;
- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
- l'agence PR n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- la personne concernée s'est opposée au traitement (cf. limitation pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par l'agence PR prévalent sur ceux de la personne concernée).

A titre d'illustration, la limitation d'un traitement peut consister en un déplacement temporaire des données, afin de les rendre inaccessibles aux utilisateurs, ou en un retrait temporaire des données d'un site internet par exemple.

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande de limitation du traitement de ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Identifier les modalités techniques de limitation** pouvant être déployées.

2/ **Déterminer la durée de la limitation** (cette durée pouvant être spécifique en fonction de chaque situation).

3/ **Procéder aux limitations requises** (cf. dans les conditions prévues par les textes) dans l'ensemble des applications et systèmes d'information de l'agence PR.

4/ **Notifier la limitation à chaque destinataire** auquel les données à caractère personnel de la personne concernée ont été communiquées afin que chacun en répercute les conséquences (à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés, étant précisé que ces exceptions sont interprétées de manière très stricte par la Cnil) + communiquer la liste de ces destinataires à la personne concernée en cas de demande de cette dernière.

2.6.1.6 Le droit d'opposition

Toute personne concernée a le droit de s'opposer, à tout moment, pour des raisons tenant à sa situation particulière, à certains traitements de données la concernant mis en œuvre par l'agence PR en qualité de responsable de traitement[90]. Les traitements concernés sont ceux nécessaires aux fins des intérêts légitimes poursuivis par l'agence PR ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont serait investie l'agence.

Toutefois, l'agence PR pourra refuser de mettre en œuvre le droit d'opposition des personnes concernées s'il établit l'existence de motifs impérieux et légitimes justifiant le traitement, qui priment sur les intérêts ou les droits et les libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense d'un droit en justice.

Par ailleurs, **la personne concernée peut s'opposer à tout moment, sans avoir à fournir de motif ou de justification, au traitement de ses données à caractère personnel à des fins de prospection, en ce compris aux opérations de profilage qui seraient liées à une telle prospection.**

Dans le cadre de l'utilisation de services de la société de l'information, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public.

[89] Cf. article 18 du RGPD.
[90] Cf. article 21 du RGPD.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

LE SAVIEZ-VOUS ?

Comme tout autre droit de la personne concernée, cette dernière doit être informée de son droit d'opposition au traitement de ces données dans les conditions visée au paragraphe du présent guide intitulé « Loyauté et transparence ».

Toutefois, pour ce qui concerne le droit d'opposition, le RGPD précise qu'au plus tard au moment de la première communication avec la personne concernée, **ce droit doit être explicitement porté à l'attention de la personne concernée et être présenté clairement et séparément de toute autre information.** Il convient donc d'en tenir compte dans le cadre de l'élaboration des mentions d'information à l'attention des personnes concernées.

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de demande d'opposition au traitement de ses données à caractère personnel reçue d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Procéder techniquement à l'opposition demandée** (cf. sous réserve de la réunion des conditions prévues par les textes), c'est-à-dire ne plus traiter les données de la personne concernée, a minima pour les finalités visées par cette dernière dans sa demande le cas échéant.

2/ Ne pas supprimer purement et simplement les données de la personne concernée mais **conserver une trace de son opposition** pour pouvoir démontrer la prise en compte de la demande et être sûr de tenir compte de cette opposition dans le cadre de traitements à venir par exemple (par exemple, aux fins de réalisation et de mise à jour de listes dites « repoussoirs » qui devront être vérifiées avant tout envoi ou toute communication, afin de s'assurer que les personnes qui se sont opposées à recevoir tel type d'envoi ou tel type de communication soient effectivement exclues des prochains envois ou des prochaines communications concernés).

[91] Cf. article 22 du RGPD. Pour en savoir plus : cf. G29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, 6 février 2018 (WP.251 rev.01).

2.6.1.7 Le droit de ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[91].

Toutefois, cette interdiction ne s'applique pas lorsque la décision :

- est autorisée par une disposition légale à laquelle l'agence PR est soumise et qui prévoit des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ;
- est fondée sur le consentement explicite de la personne concernée ;
- est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et l'agence PR.

Dans les deux dernières hypothèses, l'agence PR agissant en qualité de responsable de traitement doit a minima permettre à la personne concernée d'obtenir une intervention humaine pour l'analyse de son dossier, d'exprimer son point de vue et de contester la décision.

Par principe, les décisions automatisées précitées ne doivent en tout état de cause pas être fondées sur des données à caractère personnel dites « particulières » (données relatives à l'état de santé, données révélant la vie ou l'orientation sexuelle, données révélant des origines raciales ou éthiques, ou encore des opinions religieuses, philosophiques, syndicales, ...).

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

Dans l'hypothèse où l'agence envisagerait de déployer des traitements qui pourraient avoir pour effet ou pour objet une prise de décision individuelle fondée exclusivement sur un traitement automatisé, il convient de déployer les actions suivantes :

1/ S'assurer que ces traitements ne sont mis en œuvre que **dans les conditions prévues par les textes** (cf. ci-dessus).

2/ **Permettre en toute hypothèse à la personne concernée de faire valoir son point de vue** et de contester la décision prise sur le fondement d'une décision individuelle automatisée, dans le cadre d'un échange avec une personne « humaine ».

3/ **Pouvoir démontrer le caractère effectif de l'analyse humaine** par rapport à la « pré » décision automatisée, et la possibilité pour l'humain de revenir sur la décision automatisée et de prendre une décision différente.

2.6.1.8 Le droit de définir des directives post-mortem

Toute personne concernée par un traitement peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès[92].

Ces directives sont générales ou particulières et définissent la manière dont la personne entend que soient exercés, après son décès, ses droits en matière de protection des données à caractère personnel.

En outre, en l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés ci-dessus dans la mesure nécessaire :

- à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;
- à la prise en compte, par l'agence PR, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.

En cas de demande des héritiers, l'agence PR doit justifier, sans frais pour le demandeur, qu'elle a procédé aux opérations exigées.

Les désaccords entre héritiers sur l'exercice des droits de la personne concernée sont portés devant le tribunal de grande instance compétent.

FOCUS SUR LES BONNES PRATIQUES À DÉPLOYER

En cas de réception par l'agence PR de « directives post-mortem » de la part d'une personne concernée, il convient de déployer les actions suivantes :

1/ **Conserver la trace des directives** générales ou spécifiques ;

2/ **Mettre en œuvre un process permettant d'en tenir compte** lorsque la situation se présente (cf. lorsque l'agence est informée d'un décès d'une personne concernée) en vue du respect de ces directives par l'agence PR.

[92] Il s'agit d'une spécificité française : cf. article 85 de la Loi Informatique et libertés.

2.6.2 Le traitement des demandes

2.6.2.1 Etape 1 : Identification de la demande et redirection

En principe, une demande d'exercice des droits doit être adressée par la personne concernée au contact mentionné dans les mentions d'information (voir le paragraphe « Informations générales à fournir » ci-dessus). En ce qui concerne les traitements électroniques, il pourrait être envisagé de déployer des formulaires spécifiques pour l'exercice des droits des personnes concernées et, ainsi, **mettre en place une procédure qui permettrait d'adresser directement et automatiquement la demande au DPO** ou, à défaut, au référent en matière de protection des données à caractère personnel, sans identification et analyse préalable.

Toutefois, il peut arriver que la demande soit adressée à tout membre du personnel de l'agence PR. Ainsi, **tout membre du personnel de l'agence PR (service courrier, attaché de presse,...) doit savoir identifier la nature et le contenu d'une demande** par la personne concernée d'exercice de ses droits en matière de protection des données à caractère personnel, afin de l'adresser, aux services ou aux personnes compétentes pour la traiter et y répondre.

• Indices et éléments d'identification de la demande

Quelle que soit la personne réceptionnant une demande d'exercice d'un de ses droits par une personne concernée, le type de demande, et quelles que soient les modalités de transmission d'une telle demande (par oral, par courrier postal, par email, par l'intermédiaire d'un formulaire de contact, etc.), il importe que cette demande soit qualifiée et identifiée.

Pour faciliter et orienter la qualification des demandes reçues par une agence PR, il est proposé d'élaborer une liste de mots-clefs (ex : Cnil, DPO, demande d'accès, portabilité, opposition, etc.) ayant vocation à constituer des indices qui permettraient à toute personne recevant une demande d'identifier sa nature et de la qualifier comme pouvant potentiellement comporter une demande d'exercice de ses droits par une personne concernée, afin de la transmettre aux personnes ou aux services désignés en interne comme compétents pour la traiter. Cette liste devra bien entendu être régulièrement mise à jour par l'agence PR, en fonction des retours d'expérience, des termes utilisés par les personnes concernées à l'occasion de leurs demandes, des évolutions législatives ou réglementaires et de la doctrine des autorités de contrôle.

• Enregistrement de la demande

Toute correspondance, ou tout message, … reçu(e) et qui serait identifié(e) comme une demande d'exercice de ses droits par une personne concernée doit être enregistré(e) dans un registre interne spécifiquement créé à cet effet (ci-après le « registre « droits des personnes »).

Cette procédure d'enregistrement vise notamment à permettre :

- de **conserver une trace de la réception de la demande** et de sa date de réception ;
- d'**assurer le suivi** de l'état d'avancement de la réponse à la demande ;
- de **gérer les délais** de réponse ;
- d'**assurer la traçabilité de la réponse ;**
- d'être en mesure, le cas échéant, de démontrer que la réglementation applicable en matière de protection des données à caractère personnel a bien été respectée.

Quelle que soit la forme de la demande, celle-ci doit donc toujours être enregistrée à réception au moyen d'une saisie dans le registre « droits des personnes ».

Lorsque la demande est formulée sur un support papier (ex : courrier) ou par télécopie, elle doit également être numérisée et enregistrée en pièce jointe dans le registre « droits des personnes ». De même, les courriers électroniques mentionnant une telle demande doivent aussi être enregistrés en pièce jointe dans ledit registre.

Cet enregistrement des demandes dans ce registre doit être effectué avant la transmission de la demande à la personne en charge de la réponse à y apporter.

• Redirection de la demande à la personne / au service compétent pour la traiter

Il convient de **désigner la personne / le service en charge de la réponse aux demandes** d'exercice de leurs droits par les personnes concernées. **Il pourrait opportunément s'agir du DPO** ou, à défaut, du référent en matière de protection des données à caractère personnel. Ainsi de telles demandes doivent être redirigées vers cette personne.

Dans la mesure où l'agence PR se doit d'adresser une réponse à la demande de la personne concernée dans un délai d'un mois à compter de sa réception, il est recommandé de transmettre la demande dans les formes requises, à la personne en charge d'y répondre, immédiatement à réception, et au maximum dans un délai de deux jours ouvrés à compter de sa réception.

2.6.2.2 Etape 2 : Vérification de la demande

Une fois la demande de la personne concernée reçue par la personne compétente pour la traiter, celle-ci doit procéder aux vérifications visées ci-dessous.

Ces vérifications et les actions effectuées dans le cadre de cette étape doivent être consignées dans le registre « droits des personnes ». Tout courrier ou tout échange avec la personne concernée ou avec le demandeur (si différent de la personne concernée) est également enregistré dans le registre précité, le cas échéant en pièce jointe.

N.B. : En amont de ces vérifications, il est recommandé d'accuser réception de la demande auprès de la personne concernée.

• Vérification de la nature de la demande

Afin de s'assurer que la demande a bien été qualifiée, il convient de vérifier avant toute chose qu'il n'y a pas eu d'erreur d'appréciation lors de l'étape 1 et que la demande transmise correspond bien à une demande d'exercice de ses droits par une personne concernée. Il convient également de qualifier le(s) droit(s) que la personne concernée souhaite exercer.

Par ailleurs, il convient de vérifier si la demande porte sur un (ou des) traitement(s) de données mis en œuvre par l'agence PR en qualité de responsable de traitement ou en qualité de sous-traitant. Dans cette seconde hypothèse, il convient de vérifier dans les documents contractuels entre l'agence PR et le responsable de traitement concerné si :

- les réponses aux demandes d'exercice de leurs droits par les personnes concernées doivent être effectuées par l'agence PR : dans cette hypothèse, la présente procédure devra être appliquée à l'aune des stipulations contractuelles existant entre l'agence PR et le responsable de traitement ;
- de telles réponses incombent au responsable de traitement : dans cette hypothèse, il convient de transmettre sans délai la demande au responsable de traitement concerné, le cas échéant selon les modalités, les conditions et le formalisme prévus dans les documents contractuels.

• Vérification de la recevabilité de la demande

Vérification de l'identité du demandeur :

L'agence PR doit prendre toutes les mesures raisonnables pour vérifier l'identité de la personne concernée à l'initiative de la demande.

En effet, quel que soit le support ou le moyen par lequel la demande est adressée, il convient de s'assurer de l'identité du demandeur par tout moyen, étant précisé que le demandeur peut justifier de son identité par exemple par des données d'identité numériques lorsque ces données sont nécessaires et estimées suffisantes par l'agence PR pour authentifier ses utilisateurs (par exemple, demande adressée via un espace personnel en ligne).

En toutes hypothèses, en cas de doute raisonnable quant à l'identité de la personne physique présentant la demande (et uniquement dans cette hypothèse), il est possible de demander à cette dernière de fournir des informations supplémentaires nécessaires pour confirmer son identité. Peut ainsi être demandée à cette fin, lorsque la situation l'exige, la photocopie d'un titre d'identité portant la signature du titulaire[93].

Une fois ces vérifications effectuées, la personne en charge de la réponse à une telle demande doit vérifier qu'elle dispose de l'adresse (postale ou électronique) où ladite réponse doit être adressée. A défaut, il convient de demander des informations complémentaires à la personne ayant présenté la demande, afin de déterminer selon quelles modalités et à quelles coordonnées la réponse doit être adressée.

En tout état de cause, lorsqu'il existe un doute sur l'adresse indiquée ou sur l'identité du demandeur, la réponse à la demande doit être expédiée sous pli recommandé avec avis de réception.

En principe, lorsqu'il existe un doute raisonnable sur l'identité du demandeur ou sur l'adresse postale à laquelle la personne concernée a demandé la transmission par écrit d'informations la concernant, les textes précisent que la réponse peut être expédiée sous pli recommandé sans avis de réception, la vérification de l'adresse et de l'identité s'effectuant lors de la délivrance du pli. Toutefois, un avis de réception est recommandé pour conserver la preuve de la réception de la réponse par le destinataire (cf. dans un objectif de traçabilité).

FOCUS SUR LES DEMANDES ADRESSÉES PAR UN MANDATAIRE OU UN HÉRITIER DE LA PERSONNE CONCERNÉE

Cas spécifique du mandat :

En sus des précisions ci-dessus, lorsque la demande est présentée par une personne spécialement mandatée à cet effet par le demandeur, le mandataire doit avant toute communication justifier, de son mandat, de son identité et de celle du mandant.

Le mandat doit être spécial, fait par écrit et doit comporter a minima les indications suivantes :

› la description du traitement concerné ;
› le nom du responsable de traitement ;
› la période spécifique du mandat ;
› le périmètre du mandat, et notamment la typologie des droits que la personne souhaite exercer.

Il convient également de procéder aux vérifications formelles précitées.

Cas spécifique des héritiers :

Lorsqu'une demande est adressée par l'héritier d'une personne décédée et que cette demande a pour objet l'exercice des droits du défunt sur les données à caractère personnel de ce dernier, il convient de **s'assurer que l'héritier justifie de son identité et apporte la preuve de sa qualité d'héritier** (acte de notoriété, livret de famille, ...).

Il convient également de procéder aux vérifications formelles précitées et de vérifier que les droits visés dans la demande font partie de ceux pouvant être exercés par un héritier. Enfin, il convient de vérifier si la demande portée à la connaissance du responsable de traitement par l'héritier est conforme aux directives post-mortem éventuellement définies par la personne concernée avant son décès, si de telles directives ont été portées à sa connaissance.

[93] Cf. article 77 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la Loi Informatique et libertés.

Vérification du contenu de la demande :

Si la demande est incomplète, comporte des imprécisions ou n'inclut pas tous les éléments permettant le traitement de la demande (notamment s'agissant des vérifications mentionnées ci-dessus relatives à l'identité et à la qualité du demandeur), une demande d'information complémentaire doit être adressée par l'agence PR au demandeur.

Cette demande d'informations complémentaires peut être adressée à la personne concernée par courrier recommandé avec demande d'accusé de réception, par lettre remise contre signature ou par voie électronique.

N.B : la demande de compléments d'informations ne doit être utilisée ***que si les informations figurant dans la demande ne permettent véritablement pas d'y répondre.***

Vérification du bien-fondé de la demande :

Les droits d'accès et d'opposition à la prospection notamment commerciale sont des droits discrétionnaires. Il en est de même pour ce qui concerne la définition par la personne concernée de directives post-mortem. Celui qui les exerce n'a donc à justifier d'aucun motif.

A l'inverse, le droit d'opposition (hors traitements à des fins de prospection précités) à figurer dans un traitement nécessite de la part du demandeur de justifier sa demande par des raisons tenant à sa situation particulière.

De même, l'exercice du droit de rectification nécessite pour la personne concernée d'arguer de données inexactes ou incomplètes, si besoin en produisant une déclaration / un justificatif complémentaire.

Le droit à l'effacement (cf. « droit à l'oubli »), le droit à la portabilité, le droit à la limitation du traitement ou encore le droit à ne pas faire l'objet d'une décision automatisée sont encadrés par un certain nombre de conditions (voir supra le paragraphe sur la typologie des droits des personnes concernées).

Il convient donc de vérifier l'ensemble des conditions applicables à chaque droit exercé afin de déterminer au cas par cas si une réponse positive doit être apportée à chacune des demandes reçues.

FOCUS SUR LES DEMANDES NE RÉUNISSANT PAS LES CONDITIONS APPLICABLES

En cas de demande d'exercice de ses droits par une personne concernée qui ne réunirait pas toutes les conditions applicables, **il convient tout de même de répondre à cette personne** (dans les conditions prévues au paragraphe ci-dessus sur la vérification du contenu de la demande) **(i) afin d'expliciter à son attention les raisons pour lesquelles une réponse ou une suite positive à sa demande ne pourra pas être apportée** et de l'informer de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et/ou de former un recours juridictionnel, **ou encore (ii) en vue de tenter d'obtenir les justifications nécessaires requises le cas échéant** (par exemple, demander un justificatif en vue de procéder à une rectification souhaitée par une personne concernée).

Cette étape doit être aussi l'occasion de **vérifier si la demande n'est pas manifestement infondée ou excessive.** Dans une telle hypothèse, il peut refuser de donner suite et de répondre à la demande : la personne concernée devra toutefois en être informée. Il conviendra également de l'informer de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et/ou de former un recours juridictionnel.

FOCUS SUR LES DEMANDES MANIFESTEMENT INFONDÉES OU EXCESSIVES

L'analyse du caractère manifestement infondé ou excessif de la demande nécessite d'être **formalisée et argumentée,** et cette exception à l'obligation de donner suite aux demandes des personnes concernées doit être utilisée avec **beaucoup de prudence** dans la mesure où (i) ces notions doivent être d'interprétation stricte et que (ii) il appartiendra à l'agence PR ayant réceptionné une telle demande, dans l'hypothèse d'une réclamation ou d'un litige, de démontrer que la demande est manifestement infondée ou excessive. En tout état de cause, il convient également d'informer le demandeur des voies et délais de recours pour contester cette décision.

2.6.2.3 Etape 3 : Réponse à la demande

• Forme de la réponse à la demande

De manière générale, la réponse doit être adressée par écrit à la personne concernée. A des fins probatoires, il est recommandé d'adresser la réponse au choix par :

- courrier recommandé avec demande d'accusé de réception ;
- lettre remise contre signature ;
- courrier électronique avec demande d'accusé de réception.

Lorsque la demande est présentée sous une forme électronique, la réponse est adressée par voie électronique lorsque cela est possible (à moins que la personne concernée ne demande qu'il en soit autrement).

Dans cette hypothèse, et pour tenir compte des risques inhérents à toute circulation d'informations via internet, si la réponse a vocation à contenir des données à caractère personnel, alors la réponse ne pourra être adressée que par un moyen sécurisé dédié (par exemple : serveur FTP sécurisé, chiffrement du canal de transmission et/ou des messages et pièces jointes, ...).

En tout état de cause, dans le cas d'une réponse sous forme électronique, alors les informations demandées doivent être fournies à la personne concernée sous une forme électronique d'usage courant, conformément à l'état de l'art.

Enfin, dans tous les cas, et quel que soit le format de la réponse, il convient de s'assurer que le moyen de réponse est sécurisé.

FOCUS SUR LES DEMANDES DE CONSULTATION DES DONNÉES SUR PLACE

La consultation des données sur place peut être envisagée (par exemple par consultation directe des informations à l'écran), sous réserve de la protection des données à caractère personnel des tiers. Toutefois, **cette pratique n'est pas conseillée.** Aussi, il est recommandé dans cette hypothèse de remettre au demandeur un accusé de réception de sa demande et de lui adresser la réponse selon le formalisme précité.

[94] Cf. article 12.3 du RGPD.
[95] Cf. article 12.5 du RGPD.

• Délai de la réponse à la demande

De manière générale, le pilote doit répondre aux demandes des personnes concernées « dans les meilleurs délais ». En tout état de cause, **ce délai ne peut pas dépasser un mois à compter de la date de réception de la demande[94].**

Ce délai peut être prolongé de deux mois supplémentaires en raison de la complexité et du nombre de demandes. Dans ces circonstances, il convient d'informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

N.B : Cette prolongation de délai, par exception au délai de droit commun, est à utiliser avec beaucoup de prudence dans la mesure où les motifs d'un report sont interprétés de manière stricte.

• Coût de la réponse et des mesures éventuellement prises

En principe, aucun paiement n'est exigé pour procéder à la communication des informations demandées et / ou prendre toute mesure au titre des demandes d'exercice de leurs droits des personnes concernées afin de tenir compte de ces demandes[95].

Toutefois, **par exception, il peut être exigé de la part du demandeur le paiement de frais raisonnables basés sur les coûts administratifs** supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées, dans les hypothèses suivantes :

- si la demande porte sur un droit d'accès et que la personne concernée souhaite obtenir des copies supplémentaires (c'est-à-dire en plus de la copie initialement communiquée) ;
- lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif (étant rappelé qu'il conviendra le cas échéant de pouvoir démontrer de ce caractère manifestement infondé ou répétitif).

N.B. : Le coût des frais raisonnables correspondant aux coûts administratifs ne doit pas être une entrave à l'exercice des droits.

• Contenu de la réponse à la demande

Pour mémoire, il convient de **répondre à toute demande** formulée par une personne concernée et de motiver la réponse lorsqu'il est décidé de ne pas donner suite à une telle demande (uniquement dans les hypothèses mentionnées ci-dessous, lesquelles doivent demeurer d'interprétation restrictive), étant rappelé qu'il conviendra dans ce cas d'en informer sans tarder la personne concernée et au plus tard dans un délai d'un mois à compter de la réception de la demande et d'indiquer à la personne concernée qu'elle dispose du droit d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel pour contester une telle décision.

En cas de réponse favorable à une demande d'une personne concernée, le contenu de la réponse doit être dicté par le périmètre des droits exercés par la personne concernée dans ladite demande (pour ce qui concerne le détail des informations à communiquer et les actions à déployer, il convient de se reporter au paragraphe « Typologie des droits des personnes concernées » ci-dessus détaillant la typologie et le contour des droits des personnes concernées).

Pour mémoire, les actions réalisées en vue de répondre à la personne concernée, ainsi que les dates, modalités, … des réponses adressées sont consignées dans **le registre « droits des personnes »** qu'il convient de mettre en place au sein de l'agence PR. Tout courrier ou tout échange avec la personne concernée ou avec le demandeur (si différent de la personne concernée) est également enregistré dans le registre précité, le cas échéant en pièce jointe.

2.6.3 Propositions de courriers-types

Les modèles types ci-après sont proposés à titre d'exemples et ne sauraient être exhaustifs dans la mesure où il s'agit principalement de fournir aux agences PR une base de connaissance à titre de référentiel afin de leur faciliter l'élaboration des réponses aux personnes concernées.

Toutefois, ces modèles types ne peuvent pas tenir compte de la spécificité de chaque demande et chaque agence PR doit donc impérativement prendre en considération les circonstances particulières de chaque situation, ainsi que notamment le périmètre exact de chaque demande d'une personne concernée.

Ces modèles types doivent en tout état de cause être régulièrement complétés et mis à jour par les agences PR (cf. suite à des retours d'expérience notamment).

2.6.3.1 Modèles d'accusé de réception d'une demande

• Modèle d'accusé de réception d'une demande simple

De : [Agence PR] A : [Demandeur]

Par LRAR n°[…] ou par courrier électronique […] avec demande d'accusé de réception

A […], le […]

Objet : Votre demande de […]

Chère Madame / Cher Monsieur,

J'accuse réception de la demande de […] que vous avez formulée par [courrier postal / téléphone / email …] en date du […], parvenu à notre agence le […].

Cette demande m'a été transmise en ma qualité de [DPO / référent en matière de protection des données à caractère personnel] au sein de l'agence [à compléter avec la dénomination de l'agence PR].

Je ne manquerai pas de revenir vers vous dans les plus brefs délais et vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de nos salutations distinguées.

[Identité du signataire, titre/qualité et signature]

- **Modèle d'accusé de réception en cas de demande formulée sur place à laquelle il ne peut être répondu immédiatement**

De : [Agence PR]

A : [Demandeur]

Par lettre remise contre signature

A [...], le [...]

Objet : Votre demande de [...]

Chère Madame / Cher Monsieur,

J'accuse réception de la demande de [...] que vous avez formulée sur place en nos locaux en date du [...].

Option 1

Malheureusement, je ne peux vous donner immédiatement communication des données demandées en raison [ex : d'un risque d'atteinte aux droits des tiers, et plus précisément par nécessité de protéger la confidentialité des données d'autres personnes].

Dans ces circonstances, les informations que vous avez demandées vous seront communiquées [à choisir : par courrier postal / par courrier électronique aux coordonnées suivantes : ...] dans un délai d'un mois à compter de ce jour.

Option 2

Malheureusement, je ne peux donner immédiatement une suite favorable à votre demande / procéder immédiatement aux opérations nécessaires à la prise en compte de votre demande en raison [à compléter].

Dans ces circonstances, je ne manquerai pas de revenir vers vous dans les meilleurs délais concernant votre demande, et en tout état de cause dans un délai maximum d'un mois à compter de ce jour, afin de vous tenir informé des suites qui y seront données.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

- **Modèle de courrier / email de demande d'informations complémentaires**

De : [Agence PR] A : [Demandeur]

Par LRAR n°[…] ou par courrier électronique […] avec demande d'accusé de réception

A […], le […]

Objet : Votre demande de […]

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du […], parvenue à notre agence le […] par [courrier postal / téléphone / email …], je me permets de revenir vers vous afin de vous confirmer la bonne réception de votre demande aux termes de laquelle vous avez manifesté votre souhait d'exercer votre droit de […].

Cette demande m'a été transmise en ma qualité de [DPO / référent en matière de protection des données à caractère personnel] au sein de l'agence [à compléter avec la dénomination de l'agence PR].

Option 1

Afin de nous permettre de traiter votre demande dans des conditions nous permettant d'assurer la sécurité, la confidentialité et l'intégrité de vos données à caractère personnel, nous sommes dans l'obligation de nous assurer de votre identité.

Cette précaution nous permet de nous assurer que les données que nous pouvons être amenés à communiquer suite à des demandes telles que la vôtre sont bien adressées à la personne concernée par ces données elle-même. Il s'agit d'éviter qu'une autre personne puisse accéder aux informations vous concernant à votre insu, et inversement.

Aussi, je vous remercie de bien vouloir nous adresser sans délai une copie d'un titre d'identité signé par vos soins, par courrier électronique ([…]) ou par courrier postal à l'adresse suivante : […].

Option 2

Afin de nous permettre de traiter votre demande dans des conditions nous permettant d'assurer la sécurité, la confidentialité et l'intégrité de vos données à caractère personnel, je vous serais [reconnaissant/reconnaissante] de bien vouloir me communiquer l'adresse postale ou l'adresse de courrier électronique à laquelle vous souhaitez que notre réponse vous soit adressée.

Cette précaution vise à nous assurer que vous recevrez la réponse à votre demande selon les modalités et aux coordonnées de votre choix.

