RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES

12 FICHES SYNTHÉTIQUES SUR LE RGPD

Mai 2018

RGPD :

Adhérents du CPA :
«12 fiches synthétiques pour vous aider à être prêts.»

COLLECTIF PERFORMANCE & ACQUISITION

Contacts :
Collectif de la Performance & de l'Acquisition
8 rue Saint Fiacre
75002 Paris - France

T. (33) 01 77 45 46 23
E. contact@cpa-france.org
www.cpa-france.org
Twitter : @CPA_Performance

Noella Boullay : Déléguée Générale - nboullay@cpa-france.org
Marion Vittadello : Chargée de Communication - mvittadello@cpa-france.org

CO-RÉDACTEURS DES FICHES JURIDIQUES

Fabrice PERBOST
HARLAY AVOCATS

Caroline BELOTTI
brm AVOCATS
Membre de TGS France Avocats

Matthieu DARY
DE GAULLE FLEURANCE & ASSOCIÉS

Yves SEXER
MARCEAU AVOCATS
Avocats au Barreau de Paris

Marion LECARDONNEL
MARCEAU AVOCATS
Avocats au Barreau de Paris

Jean-Jacques BENATTAR
Perspectives AVOCATS

Grégory MARGOLINE
Perspectives AVOCATS

Noella BOULLAY
Déléguée Générale

Joy GRAND
Chargée de Communication

PRÉFACE

Le Collège Juridique du CPA, créé au cours de l'année 2017, a pour vocation d'être la voix juridique du CPA mais également d'informer et d'assister ses adhérents. Il est composé d'avocats, de juristes et de professionnels du marketing à la performance, chacun y apportant son expertise.

L'existence même du Collège Juridique est la preuve d'une certaine maturité du CPA, qui lui permet aujourd'hui de se positionner sur différents sujets légaux. Et s'il en est un qui fait l'actualité, tous medias confondus, spécialisés ou généralistes, c'est bien le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données qui abroge la directive 95/46/CE, plus communément appelé RGPD (en français : Règlement Général sur la Protection des Données) ou GDPR (en anglais : *General Data Protection Regulation*).

Le nombre d'écrits, de séminaires, d'offres, de formations et de colloques sur la mise en conformité avec le RGPD ne semble pourtant pas dissiper le brouillard dans lequel les sociétés ont encore et toujours le sentiment de se trouver face au RGPD. Malgré la date butoir du 25 mai 2018 et alors qu'on commence à apercevoir les récifs du RGPD, beaucoup de progrès restent à faire. Trop de sociétés n'ont en effet pas encore pris la mesure du RGPD et méconnaissent ses mécanismes. Pourtant, le cadre juridique relatif aux données personnelles existe déjà depuis 40 ans puisque la loi relative à l'informatique, aux fichiers et aux libertés date du 6 janvier 1978 ! Et le RGPD ne bouleverse pas les grands principes en la matière. En revanche, il renforce les obligations vis-à-vis des personnes concernées par leur traitement (par exemple, l'information et le consentement) et les sanctions applicables (jusqu'à 4% du chiffre d'affaires mondial ou 20 millions d'euros). Le RGPD apporte également quelques nouveautés (droit à la portabilité des données, suppression des formalités déclaratives, notification des incidents de sécurité auprès de la CNIL pour tous les responsables de traitements, DPO obligatoire pour certains organismes et/ou types de traitements, etc.). Dans un tel contexte, il était important que le CPA propose à ses adhérents des outils et des solutions.

« *Je vois venir des catastrophes. Pire des avocats* » chante un chœur antique dans le film Maudite Aphrodite de Woody Allen. Beaucoup penseront que cette citation pourrait s'appliquer au RGPD et à sa mise en œuvre. Le CPA a fait le pari inverse en considérant que le RGPD n'est pas une catastrophe mais plutôt une formidable opportunité et que l'aide des avocats et des juristes ne peut être que salutaire. Le mot d'ordre serait alors : « *Je vois venir le RGPD. Mais heureusement le CPA est là !* ».

C'est donc tout naturellement que le Conseil d'Administration du CPA a souhaité que le Collège Juridique s'empare de la question du RGPD avec pour feuille de route de faire simple et compréhensible sans chercher à ajouter un étage à la Tour Eiffel. Le challenge était donc énorme pour les juristes !

Dans cette logique, plutôt que de longues et sinueuses analyses, le Collège Juridique a eu à cœur d'exclure toute approche dogmatique, théorique, affective et passionnelle où le vertige et la crainte l'emporteraient sur l'analyse. Il a ainsi privilégié les solutions pratiques et les recommandations claires à l'ensemble des adhérents afin d'aider ces derniers dans l'appréhension des questions et enjeux liés au RGPD.

Le guide est constitué de 12 fiches. Dans chacune des fiches, on trouvera de manière synthétique ce qu'il convient de savoir sur chaque thème. L'accent a été mis sur la lisibilité et l'accessibilité afin d'éviter tout « juridisme » et faire en sorte que la lecture de chaque fiche ne se révèle pas absconse pour les non-juristes. Chaque fiche contient également un lien hypertexte qui renvoie vers une fiche plus détaillée pour ceux qui souhaiteraient disposer d'informations plus précises et élaborées*.

Bien évidemment, ce guide sera amené à être révisé et mis à jour au gré des évolutions légales, jurisprudentielles et doctrinales. Il a également vocation à s'enrichir au fur et à mesure des questions rencontrées par les membres du CPA afin de donner une représentation de l'expérience collective du CPA et de devenir un moyen de partager cette expérience avec les autres membres.

Si ces fiches ne permettent pas encore de totalement dissiper le brouillard qui entoure le RGPD et sa mise en œuvre, gageons qu'elles permettront à tout le moins qu'il y ait du bitume sur la route de chacun des adhérents du CPA afin de garder le cap et éviter toute sortie de route.

