HAAS AVOCATS

dolist
DATA & MESSAGING SOLUTIONS

GUIDE

E-Marketing & Protection des données

Nouvelle réglementation : Préparez-vous dès maintenant !

© Dolist / Haas Avocats - Tous droits réservés

06/03/2017

AU SOMMAIRE

Profilage & perspectives Marketing 4

Qu'est-ce que le profilage ? 4

Les techniques de profilage actuelles 4

Des opportunités marketing judicieuses 4

Le nouveau cadre juridique en matière de profilage à connaître 6

Un cadre juridique du profilage renforçant le principe d'Opt-In 6

Une protection des individus contre les abus du profilage 6

Des devoirs côté responsable du traitement des données 6

Des conséquences immédiates pour les sites et sur la gestion des cookies 7

Quels changements pour la collecte de l'opt-in sur les données de navigation ? 7

Des pratiques transparentes à mettre d'ores et déjà en place 8

Une généralisation attendue des études d'impact sur la vie privée (PIA) 9

Une obligation de sécurité et de confidentialité renforcée 10

Qui est concerné ? 10

L'anticipation du risque 10

La notification des failles de sécurité 10

Anticipation des risques : les mesures à mettre en place 11

La nomination d'un *Data Privacy Officer* - DPO 11

Les missions du DPO 11

Qui désigner en tant que DPO ? 12

En bref : la check-list pour vous préparer 14

Pour conclure 16

© Dolist / Haas Avocats - Tous droits réservés

NOUVELLE REGLEMENTATION SUR LA PROTECTION DES DONNEES : PREPAREZ-VOUS DES MAINTENANT !

Prenant en compte l'évolution des technologies digitales et des pratiques du marché, le nouveau Règlement Général européen sur la Protection des Données (RGPD) arrive prochainement pour imposer des responsabilités nouvelles aux entreprises amenées à collecter, traiter, regrouper et analyser des données personnelles et comportementales. Objectifs : protéger les consommateurs et leur redonner de la confiance dans les relations avec les entreprises.

De plus en plus avancées, les technologies numériques permettent aujourd'hui aux entreprises d'aller très loin en matière d'exploitation des données personnelles, jusqu'à un « profilage » très précis des contacts en fonction de leurs comportements - passés mais à venir également - quitte à s'avérer parfois abusifs. Un sujet d'inquiétudes croissantes côté consommateurs !

Hors, en matière de confiance, on part de loin il faut l'admettre : en France, seuls 3% font confiance aux boutiques physiques et en ligne pour la confidentialité des données[1]. Il existe pourtant derrière ce chiffre des enjeux importants pour les entreprises : la connaissance de leurs contacts, la capacité de conversion des prospects en clients, la fidélité de ces derniers, la pérennité de la relation…

La sécurité des données personnelles des individus et les efforts qu'une entreprise déploient et affichent en ce sens sont des gages de confiance pour les consommateurs pour passer à l'acte d'achat et maintenir dans le temps la relation avec une société.

Un sujet sur lequel les entreprises doivent désormais s'empresser de traiter et d'approfondir, notamment avec l'arrivée de la nouvelle Réglementation Générale sur la Protection des Données (RGPD) européenne qui vise à renforcer les droits des consommateurs et la responsabilité des entreprises ainsi qu'à homogénéiser les règles entre les Etats membres à compter de 2018.

Au-delà des enjeux de performances marketing et commerciales, les sanctions en prévision pour les contrevenants s'alourdissent avec des pénalités financières pouvant aller jusqu'à 4% du chiffre d'affaires. De quoi faire réfléchir et activer rapidement les actions de mise en conformité.

Point sur le sujet.

[1] Verint Systems Inc. 2016

© Dolist / Haas Avocats - Tous droits réservés

Profilage & perspectives Marketing

Qu'est-ce que le profilage ?

Le profilage consiste à **collecter des données à caractère personnel** au gré des visites sur un ou différents sites Internet **dans le but de dresser un profil** correspondant à une catégorie. Par exemple : un homme de 30-35 ans, vivant en milieu urbain, pratiquant le tennis, etc.

Dans une perspective marketing, le profilage **repose sur une analyse comportementale** permettant de déterminer le profil d'un individu **afin de lui proposer des offres ou services personnalisés**. Pour reprendre notre exemple, grâce au traitement des informations collectées sur le Web (par exemple, via des cookies qui collectent des informations sur la navigation), la personne ciblée – déjà connue de l'annonceur et ayant au préalable consenti à recevoir des messages e-mails de sa part – pourra directement recevoir dans sa messagerie des promotions relatives à des équipements de tennis. Cette connaissance affinée de la personne permet à l'annonceur de renforcer ses chances de conclure une vente, tout en optimisant les coûts de ses campagnes.