Option 3

[insérer toute autre demande complémentaire qui serait nécessaire pour traiter et répondre à la demande, en fonction des spécificités attachées à chaque droit – voir les paragraphes « Typologie des droits des personnes concernées » et « Etape 2 : Vérification de la demande »]

Restant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin,

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

2.6.3.2 Modèles de réponse suivant la nature de la demande

• Modèle de réponse à une demande de droit d'accès

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...] avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande d'exercice de votre droit d'accès aux données vous concernant

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [courrier postal / téléphone / email ...], visant à obtenir [à compléter], je vous prie de bien vouloir trouver ci-joint [à ajuster le cas échéant si les données ne sont pas communiquées par courrier ou email (sécurisé) mais mises à disposition via un serveur de partage de fichiers sécurisé par exemple. Idem s'agissant de la référence aux pièces jointes à la fin du présent courrier type] le détail des données vous concernant en notre possession :

- [préciser les supports et les applications depuis lesquelles les données sont issues, par exemple : des copies d'écrans de l'application xxx, un fichier sous format [...] extrait de l'application yyy, des documents numérisés enregistrés dans l'application zzz, des documents figurant dans votre dossier papier, etc.]

Pour votre parfaite compréhension, nous portons à votre connaissance la signification de certains termes, sigles, abréviations et codes couleurs [à compléter] :

- [terme / abréviation / sigle / code] : [signification]
- [etc.]

Ces informations vous concernant sont constituées :

- [à compléter avec les sources / origines des données, par exemple : des données communiquées par vous-même, des données liées au suivi, à la gestion et à l'exécution de votre contrat avec [...], des données issues des échanges entre [...] et vous-même, etc.]

Par ailleurs, nous vous informons que ces données sont traitées par nos soins pour [à compléter avec les finalités, les catégories de données, les destinataires, les durées de conservation, les droits des personnes concernées, le droit d'introduire une réclamation auprès de l'autorité de contrôle, l'existence éventuelle d'une prise de décision automatisée et la logique / l'importance / les conséquences attachées – voir le paragraphe « Le droit d'interrogation et d'accès » ci-dessus].

En espérant avoir répondu à vos attentes et en me tenant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

Pièce(s) jointe(s) [nombre] :

- [A compléter en listant toutes les pièces jointes / supports joints]

- **Modèle de réponse à une demande de portabilité**

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...]
avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande d'exercice du droit à la portabilité des données vous concernant

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [courrier postal / téléphone / email ...], visant à obtenir [à compléter], je vous prie de bien vouloir trouver en fichier joint, en format [à compléter avec un format couramment utilisé et lisible par machine, par exemple .csv], le détail des données vous concernant pouvant faire l'objet d'une portabilité à votre attention conformément aux dispositions légales et réglementaires applicables.

[le cas échéant, il convient d'envisager l'opportunité de compléter cette réponse avec une réponse de type « réponse droit d'accès » pour préciser à la personne concernée que d'autres données, non concernées par la portabilité, sont traitées par l'agence PR + détailler ces autres données, les finalités, etc.]

En espérant avoir répondu à vos attentes et en me tenant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

- **Modèle de réponse à une demande de rectification / effacement / limitation**

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...]
avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande de [...]

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [courrier postal / téléphone / email ...], visant à obtenir [à compléter], nous vous confirmons la bonne prise en compte de votre demande et avons procédé aux actions suivantes :

- [par exemple, mise à jour de vos coordonnées, effacement des données suivantes [...], marquage des données visées dans votre demande selon les modalités suivantes [...] en vue de la limitation de leur traitement pendant [...], etc.].

Toutefois, certaines informations n'ont pas pu faire l'objet de [...] pour les raisons suivantes :

- [à compléter, le cas échéant, avec la justification adossée à une impossibilité de rectification / effacement / limitation, par exemple : impossibilité d'effacer certaines informations en raison d'obligation légales incombant à l'agence PR + préciser quand la suppression sera possible, etc.]

En espérant avoir répondu à vos attentes et en me tenant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

- **Modèle de réponse à une demande d'opposition (opposition pour des raisons tenant à une situation particulière, opposition à la prospection, opposition à faire l'objet d'une décision fondée exclusivement sur un traitement automatisé)**

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...]
avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande d'opposition au traitement de vos données

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [courrier postal / téléphone / email ...], visant à obtenir [à compléter], nous vous confirmons la bonne prise en compte de votre demande.

A cet égard, nous vous précisons que nous avons procédé aux actions suivantes :

- [à compléter avec les actions effectuées, par exemple : inscription sur notre liste d'opposition, etc.]

Par conséquent :

- [à compléter avec les conséquences des mesures prises, par exemple « Nous vous confirmons que vous ne serez plus destinataire de nos messages et propositions commerciales », « Nous vous proposons de nous rencontrer [date / lieu] afin que vous puissiez nous faire part de votre point de vue et des éléments de contestation de notre décision », etc.]

En revanche, nous ne pouvons donner une suite favorable à votre demande concernant [...] pour les raisons suivantes :

- [à compléter, le cas échéant, avec la justification adossée à une impossibilité de tenir compte d'une demande d'opposition particulière]

En espérant avoir répondu à vos attentes et en me tenant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

- **Modèles de réponse en matière de droit de définir des directives post-mortem**

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...]
avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande de définir le sort de vos données après votre décès

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [courrier postal / téléphone / email ...], visant à obtenir [à compléter], nous vous confirmons la bonne prise en compte de votre demande.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

• Modèle de refus de faire droit à une demande

De : [Agence PR] A : [Demandeur]

Par LRAR n°[...] ou par courrier électronique [...]
avec demande d'accusé de réception

A [...], le [...]

Objet : Votre demande de [...]

Chère Madame / Cher Monsieur,

Dans le prolongement de votre demande du [...], parvenue à notre agence le [...] par [à compléter avec les modalités de la demande], visant à obtenir [à compléter], je suis au regret de vous annoncer que je ne peux donner une suite favorable à votre demande pour les motifs suivants :

- [à compléter avec les motifs, par exemple : en raison du caractère excessif / infondé de votre demande (+ explications justifiant de ce caractère excessif ou infondé, par exemple en raison du caractère répétitif des demandes), dans la mesure où nous ne sommes à ce jour en possession d'aucune donnée vous concernant, etc.].

Conformément aux dispositions légales et réglementaires applicables, nous vous précisions que vous disposez de la possibilité d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés ou de former un recours juridictionnel relativement à la présente décision de refus.

Restant personnellement à votre disposition pour vous fournir toute information complémentaire dont vous auriez besoin.

Je vous prie d'agréer, Chère Madame / Cher Monsieur, l'expression de mes salutations distinguées.

[Identité du signataire, titre/qualité et signature]

LE SAVIEZ-VOUS ?

La gestion et le traitement des demandes d'exercice de leurs droits par les personnes concernées sont en principe à la charge du responsable de traitement et n'incombent pas au sous-traitant. Toutefois, les textes applicables imposent à ce dernier, en vertu de son devoir de coopération, d'aider et d'assister le responsable de traitement en vue de la gestion et de la réponse à de telles demandes. En tout état de cause, une telle coopération doit être prévue contractuellement (à cet égard, voir le paragraphe « Encadrer les relations entre les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel » ci-dessus).

Par conséquent, lorsque l'agence PR est responsable de traitement, il convient, dans les contrats avec les sous-traitants de l'agence, de préciser le périmètre de l'obligation de coopération desdits sous-traitants afin de s'assurer que l'agence pourra obtenir le cas échéant tous les éléments et toutes les informations utiles en vue le cas échéant de gérer et de répondre à de telles demandes.

A l'inverse, lorsque l'agence PR est considérée comme agissant en qualité de sous-traitant, il est tout de même particulièrement opportun pour cette dernière de cadrer et de formaliser contractuellement les contours de son obligation de coopération à cet égard avec ses partenaires ou clients qualifiés de responsables de traitement.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

2.7
COMPRENDRE L'ACCOUNTABILITY ET ÉLABORER LES PROCÉDURES ET POLITIQUES INTERNES INDISPENSABLES

L'ensemble des obligations prévues par la réglementation applicable en matière de protection des données à caractère personnel est sous-tendu par le **principe dit d'« accountability »,** principe directeur qui irrigue la matière et nécessite la mise en œuvre d'un ensemble de mécanismes en vue de pouvoir démontrer le cas échéant le respect de la réglementation applicable en matière de protection des données à caractère personnel[96].

LE SAVIEZ-VOUS ?

La notion **d'« accountability »** désigne l'obligation pour les organismes traitant des données à caractère personnel de déployer les mesures organisationnelles et techniques nécessaires pour le respect de la réglementation applicable en matière de protection des données à caractère personnel, et d'être en mesure de démontrer l'effectivité et l'efficacité de ces mesures.

L'accountability implique la mise en place d'une **véritable gouvernance des données,** et notamment :

- de déployer un **processus continu et dynamique de mise en conformité** à la réglementation applicable en matière de protection des données à caractère personnel, notamment grâce à une organisation interne dédiée, ainsi qu'à un ensemble de règles contraignantes, d'outils, de procédures, de politiques et de codes de bonnes pratiques correspondantes (cf. documentation qu'il convient d'élaborer et de mettre en œuvre) ;
- d'apporter **la preuve le cas échéant que les mesures appropriées ont été prises** (cf. mécanisme permettant de démontrer l'efficacité et l'effectivité des mesures prises) : en pratique, il appartient à chacune des agences PR de pouvoir prouver / tracer les actions déployées ;
- **d'évaluer les mesures prises dans le cadre d'un contrôle continu,** pour d'une part, vérifier l'efficacité / l'effectivité desdites mesures et d'autre part, les actualiser ou les ajuster le cas échéant pour assurer leur maintien en conformité à la réglementation applicable en matière de protection des données à caractère personnel au regard de l'évolution des traitements, de leurs finalités, des exigences[97] réglementaires ou tout simplement du retour d'expérience.

FOCUS SUR LES CODES DE CONDUITE ET MÉCANISMES DE CERTIFICATION

L'application d'un code de conduite ou de mécanismes de certification[98] approuvés par la Cnil peut servir d'élément pour démontrer le respect des obligations incombant au responsable de traitement[99].

Leur application par un sous-traitant peut également servir d'élément pour démontrer l'existence des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation applicable en matière de protection des données à caractère personnel et garantisse la protection des droits de la personne concernée[100].

En tout état de cause, quel que soit le mécanisme retenu, il convient de porter une attention particulière au respect des règles et principes qu'ils édictent dans la mesure où des vérifications relatives à leur application peuvent être effectuées par la Cnil, mais également par des organismes dédiés disposant d'un niveau d'expertise approprié ou par les organismes de certification.

[96] Cf. considérant 78 et article 25 du RGPD.
[97] Cf. article 40 du RGPD.
[98] Cf. article 42 du RGPD.
[99] Cf. article 24.3 du RGPD.
[100] Cf. article 28.5 du RGPD.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

Le tableau ci-après a vocation à présenter, de manière non exhaustive, des procédures, politiques et codes de bonnes pratiques qui peuvent opportunément être élaborées et déployées au sein de chaque agence PR, en concertation avec le DPO ou, à défaut, le référent en matière de protection des données à caractère personnel :

POLITIQUE / PROCEDURE	OBJECTIFS	CONTENU
Charte de « traitement des données » / Code de bonne conduite ou de bonnes pratiques	› Diffuser une culture « protection des données » au sein de l'organisme › Favoriser l'atteinte et le maintien en condition opérationnelle de la conformité › Favoriser l'adéquation permanente entre, d'une part, les exigences de la réglementation applicable en matière de protection des données à caractère personnel et d'autre part, les contraintes opérationnelles de l'organisme	› Présentation de l'organisation interne et gouvernance en matière de protection des données à caractère personnel (désignation et missions du DPO ou, à défaut, du référent en matière de protection des données à caractère personnel, process de remontées d'informations pour tout nouveau projet ou difficultés rencontrées par des collaborateurs relatives à la protection des données à caractère personnel, ...) › Explication pratique et pédagogique des principes applicables en la matière devant être respectés par les collaborateurs (cf. bonnes pratiques attendues de la part des collaborateurs s'agissant de l'application des principes présentés aux paragraphes « Analyser la conformité des traitements de données à caractère personnel » et « Sécurité et confidentialité des données ») › Charte de bonne conduite en matière de sécurité des données, de type « les 10 règles indispensables en matière de sécurité des données » (par exemple, identifier les documents comportant des données à caractère personnel, respecter les privilèges et habilitations octroyés, ...)
Charte d'utilisation des ressources informatiques et de communications électroniques	› Fixer les règles d'utilisation des systèmes d'information et de communication mis à disposition des personnes autorisées à les utiliser dans le cadre de leur activité professionnelle	› Champ d'application (personnes, moyens et usages (outils/systèmes d'information) concernés) › Encadrement des conditions d'utilisation (usage professionnel / non professionnel, moyens d'authentification, réseaux sociaux, télétravail,...) avec indication de ce qui est autorisé (par exemple, hypothèses d'usage non professionnel toléré et/ou autorisé des moyens mis à disposition des membres de son personnel par l'employeur) / interdit (par exemple, interdiction de divulguer ses moyens d'authentification, interdiction de contourner les moyens de sécurité et de surveillance mis en place,...)

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

POLITIQUE / PROCEDURE	OBJECTIFS	CONTENU
Cahier des charges technico-fonctionnelles (ou check-list « privacy by design »)	› Attirer, pour chaque nouveau projet, l'attention des opérationnels sur le respect de la réglementation applicable en matière de protection des données à caractère personnel › S'assurer que tous les outils déployés permettront de manière effective de respecter ladite réglementation	› Présentation des principales questions qu'il convient de se poser en amont de tout nouveau projet (par exemple, le traitement a-t-il pour finalité la prospection ? par quels moyens (email ? sms ? mms ? courrier postal ? téléphone ? autres ?), en fonction des moyens choisis, le consentement est-il recueilli ? etc...) et des principes qui doivent diriger la réflexion des opérationnels (description précise du projet, analyse de sa conformité, identification des mesures à mettre en place le cas échéant,...) afin de s'assurer de la conformité des traitements de données à caractère personnel mis en œuvre avec la réglementation applicable en la matière, et ce tout au long de leur cycle de vie et/ou du projet, en application de la notion de protection des données dès la conception dite de « privacy by design »
Politique générale de sécurité des données à caractère personnel	› Définir les principes appliqués et mesures techniques et organisationnelles prises en matière de sécurité des données à caractère personnel	› Organisation en matière de sécurité des données à caractère personnel (rôle du DPO ou, à défaut, référent en matière de protection des données à caractère personnel, rôle de la DSI / du RSI / du prestataire en charge des systèmes d'information,...) › Descriptif des mesures de sécurité mises en œuvre dans ce cadre (sécurité physique des locaux et des serveurs, sécurité logique, gestion des habilitations, gestion des mots de passe, modalités de sécurisation des postes de travail,...)
Sensibilisation, information, formation	› Informer et sensibiliser, diffuser une culture « protection des données à caractère personnel » au sein de chaque agence PR	Plan de formation (format (présentiel, e-learning,...) programme, fréquence, population visée, retours sur la qualité des formations, ...) et de communication interne (newsletter, quizz, intranet, ...)
Politique de conservation, d'archivage et de purge des données	› Déterminer les durées de conservation actives et les durées d'archivage nécessaires des données en fonction des finalités poursuivies	› Tableau des durées de conservation des données (actives + archives) › Moyens techniques de gestion des durées de conservation › Rôles et responsabilités des parties prenantes
Etc.		

LE SAVIEZ-VOUS ?

Pour en assurer l'effectivité et l'efficacité, les procédures, politiques et codes de bonnes pratiques élaborés dans ce cadre doivent être applicables aux membres du personnel de l'agence PR, voire à des tiers lorsque c'est opportun. **Aussi, l'opposabilité d'une telle documentation peut être assurée de la manière suivante :**

› pour ce qui concerne les membres du personnel de l'agence PR : annexion au règlement intérieur, selon le formalisme requis par le droit du travail, ou contractualisation (par exemple, par voie d'avenant aux contrats de travail en cours et implémentation en annexe des prochains contrats de travail à conclure) ;

› pour ce qui concerne les tiers : contractualisation. A titre d'illustration, l'opposabilité de la Charte d'utilisation des ressources informatiques et de communications électroniques pourrait être opportune s'agissant des utilisateurs non membres du personnel (prestataires, visiteurs, ...) mais qui accéderaient tout de même aux outils ou au système d'information de l'agence. Il en est de même s'agissant de la Charte de « traitement des données » ou du Code de bonne conduite ou de bonnes pratiques à l'égard des prestataires accédant à des données à caractère personnel dans le cadre de leurs missions.

Enfin, le recensement des traitements de données à caractère personnel mis en œuvre dans des registres dédiés et leur mise à jour (voir le paragraphe « Recenser mes traitements et réaliser mon(mes) registre(s) des traitements » ci-dessus) s'inscrit également dans cette logique d'accountability puisque ces registres ont vocation à permettre d'avoir à tout moment une cartographie précise reflétant la pratique effective s'agissant des traitements de données à caractère personnel mis en œuvre au sein de l'agence PR.

[101] Pour mémoire, voir le paragraphe « Analyser la conformité des traitements de données à caractère personnel » ci-dessus pour le détail des principes applicables en matière de protection des données à caractère personnel.

2.8 METTRE EN CONFORMITÉ MON SITE INTERNET

Le site internet d'une agence PR, même s'il ne s'agit que d'un site « vitrine » ayant vocation à présenter l'agence et son activité, peut être un vecteur permettant de collecter des données à caractère personnel, étant précisé que **l'agence PR est en principe responsable des traitements de données à caractère personnel qu'elle réalise par ce moyen.** La conformité du site internet d'une agence PR mérite une **attention particulière** et revêt un **intérêt stratégique** dans la mesure où celle-ci permet de renforcer la confiance des visiteurs s'agissant de la manière dont leurs données sont traitées par l'agence PR.

2.8.1 La conformité des traitements de données à caractère personnel opérés par ce moyen

Parmi les actions à déployer en vue de la mise et du maintien en conformité de l'ensemble des traitements concernés avec la réglementation applicable en matière de protection des données à caractère personnel, l'agence PR doit s'assurer que l'ensemble des principes applicables[101] en la matière sont respectés sur son(ses) site(s) internet. A cette fin, l'agence PR doit notamment :

- **cartographier l'ensemble des traitements** de données à caractère personnel mis en œuvre en recensant les différents supports de collecte et **identifier la finalité** poursuivie pour chacun d'entre eux (cf. principe de limitation et de légitimité des finalités) ;

(EXEMPLES)

› le formulaire de contact peut avoir vocation à permettre à l'agence PR de recueillir des données à caractère personne à des fins de gestion, de traitement et de suivi des demandes de ses contacts et de leurs échanges avec l'agence PR au moyen ou initiés via le site internet (par exemple : demande de contact, de renseignement, de proposition de services ou de documentation sur l'agence PR, sur son activité, sur ses publications, sur des événements, ...), et des relations de l'agence PR avec ses contacts (clients, prospects, journalistes, influenceurs, ...) de manière générale ;

› le formulaire d'inscription à une newsletter peut avoir vocation à permettre à l'agence PR de recueillir des données à caractère personnel en vue de la réalisation d'opérations commerciales, de prospection, de communication, de sollicitation et de marketing de l'agence PR ;

› pour ce qui concerne les formulaires d'inscription à un espace en ligne / une newsroom, le traitement de données à caractère personnel semble être mis en œuvre à des fins de gestion et de suivi des relations de l'agence PR avec ses contacts de manière générale, en ce incluant notamment la mise à disposition d'un espace réservé sur le site internet ;

› pour ce qui concerne le formulaire de candidature à une offre d'emploi, le traitement de données à caractère personnel des candidats semble mis en œuvre par l'agence PR à des fins de suivi et de traitement des candidatures et des opérations préalables au recrutement, en ce incluant l'évaluation et la sélection de candidatures et de profils professionnels.

- identifier le **fondement juridique** permettant de justifier la mise en œuvre de chaque traitement ;

(EXEMPLES)

› le traitement de données à caractère personnel opéré au moyen du formulaire de contact semble pouvoir être fondé sur les intérêts légitimes de l'agence PR à répondre aux demandes et plus généralement à assurer la gestion et le suivi de ses relations avec ses contacts ;

› le traitement de données à caractère personnel opéré au moyen du formulaire d'inscription à une newsletter est par principe soumis au recueil du consentement des personnes concernées, consentement qui doit donc pouvoir être retiré à tout moment au moyen d'une modalité simple et équivalente à celle utilisée pour recueillir le consentement ;

› le traitement de données à caractère personnel opéré au moyen de formulaires d'inscription à un espace en ligne / une newsroom semble pouvoir être fondé sur les intérêts légitimes de l'agence PR dans le cadre de la gestion et du suivi de ses relations avec ses contacts de manière générale, en ce incluant notamment la mise à disposition d'un espace réservé sur le site internet ;

› le traitement de données à caractère personnel opéré au moyen du formulaire de candidature à une offre d'emploi, semble pouvoir être fondé sur les intérêts légitimes de l'agence PR en vue de la recherche et du recrutement de possibles nouveaux collaborateurs.

- s'assurer que les données collectées ne sont pas excessives (cf. principe de **minimisation**) ;

(EXEMPLES)

› seule l'adresse email doit être collectée à des fins de prospection par email sur le formulaire de collecte d'inscription à la newsletter, toute autre information pouvant être considérée comme excessive ;

› la collecte des données suivantes dans le cadre des opérations de recrutement n'est pas pertinente, sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou par une obligation légale : numéro de sécurité sociale, informations relatives à l'entourage familial du candidat, ...

- s'assurer de **l'exactitude et de la qualité des données** ainsi collectées ;

(EXEMPLE)

› A titre d'exemple, à la suite de l'envoi d'une communication, si celle-ci n'est pas délivrée à une personne en raison d'une erreur lors de la saisie de son adresse email dans le formulaire d'inscription dédiée, une telle adresse email ne doit pas être conservée.

- vérifier que les **destinataires** de telles données sont justifiés ;

(EXEMPLE)

› A titre d'exemple, seules les personnes intervenant dans le processus de recrutement devraient pouvoir accéder aux informations d'un candidat.

- s'assurer que **les données ne sont pas conservées pendant une durée disproportionnée ;**

(EXEMPLE)

› Voir les exemples de durées de conservation issues de la doctrine de la Cnil au paragraphe « Proportionnalité de la conservation des données à caractère personnel ».

- déterminer selon quelles modalités et sur quels supports **l'information des personnes concernées** pourra être fournie lors de la collecte leurs données. Notamment, une **mention d'information doit être déployée sur chaque formulaire** de collecte avec un lien renvoyant vers une **politique de protection des données** comportant l'ensemble des informations obligatoires, étant précisé que ladite politique de protection des données doit en tout état de cause être intégrée dans une rubrique dédiée devant être accessible via un lien hypertexte inséré en footer (ou pied de page) de toutes les pages du site internet.

(EXEMPLES)

› Voir les mentions obligatoires devant figurer dans les mentions d'information telles que rappelées au paragraphe « Loyauté et transparence ».

2.8.2 Le respect des dispositions applicables en matière de dépôt / lecture de cookies et autres technologies similaires

Par ailleurs, **lorsque le site internet de l'agence PR dépose des cookies ou autres traceurs, la réglementation dite « communications électroniques et vie privée » ou « e-privacy »** doit être respectée par ladite agence PR. En effet, il convient, sauf exception, de recueillir le consentement des utilisateurs avant toute opération d'écriture ou de lecture de cookies et autres technologies similaires (ci-après « cookies »)[102].

La Cnil a adopté **ses nouvelles lignes directrices en la matière** le 4 juillet 2019[103]. Dans cette délibération, d'une part, la Cnil réaffirme le principe qui impose de recueillir le consentement de l'utilisateur avant toute action visant à inscrire ou à accéder à des informations le concernant sur un équipement terminal de communications électroniques, c'est-à-dire à inscrire ou à lire des cookies ou autres traceurs dans son terminal. D'autre part, la Cnil précise les critères et la forme que doit prendre ce consentement. Enfin, la Cnil impose aux exploitants de cookies de pouvoir prouver le recueil du consentement des utilisateurs.

Cette délibération de la Cnil n'est qu'une première étape, cette dernière ayant soumis à consultation publique le 14 janvier 2020 un **projet de recommandation** qui a vocation (i) à présenter de manière pédagogique aux professionnels, à l'aide d'exemples concrets, les modalités pratiques visant à mettre en place des solutions (cf. module de recueil du consentement et de gestion et paramétrage des cookies) conformes et valables de recueil du consentement et d'information en matière de cookies et (ii) à présenter des bonnes pratiques qui vont au-delà du simple respect de la réglementation applicable, en vue de renforcer la protection des données et l'exercice de leurs droits par les utilisateurs / internautes[104]. A toutes fins utiles, il est précisé que **les recommandations de la Cnil s'appliquent de manière indifférenciée à l'utilisation de cookies sur un site internet mais également au sein d'une application mobile.**

[102] Cf. article 82 de la Loi Informatique et libertés, lequel transpose en droit français la directive 2002/58/CE « vie privée et communications électroniques » (ou « ePrivacy »), étant précisé qu'une réforme en la matière est en cours (cf. COM/2017/010 final - 2017/03 (COD)).

[103] Cnil, Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs).

[104] Cnil, Projet de recommandation sur les modalités pratiques de recueil du consentement prévu par l'article 82 de la loi du 6 janvier 1978 modifiée, concernant les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur dit « recommandation « cookies et autres traceurs ».

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

Ce projet de recommandation était soumis à consultation publique jusqu'au 25 février 2020 mais sa version définitive n'a pas encore été publiée. Il est donc susceptible de faire l'objet d'ajustements avant d'être adopté définitivement par la Cnil réunie en séance plénière.

Il résulte des délibérations, recommandations et communications de la Cnil, à date, qu'à l'instar du consentement tel qu'il est prévu aux termes du RGPD, **le consentement en matière de cookies et autres traceurs doit être une manifestation de volonté libre, spécifique, éclairée et univoque :**

Ce consentement doit être libre : l'utilisateur ne peut pas être contraint à consentir. Aussi, il n'est pas possible de conditionner l'accès d'un utilisateur à un site internet au consentement de ce dernier à l'installation de tout ou partie des cookies auxquels on lui demande de consentir. Il convient également de s'assurer qu'aucune influence visuelle ou grammaticale ne pousse l'utilisateur à penser que donner son consentement est obligatoire pour poursuivre la navigation ou l'utilisation du service.

Ce consentement doit être spécifique : en d'autres termes, l'utilisateur doit pourvoir donner son consentement pour chaque finalité poursuivie par les cookies et non un consentement «global» (qui peut tout de même être valable s'il s'ajoute à la possibilité d'un refus «global» et d'une possibilité de consentement finalité par finalité). En pratique, soit le site internet propose dès la 1ère page du module de gestion du consentement un choix de paramétrage «finalité par finalité», soit il propose un bouton «accepter tous les cookies» ainsi qu'un bouton «paramétrer mes cookies» (devant renvoyer l'internaute sur une page lui permettant de choisir les cookies auxquels il consent, finalité par finalité) mais il se doit dans ce cas de proposer également un bouton «refuser tous les cookies» .

Ce consentement doit être éclairé : il convient de fournir aux internautes **une information claire en des termes simples et compréhensibles** sur les différentes finalités des cookies. Il convient donc de mettre en place un module de recueil du consentement et de gestion et paramétrage des cookies détaillant notamment, pour chaque type de cookies, leur finalité, l'identité du(des) responsable(s) de traitement, la durée de vie des cookies, le droit des internautes à retirer leur consentement à tout moment, mais également la portée de leur consentement (cf. indication du fait que le consentement est facultatif + durée de validité de ce consentement), etc. Et ce afin de permettre aux utilisateurs de consentir (ou non) en pleine connaissance de cause. A cet égard, il convient notamment que le module de recueil du consentement et de gestion et paramétrage des cookies renvoie à une «politique cookies» détaillant les informations précises sur les cookies et informant l'internaute sur les moyens de s'y opposer (ex : modules de tiers permettant de refuser/supprimer simplement les cookies).

Ce consentement doit être univoque : A cet égard, la Cnil précise que le consentement doit se manifester via une action positive de l'utilisateur. **La Cnil écarte d'ailleurs expressément la possibilité de recueillir valablement un consentement au moyen de la poursuite de la navigation de l'utilisateur sur le site internet (ou l'application mobile) ou d'une case pré-cochée validant le consentement de l'utilisateur.** Il en résulte que le module de recueil du consentement et de gestion et paramétrage des cookies ne doit pas comporter de cases pré-cochées ou toute autre typologie d'acceptation par défaut (sauf pour les éventuels cookies non soumis à consentement).