Le dernier mot, mais non le moindre, sera pour les rédacteurs et contributeurs de ces fiches. Je les remercie vivement pour leur investissement, leur disponibilité, à titre gracieux, et la qualité de leur participation. Leur professionnalisme et leur implication ont permis d'élaborer des recommandations qui, j'en suis sûr, seront utiles à tous les adhérents du CPA.

Fabrice PERBOST
Président
Collège juridique du CPA

HARLAY
AVOCATS

** Ce guide exprime, à la date indiquée en première page, la position du CPA sur le RGPD, étant précisé que les réponses apportées sont à personnaliser et adapter au cas par cas. Le CPA ne fournit aucun conseil juridique. Le guide ne dispense pas les membres du CPA de consulter des avocats, juristes ou autres spécialistes habilités à donner des conseils de nature juridique. D'une manière générale, il est rappelé que le guide ne dispense pas les membres du CPA de respecter les dispositions légales et réglementaires qui leur sont applicables.*

SOMMAIRE

FICHE N°
1

Le DPO

1. Quelles sont les entités concernées ?

RT : Responsable de traitement
ST : Sous-traitant
Activité de base : Surveillance systématique et à grande échelle des personnes.
Pas de seuil de chiffre d'affaires ou de nombre de salariés.

2. Quels moyens sont mis à sa disposition ?

- Dispose de moyens pour exercer sa fonction :
  a) budget,
  b) local,
  c) formation.

3. Qui peut être désigné ?

- Indépendant : ne reçoit pas d'instructions,
- Compétences professionnelles,

INTERNE

IL PEUT ÊTRE NOMMÉ EN INTERNE :

1. En interne : le délégué ne doit pas avoir de conflit d'intérêts avec ses autres missions et agir en toute indépendance.

2. Groupe de sociétés : DPO possible et facilement joignable au sein du groupe
Ex : groupes internationaux - DPO du siège

EXTERNE

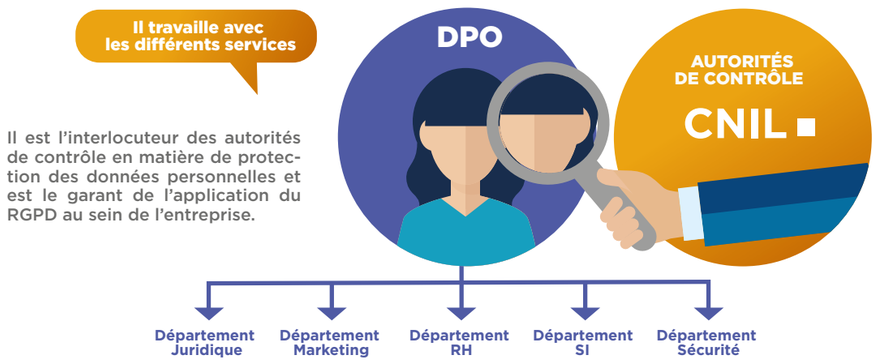
IL PEUT ETRE NOMME EN EXTERNE

DPO externalisé : cabinets d'avocats prestataires de service consultant

2. DPO mutualisé : pour des associations et autres organismes représentant des catégories de RT ou de ST
Ex : cabinets de conseil

3. Quel est le rôle du DPO ?

Le DPO ou Data Protection Officer est présenté comme le « Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme.



Fiche n°1 • Le DPO

Le DPO doit :

- Informer et conseiller le responsable du traitement ou le sous-traitant de leurs obligations issues du RGPD.
- Procéder de même à l'égard des employés qui réalisent des traitements de DCP* : action de sensibilisation des opérationnels.
- Contrôler le respect du RGPD, du droit européen ou du droit national en matière de protection des données et des règles internes en matière de protection de DCP* ; notamment au regard des droits des personnes concernées (ex : droit d'information / accès / rectification / portabilité / droit à l'oubli / notification de violations de données...)
- Le G29** explicite la notion de contrôle du respect du RGPD comme suit : collecter des informations pour identifier les traitements, analyser et vérifier leur conformité, informer, conseiller et émettre des recommandations.
- Coopérer avec l'autorité de contrôle et faire office de point de contact sur les questions relatives au traitement.

Formulaire de désignation du DPO :
https://www.cnil.fr/fr/designez-en-ligne-votre-delegue-la-protection-des-donnees-aupres-de-la-cnil

* DCP : Données à caractère personnel
**G29 : cf glossaire p.57

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

LA CARTOGRAPHIE DES TRAITEMENTS

1. Une cartographie se réalise en 5 étapes :

Afin d'identifier les changements à apporter (désignation d'un DPO, études d'impact, modification des mentions d'information, des procédures internes et des mesures de sécurité à mettre en place, etc.), une cartographie des traitements de données personnelles réalisée lors d'un audit peut être nécessaire.

La présente fiche a pour objet de présenter la méthodologie afin de réaliser la cartographie et de préparer la mise en conformité avec le RGPD.

Pourquoi effectuer une cartographie des traitements ?

Une cartographie est un recensement des traitements existants au sein d'une entreprise et permet à cette dernière de mesurer son degré d'avancement au regard des obligations en matière de données personnelles et d'identifier les écarts afin d'être conforme au RGPD (« gap analysis* »).

* Gap analysis : analyse d'écart

2. L'établissement du rapport «gap analysis*»

Une fois les réponses aux questionnaires obtenues ou interviews réalisés, il convient de les étudier et de les compiler pour faire le bilan de l'existant.
Ce rapport sera également l'occasion d'analyser la conformité de chaque traitement effectué par l'entreprise, en identifiant les points d'amélioration.

Exemple de synthèse d'un rapport « gap analysis* »

	DROIT D'INFORMATION	DESTINATION DES DONNÉES	DROIT D'INFORMATION DES PERSONNES	CONSENTEMENT ET FINALITÉ	DURÉES DE CONSERVATION DES DONNÉES	ENCADREMENT ET TRANSFERT DE DONNÉES À L'INTERNATIONAL	SÉCURITÉ INFORMATIQUE	...
TRAITEMENT 1 Fichier du personnel	✓	✗	✗	✗	✓	✓	✗	
TRAITEMENT 2 Fichier clients	✗	✗	✓	✗	✗	✗	✓	
TRAITEMENT 3 Fichier prospects	✗	✓	✗	✗	✗	✗	✗	
TRAITEMENT	✗	✗	✗	✓	✗	✗	✗	
...								