En effet, le numéro d'identification de l'ordinateur ou de la tablette, l'adresse IP, les informations fournies lors d'une inscription à un service en ligne, les sites web visités, les recherches effectuées sur Internet sont autant d'informations collectées et analysées pour réaliser un profilage.

Les techniques de profilage actuelles

D'un point de vue technique, **deux types de solutions** existent pour analyser finement le comportement d'un individu en ligne et connaître ses préférences :

- Les **cookies « *first party* »**, également dénommés « cookies de domaine », permettent d'analyser l'activité d'un internaute au sein d'un même site : son parcours de navigation, ses préférences (offres, produits ou thématiques éditoriales), son panier d'achat, etc. Ils sont directement déposés par le site en question dans l'objectif de proposer ensuite à son visiteur des offres adaptées en temps réels ou de lui adresser des messages électroniques ciblés post navigation (si celui-ci a consenti au préalable à en recevoir de l'annonceur).
- Les **cookies « *third party* »**, également appelés « cookies tiers », sont des cookies déposés par des tiers dont les contenus sont présents sur le site visité, généralement liés à des publicités et à de l'analyse de performance. Ils sont clairement associés à un nom de domaine différent de celui qui héberge la page sur laquelle navigue l'internaute. Ces cookies permettent de faire un « tracking cross sites » pour évaluer l'activité de l'élément publicitaire géré par le tiers et associent les données comportementales ou déclaratives collectées à l'internaute. Ils peuvent permettre par exemple de personnaliser les offres publicitaires affichées sur les prochains sites visités par ce même internaute.

Des opportunités marketing judicieuses

Au-delà d'actions jugées potentiellement « agaçantes » par les internautes car considérées comme inadaptées ou trop intrusives, il existe **nombre d'actions marketing pertinentes** rendues possibles grâce au profilage.

Pour le bénéfice de l'annonceur certes, mais également dans **une optique gagnante pour le consommateur**. Quelques exemples d'opportunités :

© Dolist / Haas Avocats - Tous droits réservés

- La proposition de communication personnalisée en fonction du profil et des besoins du moment des clients grâce à une meilleure connaissance de ses attentes.
- L'identification des canaux de communication ou d'achats privilégiés avec la marque pour les adresser via leur canal favori.
- Lors des échanges avec le client ou prospect identifié, la proposition d'offres incentivées (remise exceptionnelle, frais de port offertes…) pour les motiver à l'achat.
- Le développement d'opérations de fidélité avec, par exemple, le remerciement par e-mail d'un client à la suite de son passage en caisse ou la proposition de produits complémentaires ou additionnels à tarifs préférentiels.
- Le renforcement des mécaniques de rebond entre points de vente en ligne et physiques avec, par exemple, suite à une fréquentation assidue et répétée sur un produit donné sur Internet, la proposition de venir l'essayer en magasin via un e-mail dédié, un SMS ou un appel.

Les solutions techniques permettent clairement d'**affiner les connaissances d'une entreprise sur un individu,** en misant sur chaque point de contact - online ou offline - et quel que soit le canal emprunté.

© Dolist / Haas Avocats - Tous droits réservés

Le nouveau cadre juridique en matière de profilage à connaître

Un cadre juridique du profilage renforçant le principe d'Opt-In

Le règlement européen du 27 avril 2016, applicable dans les 28 Etats membres à compter du 25 mai 2018, a renforcé significativement les droits des citoyens, non pas en interdisant le profilage mais en l'encadrant plus fortement avec de **nouvelles garanties pour les personnes concernées** par ce type de traitement.

Il le définit dans son article 4 comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

Ainsi, est prévu **pour la personne le droit d'être informé de l'existence d'un profilage**. Les informations doivent aussi porter sur la logique sous-jacente, ainsi que sur l'importance et les conséquences prévues de ce traitement pour la personne concernée.[2]

Une protection des individus contre les abus du profilage

Le règlement consacre en outre le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé[3]. Il en va ainsi lorsque le profilage a, par exemple, pour objet :

- En matière de crédit ou d'assurance, l'estimation de la solvabilité ou de la santé du demandeur à son insu
- Dans le cadre d'un site de recrutement, la sélection des personnes recevant l'offre d'emploi en fonction de leurs orientations sexuelles, de leurs opinions politiques, de leur état de santé ou de tout autre critère
- En termes de prix, la modulation du tarif en fonction du profil de l'internaute.

En pratique, ces dispositions ont vocation à éviter que les responsables de traitement ne procèdent à un examen de la situation individuelle de l'intéressé et ne fondent leurs décisions que sur la seule consultation de fichiers de données personnelles en leur possession, sans permettre à l'intéressé de présenter ses observations le cas échéant.