Il est en tout état de cause **interdit d'installer des cookies en l'absence d'un tel consentement de l'utilisateur,** sauf pour ce qui concerne les hypothèses suivantes dans lesquelles le consentement de l'internaute n'est pas nécessaire (cf. cookies dits « de fonctionnement », qui ne sont toutefois pas exemptés pour autant de l'obligation d'information des utilisateurs, par exemple dans le cadre de la « politique cookies ») :

› quand le traceur *« a pour finalité exclusive de permettre ou faciliter la communication par voie électronique »* ; ou

› quand il *« est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ».*

La Cnil donne certains exemples de cookies qui peuvent entrer dans ces catégories, sous réserve qu'ils ne soient utilisés que pour l'une ou plusieurs des finalités indiquées ci-dessous (et non pour une autre finalité soumise à consentement) :

› les traceurs conservant le choix exprimé par l'utilisateur sur le dépôt de traceurs ou la volonté de celui-ci de ne pas exprimer un choix ;

› les traceurs destinés à l'authentification auprès d'un service ;

› les traceurs destinés à garder en mémoire le contenu d'un panier d'achat sur un site marchand ;

› les traceurs de personnalisation de l'interface utilisateur (par exemple, pour le choix de la langue ou de la présentation d'un service), lorsqu'une telle personnalisation constitue un élément intrinsèque et attendu par l'utilisateur du service ;

› les traceurs permettant l'équilibrage de la charge des équipements concourant à un service de communication ;

› les traceurs permettant aux sites payants de limiter l'accès gratuit à leur contenu à une quantité prédéfinie et/ou sur une période limitée.

LE SAVIEZ-VOUS ?

Certains traceurs de mesure d'audience peuvent également être exemptés du recueil du consentement sous réserve du respect des conditions suivantes :

- ils doivent être mis en œuvre par l'éditeur du site ou bien par son sous-traitant ;

- la personne doit être informée préalablement à leur mise en œuvre ;

- elle doit disposer de la faculté de s'y opposer par l'intermédiaire d'un mécanisme d'opposition facilement utilisable sur l'ensemble des terminaux, des systèmes d'exploitation, des applications et des navigateurs web. Aucune opération de lecture ou d'écriture ne doit avoir lieu sur le terminal depuis lequel la personne s'est opposée ;

- la finalité du dispositif doit être limitée à (i) la mesure d'audience du contenu visualisé afin de permettre l'évaluation des contenus publiés et l'ergonomie du site ou de l'application, (ii) la segmentation de l'audience du site web en cohortes afin d'évaluer l'efficacité des choix éditoriaux, sans que cela ne conduise à cibler une personne unique et (iii) la modification dynamique d'un site de façon globale. Les données à caractère personnel collectées ne doivent pas être recoupées avec d'autres traitements (fichiers clients ou statistiques de fréquentation d'autres sites, par exemple) ni transmises à des tiers. L'utilisation des traceurs doit également être strictement cantonnée à la production de statistiques anonymes. Sa portée doit être limitée à un seul éditeur de site ou d'application mobile et ne doit pas permettre le suivi de la navigation de la personne utilisant différentes applications ou naviguant sur différents sites web ;

- l'utilisation de l'adresse IP pour géolocaliser l'internaute ne doit pas fournir une information plus précise que la ville. L'adresse IP collectée doit également être supprimée ou anonymisée une fois la géolocalisation effectuée ;

- les traceurs utilisés par ces traitements ne doivent pas avoir une durée de vie excédant treize mois et cette durée ne doit pas être prorogée automatiquement lors des nouvelles visites. Les informations collectées par l'intermédiaire des traceurs doivent être conservées pendant une durée de vingt-cinq mois maximum).

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

Au regard de ce qui précède, il appartient à chaque agence PR de déployer les actions suivantes :

- **identifier, avec l'aide du webmaster le cas échéant, l'ensemble des cookies** utilisés sur son site internet ;
- **déterminer la catégorie à laquelle chaque cookie doit être affecté** (afin de déterminer si son installation est ou non soumise au consentement préalable de l'internaute), à savoir :
  - cookie dit « de fonctionnement », seule catégorie de cookies dont l'installation est exemptée du consentement ;
  - cookie de mesure d'audience ;
  - cookie d'interaction ou de réseau social ;
  - cookie publicitaire ;
  - etc.
- **déployer un module de paramétrage des cookies**

FOCUS SUR LE MODULE DE RECUEIL DU CONSENTEMENT ET DE GESTION ET DE PARAMÉTRAGE DES COOKIES

Lors de l'élaboration et du déploiement du module de recueil du consentement et de gestion et de paramétrage des cookies, il convient de respecter les principes suivants :

- **l'affichage de ce module doit être, techniquement, réalisé lors de toute première visite d'un internaute sur le site internet** (quelle que soit la page du site qu'il affiche en première intention) ;
- **le consentement de ce dernier ne peut être valable que pendant une période qui doit être déterminée au regard du contexte, de la portée du consentement initial et des attentes de l'utilisateur,** la Cnil préconisant dans son projet de recommandation une **durée de validité de 6 mois maximum** à l'issue de laquelle le module devra s'afficher de nouveau pour « re-demander » le consentement de l'internaute (pendant cet intervalle, si de nouveaux cookies ont vocation à être utilisés, ils ne pourront pas l'être, même pour les internautes ayant consenti à certains cookies, en l'absence d'obtention d'un nouveau consentement pour ces nouveaux cookies) ;
- **en cas de refus de consentement par l'utilisateur, alors son choix doit être enregistré** de manière à ne pas le solliciter à nouveau, pendant un certain laps de temps (et ce afin d'éviter une « pression continue » lors des prochaines visites du site internet par cet utilisateur, pression qui serait selon la Cnil susceptible de pousser l'utilisateur à accepter les cookies par lassitude), **ce laps de temps devant être au moins identique à celui pour lequel le consentement est enregistré, soit 6 mois ;**
- il est également possible de laisser à l'internaute la possibilité de retarder son choix (par exemple en lui laissant la possibilité de fermer le module avec une « croix » ou au moyen d'un clic en dehors du module). Dans une telle hypothèse, **si l'internaute décide de « retarder son choix »,** alors le module de recueil du consentement et de gestion et paramétrage des cookies pourra à nouveau s'afficher lors de sa prochaine visite sur le site internet, l'internaute pouvant être sollicité de nouveau tant qu'il n'exprime pas de choix. Bien entendu, il convient de s'assurer que, si l'utilisateur « retarde son choix » pour tout ou partie des cookies, alors les cookies soumis à consentement pour lesquels l'internaute n'a fait aucun choix ne s'installent pas (l'utilisateur devant en effet dans cette hypothèse être considéré comme ayant souhaité retarder son choix et donc comme n'ayant pas accepté le dépôt / la lecture des cookies) ;
- **il convient également que le module de recueil du consentement et de gestion et de paramétrage des cookies soit accessible via un lien hypertexte inséré en footer** (ou pied-de-page) de toutes les pages du site internet pour que l'utilisateur puisse aisément modifier ses préférences, et notamment retirer son consentement à tout moment. Pour mémoire, la Cnil recommande que la mise en place de *« solutions conviviales […] pour que les personnes puissent retirer leur consentement aussi facilement qu'elles ont pu le donner »* ;
- **le consentement recueilli sur un site internet peut être valable pour d'autres sites si, et seulement si, la liste de la totalité des sites concerné est fournie** à l'utilisateur, accessible à partir du premier niveau d'information dans le module, étant précisé qu'il conviendrait également dans une telle hypothèse de proposer à l'internaute la possibilité d'accepter / de refuser par site concerné.

En pratique, aux termes du projet de recommandation de la Cnil précité, **un certain nombre d'informations doivent être communiquées à l'utilisateur dès le premier niveau d'information (cf. 1er écran du module),** à savoir :

- **les finalités poursuivies :** la Cnil recommande que soit présentée à l'utilisateur chacune des finalités des cookies, **au moyen d'un intitulé court et mis en évidence accompagné d'un bref descriptif,** et ce avant que celui-ci puisse consentir ou non à leur utilisation. A cet égard, la Cnil précise qu'une description plus détaillée peut être rendue disponible en cliquant sur un lien hypertexte (renvoyant par exemple vers les paragraphes concernés de la « Politique cookies » et de la « Politique de protection des données » en ligne) présent au premier niveau

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

d'information. Une telle description peut également être affichée sous un bouton de déroulement que l'utilisateur doit pouvoir activer directement au premier niveau d'information, étant précisé qu'en pareille hypothèse, il conviendra tout de même également **de renvoyer à la « Politique cookies » (détaillant les finalités des cookies, leur durée de vie,…) et à la « Politique de protection des données » en ligne (étant précisé que cette dernière doit comporter l'ensemble des informations sur les traitements de données à caractère personnel mis en œuvre au moyen des cookies,** à savoir les finalités mais également les informations sur les destinataires des données collectées par ce moyen, les durées de conservation de ces données, si possible les catégories de données collectées, etc. conformément à la réglementation applicable en matière de protection des données à caractère personnel) ;

- **l'identité du(des) responsables de traitement :** selon la Cnil, il convient d'informer les utilisateurs, en complément de la liste des finalités présentées sur le premier écran, de la liste de l'ensemble des responsables de traitement. Cette information peut être réalisée depuis le premier niveau d'information via un lien hypertexte ou un bouton dédié. La Cnil souligne qu'il convient d'utiliser une dénomination descriptive et des termes clairs pour les internautes (par exemple, selon la Cnil, en utilisant une formulation telle que **« liste des sociétés utilisant des traceurs sur notre site », cette liste pouvant s'ouvrir en 2ème écran,** devant si possible regrouper lesdites sociétés en fonction de leur activité et de la finalité des traceurs utilisés, et devant contenir l'identité de ces sociétés ainsi que les cookies utilisés par chacune et **un lien vers leurs politiques de confidentialité** respectives, étant précisé qu'il est recommandé si possible à titre de bonne pratique sur le premier niveau d'information d'intégrer le nombre de sociétés tierces utilisant des cookies). Cette liste, qui peut donc être incluse dans la « Politique cookies » ou la « Politique de protection des données » en ligne lorsque des données à caractère personnel sont collectées par ce moyen (mais avec un renvoi direct au paragraphe concerné depuis l'écran de premier niveau), doit être mise à jour régulièrement, à chaque modification, en identifiant si possible toute modification avec un code couleur par exemple ou une animation spécifique ;
- **la portée du consentement de l'internaute :** il convient d'informer l'internaute le cas échéant du fait que son consentement est valable pour le suivi de sa navigation sur d'autres sites que ceux depuis lesquels son consentement est recueilli. Dans une telle hypothèse, une liste des sites / applications concernés devra être rendue accessible à l'utilisateur depuis ce premier niveau d'information. En toute hypothèse, il convient également d'indiquer **la durée de validité de son consentement et de spécifier le caractère facultatif de celui-ci.**

Par ailleurs, l'éditeur du site peut offrir une **faculté de consentir de manière globale à l'utilisation de tous les cookies soumis à consentement sur ledit site internet, sous réserve qu'il offre également une faculté de refuser de consentir de manière globale également.** A cet égard, la Cnil précise dans son projet de recommandation qu'*« il est possible de proposer des boutons d'acceptation et de refus globaux via par exemple la présentation de boutons intitulés « tout accepter » et « tout refuser », « j'autorise » et « je n'autorise pas », « j'accepte tout » et « je n'accepte rien » ou encore « je donne mon accord pour toutes les finalités » et « je ne donne pas mon accord » permettant à l'utilisateur de consentir ou de refuser, en une seule action, à plusieurs finalités ».*

S'agissant de l'obligation pour l'éditeur du site de permettre à l'internaute d'effectuer son choix finalité par finalité (cf. caractère spécifique du consentement), deux options sont envisageables :

- permettre à l'utilisateur d'accepter / de refuser les cookies finalité par finalité directement sur le premier niveau d'information (cf. 1er écran), par exemple au moyen d'un « slider » ou d'une case à cocher ou d'un bouton sous chaque finalité (ces fonctionnalités devant être à « non » ou à « refuser » par défaut, et non pré-cochées pour ce qui concerne la case à cocher) ; ou

- permettre à l'utilisateur d'« Accepter tous les cookies » ou de « Refuser tous les cookies », sous réserve qu'un bouton de type « Personnaliser mes choix en matière de cookies » (permettant à l'internaute d'ouvrir un 2ème écran afin de faire un choix finalité par finalité) soit proposé au même niveau que les deux autres boutons « Accepter tous les cookies » et « Refuser tous les cookies », et à condition que soit utilisée une police d'écriture de même taille, offrant la même facilité de lecture, et que ces boutons soient mis en évidence de manière identique.

Si possible, la Cnil recommande de laisser la possibilité à l'internaute d'accepter / refuser une par une les sociétés utilisant des traceurs sur le site (cf. fonctionnalité à intégrer par exemple dans la « liste des sociétés utilisant des traceurs sur notre site »).

Pour des exemples de « copies écrans » de mise en œuvre, il convient de se reporter un projet de recommandation de la Cnil.

En outre, il convient de mettre en œuvre des mécanismes permettant de rapporter la preuve du recueil du consentement des utilisateurs ainsi recueilli le cas échéant, notamment permettant à cette fin :

- de rapporter une **preuve individuelle du recueil du consentement** pour chaque utilisateur (par exemple, à l'aide d'un cookie spécifique permettant de conserver les choix exprimés par l'utilisateur et les informations nécessaires s'y rapportant) ; et
- de rapporter une **preuve de validité globale du consentement** en démontrant que le mécanisme déployé est conforme à la réglementation applicable en la matière (par exemple, par une mise sous séquestre auprès d'un tiers du code informatique utilisé par l'éditeur du site, pour les différentes versions de son site, une capture d'écran du rendu visuel affiché sur un terminal mobile ou bureau peut être conservée pour chaque version du site internet ; ou encore la mise en place d'audits réguliers des mécanismes de recueil du consentement mis en œuvre par les sites depuis lesquels il a été recueilli).

Bien entendu, l'obligation de prouver le consentement ne déroge pas au principe de minimisation des données. **Seules les données nécessaires à la preuve du consentement doivent être collectées.**

En outre, **si certains traitements de données à caractère personnel réalisés au moyen de l'utilisation de cookies sont soumis au consentement des personnes concernées** (cf. hypothèses de recueil du consentement visées au paragraphe « Licéité du traitement et hypothèses de consentement obligatoire » ci-dessus), **il conviendrait que ce module permette de recueillir de manière plus large le consentement à ces traitements** de la part des personnes concernées, et comporte donc également l'ensemble des mentions d'informations obligatoires au titre de la réglementation applicable en matière de protection des données à caractère personnel (sur ce point, voir le tableau « Informations générales à fournir » dans le paragraphe « Loyauté et transparence » ci-dessus).

FOCUS SUR LES PAGES DE L'AGENCE PR SUR LES RÉSEAUX SOCIAUX

Les principes et précautions susvisés s'agissant du site internet de l'agence PR doivent être déclinés sur les pages de l'agence PR sur les réseaux sociaux. Aussi, **il convient de s'assurer, pour chacune des pages de l'agence PR, qu'une mention d'information conforme à la réglementation applicable et renvoyant via un lien hypertexte à la politique complète de protection des données en ligne de l'agence PR est fournie aux visiteurs sur la page de l'agence PR** (par exemple, dans la rubrique « A propos » sur Facebook).

En outre, s'agissant des pages entreprises sur les réseaux sociaux, la Cour de Justice de l'Union européenne a considéré que **l'administrateur d'une page « fan » sur Facebook est conjointement responsable avec Facebook du traitement des données des visiteurs de sa page mis en œuvre par Facebook** dans la mesure où notamment, en créant la page, l'administrateur offre à Facebook la *« possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan, que cette personne dispose ou non d'un compte Facebook »*[105]. Les traitements de données dans cette affaire visaient notamment à permettre d'une part à Facebook d'améliorer son système de publicité et d'autre part à l'administrateur d'obtenir des statistiques sous une forme anonymisée à des fins de « gestion de la promotion de son activité ».

La Cour a relevé que **l'administrateur de ladite page disposait d'une influence sur le traitement du fait de son action de paramétrage** (cf. détermination de l'audience cible et des objectifs poursuivis ou encore détermination des critères de réalisation des statistiques). La Cour a également rappelé que, **bien que les statistiques d'audience établies par Facebook étaient transmises à l'administrateur de la page « fan » uniquement sous une forme anonymisée, l'établissement de ces statistiques reposait sur la collecte préalable, au moyen de cookies installés par Facebook, et le traitement des données à caractère personnel de ces visiteurs à de telles fins statistiques.** Elle en a conclu qu'*« il y a lieu de considérer que l'administrateur d'une page fan hébergée sur Facebook [...] participe, par son action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan ». Par conséquent, « cet administrateur doit être, en l'occurrence, qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland, de ce traitement ».*

Pour mémoire, l'éditeur d'un site internet intégrant un plug-in Facebook (cf. bouton « J'aime ») sur ledit site est également considéré comme étant conjointement responsable avec Facebook, des opérations de collecte et de communication par transmission des données à caractère personnel des visiteurs de son site internet. Voir également les conséquences d'une telle qualification au paragraphe « Relations entre responsables conjoints du traitement » ci-dessus.

[105] CJUE, aff. C-210/16, 5 juin 2018.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

LE SAVIEZ-VOUS ?

Bien qu'il ne s'agisse pas stricto sensu d'une problématique relative à la protection des données à caractère personnel, il appartient à chaque agence PR d'intégrer sur son site internet des **« mentions légales »** dans une rubrique dédiée devant être accessible via un lien hypertexte inséré en footer (ou pied de page) de toutes les pages du site internet.

Ces « mentions légales » doivent comporter les informations suivantes[106] :

- si le site internet est édité par une personne physique : nom, prénom, domicile et numéro de téléphone et, si assujettie, numéro RCS ou numéro d'inscription au répertoire des métiers (sous réserve de la possibilité pour toute personne physique de préserver son anonymat en indiquant uniquement le nom, la dénomination sociale et l'adresse de l'hébergeur de son site internet, à condition d'avoir communiqué à ce dernier ses éléments d'identification personnelle) ;
- si le site internet est édité par une personne morale : dénomination ou raison sociale, siège social, numéro de téléphone et, si assujettie, numéro RCS ou numéro d'inscription au répertoire des métiers et capital social ;
- nom du directeur ou du codirecteur de la publication ;
- nom, dénomination ou raison sociale et coordonnées (adresse postale et numéro de téléphone) de l'hébergeur du site internet.
- adresse de courrier électronique de l'agence PR ;
- numéro de TVA intracommunautaire de l'agence PR ;
- si l'activité de l'agence PR est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ;
- si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'Etat membre dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite.

L'absence de fourniture ou l'incomplétude de ces mentions est passible de sanctions pénales pouvant atteindre un an d'emprisonnement et 75 000 € d'amende (cette amende pouvant être portée au quintuple, soit 375 000 €, si la responsabilité pénale de la personne morale est retenue).

Outre ces éléments, les informations suivantes doivent également être fournie[107]:

- si l'agence PR est en état de liquidation ;
- si l'agence PR est une société commerciale dont le siège est à l'étranger, sa dénomination, sa forme juridique et le numéro d'immatriculation dans l'Etat où elle a son siège, s'il en existe un ;
- si l'agence PR a la qualité de locataire-gérant ou de gérant-mandataire ;
- si l'agence PR est bénéficiaire d'un contrat d'appui au projet d'entreprise pour la création ou la reprise d'une activité économique, la dénomination sociale de la personne morale responsable de l'appui, le lieu de son siège social, ainsi que son numéro unique d'identification ;
- si l'agence PR a constitué un patrimoine affecté en tant qu'entrepreneur individuel, l'objet de l'activité professionnelle à laquelle le patrimoine est affecté et la dénomination utilisée pour l'exercice de l'activité professionnelle incorporant son nom ou nom d'usage précédé ou suivi immédiatement des mots : «entrepreneur individuel à responsabilité limitée» ou des initiales : «EIRL» ;
- la forme sociale de l'agence PR, en toutes lettres (et non sous forme d'abréviation).

Toute contravention aux dispositions des alinéas précédents est punie de l'amende prévue pour les contraventions de la 4e classe, à savoir d'un montant pouvant s'élever jusqu'à 750 € (cette amende pouvant être portée au quintuple, soit 3 750 €, si la responsabilité pénale de la personne morale est retenue, étant rappelé que les amendes contraventionnelles peuvent se cumuler).

[106] Cf. articles 6, III et 19 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite « LCEN ».
[107] Cf. articles R.123-237 et R.123-238 du Code de commerce.

2.9
SAVOIR RÉAGIR EN CAS DE CONTRÔLE DE LA CNIL

La Cnil a notamment pour mission de contrôler l'application de la réglementation applicable en matière de protection à données à caractère personnel et de veiller au respect de celle-ci[108].

Dans ce cadre, la Cnil dispose notamment des **pouvoirs d'enquête** suivants :

- ordonner la communication de toute information dont elle a besoin pour l'accomplissement de ses missions ;
- procéder à des audits sur la protection des données à caractère personnel ;
- procéder à un examen des certifications délivrées ;
- notifier au responsable de traitement ou au sous-traitant une violation alléguée de la réglementation applicable en matière de protection des données à caractère personnel ;
- obtenir l'accès à toutes les données à caractère personnel et informations nécessaires à l'accomplissement de ses missions ;
- obtenir l'accès à tous les locaux, notamment à toute installation et à tout moyen de traitement[109].

Ces pouvoirs d'enquêtes incluent donc la possibilité d'effectuer des **contrôles** auprès de tout organisme traitant des données à caractère personnel.

Les contrôles peuvent être réalisés par la Cnil **sur sa propre initiative ou encore à la suite d'une réclamation** d'une personne concernée par exemple et peuvent se dérouler de la manière suivante :

- **sur place :** des agents de la Cnil se rendent directement au sein des locaux d'un responsable de traitement ou d'un sous-traitant afin de mener des investigations portant sur des traitements de données à caractère personnel ;
- **sur pièces :** des agents de la Cnil adressent un courrier accompagné d'un questionnaire destiné à évaluer la conformité des traitements mis en œuvre par un responsable de traitement ou un sous-traitant. Il appartient à l'organisme contrôlé de répondre à la Cnil en y joignant tout document utile permettant de les justifier ;
- **sur audition :** un courrier est adressé au responsable de traitement ou au sous-traitant afin que des représentants de l'organisme se présentent, à une date donnée, dans les locaux de la Cnil. Ces représentants devront répondre à des questions portant sur le(s) traitement(s) objet des vérifications et, le cas échéant, rendre possible un accès aux ressources informatiques de l'organisme contrôlé ;
- **en ligne :** des agents de la Cnil effectuent des vérifications, depuis les locaux de la Cnil, en consultant notamment des données librement accessibles ou rendues accessibles directement en ligne, y compris par imprudence, négligence ou du fait d'un tiers. Ces vérifications sont effectuées à partir d'un service de communication au public en ligne (par exemple, sur un site internet, une application mobile ou un produit connecté) et peuvent, le cas échéant, être réalisées sous une identité d'emprunt.

Ces types de contrôle peuvent être utilisés de manière complémentaire.

(ILLUSTRATION)

A titre d'illustration, la Cnil pourra initier ses vérifications en ligne et les poursuivre sur place. Un contrôle sur pièces pourra également être opéré préalablement à un contrôle sur place.

LE SAVIEZ-VOUS ?

Pour ce qui concerne les contrôles sur place, **il n'existe aucune obligation à la charge des agents de la Cnil de prévenir un responsable de traitement ou un sous-traitant préalablement à leur arrivée sur place.** Il en est de même pour les contrôles réalisés par les agents de la Cnil en ligne.

Dans le cadre des contrôles qu'elle réalise, **la Cnil peut demander communication de tous documents nécessaires, quel qu'en soit le support, et en prendre copie.** Les agents de la Cnil peuvent notamment accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle[110].

[108] Cf. article 57 du RGPD et article 8 de la Loi Informatique et libertés.
[109] Cf. article 58 du RGPD.
[110] Cf. article 19 de la Loi Informatique et libertés.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

LE SAVIEZ-VOUS ?

Le secret des informations ou documents auxquels les agents de la Cnil peuvent souhaiter avoir accès ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, ou par le secret des sources des traitements journalistiques. Un régime spécifique est également prévu s'agissant des données protégées par le secret médical.

En outre, **les agents de la Cnil peuvent s'entretenir avec tout personnel susceptible de détenir des informations utiles pour apprécier la conformité des traitements de données à caractère personnel** (par exemple, échanger avec un chef de service, un opérationnel, un informaticien, ...).

FOCUS SUR L'ATTITUDE À ADOPTER EN CAS DE CONTRÔLE DE LA CNIL

Quel que soit le type de contrôle réalisé, tout collaborateur qui aurait connaissance d'un tel contrôle (réception d'une convocation de la Cnil, arrivée d'agents de la Cnil à l'accueil, ...) **doit immédiatement en avertir son responsable hiérarchique ainsi que le DPO ou, à défaut, le référent en matière de protection des données à caractère personnel.** Il pourra également être fait appel à un conseil externe (par exemple, avocat) pour assister à ce contrôle.

En tout état de cause, chacun des collaborateurs doit être préparé à un tel contrôle et se doit de **coopérer avec les agents de la Cnil** en charge de ce contrôle[111]. En effet, le fait **de s'opposer au contrôle, de refuser de communiquer des renseignement, documents, données, informations,...** demandées par la Cnil et nécessaires à sa mission ou encore de **communiquer des informations** non conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée **ou qui ne présentent pas ce contenu sous une forme directement accessible constitue un délit d'entrave,** puni d'un an d'emprisonnement et de 15 000 euros d'amende (amende pouvant être portée au quintuple (soit 75 000 euros) si la responsabilité pénale de la personne morale est retenue)[112]. Ce devoir de coopération des personnes interrogées dans le cadre d'un contrôle se manifeste en pratique par l'obligation de répondre aux questions et demandes des agents de la Cnil et l'interdiction de dissimuler des informations demandées expressément par les agents de la Cnil.

De manière générale, il est recommandé d'élaborer et de déployer une **procédure interne visant à expliciter de manière pédagogique aux collaborateurs de l'agence PR les bonnes pratiques à adopter en cas de contrôle de la Cnil.**

A l'issue du contrôle, un procès-verbal est établi par les agents de la Cnil et fait état de toutes les informations recueillies par ces derniers et de leurs constations. Il recense également en annexe tous les documents qui ont été copiés dans le cadre du contrôle, et peut dans certains cas contenir une liste de documents ou informations à communiquer à la Cnil par l'organisme contrôlé dans un délai donné.

Les suites du contrôle varient en fonction des constations effectuées. Ainsi, :

- **en l'absence d'observations particulières,** la procédure de contrôle est clôturée par un courrier du Président de la Cnil ;
- si des pratiques de l'organisme contrôlé sont constitutives de **manquements peu significatifs,** la procédure de contrôle est **clôturée** par un courrier du Président de la Cnil accompagné **d'observations** (ex : demande de modification des durées de conservation, d'implémentation de mesures de sécurité, de procéder à l'information des personnes, etc.) ;
- si des **manquements plus significatifs** sont caractérisés, le Président de la Cnil peut décider de **mettre en demeure l'organisme contrôlé d'adopter des mesures, dans un délai imparti, pour se mettre en conformité et/ou transmettre le dossier à la formation restreinte de la Cnil** (cf. formation contentieuse de la Cnil) **qui pourra prononcer des sanctions administratives**[113]. La mise en demeure peut, dans certaines hypothèses (ex : en raison d'un nombre important de personnes concernées, de l'impact sur la vie privée des personnes concernées, ...), être **rendue publique** (étant précisé que dans une telle hypothèse, la clôture qui interviendrait éventuellement devrait également être rendue publique), de même que les sanctions administratives prononcées par la formation restreinte le cas échéant ;
- **en cas d'absence de réponse à la mise en demeure ou de non-respect de ses injonctions,** le dossier peut également être transmis à la **formation restreinte de la Cnil qui peut prononcer des sanctions administratives**[114]**;**
- en tout état de cause, la transmission du dossier à la formation restreinte de la Cnil n'est pas exclusive d'une dénonciation au Parquet par les services de la Cnil en vue de l'ouverture d'une procédure pénale.

[111] Cf. article 31 du RGPD qui impose une obligation de coopération avec la Cnil au responsable de traitement ou au sous-traitant et, le cas échéant, à leurs représentants, un manquement à une telle obligation pouvant être sanctionné par la Cnil (Cnil, Délibération de la formation restreinte n°SAN-2019-010 du 21 novembre 2019 concernant la société FUTURA INTERNATIONALE).
[112] Cf. article 226-22-2 du Code pénal.
[113] Pour mémoire, voir le paragraphe « Le RGPD : enjeux et opportunités » s'agissant des sanctions pouvant être prononcées par la Cnil.
[114] Idem.

PUBLIC CIBLE : DIRECTION, SERVICE JURIDIQUE

FOCUS SUR LES ACTIONS À DÉPLOYER À LA SUITE D'UN CONTRÔLE DE LA CNIL

Tout organisme traitant des données à caractère personnel se doit d'**anticiper** et d'être à même de **réagir immédiatement après un éventuel contrôle de la Cnil qui révélerait des manquements.** En outre, si un contrôle de la Cnil devait aboutir à une sanction à l'égard d'une agence PR, il convient de garder à l'esprit que **la proactivité et le délai d'intervention** de celle-ci pour remédier aux manquements, et plus généralement **sa bonne coopération,** sont des **critères qui seraient pris en compte** dans le cadre du prononcé de la sanction, a minima s'agissant de la détermination de son montant[115].