* Gap analysis : analyse d'écart

Fiche n°2 • La cartographie des traitements

3. Exemple de rétro-planning

	M -8	M -7	M -6	M -5	M -4	M -3	M -2	M -1	M
Cartographie des traitements (questionnaires, interviews et plan d'action)	✓	✓	✓						Entrée en application du réglement
Modification de contrats		✓	✓	✓					
Modification des mentions d'informations des sites internet		✓	✓	✓					
Mise en place d'un registre			✓	✓					
Revue de l'encadrement des transferts				✓	✓				
Revue des procédures de sécurité et de conservation des données				✓	✓	✓			
Réalisation d'étude d'impacts					✓	✓			
Mise en place des procédures internes					✓	✓			
Préparation des supports de formation						✓	✓		
Formation du personnel							✓	✓	
Bilan et contrôle								✓	

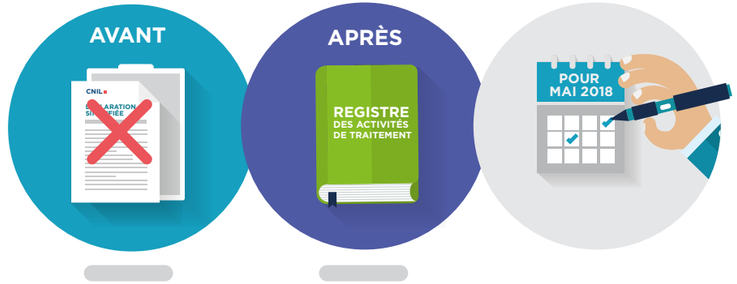
Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°
3

LE REGISTRE DES ACTIVITÉS DE TRAITEMENT

1. Le registre : la fin des déclarations CNIL

Alors que la directive de 1995 reposait en grande partie sur l'existence de formalités préalables (déclaration, autorisations), le RGPD repose sur une logique de conformité et de responsabilité, dite d'« accountability ». Ainsi, les formalités préalables à accomplir auprès de la CNIL sont révolues. A la place, les responsables de traitements et sous-traitants devront mettre en place des registres des activités des traitements effectués sous leur responsabilité (dans le cas du RT*) ou pour le compte du RT (dans le cas du ST**).



Aucune déclaration préalable,
mais tenir **UN REGISTRE**
des activités de traitement.

*RT : Responsable de traitement - **ST : Sous-traitant

2. Le registre : qui, comment et quand ?

Qui ?

Qui doit tenir un registre ?

Le registre doit être tenu par :
1. Les responsables de traitement, pour toutes les activités de traitement effectuées sous leur responsabilité.

2. Les sous-traitants, pour toutes les activités de traitement effectués pour le compte d'un responsable de traitement.

Comment ?

Comment tenir son registre ?

Il convient de recenser les traitements en fonction de leurs finalités et détailler pour chacun les mentions obligatoires. La CNIL a proposé sur son site internet un modèle de registre qui comporte un onglet général pour la liste de tous les traitements, et un onglet spécifique à chaque traitement. Ce modèle n'est toutefois pas obligatoire.

Quand ?

Obligatoire ou facultatif ?

Le texte du RGPD comporte des exceptions à cette obligation de tenue d'un registre pour les entreprises ou organisations de moins de 250 salariés. Toutefois, à la lecture du texte, ces dispenses s'avèrent en pratique limitées. La tenue du registre s'impose donc presque systématiquement.

Fiche n°3 • Le registre des activités de traitement

3. Quelles sont les informations à détailler pour chaque traitement ?

	Informations à faire figurer	Dans le registre RT*	Dans le registre ST**
Qui ?	Nom et coordonnées du RT* (+ son représentant et DPO le cas échéant) Nom et coordonnées du ST* (+ son représentant et DPO le cas échéant)	✓	✓
	Nom et coordonnées du ST*		✓
Pour-quoi ?	Finalités du traitement	✓	
	Catégories de traitement		✓
Quoi ?	Personnes concernées et catégories de données concernées	✓	
Où ?	Destinataires	✓	
	Transfert vers un pays tiers ou organisation internationale	✓	✓
Jusqu'à quand ?	Délais de conservation et d'effacement des données	✓	
Com-ment ?	Description de mesures de sécurité techniques et organisationnelles	✓	✓

*RT : Responsable de traitement - **ST : Sous-traitant

Fiche n°3 • Le registre des activités de traitement

A noter :

- **Une entreprise pourra avoir une double casquette.**
  Exemple : un hébergeur sera à la fois responsable de traitement (pour les traitements relatifs à la gestion de son personnel) et sous-traitant (pour les clients pour le compte desquels il assure l'hébergement).

- **La liste des traitements qui font chacun l'objet d'une fiche distincte doit être établie par finalité principale (et non par outil ou applicatif utilisé).**
  Exemple : La société X a mis en place plusieurs dispositifs de sécurité : caméra de vidéo surveillance, badges d'entrée pour les salariés. Ces 2 outils collectent des données personnelles. Une fiche pour le traitement « Surveillance des biens et locaux » sera créée dans le registre des activités de la société ayant pour finalités : assurer la sécurité des biens et des personnes, prévenir les risques. Mais les badges d'entrée remis aux salariés servent également à surveiller les horaires d'arrivée des salariés, ce qui correspond à un autre traitement et fera donc l'objet d'une autre fiche.