Des devoirs côté responsable du traitement des données

Dans ces hypothèses, le responsable de traitement doit alors :

- Prendre des mesures pour **protéger les droits de la personne** (intervention humaine, possibilité pour la personne d'exprimer son point de vue, de contester la décision)
- Utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage

[2] Article 13 du règlement européen du 27 avril 2016
[3] Dans son article 22

© Dolist / Haas Avocats - Tous droits réservés

- Faire en sorte de limiter et de corriger les facteurs d'erreur
- **Sécuriser les données** à caractère personnel d'une manière qui tienne compte des risques susceptibles de peser sur les intérêts et les droits de la personne concernée et qui prévienne, entre autres, les effets discriminatoires**.**

Le profilage ne doit en effet pas aboutir à une discrimination fondée sur l'utilisation ou la production de données dites sensibles, relatives à la « *race ou à l'origine ethnique, aux opinions politiques, à la religion ou aux croyances, à l'appartenance syndicale, la santé, la génétique, l'orientation ou l'identité sexuelles* ».[4]

Deux exceptions à cette dernière règle sont néanmoins prévues[5] :

- La personne concernée a donné son consentement explicite
- Le traitement est nécessaire pour des motifs d'intérêt public

L'accent est donc mis sur le **risque de discrimination illégitime** résultant de l'utilisation de mesures de profilage, ainsi que sur la **nécessité de prévoir une intervention humaine** et **d'assurer la transparence de l'utilisation du profilage** vis-à-vis de l'intéressé.

Ainsi, le profilage à des fins de marketing est autorisé dans la mesure où les principes de licéité sont respectés, à savoir si la personne en est informée et peut s'y opposer.

Des conséquences immédiates pour les sites et sur la gestion des cookies

Le Règlement Européen renforce ici un principe bien connu et établi dans le monde du marketing, à savoir le **principe de l'opt-in** qui suppose l'information et le recueil du consentement libre et éclairé de la personne visée[6]. En assurant une **information accrue de l'internaute,** ce dernier est en mesure de donner librement son consentement pour des traitements parfaitement identifiés, tant au niveau de la nature des données collectées qu'au niveau des finalités de leur collecte.

Quels changements pour la collecte de l'opt-in sur les données de navigation ?

Sauf exception, le dépôt de cookies n'est permis qu'à la condition que l'internaute ait donné son accord, après avoir reçu une information claire et complète sur les finalités de ce dépôt. La CNIL[7] considère qu'un tel consentement est recueilli dès lors que l'internaute est informé des finalités des cookies déposés sur son terminal par l'intermédiaire d'un **bandeau d'information**. Dans ce cas, la poursuite de sa navigation vaut accord au dépôt de cookies sur son terminal.

Néanmoins, dans une démarche d'anticipation du règlement européen, les entreprises peuvent d'ores et déjà renforcer le recueil du consentement de l'internaute en faisant **évoluer le bandeau** de manière à ce qu'apparaissent clairement **les finalités du dépôt de cookies**. A titre d'exemple, cette information pourrait devenir : *« En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de cookies pour mesurer notre audience, vous proposer des contenus et publicités personnalisés, ainsi que des fonctionnalités sociales. En savoir plus et gérer les cookies. Ok.* ».

[4] Article 22 alinéa 4 du règlement européen du 27 avril 2016
[4] Par l'article 22, par le biais d'un renvoi à l'article 9)2) a et g
[6] Même si cet opt-in est aménagé en matière de cookies depuis la délibération du 5 décembre 2013 de la CNIL
[7] Dans sa délibération du 5 décembre 2013

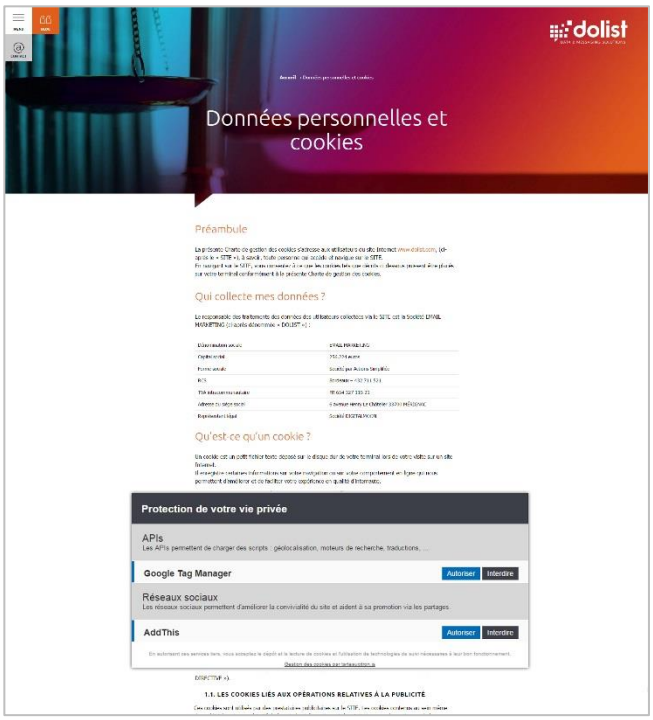
© Dolist / Haas Avocats - Tous droits réservés