Ainsi, à la suite d'un contrôle de la Cnil, il est indispensable de **déployer immédiatement les actions suivantes :**

- analyser le procès-verbal établi par la Cnil à l'issue du contrôle et faisant état de toutes les informations recueillies par les agents de la Cnil et des constatations qu'ils ont réalisées ;
- communiquer à la Cnil, dans les délais impartis, les éventuels documents et informations complémentaires qui pourraient être demandés par cette dernière dans le procès-verbal ;
- identifier les éventuels manquements qui pourraient être relevés / caractérisés, ainsi que les solutions de correction à mettre en œuvre pour y mettre fin sans délai ;
- documenter les nouvelles mesures ainsi déployées (par exemple, en mettant à jour la politique de sécurité des données à caractère personnel, en procédant à la purge des données obsolètes, en déployant de nouvelles mentions d'information, ...) ;
- vérifier de manière régulière la mise en œuvre de ces nouvelles mesures afin de s'assurer de leur effectivité et de leur efficacité.

[115] Cf. article 83 du RGPD.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

3.1
BONNES PRATIQUES EN MATIÈRE DE COLLECTE DES DONNÉES

3.1.1 Les règles d'or : transparence, loyauté et minimisation

Pour mémoire, la réglementation applicable en matière de protection des données à caractère personnel doit être respectée par tout agence PR traitant des informations se rapportant à une personne physique identifiée ou identifiable, **y compris lorsque cette personne est un professionnel. En effet, ladite réglementation n'opère aucune distinction selon que la personne concernée dont les données sont traitées est ou non un professionnel ou un consommateur.**

Aussi, dans le cadre de leur activité de conseil en relations publics, **les agences PR doivent veiller au respect de tous les principes applicables** en la matière tels que présentés au paragraphe « Analyser la conformité des traitements de données à caractère personnel » ci-dessus.

Une nuance tout de même : **lorsque l'agence PR agit en qualité de sous-traitant, il appartient au responsable de traitement de lui communiquer l'ensemble de ses instructions** visant à permettre à l'agence PR de mettre en œuvre le traitement concerné dans des conditions et selon des modalités conformes aux principes applicables en matière de protection des données à caractère personnel (à titre d'exemple, le responsable de traitement doit indiquer à l'agence PR les catégories de données qu'il convient de traiter, ou encore si l'agence PR est tenue de collecter les données à caractère personnel pour le compte du responsable de traitement, il appartient à ce dernier de communiquer l'ensemble des mentions d'information, voire de recueil du consentement, à l'attention des personnes concernées).

Pour autant, **en cas de non-conformité des instructions données à l'agence PR par le responsable de traitement au regard de la réglementation applicable en matière de protection des données à caractère personnel, et notamment des principes applicables en la matière, l'agence PR doit en alerter immédiatement ce dernier.**

Les paragraphes ci-après ont vocation à présenter aux agences PR les bonnes pratiques qui pourraient être opportunément déployées s'agissant en particulier des principes de loyauté et de transparence du traitement ainsi que de minimisation des données, ces principes étant particulièrement prégnants dans le cadre de l'activité des agences PR, étant bien entendu rappelé que le respect des autres principes applicables en la matière demeure évidemment requis.

3.1.2 Les différents types de personnes concernées et les modalités de collecte / d'information

Pour mémoire, chaque agence PR doit s'assurer que les données qu'elle traite concernant ses contacts, à savoir influenceurs, journalistes, Key Opinion Leaders (experts, hommes politiques,...), clients ou prospects, etc. ont été collectées de manière loyale et transparente : il s'agit de faire en sorte que les personnes dont les données sont traitées soient informées des caractéristiques et modalités du traitement de leur données à caractère personnel.

A cet égard, il est rappelé que l'information fournie doit comporter l'ensemble des éléments obligatoires tels que présentés dans le tableau « Informations générales à fournir » au paragraphe « Loyauté et transparence » ci-dessus. A défaut d'information des personnes concernées conforme à la réglementation applicable en matière de protection des données à personnel, le traitement de leurs données à caractère personnel est en principe illicite (sauf exceptions qui doivent faire l'objet d'une interprétation stricte).

Aussi, il est proposé ci-après à titre indicatif des recommandations permettant de déterminer sur quel support et selon quelles modalités les contacts des agences PR devraient être informés s'agissant du traitement de leurs données à caractère personnel.

3.1.2.1 Les journalistes

Il doit être fourni aux journalistes dont les données à caractère personnel sont traitées une information conforme à la réglementation applicable en matière de protection des données à caractère personnel. A cette fin, il convient d'identifier de manière exhaustive les sources et modalités de collecte des données les concernant afin de déterminer selon quelles modalités et sur quels supports l'information des journalistes pourra être fournie, de manière complète, lors de la collecte des données (sauf dans le cas où il est possible de se fonder sur l'une des exceptions à l'obligation d'information, présentées au sein du paragraphe « Loyauté et transparence » ci-dessus).

PUBLIC CIBLE : DIRECTION, MANAGERS PR

(ILLUSTRATION)

A titre d'illustration, des données à caractère personnel relatives aux journalistes sont susceptibles d'être collectées auprès des journalistes concernés eux-mêmes, lorsque ces derniers prennent contact avec l'agence PR par exemple sur le site internet de ladite agence PR ou lors d'un événement par exemple (cf. collecte directe) mais également sur des sites internet de tiers (ex : annuaires professionnels) ou encore au moyen de bases de données ou de fichiers presse de tiers (cf. collecte indirecte).

Quelle que soit la manière dont les données d'un journaliste sont collectées, celui-ci doit, en principe, être dûment informé du traitement des données à caractère personnel le concernant.

Ainsi :

- **lorsque les données sont collectées directement auprès d'un journaliste,** celui-ci doit être informé du traitement de ses données au moment où celles-ci sont collectées, par exemple de la manière suivante :

FORMULAIRE PAPIER DE COLLECTE DE DONNÉES

- Mention d'information sur le support de collecte (par exemple un formulaire à remplir par les journalistes lors d'un évènement) + sur un document complémentaire (préalable ou concomitant) comportant l'intégralité des informations requises (si l'information figurant sur le formulaire est «allégée»)

FORMULAIRE EN LIGNE DE COLLECTE DE DONNÉES, SUR LE SITE INTERNET DE L'AGENCE PR

- Mention d'information sur le support de collecte + renvoi vers une rubrique du site internet de l'agence PR comportant sa politique complète de protection des données en ligne (si l'information figurant sur le formulaire est «allégée»)

DANS UN CONTEXTE PROFESSIONNEL, PAR VOIE ORALE EN PRÉSENTIEL, PAR EXEMPLE DANS LE CADRE D'UN ÉVÈNEMENT, OU PAR TÉLÉPHONE

- Information orale du journaliste par la personne collectant de telles données concomitamment à ladite collecte. Néanmoins, pour des raisons probatoires, un tel mécanisme d'information par oral n'est pas suffisant et il est recommandé de fournir au journaliste concerné une mention d'information écrite appropriée, par exemple en intégrant une mention d'information complète dans un email dédié ou en adressant un email comportant en footer / pied de page / dans le pavé de signature une mention éventuellement allégée et renvoyant (i) vers une politique complète de protection des données en pièce jointe et/ou (ii) par un lien hypertexte à cette même politique en ligne (cf. rubrique dédiée)

PUBLIC CIBLE : DIRECTION, MANAGERS PR

(EXEMPLE)

Exemple de mention d'information « complète » pouvant être intégrée par exemple dans les emails à destination des journalistes (et plus généralement des contacts professionnels) s'agissant de l'utilisation de leurs coordonnées professionnelles [modèle « type » à adapter bien entendu au regard de la pratique effective et des caractéristiques particulières de chaque traitement mis en œuvre par l'agence PR agissant en qualité de responsable de traitement] :

[dénomination de l'agence PR qui agit en qualité de responsable de traitement], en qualité responsable du traitement, traite des données à caractère personnel vous concernant dans le cadre de son activité de conseil en relations publics et de la constitution de fichiers presse, en vue [à déterminer / préciser / compléter, par exemple : de la gestion et du suivi de ses relations avec ses contacts professionnels (journalistes, contacts presse,...), en ce incluant notamment la réalisation d'opérations commerciales, de communication et de marketing, par tout moyen et en particulier par email (notamment [à préciser : ciblage, prospection / sollicitation commerciale et personnalisation des contenus, diffusion de communiqués de presse, envoi de newsletters ou d'actualités, invitations à participer à des évènements, envoi de cartes de vœux,...]).

La plupart de ces informations sont collectées directement auprès de vous. Certaines informations (à savoir : [à détailler]) peuvent toutefois être collectées de manière indirecte [indiquer la source : par exemple au moyen de sources d'informations publiques telles que le site internet de la société pour laquelle vous travaillez,...].

Un tel traitement de vos données à caractère personnel est fondé sur la poursuite de nos intérêts légitimes à assurer la gestion et le suivi de nos relations avec nos contacts professionnels dans le cadre de notre activité de conseil en relations publics.

Les données collectées dans ce cadre sont obligatoires pour la poursuite de la finalité précitée qui, à défaut, ne pourrait pas être atteinte. Toutefois, le traitement de ces informations pour la présente finalité est strictement facultatif et vous pouvez vous y opposer à tout moment, et sans avoir à justifier d'un quelconque motif, sur simple demande aux coordonnées précisées ci-dessous.

Les données vous concernant sont destinées [à compléter avec les destinataires des données : membres de notre personnel habilités à en avoir connaissance, clients, partenaires et prestataires pouvant être amenés à intervenir dans le cadre de la réalisation des finalités susvisées,...].

Vos données pourront être conservées par nos soins en base active pendant [à compléter]. A l'issue de cette durée, lesdites données seront conservées sous forme d'archives pendant [à compléter].

Conformément aux dispositions applicables en matière de protection des données à caractère personnel, vous bénéficiez d'un droit d'interrogation, d'accès, de rectification et d'effacement de vos données, ainsi que du droit d'obtenir la limitation de leur traitement et d'un droit d'opposition (au traitement de vos données, ainsi qu'à la prospection notamment commerciale), dans les conditions et limites posées par la réglementation applicable en matière de protection des données à caractère personnel. Vous disposez également du droit de définir des directives relatives au sort de vos données à caractère personnel et à la manière dont vous souhaitez que vos droits soient exercés après votre décès. Ces droits s'exercent par courrier postal à l'adresse suivante : [à compléter] ou par email à l'adresse suivante : [à compléter avec une adresse email, étant précisé qu'il serait opportun d'avoir une adresse email dédiée à la réception de telles demandes]. Vous disposez en tout état de cause de la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (« Cnil ») si vous estimez que le traitement de vos données n'est pas effectué conformément aux dispositions légales et réglementaires applicables.

Pour en savoir plus sur le traitement de vos données à caractère personnel et vos droits associés, vous êtes invité(e) à prendre connaissance de notre « Politique de protection des données à caractère personnel » [insérer un lien vers ladite politique sur le site internet du responsable de traitement].

- **lorsque les données d'un journaliste sont collectées indirectement,** celui-ci doit, en principe, être informé du traitement de ses données dans un délai raisonnable après obtention desdites données (ne dépassant pas un mois) ou, si les données doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec cette dernière ou encore, s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Cette information pourra par exemple être fournie au journaliste par l'agence PR en intégrant une mention d'information complète dans un email dédié ou une mention d'information « allégée » en footer (cf. pied d'email / pavé de signature) renvoyant vers une politique complète de protection des données en pièce jointe et/ou en ligne (cf. lien hypertexte vers une rubrique dédiée sur son site internet).

Néanmoins, l'information des personnes concernées n'est pas requise dans des cas limités énoncés dans le cadre des exceptions à l'obligation d'information de la section 2.3.3.2 ci-dessus auquel il est renvoyé. Est simplement repris ci-dessous l'exemple évoqué dans ladite section :

(EXEMPLE)

Exemple : une agence PR (ou son client lorsque l'agence agit en tant que sous-traitant) pourrait éventuellement justifier le fait de ne pas informer individuellement les personnes concernées (à supposer que leurs coordonnées soient connues), dont elle(il) collecterait les données au moyen de différentes sources publiques (données rendues publiques par les personnes concernées sur différents sites par exemple) dans le cadre de l'élaboration de fichiers de « parties prenantes » sur un thème donné (par exemple : avis de professionnels d'un secteur particulier sur un produit alimentaire), lorsque le nombre de personnes concernées est très élevé et que leur information engendrerait un coût excessif pour l'agence ou son client le cas échéant (du fait du grand nombre de personnes concernées notamment et/ou de la multiplicité des sources sur lesquelles ces données publiques seraient collectées), constituant par là des efforts qui seraient considérés comme disproportionnés. Néanmoins, pour chaque hypothèse dans laquelle il serait envisagé de bénéficier de cette exception à l'obligation d'information, la mise en balance entre d'une part les efforts qui seraient nécessaires pour informer les personnes concernées et d'autre part l'incidence et les effets sur celles-ci d'une absence d'information individuelle doit être documentée par le responsable de traitement et le recours à cette exception strictement justifié. En outre, dans une telle hypothèse, le responsable de traitement doit tout de même prendre des mesures appropriées pour protéger les droits, les libertés et les intérêts légitimes des personnes concernées, a minima en rendant accessible au public une information générale relative au traitement concerné, notamment sur le site internet de l'agence PR ou de son client, voire sur d'autres supports opportuns et/ou appropriés le cas échéant, qu'il convient de déterminer au cas par cas. En tout état de cause, toute décision relative à l'application d'une exception à l'obligation d'information au traitement d'une agence PR ou d'un client doit être soumise à l'appréciation du DPO ou, à défaut, du référent en matière de protection des données à caractère personnel du responsable de traitement.

FOCUS SUR L'INFORMATION DES JOURNALISTES LORS DE LA PREMIÈRE COMMUNICATION AVEC CES DERNIERS

Si dans l'exemple précédent, il était prévu de contacter une portion des personnes concernées (par exemple, uniquement les personnes très favorables à un(e) cause/produit déterminé(e)), le responsable de traitement devra alors tout de même fournir bien entendu une information aux personnes contactées au moment de cette communication. Cette information pourrait se faire, par exemple, via une mention d'information conforme au modèle type précité à insérer dans le support de communication, assortie d'un lien renvoyant vers la politique de protection des données à caractère personnel de l'agence (ou du client, le cas échéant). Veuillez toutefois également vous référer à l'encadré ci-dessous concernant la problématique de l'utilisation des coordonnées, et notamment des adresses emails, des journalistes pour de la prospection.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

LE SAVIEZ-VOUS ?

LES PRÉCAUTIONS À PRENDRE EN CAS D'ACHAT / DE LOCATION D'UN FICHIER PRESSE !

Il convient de s'assurer auprès du tiers « fournisseur du fichier » (et de se faire garantir contractuellement par ce dernier) que (i) **la collecte des données des journalistes a été effectuée de manière loyale et licite** (information des personnes concernées, voire consentement le cas échéant en fonction des utilisations envisagées et des situations particulières pouvant être rencontrées) et que (ii) **les données peuvent être licitement réutilisées par l'agence PR pour les finalités souhaitées.**

ET EN PRATIQUE ?

Une garantie de la part du fournisseur du fichier s'agissant de la **titularité de l'intégralité des droits sur le fichier.**

LE CONTRAT OU LES CONDITIONS GÉNÉRALES DOIVENT COMPORTER :

Une garantie de la part du fournisseur du fichier portant sur le fait que le fichier est **constitué, mis à jour et utilisé conformément aux dispositions légales et reglementaires applicables** + ne comporte **pas d'éléments qui soient susceptibles d'engager la responsabilité** de l'agence PR à l'égard des tiers.

Une garantie de la part du fournisseur du fichier e**n matière de protection des données à caractère personnel** (information voire (i) recueil du consentement des personnes concernées ou (ii) garantie que les coordonnées communiquées sont des coordonnées professionnelles, répercussions des demandes d'exercice des droits des personnes concernées,...) **+ possibilité pour l'agence PR d'utiliser les données** pour les finalités envisagées par cette dernière (notamment prospection le cas échéant).

Une garantie de jouissance paisible et/ou d'indemnisation contre toute action de toute personne invoquant notamment une violation de la réglementation applicable en matière de protection des données à caractère personnel ou des dispositions applicables en matière de prospection, et plus généralement contre toute action qui pourrait être intentée par une personne et qui serait liée, directement ou indirectement, au non-respect par le fournisseur du fichier de ses engagements en matière de fourniture du fichier.

De manière générale, il peut être opportun de confier la réalisation de l'analyse ayant vocation à déterminer si l'insertion d'une telle clause est nécessaire et, le cas échéant, la rédaction ou la validation de la clause intégrée au contrat en matière de protection des données à caractère personnel au DPO ou, à défaut au référent en matière de protection des données à caractère personnel, ou encore à un conseil extérieur à l'agence spécialisé en la matière.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

FOCUS SUR LE CARACTÈRE PROFESSIONNEL (OU NON) DES COORDONNÉES DES JOURNALISTES

Attention, l'information d'un journaliste par email telle que proposée ci-dessus suppose que les coordonnées ainsi recueillies auprès de celui-ci soient des coordonnées utilisées notamment à des fins professionnelles (par exemple, une adresse email comportant le nom de domaine de la rédaction à laquelle il est rattaché, ou encore l'adresse email ou le numéro de téléphone figurant sur la carte de visite qui serait remise par le journaliste à un collaborateur de l'agence PR) et plus généralement qu'il puisse être qualifié de professionnel, ce qui sera en principe le cas dans la majorité des hypothèses.

A défaut, ou en cas de doute de l'agence PR, la solution la plus sécurisante d'un point de vue juridique serait de procéder à l'information de la personne concernée par un moyen de communication non soumis au consentement préalable (par exemple, par courrier postal). Il conviendrait à cette occasion de s'assurer de ce que l'adresse email et/ou le numéro de téléphone de la personne concernée constitue(nt) bien des coordonnées professionnelles (en demandant par exemple un email en retour suite au courrier postal confirmant qu'il s'agit d'une adresse email et/ou d'un numéro de téléphone utilisé(e) notamment à des fins professionnelles), afin de pouvoir fonder le traitement mis en œuvre à des fins de prospection sur l'exception dite « B to B », sous réserve bien entendu que les messages à venir de communication / sollicitation / prospection soient en rapport avec l'activité de la personne concernée (voir le paragraphe « Les hypothèses de recueil du consentement » ci-dessus). A défaut de confirmation de ce que l'adresse email et/ou le numéro de téléphone collecté(e)(s) est (sont) bien une adresse email et/ou un numéro de téléphone professionnel(le), il conviendrait de recueillir le consentement des personnes concernées dans cette situation pour pouvoir leur adresser des sollicitations par courrier électronique (à défaut, alors aucun échange par courrier électronique ne pourrait intervenir).

Pour des raisons pratiques (en particulier parce que la fourniture de l'information par un autre moyen se révélerait impossible ou engendrerait des efforts disproportionnés), **une solution dégradée** (cependant moins sécurisante juridiquement, même si le risque est limité) **pourrait consister à ce que l'information des journalistes soit réalisée dans tous les cas au moyen de l'envoi d'un email comportant une mention d'information et renvoyant vers la politique complète de protection des données à caractère personnel de l'agence PR** (en pièce jointe et/ou au moyen d'un lien hypertexte vers une rubrique dédiée en ligne) qui informerait les personnes concernées sur le traitement de leurs données à caractère personnel. **En cas de doute sur le caractère professionnel des coordonnées recueillies,** cette information serait également l'occasion de s'assurer que les coordonnées du journaliste sont bien des coordonnées professionnelles, en indiquant dans ce message, en sus de la proposition de mention d'information ci-dessus, que (i) les coordonnées collectées semblent a *priori* être « professionnelles », que (ii) le journaliste peut bien entendu contester le caractère professionnel de tout ou partie de ses coordonnées traitées par l'agence PR auprès de cette dernière via le moyen de contact qui sera précisé dans le message, et que (iii) en l'absence de retour dans un délai défini, alors ses coordonnées seront considérées comme étant « professionnelles » et continueront, sauf indication contraire de la part du journaliste, à être utilisées pour lui adresser des communications.

En tout état de cause, si une telle solution dégradée devait tout de même être retenue en raison des considérations pratiques susvisées dans les hypothèses où il existe un doute sur la qualification, alors en cas de contestation du caractère professionnel des coordonnées, il conviendrait de ne plus adresser aux journalistes concernés de sollicitation / ne plus échanger avec eux par email / sms / mms.. De même, si l'agence PR (adressant des communications par courrier électronique à la personne concernée) se voit notifier par celle-ci son opposition à la réception de tels messages, elle devra bien entendu immédiatement cesser ces communications.

3.1.2.2 Les influenceurs et les Key Opinion Leaders

Il doit être fourni aux influenceurs ou Key Opinion Leaders dont les données à caractère personnel sont traitées une information conforme à la réglementation applicable en matière de protection des données à caractère personnel. A cette fin, il convient d'identifier de manière exhaustive les sources et modalités de collecte des données les concernant afin de déterminer selon quelles modalités et sur quels supports l'information pourra leur être fournie, de manière complète, lors de la collecte des données (sauf dans le cas où il est possible de se fonder sur l'une des exceptions à l'obligation d'information, présentées au sein du paragraphe « Loyauté et transparence » ci-dessus).

(ILLUSTRATIONS)

A titre d'illustration, des données à caractère personnel relatives à ces personnes sont susceptibles d'être collectées auprès d'elles-mêmes, lorsque ces derniers prennent contact avec l'agence PR sur le site internet de ladite agence PR, dans le cadre d'échanges via les réseaux sociaux ou lors d'un événement par exemple (cf. collecte directe) mais également sur tous sites internet d'actualités ou autres, ou blogs ou encore au moyen de bases de données ou de fichiers de tiers (cf. collecte indirecte).

Quelle que soit la manière dont les données d'un influenceur ou d'un Key Opinion Leader sont collectées, celui-ci doit, en principe, être dûment informé du traitement des données à caractère personnel le concernant.

Ainsi :

- **lorsque les données sont collectées directement auprès de lui,** celui-ci doit être informé du traitement de ses données au moment où celles-ci sont collectées. En particulier, il convient que soit communiqué à l'influenceur ou au Key Opinion Leader un message comportant une mention d'information appropriée et renvoyant à une politique complète de protection des données.

Si la prise de contact émane de la personne concernée elle-même, par exemple un influenceur qui propose à l'agence PR de « collaborer » avec elle, alors il convient de déployer un tel mécanisme dans un message accusant réception de sa proposition de « collaboration ».

En cas d'échanges avec ces personnes via les réseaux sociaux, l'information peut être délivrée au moyen d'un message adressé par ce média.

Il convient également de se reporter aux bonnes pratiques présentées ci-dessus s'agissant de la collecte des données relatives aux journalistes, celles-ci pouvant utilement être déclinées pour ce qui concerne les influenceurs et les Key Opinion Leaders.

LE SAVIEZ-VOUS ?

Bien qu'il ne s'agisse pas stricto sensu d'une problématique relevant de la réglementation applicable en matière de protection des données à caractère personnel, la prise de contact par un collaborateur d'une agence PR avec un influenceur, par exemple via les réseaux sociaux, impose audit collaborateur de **l'informer qu'il travaille au sein de l'agence PR et que c'est dans ce contexte qu'il le contacte** pour le compte de l'agence PR, étant précisé que la dissimulation du fait que cette prise de contact intervient dans le cadre de l'activité de l'agence PR pourrait être sanctionnée par exemple sur le fondement des pratiques commerciales déloyales dites « trompeuses », les sanctions encourues dans ce cadre pouvant atteindre 2 ans d'emprisonnement et 300 000 € d'amende (amende pouvant être portée au quintuple lorsque la personne responsable est une personne morale, étant précisé que le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du délit, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant ce délit)[116].

[116] Cf. article L.132-2 (et suivants s'agissant des peines complémentaires encourues) du Code de la consommation.

- **lorsque les données sont collectées indirectement :** il convient de se reporter aux bonnes pratiques présentées ci-dessus s'agissant de la collecte indirecte de données relatives aux journalistes ainsi qu'aux recommandations présentées ci-dessus en matière d'achat / de location de fichiers, celles-ci pouvant le cas échéant être déclinées pour ce qui concerne les influenceurs ou les Key Opinion Leaders.

FOCUS SUR LA QUALIFICATION DE PROFESSIONNEL (OU NON) DES INFLUENCEURS / KEY OPINION LEADERS

Attention, pour mémoire, les influenceurs ou les Key Opinion Leaders au sens large ne peuvent être contactés par email sans recueil préalable de leur consentement que s'ils peuvent être considérés comme des professionnels (cf. l'exception dite « B to B ») et qu'il s'agit de leur adresse email utilisée notamment à des fins professionnelles. Il en va de même pour ce qui concerne la prise de contact par message privé sur les réseaux sociaux, qui pourrait être qualifié de courrier électronique[117]et donc soumis au même régime juridique que les emails en matière de prospection.

Aussi, par principe, les influenceurs et Key Opinion Leaders ne peuvent être contactés par de tels moyens sans recueil préalable de leur consentement que s'ils peuvent être considérés comme des « professionnels » au sens de la réglementation (cf. l'exception dite « B to B »).

Pour ce qui concerne cette population, et compte-tenu de la diversité des partenariats pouvant exister avec les marques (simple évocation d'une marque sans que celle-ci ne le demande à l'influenceur, marketing d'influence, caractère « publicitaire » ou non des publications, caractère rémunéré ou non de la « prestation », proportion dans la part des revenus de la personne concernée d'une telle rémunération, volume et typologie d'audience, activité dans le cadre d'une structure juridique créée à cet effet,...), **la qualification de « professionnel » peut être d'autant plus délicate à appréhender.** Or, si un influenceur ou un Key Opinion Leader n'est pas considéré comme professionnel, alors son consentement devrait en principe être recueilli pour pouvoir le solliciter à des fins de communication ou de marketing par l'intermédiaire des moyens précités.

Si à ce jour une définition des influenceurs a été proposée par l'autorité de régulation professionnelle de la publicité (ou « ARPP »)[118], ou encore par le législateur mais uniquement en matière de santé publique, dans le cadre de la transparence des liens d'intérêts entre les entreprises produisant ou commercialisant des produits de santé à usage humain et les influenceurs[119],

la question de la qualification qu'il convient d'attribuer aux influenceurs sur les réseaux sociaux, ou aux Key Opinion Leaders de manière générale, n'est pas clairement tranchée et des subdivisions pourraient à l'avenir se dessiner et venir expliciter les conditions dans lesquelles il convient de considérer qu'un influenceur ou un Key Opinion Leader est un « professionnel », selon des critères restant à déterminer.

En tout état de cause, il peut être opportun de se reporter aux définitions proposées dans l'article liminaire du Code de la consommation, aux termes desquelles :

- un « consommateur » désigne « toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole » ;
- un « non-professionnel » désigne « toute personne morale qui n'agit pas à des fins professionnelles » ;
- un « professionnel » désigne « toute personne physique ou morale, publique ou privée, qui agit à des fins entrant dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole, y compris lorsqu'elle agit au nom ou pour le compte d'un autre professionnel ».

En cas de doute sur la qualification d'un influenceur ou d'un Key Opinion Leader, la solution la plus sécurisante d'un point de vue juridique serait de procéder à l'information des influenceurs par un moyen de communication non soumis à consentement préalable (par exemple, par courrier postal), ce qui en pratique ne semble pas envisageable, notamment lorsque les agences PR ne disposent que du « nom d'utilisateur » ou « pseudo » ou encore « profil » d'un influenceur sur les réseaux sociaux par exemple.

[117] Au sens de l'article 1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique dite « LCEN », constitue un courrier électronique « *tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère* »

[118] L'ARPP définit l'influenceur comme « *un individu exprimant un point de vue ou donnant des conseils, par écrit, audio et/ou visuel, dans un domaine spécifique et selon un style ou un traitement qui lui sont propres et que son audience identifie* » (ARPP, Communication d'influenceurs et marques, www.arpp.org/actualite/communication-influenceurs-marques/).

[119] Cf. article 7° bis du I de l'article L. 1453-1 du Code de la santé publique, qui vise « *Les personnes qui, dans les médias ou sur les réseaux sociaux, présentent un ou plusieurs produits de santé, de manière à influencer le public* ». Voir également la délibération n° 2019-151 du 12 décembre 2019 de la Cnil portant avis sur un projet de décret en Conseil d'Etat relatif à la transparence des liens d'intérêts entre les entreprises produisant ou commercialisant des produits de santé à usage humain et les influenceurs (demande d'avis n° 19020623).