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

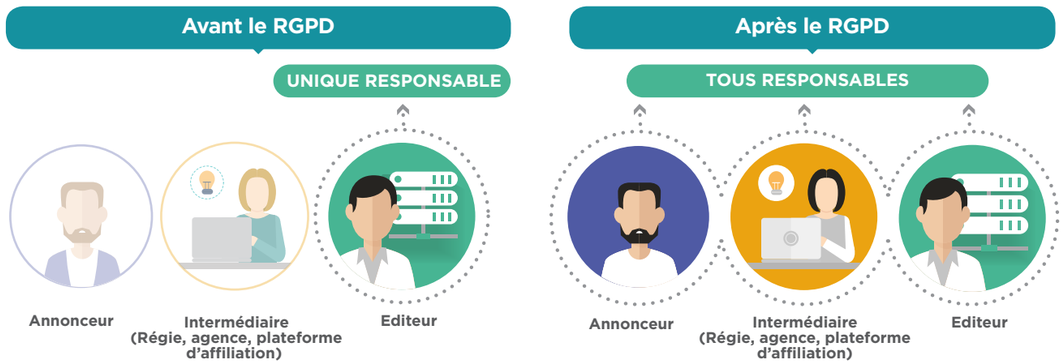
FICHE N°

4

LA RESPONSABILITÉ

1. Consécration de la Responsabilité solidaire

En cas de responsabilité conjointe de responsables du traitement et sous-traitants, chacun des responsables du traitement ou des sous-traitants pourra être tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.



« Tout tiers peut engager la responsabilité de l'ensemble ou chaque acteur de la chaine »

Fiche n°4 • La responsabilité

2. Nouvelles obligations incombant au RT et au ST : la notion d'accountability*

Exemples d'actions concrètes (non exhaustives) pouvant être mises en œuvre par le RT afin que ce dernier puisse justifier du respect du RGPD :**

- Tenir un registre des traitements de données à caractère personnel
- Adopter une procédure permettant de répondre dans les meilleurs délais à l'exercice des droits des personnes : droit d'accès, droitd'opposition, droit à l'effacement des données...
- Mettre en place une Politique de durée de conservation
- Supprimer/Archiver automatiquement toute ou partie des données lorsque la durée de conservation arrive à son terme
- Être en mesure de conserver et rapporter la preuve à tout moment du recueil du consentement
- Prendre en compte la protection des données personnelles dès la conception d'une application ou d'un traitement (Privacy by design/Privacy by default)
- Désigner un DPO
- Sensibiliser et former les membres du personnel
- Adopter des codes de conduite

...

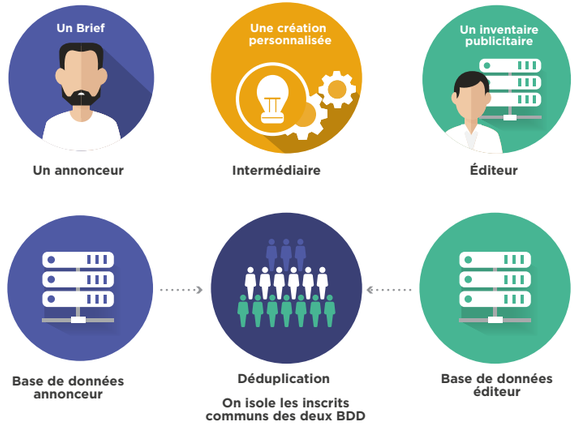
Le seul fait de ne pas fournir à l'autorité de contrôle les éléments attestant de la conformité du/des traitement(s) concerné(s) est susceptible d'entrainer une sanction. (lire notre fiche n°12 – Sanctions)

**Accountability* : cf glossaire p.56*
***RT : Responsable de traitement*

3. Cas pratique

Problématique

« Un annonceur fait appel à un intermédiaire pour identifier et négocier auprès d'éditeurs des bases de données à louer.
L'intermédiaire réalise pour le compte de son client annonceur la déduplication entre son fichier et celui de l'éditeur ».



Conclusion : chacun de ses acteurs pourra être tenu responsable en tout ou partie du préjudice subi par une personne. L'entité condamnée pourra se retourner contre son co-contractant si elle prouve que celui- ci a manqué à ses obligations légales et/ou contractuelles.

Recommandation : veiller à encadrer la responsabilité de chacune des parties au sein de vos contrats.

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°
5

L'INTERNATIONAL

1. Un champ d'application du RGPD à l'international

L'objectif du **RGPD est de soumettre tout traitement visant les ressortissants de l'UE, que ce traitement ait lieu ou non sur ledit territoire.**
Le but du législateur européen est clairement de soumettre à cette réglementation certains acteurs du web qui échappaient jusqu'à maintenant au droit des Etats membres de l'UE.

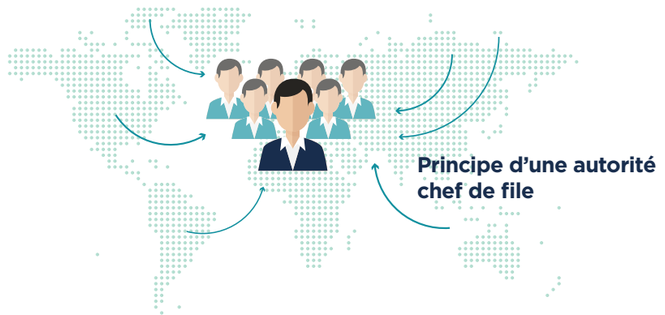
Cela permet de renforcer la compétitivité des entreprises européennes face aux acteurs des pays tiers. Désormais, le non-respect par ces entreprises de la règlementation pourra entraîner des poursuites par les autorités en charge des données personnelles ou des actions en concurrence déloyale par les entreprises disposant d'un intérêt à agir.

Fiche n°5 • L'international

2. Le guichet unique ou l'autorité chef de file

Si votre entreprise ou organisation intervient au niveau international, il convient de déterminer de quelle autorité de contrôle elle dépend.

Le principe du guichet unique est la faculté pour une société ayant des établissements dans plusieurs pays de centraliser l'ensemble de ses démarches auprès d'une seule autorité, dite « autorité chef de file ».