Si l'internaute clique sur « OK », il autorise le dépôt de cookies. Un clic sur « En savoir plus et gérer les cookies » mène l'internaute vers la page d'information sur les cookies, lui permettant d'exercer son choix.

Par ailleurs, la Commission européenne a présenté une **nouvelle proposition** de règlement[8] sur « la vie privée et les communications électroniques ». Parmi les nouvelles mesures, la commission propose que **les internautes puissent accepter ou rejeter d'emblée les cookies** sans avoir à réitérer leur refus à chaque arrivée sur un site. Tous les cookies seraient bloqués par défaut, leur activation serait alors du ressort libre de l'utilisateur. Cette demande de consentement devrait apparaître à l'ouverture du navigateur Internet.

Des pratiques transparentes à mettre d'ores et déjà en place

D'autre part, cette volonté de transparence devrait rapidement se traduire par la généralisation **sur les sites marchands et autres plateformes collectant des données** :



- De **politique de confidentialité** détaillant pour chaque typologie de traitement les données collectées, leur finalité, les personnes destinataires mais également la durée de conservation ou encore les garanties en termes de sécurité et de confidentialité apportées par le responsable de traitement.
- De **chartes de gestion des cookies** accompagnant les bandeaux d'information. Via ces Chartes, les internautes pourront directement choisir de désactiver tel ou tel cookie après avoir pu prendre connaissance de la nature de celui-ci et de ses finalités.
- De **mentions claires dans les formulaires** de collecte ou autres cases à cocher au terme desquelles les internautes donnent leur consentement. Pour respecter les exigences du Règlement, il sera sans doute nécessaire de multiplier ces cases à cocher, afin que chacune d'entre elles permette de manifester un consentement explicite pour un traitement donné et parfaitement identifiable dans chacune de ses caractéristiques.

Le cybermarchand, en tant que responsable de traitement, devra ainsi veiller à s'assurer de la mise en conformité de l'ensemble de sa plateforme digitale et ce, **dès le stade de la collecte des données** (cookies, formulaires d'inscription, etc.). Actions de fidélisation, offres promotionnelles, transmission tarifée ou non de tout ou partie du fichier client à des partenaires, etc. Chacune de ces actions devra s'inscrire dans une « politique Data » respectueuse de la législation.

Le Règlement Européen introduit ici une nouvelle responsabilité lourde de sens et de conséquences pour l'ensemble des acteurs.

[8] Proposition émise le 10 janvier 2017

© Dolist / Haas Avocats - Tous droits réservés

Une généralisation attendue des études d'impact sur la vie privée (PIA)

Le règlement européen impose désormais aux entreprises la **réalisation d'une étude d'impact sur la vie privée des traitements de données** à caractère personnel identifiés[9]. Celle-ci est requise en cas de profilage lorsque celui-ci produit des effets juridiques à l'égard d'une personne ou l'affecte significativement.

L'objectif sous-jacent est de **déterminer les mesures techniques et organisationnelles** appropriées pour assurer la meilleure protection aux données à caractère personnel en fonction de l'environnement dans lequel les données sont collectées et traitées.

Il est ainsi précisé[10] que « *L'analyse d'impact relative à la protection des données […] est, en particulier, requise dans les cas suivants :*

- « L'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 »
- Dans le cadre d'un traitement marketing qui consisterait classiquement à envoyer des messages et informations ciblées au regard du profil d'un client. L'annonceur devra notamment veiller à respecter : l'obligation d'information de la personne concernée, et, classiquement, la possibilité de se désabonner.

Au-delà des éléments d'information à faire figurer sur les sites concernés par la collecte de Data et sur les formulaires de collecte, l'étude d'impact s'attachera également à **contrôler les mesures de sécurité** et **de confidentialité** mises en œuvre **par le responsable de traitement** et, incidemment, p**ar le sous-traitant de celui-ci**, fournisseur de la solution e-marketing.

[9] Dans l'article 35
[10] Par l'article 35, 3, a) du Règlement

© Dolist / Haas Avocats - Tous droits réservés

Outre une responsabilisation nécessaire des entreprises responsables de traitement dans un contexte d'essor des nouvelles technologies, l'étude d'impact sur la vie privée favorise la confiance des personnes concernées.