PUBLIC CIBLE : DIRECTION, MANAGERS PR

Pour des raisons pratiques (en particulier parce que la fourniture de l'information par un autre moyen se révélerait impossible ou engendrerait des efforts disproportionnés), **une solution dégradée** (cependant moins sécurisante juridiquement, même si le risque est limité) pourrait, en cas **de doute sur la qualification de l'influenceur ou du Key Opinion Leader, consister à ce que l'information soit réalisée au moyen de l'envoi d'un message (message privé via les réseaux sociaux ou email par exemple) qui :**

(a) comporterait une mention d'information sur le traitement de données à caractère personnel mis en œuvre par l'agence concernant les données de la personne concernée et renverrait vers la politique complète de protection des données à caractère personnel de l'agence (au moyen d'un lien hypertexte vers une rubrique dédiée en ligne et/ou en pièce jointe si le message est adressé par email) ;

(b) viserait à s'assurer que le compte, le profil et/ou, le cas échéant, l'adresse email de l'influenceur ou du Key Opinion Leader sont bien des « coordonnées professionnelles », en indiquant dans ce message, en sus de la proposition de mention d'information ci-dessus, que (i) ces « coordonnées » semblent a priori être « professionnelles », que (ii) l'influenceur ou le Key Opinion Leader peut bien entendu contester le caractère professionnel de tout ou partie de ses « coordonnées » traitées par l'agence PR auprès de cette dernière via le moyen de contact qui sera précisé dans le message, et que (iii) en l'absence de retour dans un délai défini, alors ses « coordonnées » seront considérées comme étant « professionnelles » et continueront, sauf indication contraire de sa part, à être utilisées pour lui adresser des communications.

En tout état de cause, si une telle solution dégradée devait tout de même être retenue en raison des considérations pratiques susvisées dans les hypothèses où il existe un doute sur la qualification de l'influenceur ou du Key Opinion Leader, alors en cas de contestation du caractère professionnel de leurs « coordonnées », il conviendrait de ne plus adresser aux influenceurs ou Key Opinion Leaders concernés de sollicitation / ne plus échanger avec eux par email / messages via les réseaux sociaux. De même, si l'agence PR (adressant des communications par courrier électronique à la personne concernée) se voit notifier par celle-ci son opposition à la réception de tels messages, elle devra bien entendu immédiatement cesser ces communications.

Enfin, si ce focus se limite en termes de périmètre aux emails et messages échangés via les réseaux sociaux, les mêmes recommandations doivent être déclinées s'agissant notamment de la possibilité d'adresser des sms ou mms aux influenceurs ou Key Opinion Leaders.

LE SAVIEZ-VOUS ?

Lorsque les contacts et échanges ont lieu par l'intermédiaire des attachés de presse ou des chargés de communication d'un influenceur ou d'un Key Opinion Leader, il convient là-encore de trouver un moyen d'informer les personnes concernées du traitement de leurs données à caractère personnel.

S'il existe des exceptions à une telle information des personnes concernées, lorsque cette information est impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche, il est rappelé que la Cnil interprète strictement, voire restrictivement, ces notions d'impossibilité ou d'efforts disproportionnés. Aussi, il convient de mettre tout en œuvre pour procéder à une telle information des personnes concernées, si besoin au moyen d'une information adressée dans le cadre des échanges avec l'intermédiaire (attaché de presse ou chargé de communication) en précisant expressément que cette information doit être portée à l'attention de la personne concernée.

FOCUS SUR LES DONNÉES RELATIVES AUX PROCHES DES INFLUENCEURS

Dans le cadre de leurs échanges avec les influenceurs, les agences PR peuvent être amenées à avoir connaissance de données relatives aux proches des influenceurs (âge, sexe ou taille de vêtements des enfants, profession ou centres d'intérêts du conjoint,...) par exemple pour leur envoyer des produits, vêtements, ... à tester et à présenter dans le cadre de posts à destination de leur public, de leur audience.

Dans une telle hypothèse, il convient en principe **d'informer les personnes concernées (cf. les proches concernés) du traitement de leurs données par l'agence PR (ou par le client, lorsque l'agence agit en tant que sous-traitant).** En pratique, si l'agence PR ne dispose pas de coordonnées de ces personnes, il pourrait a minima être envisagé de s'assurer auprès de l'influenceur ayant communiqué de telles informations que ses proches ont été dûment informés par ledit influenceur s'agissant du traitement de leurs données, en présentant à cette fin à l'influenceur les caractéristiques du traitement envisagé (cf. les éléments devant figurer obligatoirement dans les mentions d'information, conformément au paragraphe « Loyauté et transparence » ci-dessus).

3.1.2.3 Les clients / prospects de l'agence PR

Afin de fournir aux contacts et interlocuteurs de l'agence PR chez ses clients ou prospects, dont les données à caractère personnel sont traitées par celle-ci en qualité de responsable de traitement, une information conforme à la réglementation applicable en matière de protection des données à caractère personnel, il convient d'identifier de manière exhaustive les sources et modalités de collecte des données les concernant afin de déterminer selon quelles modalités et sur quels supports l'information de ces derniers pourra être fournie, de manière complète, lors de la collecte des données.

(ILLUSTRATION)

A titre d'illustration, des données à caractère personnel relatives aux contacts et interlocuteurs de l'agence PR chez ses clients ou prospects sont susceptibles d'être collectées auprès desdits contacts et interlocuteurs eux-mêmes, lorsque ces derniers prennent contact avec l'agence PR sur le site internet de l'agence PR ou lors d'un événement par exemple (cf. collecte directe) mais également par l'intermédiaire des clients ou prospects eux-mêmes, ou encore sur des sites internet de tiers, voire au moyen de bases de données de tiers (cf. collecte indirecte).

Quelle que soit la manière dont les données d'un contact ou d'un interlocuteur de l'agence PR chez ses clients ou prospects sont collectées, celui-ci doit être dûment informé par l'agence PR du traitement des données à caractère personnel le concernant mis en œuvre par cette dernière.

Ainsi :

- **lorsque les données sont collectées directement auprès d'un contact ou interlocuteur de l'agence PR chez ses clients ou prospects,** celui-ci doit être informé du traitement de ses données au moment où celles-ci sont collectées, par exemple de la manière suivante :

FORMULAIRE PAPIER DE COLLECTE DE DONNÉES

- Mention d'information sur le support de collecte (par exemple un formulaire à faire remplir lors d'un évènement) + sur un document complémentaire (préalable ou concomitant) comportant l'intégralité des informations requises (si l'information figurant sur le formulaire est «allégée»)

FORMULAIRE EN LIGNE DE COLLECTE DE DONNÉES, SUR LE SITE INTERNET DE L'AGENCE PR

- Mention d'information sur le support de collecte (par exemple un formulaire de contact dédié ou d'inscription à un espace presse) + renvoi vers une rubrique du site internet de l'agence PR comportant sa politique complète de protection des données en ligne (si l'information figurant sur le formulaire est «allégée»)

DANS UN CONTEXTE PROFESSIONNEL, PAR VOIE ORALE EN PRÉSENTIEL, PAR EXEMPLE DANS LE CADRE D'UN ÉVÈNEMENT, OU PAR TÉLÉPHONE

- Information orale du contact/interlocuteur du client/prospect par la personne collectant de telles données concomitamment à ladite collecte. Néanmoins, pour des raisons probatoires, un tel mécanisme d'information par oral n'est pas suffisant et il est recommandé de fournir à la personne concernée une mention d'information écrite appropriée, par exemple en intégrant une mention d'information complète dans un email dédié ou en adressant un email comportant en footer / pied de page / dans le pavé de signature une mention éventuellement allégée et renvoyant (i) vers une politique complète de protection des données de l'agence en pièce jointe et/ou (ii) par un lien hypertexte à cette même politique en ligne (cf. rubrique dédiée).

PUBLIC CIBLE : DIRECTION, MANAGERS PR

(EXEMPLE)

Exemple de mention d'information « complète » pouvant être intégrée par exemple dans les emails à destination des interlocuteurs de l'agence PR chez ses clients / prospects dont les données ont été collectées directement auprès de ces derniers s'agissant de l'utilisation de leurs coordonnées professionnelles [modèle « type » à adapter bien entendu au regard de la pratique effective et des caractéristiques particulières de chaque traitement mis en œuvre par l'agence PR agissant en qualité de responsable de traitement]:

[dénomination de l'agence PR qui agit en qualité de responsable de traitement], en qualité responsable du traitement, traite des données à caractère personnel vous concernant en vue [à déterminer / préciser / compléter, par exemple : de la gestion et du suivi de ses relations, notamment contractuelles et commerciales, avec ses clients, prospects, et plus généralement contacts, en ce incluant notamment la réponse aux demandes d'information, la gestion des comptes clients, la gestion et le suivi de la fourniture des prestations au titre du contrat conclu, la gestion et le suivi des opérations de comptabilité y afférentes, et en particulier la gestion et le suivi de la facturation et des transactions associées, mais également la réalisation d'opérations commerciales, de communication et de marketing, par tout moyen et en particulier par email (notamment [à préciser : ciblage, prospection / sollicitation commerciale et personnalisation des contenus, envoi de newsletters ou d'actualités, invitations à participer à des évènements, envoi de cartes de vœux,...]).

La plupart de ces informations sont collectées directement auprès de vous. Certaines informations (à savoir : [à détailler]) peuvent toutefois être collectées de manière indirecte [indiquer la source : par exemple au moyen de sources d'informations publiques telles que le site internet de la société pour laquelle vous travaillez,...].

Un tel traitement de vos données à caractère personnel est fondé, en fonction des sous-finalités poursuivies, sur [par exemple : la poursuite de nos intérêts légitimes à assurer la gestion et le suivi des relations, notamment commerciales, avec nos clients, prospects et plus généralement contacts et/ou l'exécution du contrat conclu avec l'agence PR et/ou le respect d'obligations légales et réglementaires qui incombent à l'agence PR (a minima pour ce qui concerne la gestion et le suivi des opérations de comptabilités liées aux missions par exemple)].

Les données collectées dans ce cadre sont obligatoires pour la poursuite de la finalité précitée qui, à défaut, ne pourrait pas être atteinte. Toutefois, le traitement de ces informations en vue de la réalisation d'opérations de communication et de marketing est strictement facultatif et vous pouvez vous y opposer à tout moment, et sans avoir à justifier d'un quelconque motif, sur simple demande aux coordonnées précisées ci-dessous.

Les données vous concernant sont destinées [à compléter avec les destinataires des données : membres de notre personnel habilités à en avoir connaissance, partenaires et prestataires pouvant être amenés à intervenir dans le cadre de la réalisation des finalités susvisées, ...].

Vos données pourront être conservées par nos soins en base active pendant [à compléter]. A l'issue de cette durée, lesdites données seront conservées sous forme d'archives pendant [à compléter].

Conformément aux dispositions applicables en matière de protection des données à caractère personnel, vous bénéficiez d'un droit d'interrogation, d'accès, de rectification, d'effacement et à la portabilité de vos données, ainsi que du droit d'obtenir la limitation de leur traitement et d'un droit d'opposition (au traitement de vos données, ainsi qu'à la prospection notamment commerciale) dans les conditions et limites posées par la réglementation applicable en matière de protection des données à caractère personnel. Vous disposez également du droit de définir des directives relatives au sort de vos données à caractère personnel et à la manière dont vous souhaitez que vos droits soient exercés après votre décès. Ces droits s'exercent par courrier postal à l'adresse suivante : [à compléter] ou par email à l'adresse suivante : [à compléter avec une adresse email, étant précisé qu'il serait opportun d'avoir une adresse email dédiée à la réception de telles demandes]. Vous disposez en tout état de cause de la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (« Cnil ») si vous estimez que le traitement de vos données n'est pas effectué conformément aux dispositions légales et réglementaires applicables.

Pour en savoir plus sur le traitement de vos données à caractère personnel et vos droits associés, vous êtes invité(e) à prendre connaissance de notre « Politique de protection des données à caractère personnel » [insérer un lien vers ladite politique sur le site internet du responsable de traitement].

- **lorsque les données sont collectées indirectement auprès d'un contact ou d'un interlocuteur de l'agence PR chez ses clients ou prospects,** celui-ci doit, en principe, être informé du traitement de ses données dans un délai raisonnable après obtention desdites données par l'agence PR (ne dépassant pas un mois), ou, si les données doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec cette dernière ou encore, s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Cette information pourra par exemple être fournie au contact ou interlocuteur de l'agence PR en intégrant une mention d'information complète dans un email dédié ou une mention d'information « allégée » en footer (cf. pied d'email / pavé de signature) renvoyant vers la politique complète de protection des données de l'agence PR en pièce jointe et/ou en ligne (cf. lien hypertexte vers une rubrique dédiée sur son site internet).

LE SAVIEZ-VOUS ?

Il convient également, lorsque les données des contacts ou interlocuteurs sont communiquées par exemple par les clients dans le cadre de l'entrée en relation contractuelle avec l'agence PR, **de mentionner dans les documents contractuels conclus avec le client que celui-ci s'engage à informer ses collaborateurs (et en garantit l'agence)** du traitement de leurs données à caractère personnel par l'agence PR dans le cadre de l'exécution du contrat.

Il convient également de se reporter aux recommandations présentées ci-dessus en matière d'achat / de location de fichiers, celles-ci pouvant le cas échéant être déclinées pour ce qui concerne les contacts ou interlocuteurs chez les clients et prospects.

3.1.3 Les données pouvant être collectées

Pour mémoire, seules les données à caractère personnel **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies peuvent être traitées par les agences PR agissant en qualité de responsable de traitement dans le cadre de leur activité (ou par leurs clients lorsque l'agence agit en tant que sous-traitant).**

(ILLUSTRATIONS)

A titre d'illustration, la collecte et le traitement de données relatives à l'identité, aux coordonnées, à la rédaction ou au média de rattachement ou encore à l'historique des échanges peuvent par exemple être justifiés pour ce qui concerne la gestion et le suivi de la relation d'une agence PR avec les journalistes, influenceurs, ...

Par ailleurs, la collecte et le traitement de données relatives à l'identité, aux coordonnées, au poste occupé ou encore à l'historique des échanges d'une agence PR avec ses clients peuvent par exemple être justifiés pour ce qui concerne la gestion et le suivi de la relation d'une agence PR avec lesdits clients.

En pratique, il convient de **manière pragmatique,** pour déterminer si telle ou telle donnée peut être collectée, traitée,... **de se poser les questions suivantes :**

- ai-je strictement besoin de cette information au moment où je la demande ?
- pourrais-je le justifier au cas où une demande en ce sens me serait adressée par une autorité de contrôle ?

(EXEMPLE)

Puis-je demander à un journaliste de me transmettre une copie de sa carte identité ou de son passeport pour l'organisation d'un voyage de presse. Quels sont les bons réflexes à adopter ?

La collecte d'une copie d'un document d'identité pourrait être considérée comme excessive, et donc non conforme au principe de minimisation des données.

Si le déplacement est en France, et en fonction du moyen de transport envisagé, certaines informations peuvent toutefois être demandées au journaliste pour organiser son déplacement (par exemple, collecte de sa date de naissance pour réserver des billets de train).

Si le déplacement est à l'étranger, il peut également être nécessaire et justifié pour l'agence PR de demander au journaliste le numéro de son passeport. Toutefois, comme indiqué ci-dessus, la photocopie de son passeport pourrait être excessive.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

En tout état de cause, quelle que soit la typologie des données traitées par l'agence PR, cette dernière doit s'assurer que l'ensemble des données traitées par l'agence PR et intégrées dans les fichiers et bases de données adossées aux applications et outils utilisés au sein de ladite agence sont exactes et tenues à jour (voir à cet égard le paragraphe « Exactitude et qualité des données » ci-dessus).

FOCUS SUR LES ZONES DE COMMENTAIRES LIBRES

Si dans l'exemple précédent, il était prévu de contacter Pour mémoire, **le principe de minimisation s'applique quelles que soient les modalités de collecte,** de saisie et de traitement des données dans les applications, fichiers, etc. utilisés. Les « champs de commentaires libres » ou « zones de saisie libre » (de type champs « commentaires », « observations », « remarques », « autres », « bloc-notes »,...) doivent notamment être utilisés avec **prudence** (minimisation et proportionnalité des données, objectivité,...), conformément aux recommandations de la Cnil en la matière.

Les zones de commentaires libres permettent en effet de renseigner des informations relatives à la connaissance de leurs clients, de leurs contacts, à l'historique des relations,..., ce qui peut être justifié et légitime, mais de telles zones constituent tout de même un risque de **collecte de données excessives ou inappropriées.**

Ainsi, pour ce qui concerne les zones de commentaires libres, il convient de :

- favoriser dans les outils / applications / fichiers, lorsque cela est possible, par exemple **l'utilisation de menus déroulants ou de cases à cocher,** plutôt que de prévoir des zones de commentaires libres ;
- **sensibiliser les utilisateurs** des outils / applications / fichiers concernés sur ce qu'il est possible ou non d'indiquer dans de telles zones, par exemple au moyen d'une charte de « bonnes pratiques » ayant vocation à rappeler les règles applicables (de type « ce que je peux écrire » vs « ce que je ne peux pas écrire »). En effet, compte tenu des extractions qui peuvent être effectuées par les membres des agences PR, et de l'utilisation parfois massive des fichiers / tableaux Excel, et bien que de telles pratiques doivent être limitées, la sensibilisation de ces derniers est une priorité. A titre d'illustration, l**a saisie de données sensibles dans de telles zones de commentaires libres est à proscrire** (voir à cet égard les bonnes pratiques à adopter en matière de traitement de données sensibles présentées ci-après). **Il en va de même s'agissant de propos insultants ou injurieux.** En revanche, lorsque de telles zones sont utilisées, celles-ci peuvent par exemple permettre d'indiquer un évènement auquel a participé un Key Opinion Leader ou encore des informations utiles pour la gestion d'une communication de crise, sous réserve du respect des précautions susvisées ;
- **insérer dans les outils / applications / fichiers concernés un message d'avertissement** à l'attention des personnes en charge de la saisie de tels champs comportant les recommandations et précautions appropriées sur ce qu'il est possible ou non d'indiquer dans les zones de commentaires libres ;
- **formaliser et déployer une politique interne de revue et de monitoring des zones de commentaires libres** (ex : dictionnaire de mots interdits et blocages ou a minima alertes associés dans les outils / applications / fichiers, vérifications régulières au moyen de requêtes par « mots-clés »,...).

En tout état de cause, l'utilisation de ces zones de commentaires libres doit être **limitée à ce qui est strictement nécessaire.**

PUBLIC CIBLE : DIRECTION, MANAGERS PR

LE SAVIEZ-VOUS ?

L'UTILISATION D'EXTRACTIONS / EXPORTS / REQUÊTES PRÉSENTE UN RISQUE MAJEUR DE NON-CONFORMITÉ À LA RÉGLEMENTATION APPLICABLE EN MATIÈRE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL !

S'agissant des extractions, exports ou requêtes qui peuvent être réalisés (par exemple sous forme de tableurs Excel) à partir des outils métiers, applications ou bases de données mis à la disposition des collaborateurs de l'agence PR, ces pratiques doivent faire l'objet d'une attention particulière.

En effet, **il convient, pour chaque extraction, export ou requête effectué de s'assurer au cas par cas du respect des principes applicables en matière de protection des données à caractère personnel :** absence de détournement de finalité, données extraites minimisées (cf. limitées au strict nécessaire), durées proportionnées, destinataires justifiés, etc.

Une **sensibilisation des utilisateurs** des outils, applications et bases de données doit donc être déployée au sein de l'agence à cette fin. La mise en place de **messages d'avertissement** à l'attention de ces derniers **dans les outils permettant d'effectuer des extractions, exports ou requêtes** est également une bonne pratique opportune à implémenter afin de porter à la connaissance des personnes disposant de cette faculté, lors de chaque connexion ou avant chaque extraction, export ou requête (directement sur les écrans de l'outil ou de l'application utilisé par exemple), les principes à respecter dans ce cadre.

Par ailleurs, dans le cadre de leur activité « cœur de métier », les agences PR peuvent également être amenées à traiter des **données sensibles** telles que des opinions politiques ou des convictions philosophiques qui peuvent par exemple être révélées à travers les sujets de prédilection ou publications d'un journaliste ou encore la rédaction ou le média auquel il appartient, voire le parti politique auquel une personne est adhérente.

Pour mémoire, **le traitement de telles données en est principe interdit, sauf dans certaines hypothèses spécifiques parmi lesquelles :**

- si ces données ont été manifestement rendues publiques par la personne concernée ;
- si la personne concernée y a consenti, dans les conditions et selon les modalités présentées aux paragraphes y afférents ci-dessus, ce consentement devant être explicite ;

étant rappelé que ces exceptions autorisant de traiter des données sensibles **doivent être interprétées de manière très stricte.**

FOCUS SUR LES DONNÉES DÉDUITES DES INTERVENTIONS, PUBLICATIONS OU ENCORE DÉCLARATIONS DES JOURNALISTES OU DE KEY OPINION LEADERS (PERSONNALITÉS PUBLIQUES, EXPERTS, ...)

Dans le cadre de leur activité « cœur de métier », les agences PR peuvent être amenées à réaliser une **cartographie des parties prenantes** pour pouvoir prodiguer à leurs clients des conseils quant à leur stratégie de communication.

A cette fin, pourront notamment être collectées et traitées par les agences PR des **informations issues des interventions, publications ou encore déclarations de journalistes ou de Key Opinion Leaders.**

L'analyse de ces informations réalisée par l'agence PR peut être susceptible de révéler des données sensibles relatives à ces personnes (opinions politiques, convictions philosophiques, appartenance syndicale,...) si bien qu'en principe, comme rappelé ci-dessus, **il conviendrait que ces données aient été manifestement rendues publiques par la personne concernée ou que cette dernière ait consenti à leur traitement pour qu'une telle utilisation par les agences PR soit licite.**

Pour ce qui concerne par exemple l'appartenance syndicale du secrétaire général d'une confédération syndicale ou encore les opinions politique d'un député s'étant présenté comme étant rattaché à un parti politique, il peut être considéré que de telles données sensibles les concernant ont été « manifestement rendues publiques » par ces derniers.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

Toutefois, **pour ce qui concerne les données déduites des interventions, publications ou encore déclarations** (par exemple, propos laissant penser qu'une personne semble en faveur de la gestation pour autrui, anti-avortement ou encore partisan d'un courant de pensée philosophique), il demeure **un risque que de telles informations ne soient pas considérées « per se » comme ayant été « manifestement rendues publiques »** puisqu'un exercice de déduction et d'analyse serait réalisé.

Néanmoins, il pourrait le cas échéant raisonnablement être soutenu que **l'intention,** derrière cette exception à l'obligation de recueillir le consentement des personnes concernées, ait été de permettre aux responsables de traitement d'exploiter les données mises à la disposition du public par les personnes concernées, même si ce n'est pas exactement dans le même format que celui sous lequel lesdites données ont été à l'origine rendues publiques. Dans la mesure où **les personnes dont il est ici question, sont des journalistes et des Key Opinion Leaders (personnalités publiques, experts, etc.), parfaitement conscients des conséquences et de l'utilisation éventuelle qui sera faite de leurs propos/écrits** (i.e. en aucun cas des personnes vulnérables), il semble qu'une interprétation trop stricte de cette exception priverait ladite exception de sa raison d'être : elle ne s'appliquerait alors qu'aux activités de traitement utilisant les données dans un format strictement identique à celui des données rendues publiques par la personne concernée. En substance, personne ne pourrait alors jamais commenter ou analyser la position publique d'un journaliste ou d'un Key Opinion Leader sur une question. Aussi, il pourrait être soutenu que ces informations ont été « manifestement rendues publiques », **sous réserve bien entendu que les agences PR procèdent à un traitement « objectif » de telles informations,** avec la plus grande précaution et sans extrapolation trop « subjective » qui viendrait contrarier le raisonnement présenté ci-dessus.

Le recueil du consentement, dans les conditions et selon les modalités présentées aux paragraphes y afférents ci-dessus, demeure toutefois requis pour qu'une agence PR puisse déduire de ces informations des données sensibles et les traiter, lorsque les personnes concernées sont des citoyens autres que des journalistes ou des Key Opinion Leaders. (ce qui ne sera a priori pas souvent le cas compte-tenu de l'activité des agences PR).

En tout état de cause, pour mémoire, le traitement par une agence PR d'informations issues des interventions, publications ou encore déclarations de journalistes ou Key Opinion Leaders requiert également, en principe, que ces derniers soient dûment informés d'un tel traitement (à cet égard, voir le paragraphe « Loyauté et transparence » ci-dessus).

(EXEMPLES)

Exemples de cas pratiques au regard de la réglementation applicable en matière de protection des données à caractère personnel

• **CAS N°1 :** Un client demande à un collaborateur d'une agence PR les coordonnées (nom, média, mail ou numéro de téléphone) d'un journaliste (pour le contacter lui-même, pour lui envoyer sa carte de vœux, pour le remercier suite à la publication d'un article,...). Ce collaborateur peut-il les communiquer au client ?

En pratique, une telle communication n'est possible que sous réserve (i) que la finalité poursuivie par le client ne soit pas incompatible avec celle poursuivie par l'agence PR, (ii) qu'une telle transmission puisse être justifiée (cf. principe de justification des destinataires), et (iii) que le journaliste en question ait été informé du traitement de ses données par l'agence PR, conformément aux règles applicables en la matière[120]. A cet égard, il convient notamment de s'assurer que les clients de l'agence PR sont bien identifiés parmi les destinataires des données concernant le journaliste dans la mention d'information qui a été portée à sa connaissance. Attention : le client devra en tout état de cause (i) informer le journaliste du traitement qu'il met lui-même en œuvre et dont il est responsable dans les conditions et selon les modalités rappelées ci-dessus en cas de collecte indirecte de données, voire (ii) recueillir le consentement du journaliste si le moyen de communication qu'il envisage pour échanger avec ce dernier est soumis au consentement préalable et qu'il ne peut bénéficier d'une des exceptions applicables.

Point d'attention : vérifier les garanties demandées par le client dans une telle hypothèse avant de lui communiquer les données sollicitées (afin notamment que l'agence ne s'engage pas sur des garanties qu'elle ne pourrait pas fournir ou dont elle n'a pas la maîtrise).

[120] Voir le paragraphe « Loyauté et transparence » ci-dessus

PUBLIC CIBLE : DIRECTION, MANAGERS PR

• **CAS N°2 :** Un collaborateur de l'agence PR demande à un autre collaborateur les coordonnées d'un journaliste (son numéro de téléphone mobile, son adresse email,...). Une telle communication est-elle possible ?

Dans cette situation, il convient en particulier (i) de s'assurer que l'utilisation de ces données envisagée par le collaborateur ayant formulé une telle demande est compatible avec la finalité poursuivie par l'agence PR (notamment avec la gestion et le suivi de ses relations avec les journalistes) mais également (ii) que ses missions justifient qu'il ait accès à de telles données (cf. gestion des habilitations[121]). Par exemple, la transmission de données relatives à un journaliste à un collaborateur de la Direction des ressources humaines n'est a priori pas justifiée.

De manière générale, pour toute communication de données à caractère personnel traitées par une agence PR (cf. cas n°1 et n°2), il convient notamment :

- de vérifier qu'une telle transmission peut être justifiée (cf. principe de justification des destinataires) et que la finalité de réutilisation envisagée n'est pas incompatible avec la finalité initiale du traitement par l'agence PR ;
- de s'assurer que cette transmission est prévue dans la mention d'information qui a été fournie à la personne concernée (cf. principe de loyauté et de transparence, notamment s'agissant des destinataires des données) ;
- d'indiquer au destinataire, lorsque celui-ci est justifié, la finalité pour laquelle ces données à caractère personnel sont traitées par l'agence PR ;
- de s'assurer auprès du destinataire (et de se le faire garantir) que ce dernier utilisera les données de manière strictement conforme à la réglementation applicable en matière de protection des données à caractère personnel et dans le respect de ses propres obligations en matière de protection des données à caractère personnel.

[121] Voir le paragraphe « Justification des destinataires » ci-dessus

• **CAS N°3 :** Un client transmet à l'agence PR le fichier presse utilisé par la précédente agence à laquelle il faisait appel ou un freelance transmet à l'agence PR avec laquelle il collabore un fichier presse récupéré au cours de ses précédentes missions. Une telle communication est-elle autorisée ?

Une telle pratique peut engendrer des risques sur le plan de la responsabilité pénale (par exemple, « vol de données ») ou de la responsabilité civile (par exemple, concurrence déloyale) en droit commun.

En matière de protection de données à caractère personnel, il convient de s'assurer que les personnes concernées ont été dûment informées du traitement de leurs données et que l'agence PR peut licitement utiliser ce fichier (voir sur ce point l'ensemble des recommandations ci-dessus s'agissant de l'achat / de la location de fichiers).

A sécuriser contractuellement !