L'instauration du principe du guichet unique va permettre aux entreprises :
- de disposer d'un seul interlocuteur au sein de l'UE (demandes d'autorisation, contrôles, sanctions)
- de diminuer les contraintes administratives et les coûts afférents à l'obligation de se conformer à chacun des droits nationaux.

3. La gestion des transferts internationaux des données

Par transfert international de données, il faut entendre tout transfert en dehors de l'UE.

Le législateur encadre ce transfert car il veut s'assurer que le destinataire des données va offrir un même niveau de protection que celui auquel est soumis le responsable de traitement ou le sous-traitant sur le territoire de l'UE.

Sécuriser les transferts de données personnelles à l'international

- Avant de transférer en dehors de l'Union européenne, les données doivent être sécurisées.
- Il convient d'encadrer ce transfert par des instruments juridiques.

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°

6

PRIVACY BY DESIGN

1. Privacy by Design (protection de la vie privée dès la conception)

L'approche « Privacy By Design » consiste pour une entreprise à développer des produits et des services en prenant en compte, dès leur conception et tout au long de leur cycle de vie, les aspects liés à la protection de la vie privée et des données à caractère personnel.

Cela implique de prendre en compte, dès la conception de projets informatiques destinés à traiter des données personnelles, les exigences en matière de protection de la vie privée et les intégrer aux systèmes informatiques, aux infrastructures des réseaux et aux pratiques de l'entreprise.

Avant le RGPD

Après le RGPD

Fiche n°6 • Privacy by design

2. Privacy By Default (protection de la vie privée par défaut)

L'approche « Privacy By Default » implique que soit mis en oeuvre des mécanismes garantissant que, par défaut, seules seront traitées les données à caractère personnel nécessaires et pertinentes à chaque finalité spécifique du traitement. Le RGPD prévoit des exemples de mesures pouvant être appliquées au titre du Privacy by design :

- **La pseudonymisation des données :**
  elle permet de ne plus pouvoir associer des données à une personne physique précise sans avoir recours à des informations supplémentaires
- **La minimisation des données :**
  elle consiste à ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement

Avant le RGPD

Message de géolocalisation par défaut pendant l'utilisation d'une application - push de notification envoyé

Après le RGPD

La géolocalisation devra être activée dans les paramètres. Par défaut, elle sera inactive.

3. Les mesures organisationnelles

- **Formaliser** un cahier des charges traduisant les contraintes juridiques en matière de protection des données personnelles en contraintes techniques devant être respectées pour tout nouveau projet,
- **Rédiger** une charte dédiée à l'encadrement de l'utilisation des systèmes d'information de l'entreprise,
- **Sensibiliser** le personnel aux enjeux de sécurité et de confidentialité des données,
- **Mettre en place** une politique de gestion des incidents liés aux systèmes d'information, d'archivage et de conservation des données...

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°
7

LE DROIT D'INFORMATION

1. Quelles sont les mentions ?

COLLECTE DIRECTE : Les anciennes mentions sont maintenues.

En plus, les nouvelles mentions demandées sont les suivantes :

Modifications de fond :

- Base légale du traitement c'est-à-dire, le fondement du traitement, soit le consentement soit l'exécution d'un contrat, soit les intérêts légitimes
- Droit de retrait du consentement (si le traitement est fondé sur le consentement)
- Portabilité
- Limitation
- L'existence d'une prise de décision automatisée, y compris un profilage, et, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée
- La référence aux garanties appropriées ou adaptées en cas de transfert vers un état tiers et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition

Modifications de forme :

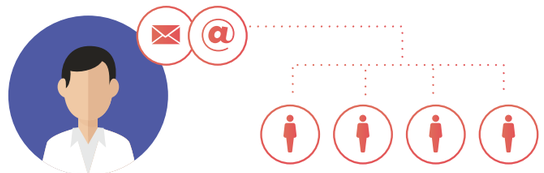
- Coordonnées du DPO
- Droit de saisine de la CNIL

Fiche n°7 • Le droit d'information

COLLECTE INDIRECTE

2 informations supplémentaires :

- Les catégories de données concernées
- 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



COLLECTE DIRECTE

Je collecte pour mon compte

COLLECTE INDIRECTE

- **Je collecte pour mes partenaires**
- **J'exploite la base d'un tiers qui a récolté les opt'ins partenaires.**

Fiche n°7 • Le droit d'information

2. Quand et comment informer ?

Quand ?

- **COLLECTE DIRECTE** : Lors de la collecte, par le RT*
- **COLLECTE INDIRECTE** : a) Dans un délai raisonnable mais ne dépassant pas un mois

  b) Si les DCP* doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne

Comment ?

QUALITÉ DES INFORMATIONS :

CONCISE
TRANSPARENTE
COMPRÉHENSIBLE
AISÉMENT ACCESSIBLE
EN DES TERMES CLAIRS ET SIMPLES

MENTIONS SUR

*RT : Responsable de traitement *DCP : Données à caractère personnel

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°
8

LE CONSENTEMENT

1. Les caractéristiques du consentement au sens du RGPD

SPECIFIQUE

- Un consentement distinct doit pouvoir être donné (ou non) pour chaque finalité* envisagée.
- Le consentement au traitement de ses données à caractère personnel ne peut pas être dilué dans l'acceptation des conditions générales de vente.

ECLAIRÉ

- La demande doit être claire et concise, ne pas induire en erreur.
- La personne doit être informée sur le traitement (l'identité du responsable du traitement, finalités du traitement, durée de conservation...) et sur ses droits.
- Ces informations doivent être transmises d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Elles ne doivent pas être ambigües.

LIBRE

- La personne concernée doit pouvoir donner, refuser ou retirer son consentement sans subir de préjudice.
- Le consentement est présumé ne pas avoir été donné librement si l'accès à un service est subordonné au consentement au traitement de données à caractère personnel qui ne sont pas nécessaires à la fourniture de ce service.

UNIVOQUE

- Une déclaration ou un acte positif clair.
- Pas de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.
- Conséquences : techniques d'opt-in valides, techniques d'opt-out ou d'opt-in «passif» à proscrire.