Une obligation de sécurité et de confidentialité renforcée

Si la CNIL (Commission Nationale de l'Informatique et des Libertés) a eu, à plusieurs reprises, l'occasion de confirmer que **l'obligation de sécurité**[11] n'était pas une obligation de résultat, la Commission a également précisé que l'obligation de moyens imposée au responsable de traitement **pouvait tendre vers l'obligation de résultat en fonction de plusieurs critères** : nature des données traitées, risques encourus par les personnes visées par les traitements au regard de leur vie privée, moyens humains, matériels et financiers dont dispose le responsable de traitement pour lui permettre d'assurer la sécurité de ses Systèmes d'Information etc.

Qui est concerné ?

Un exemple concret : Madame *Toutlemonde,* qui vient d'ouvrir sa boutique en ligne de vente de bijoux fantaisies, ne va ainsi pas avoir la même obligation de sécurité que l'hôpital de sa commune qui traite des données sensibles au sein d'un système d'informations complexe - géré par une Direction des Systèmes d'Information composée de plusieurs personnes - ou qu'un groupe international collectant des données comportementales à grande échelle. Madame *Toulemonde* aura une obligation de moyens limitée aux engagements qui encadrent les traitements standards relatifs aux clients/prospects[12]. Tandis que l'hôpital ou le groupe international se verront appliquer une obligation de moyens renforcée tendant vers une obligation de résultat et pourront voir leur responsabilité engagée faute de justifier de la mise en place de dispositifs techniques et organisationnels irréprochables.

L'anticipation du risque

Le Règlement ajoute ainsi un paramètre important : **l'anticipation du risque**. Ainsi, selon le législateur européen, les **mesures techniques et organisationnelles** devant être mises en place pour **assurer la sécurité des données** devront désormais **tenir compte de la nature, la portée, le contexte et les finalités du traitement** ainsi que de la **probabilité et de la gravité du risque** pour les droits et libertés des personnes physiques.

Une logique qui fait directement écho au **principe de *Privacy By design***[13]. En application de ce principe, le responsable de traitement a pour obligation de mettre en place en amont les actions juridiques et techniques adéquates afin de **diminuer les risques portant sur la sécurité et la confidentialité des données** à caractère personnel.

La notification des failles de sécurité

Le règlement impose également au responsable de traitement de notifier toute faille de sécurité à l'autorité de contrôle (la CNIL en France) dans les 72 heures à partir du moment où il aura connaissance de la violation, sauf si celle-ci est insusceptible de porter atteinte aux droits des personnes.[14]

[11] Figurant à l'article 34 de la loi n°78-17 du 6 janvier 1978 modifiée
[12] Figurant dans la Norme Simplifiée 48
[13] Introduit à l'article 25 du Règlement
[14] Article 33 du règlement

© Dolist / Haas Avocats - Tous droits réservés

Par ailleurs, il devra prévenir les personnes concernées s'il apparaît probable que la violation représente un risque pour elles.[15]

Une telle obligation de notification n'est pas sans conséquence pour l'entreprise responsable des traitements. Celle-ci devra en effet mettre en place toutes les mesures nécessaires pour garantir la sécurité de son système d'information aux risques de voir ses lacunes exposées au plus grand nombre. L'enjeu, en termes de réputation, est donc majeur.

Anticipation des risques : les mesures à mettre en place

Dans cette optique, le Règlement impose plusieurs actions : pseudonymisation des données, élargissement de l'obligation de notification des failles de sécurité ou encore, adhésion à des codes de bonnes conduites. L'obligation de sécurité est en outre diffusée dans le cadre des **relations entre responsables de traitement et sous-traitants** avec une obligation de contractualisation généralisée et renforcée.

Pour l'ensemble de ces mesures, l'aspect juridique constitue un rouage essentiel. Chaque responsable de traitement devra ainsi s'assurer – et être en mesure de justifier - de la mise en place :

- D'un **registre des traitements**, la tenue de ce registre ayant vocation à remplacer certaines formalités préalables. Cette obligation est également mise à la charge des sous-traitants, ce qui constitue une nouveauté importante du dispositif prévu par le Règlement. Or, la mise en place d'un tel registre suppose, en amont, la réalisation d'une cartographie des traitements en cause basée sur un **audit de traitement** prenant en compte les points de vue juridiques et techniques.
- La formalisation d'un **référentiel sécurité** incluant : une politique de gestion des incidents liés aux systèmes d'information, une politique d'habilitation, une politique d'archivage et de conservation des données ou encore une Charte dédiée à l'encadrement de l'utilisation des Systèmes d'information de l'entreprise.
- Le déclenchement régulier et l'analyse de **tests d'intrusion**.
- La mise en place de clauses dans les contrats de **sous-traitance** imposant une procédure d'audit.
- La **sensibilisation du personnel** aux enjeux de sécurité et de confidentialité des données (formation, notes de services, livres blancs et autres communications internes à l'entreprise).