3.2
BONNES PRATIQUES EN MATIÈRE D'UTILISATION DES DONNÉES

3.2.1 Les modes de communication

Dans le cadre de leur activité « cœur de métier », les agences PR peuvent être amenées à utiliser des données à caractère personnel dans les situations suivantes par exemple :

- envoi de sa propre newsletter à ses clients / prospects ;
- invitations à des événements adressées à ses clients, à des journalistes / influenceurs / Key Opinion Leaders ;
- envoi de communiqués de presse aux journalistes / influenceurs / Key Opinion Leaders ;
- prise de contact par téléphone, sur les réseaux sociaux, par email, par courrier postal, par sms,... avec des journalistes / influenceurs / Key Opinion Leaders.

Il convient de garder à l'esprit que l'ensemble de ces activités constituent des opérations de « prospection » au sens du droit. Ainsi, de telles opérations sont soumises à un régime juridique spécifique, en fonction du mode de communication utilisé[122], tel que décrit au paragraphe « Le cas particulier de la prospection par courrier électronique, télécopie ou système automatisé de communications électroniques » ci-dessus.

Pour mémoire, le régime de la prospection peut être synthétisé comme suit :

PROSPECTION AUTORISÉE UNIQUEMENT SI RECUEIL PRÉALABLE DU CONSENTEMENT		
Prospection par courrier électronique (email, sms, mms) Exception 1 : exception dite des « produits et services analogues » Exception 2 : exception dite du « B to B »	Prospection par télécopie	Prospection par système automatisé de communications électroniques

PROSPECTION AUTORISÉE SI ABSENCE D'OPPOSITION		
Appel téléphonique avec intervention humaine	Courrier postal	Courrier électronique (email, sms, mms) s'il est possible de se prévaloir de l'exception dite des « produits ou services analogues » ou encore de l'exception dite du « B to B »

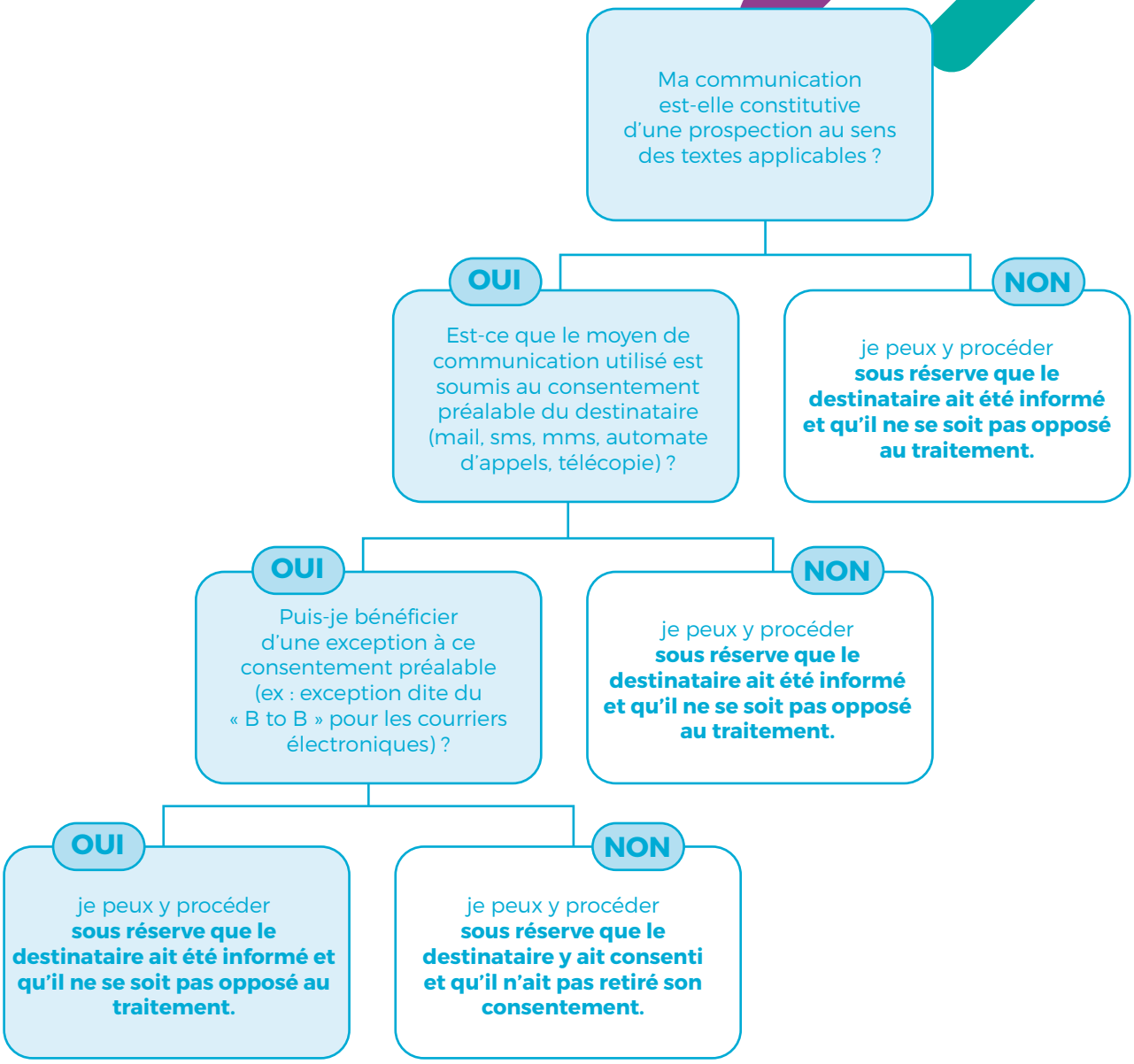
A contrario, ne constituent pas des opérations de prospection l'utilisation des données des contacts ou interlocuteurs d'une agence PR chez ses clients dans le cadre de l'exécution du contrat de prestation de services conclu avec ces derniers par exemple (échange d'emails relatifs à un projet confié à l'agence PR, à la facturation, ...).

Enfin, en tout état de cause, quel que soit le support utilisé pour **les opérations de sollicitation, les personnes concernées disposent d'un droit d'opposition au traitement de leurs données par l'agence PR à des fins de prospection, auquel l'agence PR est tenue de faire droit**[123]. Les personnes concernées doivent être informées notamment de l'existence d'un tel droit dans les mentions d'information qui doivent leur être fournies par l'agence PR s'agissant du traitement de leurs données par cette dernière (voir à cet égard le paragraphe « Loyauté et transparence » ci-dessus), étant précisé que l'agence PR doit bien entendu indiquer un moyen ou des coordonnées valables auxquelles le destinataire peut utilement transmettre une demande tendant à obtenir que les communications cessent sans frais autres que ceux liés à la transmission de celle-ci[124].

[122] Voir notamment les pages de la Cnil relatives à la prospection commerciale par courrier électronique (28 décembre 2018) et à la prospection commerciale par courrier postal et par téléphone (6 décembre 2019).
[123] Voir notamment les pages de la Cnil relatives à la prospection commerciale par courrier électronique (28 décembre 2018) et à la prospection commerciale par courrier postal et par téléphone (6 décembre 2019).
[124] Cf. article 21 du RGPD. Pour en savoir plus, voir le paragraphe « Le droit d'opposition » ci-dessus.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

Aussi, avant de communiquer avec un prospect, un client, un journaliste, un influenceur, un Key Opinion Leader, il convient de se poser les questions suivantes, représentées ci-dessous sous la forme d'un algorithme juridique ou « arbre de décision » :



En outre, les messages de sollicitation qui sont adressés doivent comporter une possibilité permettant aux destinataires de s'opposer à recevoir de nouvelles sollicitations ultérieures.

Aussi, lorsqu'il est envisagé par l'agence PR d'adresser, en qualité de responsable de traitement, de la prospection par courrier électronique à ses clients, prospects, et plus généralement contacts, ou encore à des journalistes ou à des Key Opinion Leaders, il convient d'insérer en footer / pied-de-page de chacun des emails adressés dans ce contexte, outre une mention d'information adaptée lorsque tel est nécessaire, une mention spécifique de type :

OPTION 1 : « Si vous souhaitez vous désabonner de la newsletter de [désignation de l'agence PR], rendez-vous sur cette page [insérer un lien vers une page permettant au destinataire de gérer, de manière simple et dénuée d'ambiguïté, sans frais, ses « préférences » en termes de prospection commerciale] ».

OPTION 2 : « Pour vous désinscrire des communications de [désignation de l'agence PR] par emails, rendez-vous sur cette page [insérer un lien vers une page permettant au destinataire de gérer, de manière simple et dénuée d'ambiguïté, sans frais, ses « préférences » en termes de prospection commerciale] ».

OPTION 3 : « Vous ne souhaitez plus recevoir l'actualité de [désignation de l'agence PR] par emails ? Cliquez-ici [insérer un lien vers une page permettant au destinataire de gérer, de manière simple et dénuée d'ambiguïté, sans frais, ses « préférences » en termes de prospection commerciale] »

De même, lorsque la prospection commerciale est adressée par sms ou par mms, il conviendra d'intégrer un lien de type :

« STOP SMS » [+ numéro court ou un lien vers une page web pour se désabonner].

Un procédé similaire doit être prévu s'agissant des opérations de prospection qui seraient réalisées par télécopie ou par système automatisé de communications électroniques, mais également pour les envois par courrier postal ou encore en cas d'appels téléphoniques de type « télémarketing ».

Enfin, pour mémoire, il convient de **conserver une trace** de toute demande d'opposition qui serait reçue par l'agence PR ainsi que de son traitement par l'agence, notamment afin de conserver une preuve de sa prise en compte effective (voir à cet égard le paragraphe « Le traitement des demandes » ci-dessus).

(ILLUSTRATION)

A titre d'illustration, lorsqu'un contact chez un prospect indique à l'agence PR qu'il ne souhaite plus recevoir de communiqués de presse relatifs à un sujet en particulier ou à un client par exemple, il convient en pratique (i) de suivre les différentes étapes de traitement des demandes telles que présentées ci-avant dans le paragraphe dédié, (ii) d'identifier ledit destinataire dans les outils / applications / fichiers utilisés par l'agence PR comme refusant de recevoir de telles communications et (iii) supprimer les coordonnées de ce destinataire concerné des listes de diffusion correspondantes (tout en s'assurer que l'information de l'opposition de celui-ci est bien enregistrée dans la « liste repoussoir » qui doit être vérifiée avant envoi de toute communication).

FOCUS SUR L'OPPOSITION DES PERSONNES CONCERNÉES À RECEVOIR DES SOLLICITATIONS

ATTENTION :

- bien entendu, il ne suffit pas de laisser au destinataire la possibilité de s'opposer à recevoir des communications ou à être contacté, **il convient que les demandes de ce dernier en ce sens soient suivies d'effet, c'est-à-dire qu'il ne reçoive plus les communications ou ne soit plus contacté s'il en a fait la demande !**
- même si l'agence PR met en place des procédés automatisés de gestion des demandes d'opposition ou informe le destinataire de divers moyens de contacts dédiés permettant à ce dernier d'exercer ses droits, **il convient d'être en mesure de gérer toute demande en ce sens et d'en répercuter, éventuellement manuellement, les conséquences dans les outils / applications / fichiers utilisés, même si ces demandes ne sont pas formulées par les moyens mis explicitement à disposition des destinataires à cette fin.** A titre d'illustration, les demandes qui seraient formulées au moyen de la messagerie privée proposée par un réseau social devront être prises en compte, tout comme les demandes qui arriveraient sur une adresse de messagerie électronique dédiée par exemple.

PUBLIC CIBLE : DIRECTION, MANAGERS PR

LE SAVIEZ-VOUS ?

Dans le cadre de la mise en place d'un processus permettant aux personnes concernées de s'opposer au traitement de leurs données à caractère personnel à des fins de prospection / sollicitation, il est possible de permettre à celles-ci de **gérer leurs préférences** selon les thématiques ou sujets abordés dans les communications ou encore selon les types de communication, à l'aide de cases à cocher par exemple (cf. **granularité** des modalités d'exercice du droit d'opposition), étant précisé que les personnes concernées doivent pouvoir **s'opposer de manière globale** à l'ensemble des communications adressées à des fins de prospection.

En effet, à titre d'illustration, si une personne concernée s'oppose à la réception de prospection par email en cliquant sur le lien prévu à cet effet dans un email reçu, tel que proposé ci-dessus, alors il convient en principe de ne plus lui adresser d'emails de prospection (du tout !). Toutefois, est-ce que la demande du destinataire concerne uniquement les emails portant sur la thématique de l'email via lequel il a exercé son droit d'opposition ou tous les emails portant sur toutes les thématiques ? Est-ce que la demande concerne uniquement les emails ou tous les moyens de communication ? etc. Il en est de même lorsqu'une personne exprime son souhait de ne plus être appelée : est-ce que cette opposition doit être étendue à toutes les communications ? uniquement aux appels téléphoniques ? uniquement aux appels téléphoniques portant sur une thématique particulière ?

Il résulte de ce qui précède que de telles demandes, si elles ne sont pas précises, peuvent être sources de confusion ou de difficultés d'interprétation, et donc sources de risque juridique pour l'agence. En outre, il serait dommage pour une agence de se priver d'adresser tout type de communications alors que le destinataire s'oppose à recevoir uniquement certaines de ces communications ou uniquement par certains vecteurs…

Aussi, il est opportun de prévoir **un process permettant aux destinataires des communications de gérer les types de communications qu'ils souhaitent ou non recevoir :**

- par thématique ;
- par expéditeur ;
- par type de moyen de communications ;
-…

A titre d'exemple, le lien à insérer dans un email et permettant au destinataire d'une communication de se désabonner pourra utilement renvoyer vers une page web lui permettant de gérer ses choix, ses préférences. Attention tout de même, cette page doit permettre au destinataire de faire ses choix facilement et sans que le process à suivre puisse être interprété comme créant un empêchement à exercer ses choix de manière simple et effective (notamment, une possibilité « tout refuser » devrait lui être proposée par exemple).

En tout état de cause, pour faciliter la gestion, le traitement et le suivi des demandes d'opposition, et limiter les risques de ne pas tenir compte d'une demande d'opposition par exemple, il convient de **centraliser les préférences des personnes concernées en matière de prospection dans un outil, une application ou un fichier dédié(e) et unique par public concerné.** En effet, les extractions de fichiers « contacts » / « presse » / … entraînent une duplication des données à caractère personnel traitées par l'agence PR et la multiplicité des supports dans lesquelles elles sont stockées rend extrêmement difficile, voire impossible, en l'absence de process centralisé, la gestion des demandes d'exercice des droits qui seraient adressées par les personnes concernées.

A titre d'illustration, la centralisation des données dans un outil, une application ou un fichier dédié(e) et unique par public concerné pourrait être particulièrement opportune pour ce qui concerne les demandes d'opposition émanant des influenceurs dans la mesure où la gestion de telles demandes qui seraient formulées par message privé via un réseau social par exemple ne semble pas pouvoir être automatisée. Il appartiendra alors à tout collaborateur de l'agence PR, avant de contacter un influenceur, de vérifier dans l'outil, l'application ou le fichier dédié(e) aux influenceurs s'il est possible ou non de le contacter par messagerie privée, pour le sujet envisagé,… afin d'assurer l'effectivité des éventuelles demandes d'opposition qui auraient pu être formulées par l'influenceur concerné.

FOCUS SUR LA PROSPECTION ENVOYÉE PAR L'AGENCE PR POUR LE COMPTE DE SES CLIENTS

Lorsque l'agence PR agit en qualité de sous-traitent pour le compte d'un client responsable du traitement (par exemple, lorsque l'agence PR envoie à une liste de contacts d'un client une newsletter ou un communiqué pour le compte du client et selon les instructions de ce dernier), alors l'appréciation du fondement juridique approprié pour de tels envois, l'information des personnes concernées ou encore les modalités d'opposition à l'envoi de telles communications, et plus généralement **l'ensemble des principes et précautions susvisés dans le présent paragraphe relatif aux modes de communication relèvent de la responsabilité du client, en raison de sa qualité de responsable de traitement.**

Pour autant, et pour mémoire, **en cas de non-conformité des instructions données à l'agence PR par le responsable de traitement au regard de la réglementation applicable en matière de protection des données à caractère personnel, et notamment des principes applicables en la matière, l'agence PR doit en alerter immédiatement ce dernier.**

En cas d'opposition à une communication qui serait reçue par l'agence PR et qui concernerait les envois réalisés pour le compte de son client, **il convient d'en répercuter les conséquences au sein des outils, applications, bases de données, … utilisé(e)s par l'agence PR dans ce cadre et de remonter cette information au client,** le cas échéant selon les conditions et modalités prévues au contrat conclu avec ce dernier.

Néanmoins, et sous réserve de la granularité choisie par le responsable de traitement (cf. encadré ci-dessus), l'exercice du droit d'opposition à de telles communications au nom du client signifie qu'il ne sera plus possible de lui en envoyer pour le compte du client concerné mais ne signifie pas pour autant nécessairement que l'agence PR ne pourra plus adresser sa propre prospection à de tels contacts en tant que responsable de traitement ou encore les communications qu'elle pourrait être amenée à effectuer pour le compte de ses autres clients. Chaque situation devra donc faire l'objet d'une analyse au cas par cas pour en déterminer les conséquences concrètes et effectives à déployer, en concertation avec le client concerné.

3.2.2 La conservation des données traitées

Pour mémoire, comme indiqué ci-dessus au paragraphe « Proportionnalité de la conservation des données à caractère personnel », la conservation illimitée des données à caractère personnel est par principe interdite.

(ILLUSTRATIONS)

A titre d'illustration, la Cnil recommande de ne pas conserver les données de clients au-delà de la durée strictement nécessaire à la gestion de la relation commerciale et qu'elles peuvent être conservées à des fins de prospection commerciale au maximum pendant 3 ans à compter de la fin de cette relation commerciale. Pour les prospects, la Cnil recommande de conserver les données pendant maximum 3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect. Au-delà, les données peuvent être archivées pendant les délais légaux de prescription et les durées obligatoires de conservation[125].

Par ailleurs, la Cnil recommande de ne pas conserver les données de fournisseurs au-delà de la durée de la relation avec le fournisseur augmentée des délais légaux de prescription et des durées de conservation obligatoire[126].

Enfin, en l'absence de recommandations spécifiques relatives aux données des journalistes, des influenceurs ou encore Key Opinion Leaders, les durées précitées pourraient tout de même être un point de départ en vue de la détermination par l'agence de durées de conservation maximum des données.

[125] Cnil, Délibération n° 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects, NS-048.
[126] Cnil, Délibération n°2005-005 du 18/01/2005 décidant de la dispense de déclaration des traitements relatifs à la gestion des fichiers de fournisseurs comportant des personnes physiques, DI-004.

Ainsi, pour chaque finalité poursuivie, l'agence PR doit déterminer une durée de conservation maximum des données à caractère personnel qu'elle traite (sous forme de données d'utilisation « courante » puis d'« archives ») ainsi que le point de départ d'une telle durée.

Lorsque le point de départ est « glissant » (par exemple, lorsque le point de départ est le dernier contact avec la personne concernée émanant de cette dernière), il convient de pouvoir **tracer les dates de ces différents contacts** afin que la computation de la durée de conservation soit effective en pratique.

Pour parvenir à gérer de manière précise les durées de conservation, il convient d'automatiser si possible ce processus, celui-ci devant permettre de gérer :

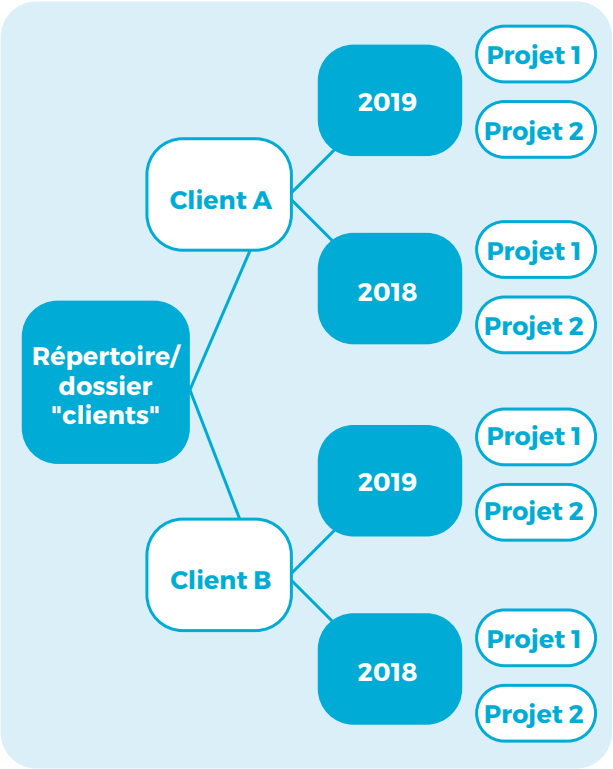
- le suivi des contacts avec les personnes concernées : pour chaque contact, il convient en effet de tracer la date, les modalités et le moyen de contact ;
- la durée de conservation des données sous forme active puis sous forme d'archives, à compter du point de départ pertinent (à titre d'exemple, c'est en principe le dernier contact émanant de la personne concernée dont il doit être tenu compte et non le dernier contact « tout court »).

Si tel n'est pas le cas ou n'est pas envisageable en fonction de l'organisation de l'agence PR concernée, il convient *a minima* d'élaborer et de déployer en interne une politique manuelle de conservation, d'archivage et de purge des données.

(ILLUSTRATIONS)

A titre d'illustration, pour ce qui concerne les données qui seraient conservées dans des fichiers au sein de « répertoires réseau » de l'agence PR, il pourrait être envisagé d'organiser un système de classement par client et, au sein de chaque « répertoire/dossier client », d'intégrer un « répertoire/dossier » par année puis un sous-répertoire par opération ou projet du client, et ce afin de faciliter la mise en œuvre manuelle d'une telle politique de conservation, d'archivage et de purge des données.

De manière schématique, il s'agirait par exemple de mettre en place l'architecture suivante sur les répertoires réseau :



Une fois cette architecture créée, un process spécifique pourrait être formalisé et documenté afin que les durées de conservation puissent être gérées a minima année par année.

FOCUS SUR LES EXTRACTIONS SOUS FORME DE TABLEURS EXCEL DES FICHIERS DE CONTACTS

lLa mise en œuvre d'un processus de gestion des durées de conservation au sein d'une agence PR requiert une attention et une rigueur de la part de l'ensemble des collaborateurs. Pour en assurer l'effectivité et l'efficacité, il est recommandé de **centraliser les données dans un outil / une application métier unique** (pour chacun des finalités poursuivies et/ou par public concerné).

Ainsi, la pratique selon laquelle un collaborateur procède à des **extractions sur son poste de travail,** en format Excel, de fichiers de contacts (clients, prospects, journalistes, influenceurs,...) conservés dans un outil / une application métier doit être **proscrite ou, a minima, limitée** à ce qui est strictement nécessaire, pour des hypothèses précises et uniquement pour un laps de temps assez court.

En effet, une telle pratique entraîne une duplication des données à caractère personnel traitées par l'agence PR et la multiplicité des supports dans lesquelles elles sont stockées **rend extrêmement difficile, voire impossible,** la gestion des durées de conservation des données à caractère personnel au sein de l'agence PR.

Ainsi, il appartient à chaque agence PR de déterminer s'il est opportun de tolérer une telle pratique et, dans l'affirmative, de définir les conditions dans lesquelles les collaborateurs y sont autorisés. Par exemple, de telles extractions pourraient être autorisées pour élaborer un listing pour un évènement précis ou pour une campagne déterminée, en précisant que le fichier Excel ainsi extrait devra être enregistré dans le répertoire réseau / dossier approprié et supprimé définitivement par le collaborateur de son poste de travail au plus tard une fois l'événement ou la campagne réalisé.

3.2.3 Le recours à des prestataires

Pour mémoire, la qualification des différents acteurs doit faire l'objet d'une attention particulière, et ce notamment en raison des obligations attachées à la qualification de responsable, le cas échéant conjoint, de traitement et de sous-traitant et des éléments devant être contractualisés pour encadrer les rôles et responsabilités de chacun (voir à cet égard le paragraphe « Encadrer les relations avec les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel ».

(EXEMPLES)

EXEMPLE 1 : LE PRESTATAIRE DE ROUTAGE / D'ENVOI D'EMAILINGS

A titre d'illustration, le prestataire de routage / d'envoi d'emailings, auquel une agence PR, en qualité de responsable de traitement, peut avoir recours pour la diffusion de communiqués de presse ou d'invitations au nom et pour le compte de l'agence PR, agit en qualité de sous-traitant pour le compte de ladite agence PR. Dans cette hypothèse, un contrat devant comporter les éléments obligatoires au titre de l'article 28 du RGPD relatifs à l'objet et à la durée du traitement, à la nature et à la finalité du traitement, aux types de données à caractère personnel pouvant être traitées et aux catégories de personnes concernées, ainsi que les obligations et les droits du prestataire et de l'agence PR doit être conclu par cette dernière avec le prestataire de routage d'emailings auquel elle fait appel. En outre, si le prestataire fournit à l'agence PR une liste de contacts auxquels celle-ci pourrait adresser ses communications, il convient de s'assurer contractuellement que les données ont été collectées de manière loyale et licite et que l'agence PR peut licitement les utiliser.

Pour un autre exemple, lorsque l'agence PR fait appel à un prestataire de routage / d'envoi d'emailings pour la diffusion de courriers électroniques à l'attention de destinataires dont les coordonnées ont été communiquées par un client de l'agence, alors l'agence PR peut dans certains cas être considérée comme agissant en qualité de sous-traitant pour le compte de ce client. Dans cette hypothèse, le prestataire de routage d'emailings est un « sous-traitant de second niveau » ou « sous-traitant ultérieur ». Un contrat comportant les mêmes obligations en matière de protection de données que celles imposées à l'agence PR dans le contrat conclu entre le client et l'agence PR doit être conclu entre le prestataire de routage d'emailings et l'agence PR.

Par ailleurs, dans le cas où l'agence a recours à des prestataires hors Union européenne ou qui hébergent ou stockent ou traitent les données hors Union européenne, des clauses contractuelles spécifiques complémentaires doivent également être prévues pour assurer une protection effective des données à caractère personnel traitées.

(EXEMPLES)

EXEMPLE 2 : LES FREELANCES

Lorsque l'agence PR a recours à des freelances (spécialisés par exemple dans la communication de crise ou la communication stratégique), ces derniers peuvent être considérés comme agissant en qualité de sous-traitants de l'agence PR lorsqu'ils accèdent à des données à caractère personnel dans le cadre de leurs missions. Aussi, une clause spécifique comportant l'ensemble des éléments susvisés qui sont obligatoires au titre de l'article 28 du RGPD doit être insérée dans le contrat de freelance.

A titre de bonnes pratiques visant à s'assurer de l'encadrement contractuel des relations entre l'agence PR et les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel, et ce en fonction de l'organisation de l'agence PR, il doit être envisagé :

- que les opérationnels soient tenus **d'informer immédiatement et systématiquement le service juridique de l'agence PR et/ou le DPO ou, à défaut, le référent** en matière de protection des données à caractère personnel **dès lors qu'il est envisagé de faire appel à un tiers dans le cadre de traitements de données à caractère personnel** afin de faire valider les contrats à conclure, étant précisé qu'en fonction de la situation rencontrée il pourrait également être opportun de faire appel à un conseil extérieur à l'agence spécialisé en la matière ; ou encore
- que **des modèles de clauses types / d'avenants types** soient élaborés et mis à disposition des opérationnels et que ces derniers soient en mesure de les ajuster, étant précisé qu'en cas d'incertitude ou de doute sur la qualification des parties ou sur le contenu des clauses contractuelles à ajuster, ils devraient être tenus d'en informer immédiatement et systématiquement le service juridique de l'agence PR et/ou le DPO ou, à défaut, le référent en matière de protection des données à caractère personnel.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

4.1
BONNES PRATIQUES EN MATIÈRE DE COLLECTE DES DONNÉES

4.1.1 Les règles d'or : transparence, loyauté et minimisation

Pour mémoire, la réglementation applicable en matière de protection des données à caractère personnel doit être respectée par tout agence PR traitant des informations se rapportant à une personne physique identifiée ou identifiable, **y compris lorsque cette personne est un candidat à une offre d'emploi au sein de l'agence PR ou un membre du personnel de l'agence PR.**

Aussi, dans le cadre de leurs activités de ressources humaines, les agence PR agissent en qualité de responsable de traitement et doivent de ce fait veiller au respect de tous les principes applicables en la matière tels que présentés au paragraphe « Analyser la conformité des traitements de données à caractère personnel » ci-dessus.

Les paragraphes ci-après ont vocation à présenter aux agences PR les bonnes pratiques qui pourraient être opportunément déployées s'agissant en particulier des principes de loyauté et de transparence du traitement ainsi que de minimisation des données, étant bien entendu rappelé que le respect des autres principes applicables en la matière demeure évidemment requis.