*Finalité: cf glossaire p.57

Fiche n°8 • Le consentement

2. Exemple du recueil du consentement :

Il y a d'autres moyens d'expression du consentement :
Le checkbox n'est pas le seul moyen employé : case à coher, bouton, liens

☑ «J'accepte de recevoir des offres commerciales des partenaires de la SOCIETE X ainsi que les newsletters de la SOCIETE X »

Le consentement n'est pas conforme :

- Il ne peut pas être donné finalité* par finalité
- **La case est pré-cochée**

☐ «J'accepte de recevoir par email les newsletters de SOCIETE X»

☐ «J'accepte de recevoir les offres commerciales des partenaires de SOCIETE X»

Le consentement semble être conforme (sous réserve des autres conditions) :

- Il peut être donné finalité par finalité
- **Les cases ne sont pas pré-cochées**

*Finalité : cf glossaire p.57

Fiche n°8 • Le consentement

3. Quelques exceptions

Les données personnelles d'une personne peuvent être traitées sans son consentement dans certains cas.

Exemples :

Le traitement est nécessaire **à l'exécution d'un contrat** auquel la personne concernée est co-contractante.

Exemples : traitement de son adresse pour que des produits achetés en ligne puissent être livrés ; traitement des informations bancaires pour que les salariés puissent être payés.

Le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.

Attention ces exceptions sont strictement encadrées !

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°

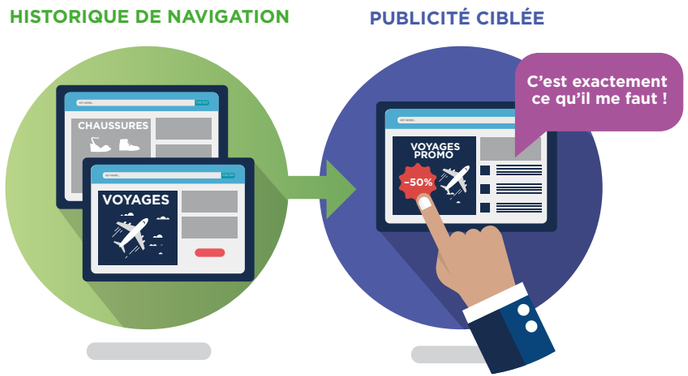
9

LE PROFILAGE

1. Définition du profilage

Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel 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.

Exemple de profilage :



Fiche n°9 • Le profilage

2. Le profilage est licite sous certaines conditions

Il y a lieu de respecter les dispositions du RGPD dont notamment l'obligation :

- d'informer de manière spécifique la personne concernée,
- de fournir des garanties permettant d'encadrer le risque d'atteinte à la vie privée,
- d'assurer la sécurité et de protéger les données personnelles lors de la collecte et du traitement des données,
- d'accorder à la personne concernée un droit d'accès à son profil et aux données collectées la concernant,
- d'accorder à la personne concernée le droit de modifier ou corriger les données inexactes ou incomplètes la concernant,
- d'accorder à la personne concernée le droit de s'opposer à tout moment à son profilage.

Comment utiliser les données obtenues à l'aide du profilage ?

Par principe, est interdit l'usage du profilage pour prendre une décision individuelle à l'encontre d'un individu qui produit des effets juridiques à son égard (par ex. le fait d'exclure ou de blacklister un individu, de refuser une candidature) ou l'affecte « de manière significative de façon similaire ».

Toutefois, sauf exception (données personnelles particulières ou concernant des enfants, motifs de sécurité publique, d'intérêt public, etc.), la prise de décision individuelle basée sur un profilage est permise lorsqu'elle est :

- nécessaire à l'exécution ou la conclusion d'un contrat entre la personne concernée et le responsable du traitement,
- autorisée par la législation de l'UE ou celle d'un Etat membre auquel est soumis le responsable de traitement,
- fondée sur le consentement explicite de la personne concernée.

Fiche n°9 • Le profilage

ERREURS A EVITER	RECOMMANDATIONS
Collecter et agréger un large volume de données concernant un individu à des fins de profilage.	**Respect du principe de proportionnalité et de minimisation :** Il importe de ne collecter que les données strictement nécessaires à la finalité envisagée. De plus, les données sensibles devraient être exclues sauf dérogation prévue par le RGPD. **Analyse d'impact :** Plus le volume de données sera important, plus le risque que le traitement porte atteinte à la vie privée des individus sera élevé et nécessitera au préalable de conduire une analyse d'impact.
Procéder à un profilage à l'insu des individus (à partir d'une source de données publiques ou non).	**Information des personnes concernées :** Fournir une information claire, pertinente et séparée de toute autre information (concernant l'existence du profilage, ses sources, ainsi que les catégories de données utilisées dans le profil et le droit de s'y opposer) aux personnes concernées et s'assurer de recueillir leur consentement ou de justifier de la légalité du traitement. L'information doit être simple mais compréhensible et utile, sans avoir besoin d'aller dans le détail du fonctionnement de l'algorithme.
Prendre systématiquement des décisions individuelles automatisées sur la base du profilage	**Analyser l'impact de la décision individuelle :** Déterminer si les décisions individuelles sont susceptibles de produire des effets juridiques à l'encontre des personnes concernées ou de les affecter de manière significative. Si oui, effectuer des vérifications humaines et manuelles complémentaires.