La nomination d'un *Data Privacy Officer* - DPO

Le règlement européen prévoit la nomination d'un **Délégué à la Protection des Données** (DPO) qui a vocation à remplacer le Correspondant Informatique et Libertés (CIL).[16] Le DPO serait rendu obligatoire dans certaines structures, des clarifications restants encore en attente sur ce point. De notre point de vue, il semble toutefois que le DPO tend à s'imposer pour toutes les sociétés étant amenées à utiliser des données à des fins de profilage marketing ou à traiter des données « à risque », ainsi que pour le secteur public.

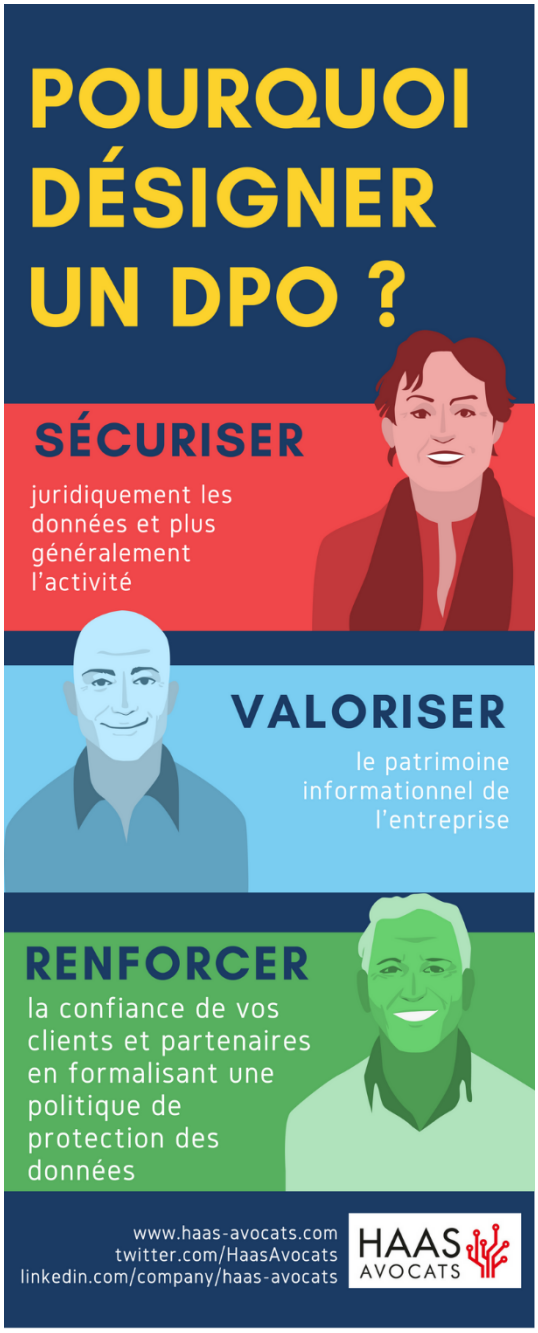
Les missions du DPO

[15] Article 34 du règlement
[16] Article 33 du règlement

© Dolist / Haas Avocats - Tous droits réservés

Le DPO se pose comme un **garant de la conformité** au sein des entreprises. Les missions qui lui sont confiées sont particulièrement étendues et couvrent, a minima, les points suivants :

- **Informer et conseiller** le responsable du traitement - ou le sous-traitant - ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en matière de protection des données
- Contrôler le **respect du droit en matière de protection des données** à caractère personnel et des règles internes, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement et les audits s'y rapportant
- Sur demande, dispenser des **conseils sur l'analyse d'impact** relative à la protection des données et vérifier l'exécution de celle-ci
- Coopérer et faire office de **point de contact pour l'autorité de contrôle** sur les questions relatives au traitement : consultation préalable et consultations sur tout autre sujet
- Tenir compte, dans l'accomplissement de ses missions, du **risque associé aux opérations de traitement** compte tenu de la nature, de la portée, du contexte et des finalités du traitement.



Le DPO veille au respect du droit de la protection des données. Il doit donc **s'assurer de la conformité juridique des traitements**, au-delà des simples conseils et consultations. Par conséquences : une telle fonction implique des compétences particulières et, pour les entreprises, le choix peut s'avérer parfois cornélien entre externalisation et désignation interne.

Qui désigner en tant que DPO ?