4.1.2 Les différents types de personnes concernées et les modalités de collecte / d'information

Pour mémoire, chaque agence PR doit s'assurer que les données qu'elle traite concernant des candidats à un emploi, membres du personnel, stagiaires, intérimaires,... ont été collectées de manière loyale et transparente : il s'agit de faire en sorte que les personnes dont les données sont traitées soient informées des caractéristiques et modalités du traitement de leur données à caractère personnel.

A cet égard, il est rappelé que l'information fournie doit comporter l'ensemble des éléments obligatoires tels que présentés dans le tableau « Informations générales à fournir » au paragraphe « Loyauté et transparence » ci-dessus. A défaut d'information des personnes concernées conforme à la réglementation applicable en matière de protection des données à caractère personnel, le traitement de leurs données à caractère personnel est en principe illicite.

Aussi, il est proposé ci-après à titre indicatif des recommandations pouvant aider les agences PR à déterminer sur quel support et selon quelles modalités l'information des candidats à un emploi, membres du personnel, stagiaires, intérimaires,... s'agissant du traitement de leurs données à caractère personnel pourra être réalisée.

4.1.2.1 Les candidats postulant à un emploi au sein de l'agence PR

Afin de fournir aux candidats postulant à un emploi au sein de l'agence PR dont les données sont traitées par l'agence PR une information conforme à la réglementation applicable en matière de protection des données à caractère personnel, il convient d'identifier de manière exhaustive les sources et modalités de collecte des données les concernant afin de déterminer selon quelles modalités et sur quels supports l'information desdits candidats pourra être fournie, de manière complète, lors de la collecte des données.

(ILLUSTRATION)

A titre d'illustration, des données à caractère personnel relatives aux candidats à une offre d'emploi sont susceptibles d'être collectées auprès des candidats concernés eux-mêmes, sur le site internet de l'agence PR (cf. collecte directe) mais également sur des sites internet de tiers spécialisés dans le recrutement ou encore auprès de cabinets de recrutement (cf. collecte indirecte).

Quelle que soit la manière dont les données d'un candidat à une offre d'emploi sont collectées, celui-ci doit être dûment informé par l'agence PR du traitement des données le concernant mis en œuvre par cette dernière.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

La Cnil recommande que les personnes chargées du recrutement prennent toutes les dispositions nécessaires pour informer le candidat, dans un délai raisonnable, de l'issue donnée à sa candidature, des caractéristiques du traitement de ses données à caractère personnel (dénomination de l'agence PR responsable du traitement, finalités poursuivie, durée de conservation des données, destinataires,...) ainsi que de la possibilité de demander la restitution ou la destruction des informations le concernant[127] .

Ainsi :

- **lorsque les données sont collectées directement auprès d'un candidat à une offre d'emploi,** celui-ci doit être informé du traitement de ses données au moment où celles-ci sont collectées, par exemple de la manière suivante :

FORMULAIRE PAPIER DE COLLECTE DE DONNÉES	FORMULAIRE EN LIGNE DE COLLECTE DE DONNÉES, SUR LE SITE INTERNET DE L'AGENCE PR	CANDIDATURE ADRESSÉE PAR COURRIER OU EMAIL À L'AGENCE PR
• Mention d'information sur le support de collecte (par exemple un formulaire papier de recrutement) + sur un document complémentaire (préalable ou concomitant) comportant l'intégralité des informations requises (si l'information figurant sur le formulaire est «allégée»)	• Mention d'information sur le formulaire de collecte dédié au recrutement sur le site internet de l'agence + renvoi vers une rubrique du site internet de l'agence PR comportant sa politique complète de protection des données en ligne (si l'information figurant sur le formulaire est « allégée »)	• Accusé de réception de la candidature (sans délai) comportant une mention d'information complète ou en footer / pied de page / dans le pavé de signature une mention éventuellement allégée et renvoyant (i) vers la politique complète de protection des données de l'agence en pièce jointe et/ou (ii) par un lien hypertexte à cette même politique en ligne (cf. rubrique dédiée)

- **lorsque les données d'un candidat sont collectées indirectement,** celui-ci doit, en principe, être informé du traitement de ses données dans un délai raisonnable après obtention desdites données par l'agence PR (ne dépassant pas un mois) ou, si les données doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec cette dernière ou, s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Cette information pourra par exemple être fournie au candidat dès réception de ses coordonnées par l'agence PR en intégrant une mention d'information complète dans un email dédié ou une mention d'information « allégée » en footer (cf. pied d'email / pavé de signature) renvoyant vers la politique complète de protection des données de l'agence PR en pièce jointe et/ou en ligne (cf. lien hypertexte vers une rubrique dédiée sur son site internet).

Il convient également s'assurer et de se faire garantir contractuellement auprès du tiers ayant communiqué des données relatives à des candidats (par exemple, sites internet spécialisés dans le recrutement ou cabinets de recrutement), que (i) la collecte des données des candidats a été effectuée de manière loyale et licite (information des personnes concernées, etc.) et que (ii) les données peuvent être licitement réutilisées par l'agence PR aux fins d'étude et d'analyse des candidatures ainsi que de gestion de ses processus de recrutement.

[127] Cnil, Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

LE SAVIEZ-VOUS ?

Bien qu'il ne s'agisse pas stricto sensu d'une problématique relevant de la réglementation applicable en matière de protection des données à caractère personnel, il est précisé que **le candidat à un emploi doit être expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard**[128].

En outre, selon la Cnil, si des techniques d'aide au recrutement devaient être utilisées avec **pour effet ou objet la définition d'un profil ou de la personnalité du candidat,** alors il conviendrait de déployer un processus selon lequel :

- le **consentement** explicite du candidat devrait être recueilli ;
- le candidat devrait ensuite être **informé des résultats, pouvoir obtenir une intervention humaine,** exprimer son point de vue / faire valoir ses observations et contester la décision ;
- en tout état de cause, **une candidature ne peut être exclue sur le seul fondement de méthodes et techniques automatisées** d'aide au recrutement et doit faire l'objet d'une appréciation humaine (la Cnil recommandant d'ailleurs à ce titre que les outils d'évaluation automatisés excluant toute appréciation humaine sur la candidature soient proscrits)[129].

[128] Cf. article L.1221-8 du Code du travail.
[129] Cnil, Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

FOCUS SUR LA COLLECTE DE DONNÉES AUPRÈS DE « RÉFÉRENCES PROFESSIONNELLES »

Dans le cadre des opérations de recrutement, un employeur peut souhaiter obtenir des informations relatives à un candidat à un emploi auprès de ses anciens employeurs / de collaborateurs de son ancienne équipe (cf. poste(s) occupé(s) précédemment par ledit candidat) ou de son employeur actuel / de collaborateurs de son équipe actuelle (cf. poste occupé au moment des opérations de recrutement par ledit candidat) ou de tout autre tiers dans l'environnement professionnel du candidat susceptible de fournir à l'agence PR des informations sur ledit candidat (par exemple, auprès d'un client).

Si une telle pratique n'est pas en tant que telle interdite, sous réserve bien entendu du respect de l'ensemble des principes applicables en matière de données à caractère personnel, les précautions suivantes doivent être adoptées par l'agence PR :

- il convient de s'assurer qu'**aucune « référence professionnelle » sur les candidats n'est recueillie** auprès de l'environnement professionnel passé ou présent du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients, ...) à son insu (cf. nécessité d'en informer le candidat) ;
- il convient de s'**interdire le recours éventuel à des « références personnelles » aux fins de diligenter une enquête dite « de moralité »** par exemple et, en tout état de cause, faire preuve de modération et de mesure dans les informations demandées aux tiers.

En outre, les personnes contactées dans ce cadre doivent être dûment informées du traitement de leur données à caractère personnel mis en œuvre par l'agence PR à leur égard, conformément à la réglementation applicable en matière de protection des données à caractère personnel (cf. hypothèse de collecte indirecte de données).

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

FOCUS SUR LA COLLECTE DE DONNÉES « EN LIGNE »

Comme tout employeur à la recherche de profils professionnels en vue de postes à pourvoir, les agences PR peuvent être amenées à rechercher des informations sur de potentiels candidats en ligne, par exemple via les sites de recrutement spécialisés ou encore au moyen d'informations disponibles sur les réseaux sociaux.

A titre liminaire, il convient de préciser qu'une telle pratique doit être utilisée avec précautions.

Par ailleurs, selon la Cnil, il convient de distinguer 3 situations différentes :

- **si l'employeur recherche des informations sur des sites de recrutement pour lesquels il achète des accès (Monster, APEC , Cadremploi, etc.) :** la recherche est considérée comme loyale car en s'inscrivant sur ces sites, la personne concernée a été informée et/ou a donné son accord pour la diffusion de ses données. Attention tout de même : une telle information et/ou un tel consentement dépendent de ces sites et l'agence PR n'a pas « la main » dessus. Par conséquent, il convient en principe (i) que l'agence s'assure que de tels sites internet lui garantissent que les données ont été collectées et sont traitées de manière loyale et licite et (ii) **que l'agence PR prévoit en tout état de cause d'adresser immédiatement suite à la collecte / au traitement des données d'une personne concernée, une information dédiée** à l'attention de cette personne conforme à la réglementation applicable en matière de protection des données à caractère personnel ;
- **si l'employeur recherche des informations sur des réseaux sociaux professionnels (Linked-In, Viadeo, Doyoubuzz, etc.) :** la recherche est loyale car l'objectif professionnel de ces réseaux est clairement identifié. Aucune information relative à la vie privée de la personne n'apparaît en principe sur ces sites, mais il lui appartient de maîtriser les données qu'ils diffusent ainsi sur elle. En tout état de cause, les mêmes précautions que celles visées pour les sites de recrutement ci-contre doivent être prises ;
- **si l'employeur recherche des informations sur des réseaux sociaux personnels (Facebook, Copains d'avant, Twitter, des forums,...) ou en tapant un nom sur Google ou dans tout autre moteur de recherche :** ces sites révèlent souvent de nombreuses informations relatives à la vie privée. L'employeur **n'a pas le droit** de collecter ces informations, une telle collecte s'apparentant à une enquête de « moralité », par principe interdite.

ATTENTION : même dans les cas considérés par la Cnil comme des hypothèses « autorisées », il convient de s'assurer que :

- le site ou le réseau social concerné par les recherches est clairement identifié comme ayant un objectif professionnel ;
- les informations recueillies par l'agence sont strictement professionnelles, pertinentes et nécessaires pour le poste concerné à pourvoir ;
- la personne concernée est informée de ce traitement de données à caractère personnel au plus tôt, et conformément à la réglementation applicable en matière de protection des données à caractère personnel.

Enfin, il est rappelé qu'il convient de ne **collecter que les informations issues de profils dits « publics » + en cas de prise de contact de se présenter sous sa véritable identité (+ nom de l'agence) + d'expliquer l'objectif de recrutement poursuivi** (ex: ne pas « demander quelqu'un en contact » pour visualiser un profil plus complet sans expliquer les véritables intentions et objectifs poursuivis).

FOCUS SUR LA CONSTITUTION D'UN VIVIER DE CANDIDATURE / D'UNE CVTHÈQUE

En cas d'issue négative donnée à une candidature, l'agence PR peut souhaiter conserver les informations envoyées par le candidat concerné (cf. CV et lettre de motivation) si toutefois son profil est susceptible d'intéresser l'agence PR pour un futur poste.

Outre le fait que le candidat doit en être informé, par exemple dans le courrier ou dans l'email rejetant sa candidature, il convient de garder à l'esprit que **ces informations ne peuvent, selon la doctrine de la Cnil, être conservées sous forme « active » dans la CVthèque que pendant une durée maximum de deux ans** à compter de la réception de la candidature. Si l'agence PR souhaite conserver sa candidature plus longtemps, alors il conviendra (i) qu'une telle durée allongée puisse être justifiée (ex : marché tendu, profil rare et difficulté de recrutement pour certains postes par exemple) et (ii) de recueillir le consentement du candidat à cette fin, après lui avoir par exemple proposé de mettre à jour ses informations (cf. à défaut, risque de CV obsolète).

4.1.2.2 Les membres du personnel

Afin de fournir aux membres du personnel de l'agence PR dont les données sont traitées par l'agence PR dans le cadre de la gestion des ressources humaines (en ce incluant notamment la gestion administrative du personnel et la gestion de la paie) une information conforme à la réglementation applicable en matière de protection des données à caractère personnel, il convient d'identifier de manière exhaustive les sources et modalités de collecte des données les concernant afin de déterminer selon quelles modalités et sur quels supports l'information des membres du personnel pourra être fournie, de manière complète, lors de la collecte des données.

(ILLUSTRATION)

A titre d'illustration, des données à caractère personnel relatives aux membres du personnel de l'agence PR sont susceptibles d'être collectées auprès des membres du personnel eux-mêmes lors de leur embauche par exemple mais également tout au long de leur vie professionnelle au sein de l'agence.

Quelle que soit la manière dont les données d'un membre du personnel sont collectées, celui-ci doit être dûment informé par l'agence PR du traitement des données le concernant mis en œuvre par cette dernière, en principe au moment de la collecte de ses données.

A cet égard, la Cnil précise que si le RGPD n'impose aucune forme spécifique, une information écrite doit être privilégiée de manière à pouvoir justifier de son contenu, ainsi que du moment où elle a été délivrée.

A titre d'illustration, les pratiques suivantes doivent être déployées :

FORMULAIRE PAPIER DE COLLECTE DE DONNÉES

- Mention d'information sur le support de collecte (par exemple un formulaire papier d'embauche, à remettre en main propre ou par email) + sur un document complémentaire (préalable ou concomitant) comportant l'intégralité des informations requises (si l'information figurant sur le formulaire est « allégée »), tel qu'une notice dédiée, un livret d'accueil, une note interne ou tout autre document qui pourrait être remis / envoyé au membre du personnel dans le cadre de l'embauche.

EN TOUT ÉTAT DE CAUSE

- Il convient de fournir aux membres du personnel une mention d'information écrite appropriée (et de conserver la preuve de cette communication), par exemple en intégrant une mention d'information complète dans une notice dédiée, un livret d'accueil, une note interne ou tout autre document qui pourrait être remis dans le cadre de l'embauche.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

(EXEMPLE)

Exemple de mention d'information « complète » pouvant être intégrée par exemple dans une notice dédiée, un livret d'accueil, une note interne ou tout autre document qui pourrait être remis /envoyé au membre du personnel dans le cadre de l'embauche [modèle « type » à adapter au regard de la pratique effective et des caractéristiques particulières de chaque traitement mis en œuvre par l'agence PR agissant en qualité de responsable de traitement] :

[dénomination de l'agence PR qui agit en qualité de responsable de traitement], en qualité responsable du traitement, traite des données à caractère personnel vous concernant en vue de [à déterminer / préciser / compléter, par exemple :

- la gestion administrative du personnel (gestion du dossier professionnel des salariés, réalisation d'états statistiques ou de listes de salariés pour répondre à des besoins de gestion administrative, gestion des annuaires internes et des organigrammes, gestion des dotations individuelles en fournitures, équipements, véhicules et cartes de paiement, gestion des élections professionnelles et des réunions des instances représentatives du personnel, etc.) ;
- la mise à disposition des personnels d'outils informatiques (suivi et maintenance du parc informatique, gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux, mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, gestion de la messagerie électronique professionnelle, gestion des réseaux privés virtuels internes, etc.) ;
- l'organisation du travail (gestion des agendas professionnels / gestion des tâches des personnels) ou encore la gestion du temps de travail et du temps de présence (horaires), et plus généralement la gestion et le suivi de l'activité des membres du personnel ;
- la communication interne de [à compléter avec la dénomination de l'agence PR] ;
- la gestion des carrières et de la mobilité (évaluation professionnelle des personnels, gestion des compétences professionnelles internes, validation des acquis de l'expérience professionnelle, simulation de carrière, gestion de la mobilité professionnelle) ;
- la formation des personnels (suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions de formation, évaluation des connaissances et des formations) ;
- de la gestion de la paie, en ce incluant notamment le calcul et le paiement des rémunérations et accessoires et des frais professionnels ainsi que le calcul des retenues déductibles ou indemnisables opérées conformément aux dispositions légales et conventionnelles applicables, la gestion des absences / arrêts maladies / congés, l'élaboration et la remise des bulletins de paie, la gestion des saisies sur salaire ou avis à tiers détenteur le cas échéant, ainsi que la réalisation des déclarations à l'administration fiscale et aux organismes de protection sociale, de retraite, de prévoyance et de mutuelle obligatoire, mais également le calcul des cotisations et versements donnant lieu à retenue à la source ;
- la tenue des comptes relatifs à l'intéressement et à la participation ;
- la réalisation de tous traitements statistiques non nominatifs, liés à l'activité salariée dans l'entreprise ;
- la fourniture des écritures de paie à la comptabilité ;
- la tenue du registre unique du personnel ;
- la sécurisation des biens et des personnes au moyen de dispositif de contrôle des accès par badges et/ou de vidéosurveillance ;
- la gestion et du suivi des activités juridiques, en ce incluant notamment la rédaction ou la négociation de contrats ainsi que le suivi juridique associé mais également la gestion et le suivi de toute demande juridique (en ce incluant la gestion, le traitement et le suivi des demandes d'exercice de leurs droits par les personnes concernées dont les données sont traitées et des réponses à y apporter), de tout projet impliquant des problématiques juridiques et la réalisation de toute formalité juridique requise (déclarations, demandes d'autorisations administratives ou autres, actes de secrétariat juridique et documents sociaux tels que les convocations aux assemblées générales,...) ;
- de la gestion et du suivi des éventuels précontentieux et contentieux y afférents, en ce incluant notamment la préparation, l'exercice et le suivi des contentieux ainsi que l'exécution des décisions rendues ;
- de la gestion et de suivi des actions disciplinaires ou ayant pour objectif la constatation, l'exercice ou à la défense d'un droit en justice (incluant, le cas échéant, l'exécution des décisions rendues)].

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

La plupart de ces informations sont collectées directement auprès de vous. Certaines informations (à savoir : [à détailler]) peuvent toutefois être collectées de manière indirecte [indiquer la source].

Un tel traitement de vos données à caractère personnel est fondé, en fonction des sous-finalités poursuivies, sur [par exemple : l'exécution de votre contrat de travail conclu avec [à compléter avec la dénomination de l'agence PR], et/ou nos intérêts légitimes, à savoir la gestion du personnel au sens large, et/ou le respect d'obligations légales ou réglementaires qui s'imposent à [à compléter avec la dénomination de l'agence PR]].

Les données collectées dans ce cadre sont nécessaires pour la poursuite des finalités précitées qui, à défaut, ne pourraient pas être atteintes.

Les données vous concernant sont destinées [à compléter :

- aux membres du personnel habilités à en avoir connaissance au sein de l'agence (en particulier aux personnes habilitées chargées de la gestion du personnel ou de la gestion de la paie), voire à tous les membres du personnel pour certaines données et/ou finalités (cf. organigramme / annuaire / trombinoscope interne) ;
- aux personnes habilitées chargées d'assurer la sécurité des personnes et des biens, pour les besoins du contrôle d'accès aux locaux et aux outils de travail ;
- aux instances représentatives du personnel ;
- aux organismes gérant les différents systèmes d'assurances sociales, d'assurances chômage, de retraite, de prévoyance, et de caisses de congés payés ;
- aux organismes publics et aux administrations également habilitées à en avoir connaissance pour les finalités précitées ;
- aux organismes sociaux et fiscaux, et plus généralement services comptables et organismes habilités à recevoir les données traitées dans ce cadre en vertu des règles de comptabilité ;
- aux organismes financiers intervenant dans la gestion des comptes de l'agence et des membres du personnel et aux entités chargées de l'audit et du contrôle financier de l'agence ;
- aux organismes de mutuelle obligatoire ;
- aux partenaires et prestataires auxquels l'agence a recours, à savoir les partenaires et prestataires de cette dernière pouvant être amenés à intervenir dans le cadre de la réalisation des finalités susvisées, ou aux fins de mise à disposition et/ou de maintenance des outils et applications utilisés par l'agence dans le cadre des finalités du présent traitement (notamment prestataire informatique, prestataires en charge de la maintenance des services de téléphonie, du copieur ou du système de badges ou de vidéo, expert-comptable mais également éditeur du logiciel de comptabilité utilisé par l'agence,...) ;
- aux clients ou aux fournisseurs de l'agence, voire à certains cocontractants de cette dernière pour certaines données et/ou finalités].

Vos données pourront être conservées par nos soins en base active pendant [à compléter]. A l'issue de cette durée, lesdites données seront conservées sous forme d'archives pendant [à compléter]. Toutefois, en cas de procédure, notamment judiciaire, initiée avant le terme des durées ci-dessus et qui nécessiterait la conservation par [à compléter avec la dénomination de l'agence] de vos données à caractère personnel notamment en vue de la constatation, de l'exercice ou de la défense des droits de [à compléter avec la dénomination de l'agence], ces dernières seront conservées jusqu'à l'issue de ladite procédure. Dans cette hypothèse, vos données pourront être communiquées aux auxiliaires de justice et officiers ministériels intervenant dans le cadre du différend (avocat, huissiers, notaires,...), ainsi qu'à l'autorité saisie du litige.

Conformément aux dispositions applicables en matière de protection des données à caractère personnel, vous bénéficiez d'un droit d'interrogation, d'accès, de rectification, d'effacement et de portabilité de vos données, ainsi que du droit d'obtenir la limitation de leur traitement et d'un droit d'opposition (au traitement de vos données, ainsi qu'à la prospection notamment commerciale), dans les conditions et limites posées par la réglementation applicable en matière de protection des données à caractère personnel. Vous disposez également du droit de définir des directives relatives au sort de vos données à caractère personnel et à la manière dont vous souhaitez que vos droits soient exercés après votre décès. Ces droits s'exercent par courrier postal à l'adresse suivante : [à compléter] ou par email à l'adresse suivante : [à compléter avec une adresse email, étant précisé qu'il serait opportun d'avoir une adresse email dédiée à la réception de telles demandes]. Vous disposez en tout état de cause de la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (« Cnil ») si vous estimez que le traitement de vos données n'est pas effectué conformément aux dispositions légales et réglementaires applicables.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

Les membres du personnel peuvent également être informés du traitement de leurs données par l'agence PR **dans le contrat de travail.** Toutefois, le déploiement d'un tel processus **pourrait être délicat en pratique** puisque (i) le contrat de travail est négociable, ce qui pourrait mener à des ajustements de ladite mention et (ii) pour les contrats en cours (cf. membres du personnel déjà en poste), il conviendrait de procéder par voie d'avenant pour intégrer une mention d'information à ces contrats, étant rappelé qu'un membre du personnel pourrait tout à fait refuser de signer un tel avenant. En tout état de cause, la mention d'information à l'attention des salariés ne devant pas par principe être nécessairement contractualisée, alors il n'est pas requis de l'intégrer dans le contrat de travail.

Des processus similaires pourraient être déployés s'agissant de **l'information des stagiaires** ayant vocation à effectuer leur stage au sein de l'agence PR (cf. insertion d'une mention d'information dans le livret d'accueil des stagiaires ou dans un document dédié,...), sous réserve comme pour les membres du personnel de conserver la preuve de la remise de ces documents.

FOCUS SUR DES HYPOTHÈSES DE COLLECTE INDIRECTE DE DONNÉES

• Le cas des intérimaires

Dans l'hypothèse du recours à un intérimaire, les données à caractère personnel relatives à ces derniers et nécessaires à leur embauche sont susceptibles d'être communiquées à l'agence PR concernée par l'entreprise de travail temporaire qui met à disposition l'intérimaire.

Dans une telle situation, il convient **d'informer les intérimaires du traitement de leurs données par l'agence PR (cf. document d'information dédié par exemple), et ce dès la collecte de leurs données.**

Il convient également de s'assurer dans le contrat de mise à disposition entre l'entreprise de travail temporaire et l'agence PR que l'entreprise de travail temporaire garantit l'agence du fait que l'intérimaire concerné a été dûment informé s'agissant du traitement de ses données par l'agence PR, que ses données ont été collectées de manière loyale et licite et que les données concernant l'intérimaire communiquées dans ce cadre à l'agence PR peuvent être licitement réutilisées par cette dernière.

• Le cas des proches des membres du personnel

Dans le cadre d'une embauche, des données relatives aux proches des membres du personnel sont susceptibles d'être collectées (par exemple : coordonnées des personnes à contacter en cas d'urgence).

Dans une telle hypothèse, il convient **d'informer les personnes concernées (cf. les proches concernés) du traitement de leurs données par l'agence PR.** En pratique, celles-ci doivent être informées du traitement de ses données dans un délai raisonnable après obtention desdites données par l'agence PR (ne dépassant pas un mois) ou, si les données doivent être utilisées aux fins de communication avec la personne concernée, au plus tard au moment de la première communication avec cette dernière ou, s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois. Il pourra être procédé à l'information de ces personnes par un moyen de communication non soumis à consentement préalable (par exemple, par courrier postal).

A défaut de faisabilité d'une telle pratique (cf. si la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, situations qui, pour mémoire, doivent être interprétées de manière stricte), notamment si l'agence PR ne dispose pas de coordonnées de ces personnes par exemple, il pourrait a minima être envisagé de s'assurer auprès du membre du personnel ayant communiqué de telles informations que ses proches ont été dûment informés par lui-même s'agissant du traitement de leurs données par l'agence PR, en présentant à cette fin au membre du personnel les caractéristiques du traitement envisagé par l'agence PR (cf. les éléments devant figurer obligatoirement dans les mentions d'information, conformément au paragraphe « Loyauté et transparence » ci-dessus).

4.1.3 Les données pouvant être collectées

Pour mémoire, seules les données à caractère personnel **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités poursuivies peuvent être traitées par les agences PR dans le cadre de la gestion de leurs opérations de recrutement et de la gestion de leurs ressources humaines (en ce incluant notamment la gestion administrative du personnel et la gestion de la paie).**

En tout état de cause, quelle que soit la typologie des données traitées par l'agence PR, cette dernière doit s'assurer que l'ensemble des données traitées par l'agence PR et intégrées dans les fichiers et bases de données adossées aux applications et outils utilisés au sein de ladite agence sont exactes et tenues à jour (voir à cet égard le paragraphe « Exactitude et qualité des données » ci-dessus).

• Dans le cadre des opérations de recrutement

A titre d'exemple, dans le cadre de la gestion des opérations de recrutement, les données suivantes peuvent bien entendu être collectées et traitées :

- identité ;
- coordonnées et moyens de contacts ;
- études, formations suivies, diplômes ;
- expériences professionnelles.

A l'inverse, la Cnil considère, dans le cadre des opérations de recrutement, qu'a minima les données suivantes **ne doivent pas, par principe, être collectées :** date d'entrée en France ; date de naturalisation ; modalités d'acquisition de la nationalité française ; nationalité d'origine ; numéros d'immatriculation ou d'affiliation aux régimes de sécurité sociale ; détail de la situation militaire : sous la forme « objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade » ; adresse précédente ; entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint ainsi que nom, prénom, nationalité, profession, employeur, des parents, des beaux-parents, des frères et sœurs et des enfants) ; état de santé ; taille ; poids ; vue ; conditions de logement (propriétaire ou locataire) ; vie associative ; domiciliation bancaire ; emprunts souscrits[130].

Elle ajoute qu'il est **interdit de collecter et de conserver, sauf accord exprès du candidat,** des données qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales, les informations relatives à la santé ou à la vie sexuelle des personnes. L'accord exprès qui doit être recueilli par écrit pour le traitement de telles données ne saurait, à lui seul, justifier la collecte de ces données si ces dernières sont dépourvues de lien direct et nécessaire avec l'emploi proposé. Aussi, de telles informations ne peuvent-elles être collectées, sous réserve des interdictions légales, que lorsqu'elles sont justifiées par la spécificité du poste à pourvoir.

FOCUS SUR LES ZONES DE COMMENTAIRES LIBRES

Dans le cadre de la réception et de l'étude des candidatures, ou encore des entretiens d'embauche, des notes peuvent être prises par les personnes en charge du recrutement, étant précisé que **ces notes, même éventuellement manuscrites, peuvent être constitutives de traitements de données à caractère personnel.**

Par conséquent, le contenu de ces notes, appréciations, évaluations,... est soumis au respect de la réglementation applicable en matière de protection des données à caractère personnel et doit donc en tout état de cause demeurer proportionné, justifié, adéquat et objectif.

En effet, **le principe de minimisation s'applique quelles que soient les modalités de collecte,** de saisie et de traitement des données dans les applications, fichiers, etc. utilisés. A cet égard, il est renvoyé aux recommandations ci-dessus relatives aux zones de commentaires libres.