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

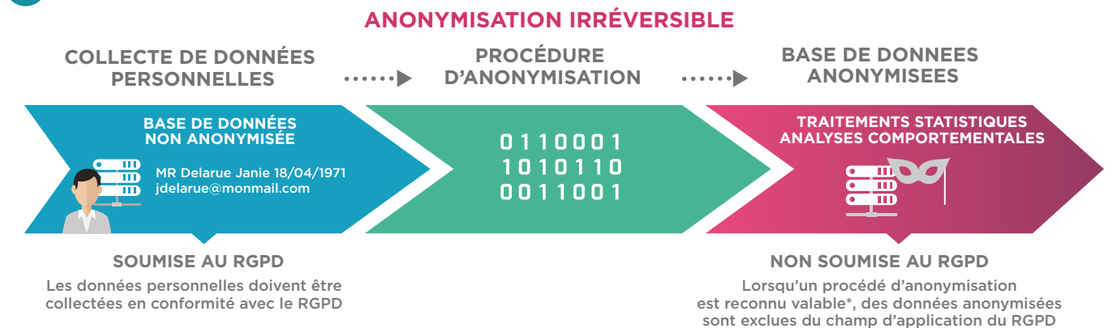
FICHE N°
10

L'ANONYMISATION

1. Définition de l'anonymisation

L'anonymisation consiste en une modification des données personnelles collectées en vue de les rendre anonymes afin d'empêcher, de façon irréversible, qu'une personne soit identifiée ou identifiable. Les données anonymisées sont ainsi des données qui ne permettent pas ou ne permettent plus d'identifier, directement ou indirectement notamment par un procédé d'individualisation, de corrélation ou d'inférence, une personne physique.

2. Intérêts de l'anonymisation

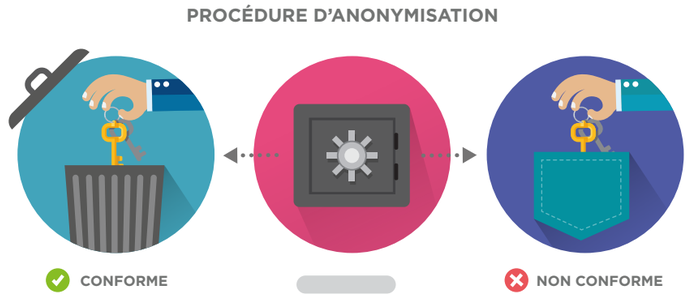


* Le RGPD ne précise pas quelles sont les techniques reconnues comme valables, mais le G29 a apporté un éclairage sur les principes techniques envisageables (randomisation et généralisation) et leur mise en œuvre.

Fiche n°10 • L'anonymisation

3. Démarches à entreprendre

S'assurer de l'impossibilité de ré-identification des individus concernés.
Il est recommandé (bien que cela ne soit pas obligatoire) de recueillir l'avis préalable de la CNIL.



LA PROCÉDURE POUR ÊTRE VALIDE DOIT ÊTRE IRRÉVERSIBLE.

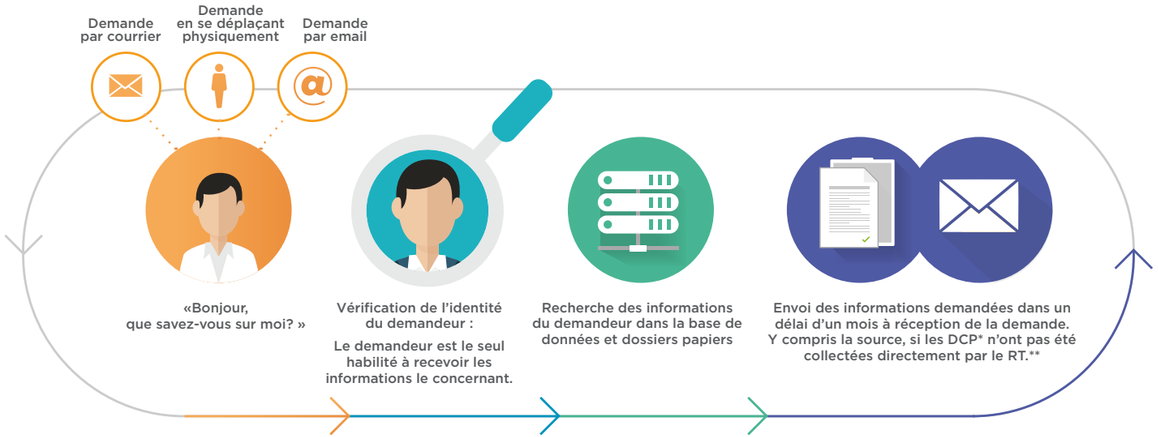
Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

FICHE N°
11

LE DROIT D'ACCÈS

1. Qu'est-ce qu'un droit d'accès ?

Toute personne a le droit de demander à un responsable de traitement ou à un sous-traitant les informations personnelles dont il dispose le concernant.



*DCP : donnée à caractère personnel - ** RT : Responsable de traitement

2. Qui doit répondre au droit d'accès ?

S'il y a un sous-traitant, le contrat entre les deux parties (RT* et ST*) doit prévoir le rôle de chacun :

- Qui répond à la personne concernée ?
- Dans quel délai ?
- Sous quel format ?

2 exemples de clauses proposées par la CNIL sur les contrats :

Modèles de clauses de la CNIL

Option A

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] (indiquer un contact au sein du responsable de traitement).

Option B

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

1. https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses : Ces clauses n'ont pas été validées à ce jour par la Commission Européenne.

2. Les clauses contractuelles types de la commission européenne en cas de transfert hors UE prévoient également des stipulations particulières.

*RT : Responsable de traitement - **ST : Sous-traitant

Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org

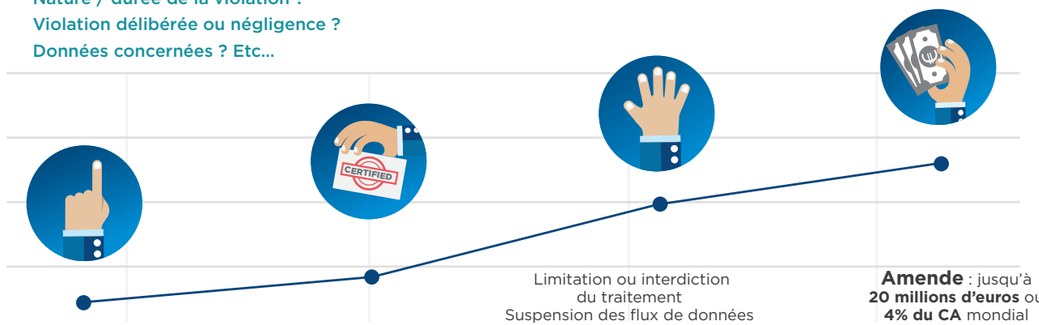
FICHE N°
12

LES SANCTIONS

1. Proportionnalité des sanctions CNIL

Choix de la sanction et montant de l'amende proportionnés à la gravité du manquement :

Nature / durée de la violation ?
Violation délibérée ou négligence ?
Données concernées ? Etc...