Le Délégué à la Protection des Données est désigné sur la base de ses **qualités professionnelles**, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa **capacité à accomplir ses missions**.

Il 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**. Externaliser cette fonction peut apparaître une solution stratégique tant au niveau de la gouvernance interne qu'au niveau des coûts.

Il est soumis au secret professionnel ou à une **obligation de confidentialité** en ce qui concerne l'exercice de ses missions.

© Dolist / Haas Avocats - Tous droits réservés

Au regard de ces dispositions, constatons que si la logique d'indépendance qui était l'une des bases du statut du CIL perdure, un renforcement des **exigences de compétences en matière juridique** est opéré pour le DPO. Du reste, ce renforcement suit logiquement l'**élargissement des missions** du DPO avec, en premier lieu, l'obligation de contrôle de la mise en conformité juridique des traitements.

© Dolist / Haas Avocats - Tous droits réservés

En bref : la check-list pour vous préparer

Protection des droits à la personne	
✔	Recueillir le consentement des individus pour la collecte de données comportementales (cookies) via une action positive et explicite du contact (exemple : case à cocher) et en conserver la preuve.
✔	Limiter la collecte des données au strict minimum requis pour l'accomplissement d'un objectif (principe de minimisation).
✔	Respecter les grands principes liés au traitement des données (licéité, loyauté, transparence, limitation des finalités, limitation de conservation, minimisation, exactitude, intégrité et confidentialité des données) et être en mesure de démontrer, à tout moment, leur respect. (« *accountability* »).
✔	Prendre en compte que, pour les contacts de moins de 16 ans, leur consentement n'est valable que s'il est accordé par leur responsable légal.
✔	S'assurer que l'utilisation des données dans un objectif de profilage ne soit pas discriminante (basée notamment sur l'origine, l'orientation sexuelle, l'état de santé, les opinons politiques, religieuses ou syndicales).
✔	En plus des droits d'accès, de correction et de suppression des données, mettre en place un droit à l'effacement des données (« droit à l'oubli numérique »).
✔	Assurer le transfert des données à un tiers dès lors que la personne concernée par le traitement le réclame (droit de portabilité).
✔	S'assurer que la gestion et le traitement des données se réalisent dans le cadre des frontières européennes, hors dérogations spécifiques.
✔	Ne pas vendre, partager ou louer les données personnelles, hors consentement explicite des contacts.
Informations aux personnes	
✔	Expliquer clairement quelles sont les informations collectées, cédées, partagées sur les formulaires d'inscription et dans les mentions légales du site. Mentionner également les raisons de leur collecte.
✔	Lister les données personnelles détenues précisant leur sensibilité, source, caractère obligatoire ou non, les destinataires (y compris hors UE) et leur durée de conservation.
✔	Répertorier tous les traitements de l'entreprise faisant intervenir des données personnelles (par exemple la collecte, conservation, modification, utilisation, diffusion, etc.).
✔	Définir la politique de confidentialité/mentions légales de l'entreprise, notamment en matière d'utilisation des données personnelles.

© Dolist / Haas Avocats - Tous droits réservés

✔	Rendre accessible la politique de confidentialité/mentions légales depuis tous les modes de collecte (formulaires notamment) et depuis la page d'accueil du site.
✔	Mettre en place la charte de protection des données personnelles et de gestion des cookies (définition, usage, désactivation des cookies, durée de conservation, droits d'accès/d'opposition) et la valoriser sur le(s) site(s) de l'entreprise.
✔	Fournir les détails de la collecte d'un contact sur demande (date, adresse IP, mode de collecte, etc.).
Obligations de sécurité & d'anticipation des risques	
✔	S'assurer que les prestataires ayant accès aux données ou en lien avec la gestion des données respectent les obligations de sécurité et de protection des données.
✔	Réaliser une étude d'impact sur la vie privée (« *Privacy Impact Assessment* » - PIA) permettant d'évaluer l'adéquation des mesures prises par le responsable de traitement au regard des risques encourus sur la vie privée.
✔	Garantir que, par défaut, seules les données qui sont nécessaires au regard de la finalité de chaque traitement sont traitées : limiter la quantité de données collectées, anonymiser les données, limiter la durée de conservation, etc. *(« Privacy by default »)*
✔	Nommer un « *Data Privacy Officer* » (DPO) si : • l'entreprise ou le sous-traitant appartient au secteur public • l'activité principale amène à réaliser un suivi régulier et systématique des personnes à grande échelle • l'activité principale implique un traitement à grande échelle des données sensibles (origine, santé, orientation sexuelle, opinion politique etc.) ou relatives à des condamnations. Le DPO est en charge de la protection des données, de la sensibilisation des collaborateurs de l'entreprise et du suivi de l'évolution du traitement des données. Gérant les dimensions techniques, réglementaires et la mesure du risque, il doit tout mettre en œuvre pour mettre et maintenir l'entreprise en conformité.
✔	Mettre en place un registre des traitements des données pour l'entreprise et ses sous-traitants avec une liste des mesures précisant : le nom, les coordonnées du responsable ou du DPO, la finalité, les personnes concernées, les destinataires, les transferts de données hors UE, les délais prévus pour l'effacement des données, la description des mesures de sécurité mises en place.
✔	Réaliser régulièrement des tests techniques d'intrusion / accès aux données avec tenue d'un registre des incidents de sécurité détaillés.
✔	Ajouter dans les contrats de sous-traitance d'une clause imposant un audit de sécurité.
✔	Sensibiliser le personnel aux enjeux de confidentialité et de sécurité des données.