[130] Cnil, Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

- **Dans le cadre de la gestion administrative du personnel**

La collecte d'un certain nombre de données peut être nécessaire pour l'agence PR dans le cadre de la gestion administrative de son personnel au sens large (en ce incluant notamment la gestion du dossier professionnel des membres du personnel, la réalisation d'états statistiques ou de listes de membres du personnel pour répondre à des besoins de gestion administrative, la gestion des annuaires internes et des organigrammes, la gestion des dotations individuelles en fournitures et équipements, la gestion des élections professionnelles et des réunions des instances représentatives du personnel, la mise à disposition d'outils informatiques, la gestion des carrières et de la mobilité, la formation professionnelle,...).

En effet, dans ce cadre, le traitement des données suivantes peut être nécessaire au regard des finalités poursuivies : identité, date et lieu de naissance, date et conditions d'embauche ou de recrutement, dates et suivi des entretiens d'évaluation[131], compétences professionnelles, formation suivie, historique des visites médicales,... En tout état de cause, les informations pouvant être demandées à un candidat à l'embauche, doivent présenter un lien direct avec l'appréciation de ses qualités et compétences professionnelles, et ne doivent donc pas porter sur la composition de sa famille, sur des informations relatives à ses proches, ...[132]

Toutefois, certaines informations dites « sensibles », hautement personnelles ou non strictement nécessaires au regard de la finalité poursuivie doivent faire l'objet d'une attention particulière de la part des agences PR.

(ILLUSTRATIONS)

A titre d'illustration, en vertu du principe de minimisation, la collecte systématique d'une copie du **permis de conduire** des membres du personnel est excessive dans le secteur des agences PR. Si toutefois le poste de certains membres du personnel se caractérise par des déplacements professionnels et que ces derniers se voient affecter un véhicule de fonction ou qu'un véhicule de service peut, dans certaines situations, leur être mis à disposition par l'agence PR, il pourrait être nécessaire pour l'agence PR d'obtenir des informations relatives à leur permis de conduire (cf. pour la dénonciation obligatoire auprès de l'ANTAI d'infractions commises par des salariés conduisant des véhicules de fonction ou de service). Néanmoins, dans cette hypothèse, la collecte d'une attestation sur l'honneur peut être suffisante au regard de la finalité poursuivie.

Par ailleurs, la **carte grise** attachée au véhicule appartenant à un membre du personnel ne nécessite en tout état de cause pas d'être collectée (y compris pour gérer les accès au parking de l'agence PR par exemple).

Pour une autre illustration, il en est de même de la demande de communication d'un **extrait de casier judiciaire,** pratique qui doit être purement et strictement interdite compte tenu du secteur d'activité concerné.

L'utilisation de la **photographie des membres du personnel** doit également faire l'objet d'une attention particulière. En effet, outre certaines utilisations qui peuvent éventuellement être justifiées par exemple pour des raisons de sécurité (ex : photographie devant figurer sur un badge d'accès), le consentement des personnes concernées est en principe requis pour l'utilisation de leur photographie (tant sur le plan de la réglementation applicable en matière de protection des données à caractère personnel que pour des aspects liés au droit à la vie privée et au droit à l'image). Or, en raison notamment du lien de subordination existant entre un employeur et les membres de son personnel, le recueil d'un tel consentement peut être délicat à démontrer ou encore être remis en cause. En tout état de cause, les informations pouvant être demandées à un candidat à l'embauche, doivent présenter un lien direct avec l'appréciation de ses qualités et compétences professionnelles, et ne doivent donc pas porter sur la composition de sa famille, sur des informations relatives à ses proches, ... Une analyse casuistique doit donc être menée pour toute utilisation envisagée d'une telle information, que ce soit à des fins de communication interne (ex : trombinoscope ou annuaire interne, newsletter interne,...) ou de communication externe (ex : pavé de signature email, pages de l'agence sur les réseaux sociaux, newsletter de l'agence,...).

Pour un autre exemple, s'agissant des **données relatives à l'appartenance syndicale** d'un membre du personnel, seules peuvent être collectées et traitées les informations liées à l'appartenance déclarée (cf. manifestement rendue publique) d'un membre du personnel qui se présente aux élections professionnelles sous l'égide d'un syndicat.

En outre, des **données de santé** peuvent dans certains cas être collectées et traitées par l'agence PR en qualité d'employeur. Toutefois, la collecte et le traitement de telles données de santé ne peuvent être justifiés et autorisés par principe que si un tel traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée.

[131] Sur ce point, voir également les précautions applicables s'agissant des zones de commentaires libres et des méthodes automatisées d'évaluation.
[132] Pour en savoir plus, voir Cnil, référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel, 21 novembre 2019

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

La mise en place de **dispositifs de vidéosurveillance** dans les locaux doit également être l'objet d'une attention particulière : légitimité et proportionnalité du dispositif (qui ne doit en tout état de cause pas filmer les membres du personnel de manière permanente à leur poste de travail ou encore les lieux de repos ni les accès aux locaux des représentants du personnel), information des personnes concernées par une note interne + par voie d'affichage dans les locaux (le fait que la caméra soit visible des personnes concernées n'étant pas suffisant pour considérer que la personne concernée a été informée conformément à la réglementation applicable en matière de protection des données à caractère personnel !), durée de conservation strictement limitée à ce qui est nécessaire (cf. quelques jours), etc.

- **Dans le cadre de la gestion de la paie, de l'épargne salariale et des déclarations sociales obligatoires**

La Cnil considère que les informations traitées par un employeur dans le cadre de l'établissement des fiches de paie et des obligations légales connexes peuvent être les suivantes : numéro de sécurité sociale dans les conditions fixées par le droit applicable, numéros attribués par les organismes d'assurances sociales, de retraite et de prévoyance, situation familiale, situation matrimoniale, enfants à charge, régime et base de calcul de la rémunération, éléments déterminant l'attribution d'un complément de rémunération, congés et absences donnant lieu à retenues déductibles ou indemnisables, ainsi que toute retenue légalement opérée par l'employeur, frais professionnels, taux de prélèvement à la source, données transmises via la Déclaration sociale nominative.

Toutefois, certaines informations hautement personnelles ou non strictement nécessaires au regard de la finalité poursuivie doivent faire l'objet d'une attention particulière de la part des agences PR.

(ILLUSTRATION)

A titre d'illustration, en cas de **retenues sur salaires,** il convient de ne conserver que les informations nécessaires à la réalisation de la paie chaque mois, et non les éléments complémentaires ayant pu être reçus dans ce cadre (par exemple, le détail de l'avis à tiers détenteur).

LE SAVIEZ-VOUS ?

Le numéro de sécurité sociale est fréquemment recueilli lors de l'embauche d'une personne dans le cadre d'une fiche de renseignement. Toutefois, il est rappelé que ce numéro **ne peut être traité par l'employeur que pour une finalité de gestion de la paie, de gestion de l'épargne salariale et de réalisation des déclarations sociales obligatoires à la charge de l'employeur (et non dans le cadre de la gestion administrative du personnel stricto sensu)** [133].

Aussi, il est recommandé de définir un processus de recueil du numéro de sécurité sociale qui permette la saisie de cette information directement dans le logiciel de gestion de la paie ou dans les applications dédiées à la réalisation des déclarations sociales obligatoires de l'employeur, mais non la conservation de cette information sur d'autres supports. A minima, il serait opportun de supprimer / occulter le numéro de sécurité des différents documents papiers sur lesquels il peut figurer une fois saisi dans les applications précitées.

En tout état de cause, il convient de **ne pas recueillir de copie de l'attestation de sécurité sociale et de la carte vitale** d'un membre du personnel. Le fait de demander la présentation de l'attestation de sécurité sociale ou de la carte vitale pourrait être suffisant pour vérifier ou obtenir le numéro de sécurité sociale d'un membre du personnel.

Par ailleurs, le numéro de sécurité sociale ne doit pas figurer sur le **contrat de travail** des membres du personnel ni dans le **registre du personnel.**

De même, pour ce qui concerne **l'affiliation à la mutuelle et/ou à la prévoyance éventuellement proposée par l'agence PR aux membres de son personnel,** le formulaire dédié doit être renseigné par chaque membre du personnel concerné lui-même. En outre, **ce formulaire ainsi que les documents justificatifs requis par l'organisme de mutuelle / de prévoyance doivent être adressés directement à l'organisme en question par le membre du personnel concerné** (et non transmis par une personne qui serait en charge des ressources humaines au sein de l'agence PR par exemple).

[133] Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

4.2
BONNES PRATIQUES EN MATIÈRE D'UTILISATION DES DONNÉES

4.2.1 L'utilisation des données pour des finalités RH

Comme indiqué au paragraphe « Limitation et légitimité des finalités » ci-dessus, l'agence PR ne peut traiter des données à caractère personnel que pour des finalités, des objectifs clairement définis et légitimes, et il n'est pas possible de réutiliser ces données pour des finalités ultérieures incompatibles avec les finalités initiales (cf. risque de détournement de finalité).

LE SAVIEZ-VOUS ?

Le principe de limitation et de légitimité des finalités poursuivies par l'agence PR s'applique également dans le cadre des traitements mis en œuvre par cette dernière en matière de ressources humaines.

Ainsi, pour tout traitement mis en œuvre en la matière, et afin de déterminer si ce principe est respecté, il convient de **se poser les questions suivantes :**

- à quoi les données collectées vont-elles servir ?
- l'utilisation envisagée par l'agence PR est-elle légitime (notamment au regard de l'activité de l'agence PR et des droits et libertés des personnes) ?
- comment procéder pour informer les personnes concernées d'une telle utilisation de leurs données et s'assurer qu'elles ont compris la raison pour laquelle leurs données sont collectées ?

Aussi, il appartient en particulier aux personnes en charge des ressources humaines de s'assurer que les données collectées dans ce cadre ne sont effectivement traitées que pour les finalités ainsi définies en amont par l'agence PR et pour lesquelles les personnes concernées ont été informées.

[134] Cf. article L.3243-2 du Code du travail.
[135] Cf. article D.3243-7 du Code du travail.

(ILLUSTRATIONS)

A titre d'illustration, les données traitées par une agence PR dans le cadre de ses opérations de recrutement ne peuvent pas en principe être réutilisées pour proposer des offres commerciales aux candidats ni ne peuvent être communiquées à une autre agence PR (même au sein du même groupe), sauf à avoir recueilli préalablement le consentement du candidat à cette fin, étant toutefois précisé que cette hypothèse doit être limitée aux cas strictement nécessaires dans la mesure où le consentement des personnes concernées pourrait ne pas être considéré comme étant donné de manière valable (cf. risque qu'il soit considéré comme n'étant pas donné librement car émanant d'un candidat, par principe considéré comme une personne vulnérable).

Pour ce qui concerne les dispositifs de vidéosurveillance mis en place au sein d'une agence PR, si de tels dispositifs peuvent être justifiés pour assurer par exemple la sécurité des personnes et des biens au sein de l'agence, les images ainsi captées ne doivent pas permettre à l'employeur de surveiller les membres du personnel de manière permanente à leur poste de travail, notamment pour calculer par ce moyen le temps de travail effectif d'un collaborateur par exemple.

FOCUS SUR L'OPPOSITION DES MEMBRES DU PERSONNEL À LA REMISE DU BULLETIN DE PAIE SOUS FORME ÉLECTRONIQUE

L'agence PR ne peut procéder à la remise d'un bulletin de paie sous forme électronique que sous réserve que chaque membre du personnel concerné ne s'y soit pas opposé[134].

Ainsi, lorsque l'agence PR décide de procéder à la remise du bulletin de paie sous forme électronique, elle doit **informer chaque salarié concerné par tout moyen conférant date certaine, un mois avant la première émission du bulletin de paie sous forme électronique ou au moment de l'embauche,** de son droit de s'opposer à l'émission du bulletin de paie sous forme électronique.

Tout salarié peut faire part de son opposition à tout moment, préalablement ou postérieurement à la première émission d'un bulletin de paie sous forme électronique, en la notifiant à l'employeur par tout moyen lui conférant une date certaine. Dans cette hypothèse, la demande du salarié prend effet dans les meilleurs délais et au plus tard trois mois suivant ladite notification[135].

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

LE SAVIEZ-VOUS ?

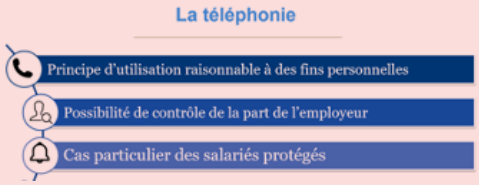
L'employeur peut **fixer les conditions et limites de l'utilisation des outils mis à disposition des membres de son personnel.** Il peut également mettre en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions aux outils/applications ou des sites visités, poste par poste, et plus généralement tout outil de contrôle d'activité et de productivité.

Toutefois, de tels dispositifs ne peuvent être déployés que sous réserve (i) d'avoir consulté et informé les représentants du personnel, (ii) d'en avoir dûment informé les salariés et (iii) de ne pas conserver les données plus longtemps que ce qui est strictement nécessaire.

En tout état de cause, les règles d'utilisation des outils mis à disposition des membres du personnel ainsi que du système d'information de l'agence de manière générale doivent être formalisées dans une charte d'utilisation des ressources informatiques et de communications électroniques.

FOCUS SUR LA TÉLÉPHONIE

L'employeur peut mettre à disposition de ses collaborateurs des outils de téléphonie fixe et/ou mobile. Dans ce cadre, les recommandations de la Cnil sont les suivantes :



©Cnil

Un employeur peut assurer la surveillance de l'utilisation des outils de téléphonie par ses salariés, mais **ne doit pas par principe accéder à l'ensemble des numéros appelants / appelés** (les 4 derniers chiffres devant être occultés).

Toutefois, **un employeur peut éditer, soit par l'intermédiaire de l'autocommutateur qu'il aura mis en place, soit par l'intermédiaire de l'opérateur auprès duquel il est client, l'intégralité des numéros de téléphone appelés ou le détail des services de téléphonie utilisés dans les deux cas suivants :**

- dans le cas où un remboursement est demandé aux salariés pour les services de téléphonie utilisés à titre privé, lorsque le montant demandé est contesté par le salarié auquel il se rapporte, un relevé justificatif complet des données relatives à l'utilisation des services de téléphonie comprenant l'intégralité des numéros de téléphone appelés peut être établi à des fins de preuves ;
- dans le cas où l'employeur constate une utilisation manifestement anormale au regard de l'utilisation moyenne constatée au sein de l'entreprise ou de l'organisme privé et public des services de téléphonie, un relevé justificatif complet des numéros de téléphone appelés ou des services de téléphonie utilisés peut être établi de façon contradictoire avec le salarié concerné.

Par ailleurs, **une attention particulière doit être portée à la confidentialité des communications des instances représentatives du personnel (IRP) :**

- mettre à leur disposition une ligne téléphonique dédiée à leurs fonctions d'IRP, non reliée au système de téléphonie fixe de l'entreprise ;
- s'assurer, notamment techniquement, de ne pas avoir accès aux communications reçues / émises par ces derniers dans le cadre de leurs fonctions d'IRP, ni à leur relevé de communications détaillé.

En outre, les données à caractère personnel relatives à l'utilisation des services de téléphonie ne peuvent être conservées au-delà du délai prévu à l'article L. 34-2 du code des postes et des communications électroniques, à savoir **un an courant à la date de l'exigibilité des sommes dues en paiement des prestations des services de téléphonie.**

4.2.2 Le départ d'un membre du personnel

Pour mémoire, comme indiqué ci-dessus au paragraphe « Proportionnalité de la conservation des données à caractère personnel », la conservation illimitée des données à caractère personnel est par principe interdite.

Ainsi, pour chaque finalité poursuivie en matière de ressources humaines, l'agence PR doit déterminer une durée de conservation maximum des données à caractère personnel qu'elle traite (sous forme de données d'utilisation « courante » puis d'« archives ») ainsi que le point de départ d'une telle durée.

Pour parvenir à gérer de manière précise les durées de conservation, il convient d'automatiser si possible ce processus (a minima pour les traitements mis en œuvre sur un support informatique), celui-ci devant permettre de gérer la durée de conservation des données en « base active » puis sous forme d'archives, à compter du point de départ pertinent.

Si tel n'est pas le cas (par exemple pour ce qui concerne les traitements de données à caractère personnel mis en œuvre en format papier) ou n'est pas envisageable en fonction de l'organisation de l'agence PR concernée, il convient a minima d'élaborer et de déployer en interne une politique et des process manuels d'archivage et de purge des données.

(ILLUSTRATIONS)

A titre d'illustration, pour ce qui concerne le registre unique du personnel en version papier, il pourrait être envisagé de biffer les données une fois que celles-ci ne sont plus nécessaires au regard de la finalité poursuivie. A cet égard, l'article R.1221-26 du Code du travail précise que « Les mentions portées sur le registre unique du personnel sont conservées pendant cinq ans à compter de la date à laquelle le salarié ou le stagiaire a quitté l'établissement ». Ainsi, à l'issue d'un tel délai, il conviendrait de procéder à une anonymisation manuelle en biffant les données du salarié ayant quitté l'agence PR.

Par ailleurs, les recommandations présentées ci-dessus s'agissant des extractions sous forme de tableurs Excel des fichiers de contacts peuvent également être déclinées s'agissant **des fichiers Excel de recrutement ou de gestion et de suivi du personnel (ex : statistiques, gestion et suivi des effectifs, reportings,...) qui ne seraient pas centralisés.**

[136] Cnil. Délibération n°2005-002 du 13/01/2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels. NS-046.
[137] Cnil. référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel. 21 novembre 2019».
[138] Cnil. référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel. précité».

(ILLUSTRATIONS)

S'agissant du registre unique du personnel, la Cnil recommande de conserver les données relatives à un membre du personnel pendant la durée pendant laquelle ce dernier fait partie des effectifs, puis de les archiver pendant 5 ans à compter de son départ de l'organisme.

En matière de gestion des mandats des représentants du personnel, la Cnil recommande d'appliquer les durées de conservation suivantes :

- s'agissant de la nature du mandat et du syndicat d'appartenance : conservation en base active pendant six mois après la fin du mandat puis archivage pendant six ans (cf. délai de prescription pénale pour les délits) ;
- s'agissant de données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à crédit d'heures de délégation (par exemple : exercice d'un mandat électif ou représentatif syndical) : conservation en base active pendant le temps de la période de sujétion de la personne concernée puis archivage pendant six ans (cf. délai de prescription pénale pour les délits).

Bien entendu, pour certaines informations, une durée moindre et/ou un point de départ différent doivent toutefois être envisagés pour le calcul des durées de conservation.

A titre d'illustration :

- les éléments afférents à des sanctions disciplinaires qui seraient prononcées doivent être supprimés en cas d'amnistie ;
- dans le cadre de la procédure de désignation par l'employeur des auteurs de contraventions au Code de la route auprès de l'ANTAI, les données pertinentes ne peuvent être conservées que le temps de procéder à la désignation, qui ne saurait en tout état de cause excéder quarante-cinq jours à compter de la réception de l'avis de contravention. A l'issue de cette période, les données peuvent être archivées, en archivage intermédiaire, au maximum le temps de la prescription en matière contraventionnelle, à savoir douze mois[137];
- s'agissant des données de connexion (par exemple à des outils ou applications), la Cnil considère qu'une durée de conservation de l'ordre de six mois est suffisante. A l'issue de cette période, ces données pourraient être archivées pendant les délais de prescription, dans certaines hypothèses.

Par ailleurs, en matière de gestion de la paie, la Cnil recommande d'appliquer les durées de conservation suivantes :

- s'agissant du bulletin de salaire : conservation en base active pendant un mois puis archivage pendant cinq ans par principe et cinquante ans en version dématérialisée ;
- s'agissant des éléments nécessaires au calcul de l'assiette : conservation en base active pendant un mois puis archivage pendant six ans ;
- s'agissant de la saisie des données calcules (DSN) : conservation en base active pendant le temps nécessaire à l'accomplissement de la déclaration puis archivage pendant six ans [138].

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

FOCUS SUR LA GESTION DES HABILITATIONS EN CAS DE DÉPART D'UN MEMBRE DU PERSONNEL

Il est recommandé d'élaborer **une procédure de gestion des collaborateurs sortants** et, en cas de départ, a minima :

- exiger la restitution du matériel informatique mis à disposition du collaborateur sortant ;
- supprimer les accès du membre du personnel sortant aux outils / applications auxquel(le)s il pouvait accéder dans le cadre de ses fonctions ;
- supprimer le compte utilisateur de type annuaire « LDAP » ou « Active Directory » du collaborateur sortant (et non uniquement le suspendre, ou alors pendant une durée strictement limitée, justifiée et proportionnée, et ce seulement en vue de la poursuite de l'activité).

Attention : la désactivation / suppression du compte utilisateur de type annuaire « LDAP » ou « Active Directory » d'un salarié parti n'est pas suffisante pour désactiver ses accès à toutes les applications, notamment pour ce qui concerne les applications en SaaS par exemple. A titre d'illustration, une adresse email, même désactivée, peut toujours être constitutive d'un identifiant valable pour se connecter à telle ou telle application. Une attention particulière doit être portée sur ce point et il convient donc de s'assurer que tous les identifiants et mots de passe d'un salarié parti sont bloqués pour l'ensemble des applications.

A cette fin, il est recommandé de mettre en place un processus interne permettant par exemple à la direction informatique ou au prestataire informatique de l'agence PR d'être informé(e) dès que possible du départ d'un membre du personnel et de la date du fin de son préavis afin que les mesures requises puissent être prises en temps utile.

Un processus similaire pourrait être déployé s'agissant des prestataires, et notamment des freelances, auxquels l'agence PR ferait appel et qui bénéficieraient notamment de tels droits d'accès aux outils / applications que l'agence PR mettrait à leur disposition. Dans ce cadre, il est également recommandé de ne créer que des comptes nominatifs (et non génériques) et de limiter la durée de vie de leur compte respectif à la durée initialement prévue pour leur mission, étant précisé que cette durée pourra bien entendu être prolongée le cas échéant en fonction de la mission confiée et de son évolution.

LE SAVIEZ-VOUS ?

Pour mémoire : les messages électroniques échangés par un salarié au moyen de sa messagerie professionnelle sont présumés être professionnels, et l'employeur peut donc y avoir accès.

Toutefois, compte tenu du principe jurisprudentiel du **« droit à la vie privée résiduelle, même sur son lieu de travail »,** les messages des salariés identifiés comme personnels ne peuvent être accédés par l'employeur, sauf exceptions particulières, qu'en présence du salarié (cf. nécessité de définir, par exemple dans la charte d'utilisation des ressources informatiques et de communications électroniques, les règles de nommage pour les emails personnels).

Par conséquent, les pratiques consistant à « re-router » les emails ou encore à ouvrir l'accès à la messagerie d'un ancien salarié à un autre salarié pourraient être contraire à ces principes et au secret des correspondances privées.

La Cnil recommande donc ce qui suit :

- **information du salarié, avant son départ, sur la possibilité de récupérer et/ou supprimer ses messages personnels ;**
- **message automatique d'absence / de départ ;**
- **pas d'utilisation de l'adresse email par une autre personne ;**
- **pas de « re-routage » des emails vers une autre personne ;**
- **durée de conservation limitée.**

4.2.3 Le recours à des prestataires

Pour mémoire, la qualification des différents acteurs doit faire l'objet d'une attention particulière, et ce notamment en raison des obligations attachées à la qualification de responsable, le cas échéant conjoint, de traitement et de sous-traitant et des éléments devant être contractualisés pour encadrer les rôles et responsabilités de chacun (voir à cet égard le paragraphe « Encadrer les relations avec les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel ».

(EXEMPLE)

L'externalisation de la gestion de la paie

A titre d'illustration, le prestataire informatique fournissant le logiciel de paie ou le cabinet comptable en charge de la paie, auquel une agence PR peut avoir recours dans le cadre de la gestion de la paie des membres de son personnel, peuvent agir en qualité de sous-traitant pour le compte de l'agence PR, cette dernière étant responsable de traitement. Dans cette hypothèse, un contrat devant comporter les éléments obligatoires au titre de l'article 28 du RGPD relatifs à l'objet et à la durée du traitement, à la nature et à la finalité du traitement, aux types de données à caractère personnel pouvant être traitées et aux catégories de personnes concernées, ainsi que les obligations et les droits de chacune des parties doit être conclu par l'agence PR avec le prestataire informatique fournissant le logiciel de paie ou le cabinet comptable en charge de la paie.

Dans le cas où l'agence a recours à des sous-traitants hors Union européenne ou qui hébergent ou stockent ou traitent les données hors Union européenne, des clauses contractuelles spécifiques complémentaires doivent également être prévues pour assurer une protection effective des données à caractère personnel traitées.

Par ailleurs, dans la mesure où des données hautement personnelles sont susceptibles d'être traitées dans ce cadre (notamment le numéro de sécurité sociale des membres du personnel), une attention particulière doit être portée sur les mesures de sécurité mises en œuvre par le sous-traitant, ainsi qu'aux mesures de sécurisation des données échangées. A titre d'exemple, il n'est pas concevable d'adresser à un sous-traitant des données de paie via un email non sécurisé, et il convient de privilégier un moyen d'échange sécurisé, de type « serveur d'échange de fichiers sécurisé » (ex : FTP sécurisé).

A titre de bonnes pratiques visant à s'assurer de l'encadrement contractuel des relations entre l'agence PR et les différents acteurs intervenant dans le cadre d'un traitement de données à caractère personnel, et ce en fonction de l'organisation de l'agence PR, il doit être envisagé :

- que les opérationnels soient tenus **d'informer immédiatement et systématiquement le service juridique de l'agence PR et/ou le DPO ou, à défaut, le référent** en matière de protection des données à caractère personnel **dès lors qu'il est envisagé de faire appel à un tiers dans le cadre de traitements de données à caractère personnel** afin de faire valider les contrats à conclure, étant précisé qu'en fonction de la situation rencontrée il pourrait également être opportun de faire appel à un conseil extérieur à l'agence spécialisé en la matière ; ou encore
- que **des modèles de clauses types / d'avenants types** soient élaborés et mis à disposition des opérationnels et que ces derniers soient en mesure de les ajuster, étant précisé qu'en cas d'incertitude ou de doute sur la qualification des parties ou sur le contenu des clauses contractuelles à ajuster, ils devraient être tenus d'en informer immédiatement et systématiquement le service juridique de l'agence PR et/ou le DPO ou, à défaut, le référent en matière de protection des données à caractère personnel.

PUBLIC CIBLE : DIRECTION, RESPONSABLES RH

FOCUS SUR LA QUALIFICATION DES ORGANISMES DE FORMATION

Dans le cadre de la gestion de la formation des membres de son personnel, l'agence PR peut être amenée à communiquer des données à caractère personnel de ses salariés à des organismes de formation.

Les organismes de formation sont donc amenés à collecter et à traiter les données desdits salariés dans ce cadre et se pose la question de savoir s'ils doivent être qualifiés de sous-traitant agissant pour le compte de l'agence.

A cet égard, si une telle qualification de sous-traitant est possible, il doit également être relevé que les organismes de formation traitent les données des salariés de leurs entreprises clientes pour les finalités suivantes :

- **l'organisation, la gestion et le suivi des sessions de formation** (organisation des sessions de formation, gestion, traitement et suivi des pré-inscriptions et inscriptions, facturation et comptabilité associées et réalisation des formalités administratives éventuelles en relation avec les OPCO en vue de la facturation de la formation le cas échéant, envoi des convocations, suivi des émargements, délivrance d'attestations de formation, gestion et suivi des évaluations et des questionnaires de satisfaction, réalisation de statistiques dans le cadre des bilans de satisfaction,...) ;
- **la gestion de son activité en tant qu'organisme de formation référencé** (en ce incluant notamment la gestion et le suivi de la qualité, notamment en vue du maintien des certifications associées) ;
- **la gestion et le suivi de la relation avec les participants, les sociétés clientes, les prospects, et plus généralement les contacts,** en ce incluant notamment la réponse aux demandes d'informations éventuelles, la réalisation d'opérations commerciales, de communication et de marketing le cas échéant (notamment ciblage, prospection commerciale et personnalisation des offres, création et envoi des catalogues de formation,...).

S'agissant des finalités précitées, il pourrait être considéré que les organismes de formation bénéficient d'un véritable pouvoir décisionnaire, si bien qu'ils pourraient dans certains cas pouvoir être qualifiés de responsables de leur propre traitement de données à caractère personnel mis en œuvre pour des finalités qui leur sont propres.

Aussi, il est nécessaire en cas de recours à ces organismes, (i) de procéder à une analyse spécifique **permettant de déterminer précisément la qualification ainsi que la répartition des rôles et responsabilités entre l'agence PR et les organismes de formation auxquels l'agence PR aurait recours,** et ce *in concreto* en fonction des pratiques effectives, afin (ii) d'encadrer les relations contractuelles entre ces parties conformément à la réglementation applicable en matière de protection des données à caractère personnel.