© Dolist / Haas Avocats - Tous droits réservés

Pour conclure

Le Règlement européen, faisant écho aux préoccupations des citoyens, renforce considérablement les **droits des individus** sur leurs données personnelles.

Ainsi, d'un système de responsabilité vertical où le responsable de traitement devait répondre de ses obligations en matière de protection des données personnelles, le Règlement nous projette dans un modèle horizontal où **tous les acteurs impliqués dans le traitement peuvent directement engager leur responsabilité** (le responsable de traitement tout comme ses sous-traitants).

Il appartient dès lors aux professionnels de **se préparer activement** à la mise en œuvre des principes du Règlement dont la violation donnera lieu à d'importantes sanctions à compter de mai 2018. Pour rappel, **le Règlement alourdit les sanctions** infligées par les autorités de contrôle qui peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

Au-delà du coût financier qu'engendre une violation des dispositions du Règlement, l'entreprise contrevenante met directement **en jeu sa réputation et sa crédibilité**.

Dans ce contexte, la désignation de DPO constitue sans nul doute un élément clé de la mise en conformité des entreprises.

Cette mise en conformité, a priori contraignante, doit néanmoins être vue comme une réelle **opportunité de développement** tant dans l'univers digital que dans le monde physique. Tous les acteurs sont concernés, TPE-PME, grandes entreprises industrielles, SSII, entreprises publiques, collectivités territoriales, etc.

En adoptant une politique de protection des données adéquate, il s'agit d'**assurer non seulement sa sécurité juridique** mais également de **renforcer son image** vis-à-vis de ses clients comme de ses partenaires.

© Dolist / Haas Avocats - Tous droits réservés

HAAS AVOCATS

Externalisez votre DPO

Le Data Protection Officer (DPO) devient obligatoire* avec le nouveau règlement européen. Préparez-vous !

Le cabinet HAAS Avocats propose un contrat de prestations de services clé en main permettant d'externaliser la fonction de DPO et d'assurer la conformité à la réglementation applicable à la protection des données.

Contactez-nous. 01 56 43 68 80 - www.haas-avocats.com - contact@haas-avocats.com

*pour le secteur public et dans certaines conditions pour le secteur privé à compter de mai 2018

dolist
DATA & MESSAGING SOLUTIONS

Auditez vos pratiques Data & Marketing

Besoin d'améliorer la qualité de votre base de données, la délivrabilité de vos campagnes ou d'optimiser votre stratégie e-mail marketing ?

Améliorez vos performances marketing !

Nos consultants posent un regard extérieur sur vos pratiques pour en identifier les forces et faiblesses et vous fournir des leviers de progression significatifs.

Découvrez nos différents audits →

info@dolist.com - **www.dolist.com**

À propos de HAAS Avocats

Cabinet français indépendant, HAAS AVOCATS offre à ses clients un très large éventail de compétences en droit de la propriété intellectuelle, des nouvelles technologies, de l'information et de la communication, de l'e-commerce, de la protection des données personnelles pour guider les entreprises à toutes les étapes de leur développement.

Standard : **+33 (0)1 56 43 68 80**
E-mail : **contact@haas-avocats.com**
Infos et actualités : **www.haas-avocats.com**

Paris : 32 rue La Boétie
75 008 Paris

À propos de Dolist

Experte du e-marketing et de la smart data, Dolist propose un ensemble de services et d'outils dédiés aux enjeux divers de l'adressage digital. Du conseil stratégique à l'accompagnement opérationnel, Dolist optimise et révèle le potentiel des données et des messages pour permettre aux annonceurs d'engager leurs clients de manière durable.

Standard : **+33 (0)5 57 26 25 70**
E-mail : **info@dolist.com**
Infos et actualités : **www.dolist.com**

Paris : 28 rue Notre Dame des Victoires
75002 Paris
Bordeaux : 6 avenue Henry Le Châtelier
33700 Mérignac