Rappel à l'ordre, mise en demeure

Retrait d'une certification*

Limitation ou interdiction du traitement
Suspension des flux de données vers un destinataire hors UE

Amende : jusqu'à **20 millions d'euros** ou **4% du CA** mondial (montant le plus élevé retenu)

Amende Administrative

* le RGPD encourage la mise en place de mécanismes de certification et labels en matière de données personnelles. Une société « certifiée RGPD » pourra se voir retirer sa certification en cas de manquement.

Fiche n°12 • Les sanctions

2. Comment contester une décision de la CNIL ?

Etape 1

Sanction CNIL

Etape 2

Peut faire l'objet d'un recours de la société / personne devant le juge (Conseil d'État)

Etape 3

Décision du Conseil d'État
- La responsabilité de la société / personne
- La proportionnalité
- La sanction

Fiche n°12 • Les sanctions

3. Autres sanctions :

**A côté de ces sanctions administratives infligées par la CNIL,
une société qui a manqué à ses obligations s'expose également à :**

- une action en dommages-intérêts des éventuelles victimes devant les juridictions civiles,
- des sanctions pénales (5 ans d'emprisonnement et 300.000 euros d'amende, ou jusqu'à 1.5 millions d'euros d'amende pour les personnes morales),
- le cas échéant, d'autres sanctions qui seront déterminées lors de la révision de la loi informatique et libertés.

4. Etre conforme en mai 2018 ? Oui, mais...

« Il ne faut pas voir le RGPD comme un couperet en 2018 »

« Il faut déconstruire cette idée qu'il y aura un coup de tonnerre en mai 2018 et que, comme des petits soldats, il faut que les entreprises soient prêtes à 100 %. »

Isabelle Falque-Pierrotin,
présidente de la CNIL

*https://www.contexte.com/article/numerique/rgpd-cnil-falque-pierrotin_71510.html

**Pour en savoir plus, lisez l'intégralité de la fiche.
Nous contacter : contact@cpa-france.org**

GLOSSAIRE

Accountability : L'Accountability désigne l'obligation pour le RT et le ST de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données

Anonymisation : consiste dans le résultat du traitement de données à caractère personnel dans le but d'empêcher irréversiblement l'identification de la personne concernée. On distingue l'anonymisation irréversible et l'anonymisation réversible, dénommée pseudonymisation.

Anonymisation irréversible : consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement et indirectement identifiantes sont supprimées rendant impossible toute ré-identification des personnes.

Anonymisation réversible : consiste en une technique qui permet de remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. Cette technique permet la levée de l'anonymat ou l'étude de corrélations en cas de besoin.

Archivage : il existe 3 types d'archives : la base active (autrement appelée « archives courantes »), les archives intermédiaires (accès restreint, étape intermédiaire avant suppression), les archives définitives (données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction).

Collecter : consiste à récupérer des données à caractère personnel par tout moyen (en ligne ou via un site web, par téléphone, dans un carnet, auprès de tiers, coupons, etc.).

DCP (Donnée à caractère personnel) : toute information identifiant directement ou indirectement une personne physique (ex. nom, n° d'immatriculation, n° de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale, n° de compte bancaire, NIR, etc.).

Donnée sensible : information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes concernées.

Droit d'accès direct : toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'opposition : toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification : toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Finalité d'un traitement : objectif principal d'une application informatique ou d'un fichier contenant des données à caractère personnel. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, abonnements, newsletters, etc.

G29 : groupe composé des autorités de protection des données à caractère personnel des Etats Membres de l'Union Européenne, de représentants d'institutions et organismes de l'Union Européenne ainsi que d'un représentant de la Commission Européenne institué par l'article 29 de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Incident : demande formulée par une personne souhaitant exercer son droit d'accès et de rectification, voire d'opposition, de suppression, de limitation des données ou de portabilité des données.

Interconnexion : la mise en relation automatisée d'informations provenant de fichiers ou de traitements qui étaient au préalable distincts.

Minimisation : seules les données strictement nécessaires à la réalisation des finalités peuvent être collectées par le responsable de traitement : c'est le principe de minimisation conformément à l'article 5 du Règlement 2016/679.

RT (Responsable du traitement) : toute personne physique ou morale qui détermine les finalités et les moyens de toute opération (collecte, enregistrement, modification, suppression, etc.), appliquée à des données à caractère personnel.

ST (Sous-Traitant) (ou prestataire) : toute personne traitant des données à caractère personnel pour le compte du responsable du traitement.

Traitement automatisé de données : toute opération ou de tout ensemble d'opérations, réalisés par des moyens automatiques, qui portent sur les données, réalisées par un logiciel spécialement développé à cette fin, résultant de l'utilisation d'un outil informatique usuel (par exemple, une feuille de tableur ou un serveur informatique) ou du seul fonctionnement d'un système d'information (échanges de données sur un réseau).

Traitement de données : collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation d'un fichier contenant des données à caractère personnel. Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Transfert de données : toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers ou toutes données dont un tiers situé hors de France peut avoir accès.

**«Et maintenant,
vous sentez-vous prêts ?»**

Pour en savoir plus,
retrouvez toutes nos fiches détaillées.

Contactez-nous

COLLECTIF
PERFORMANCE
& ACQUISITION

Contacts :
Collectif de la Performance & de l'Acquisition
8 rue Saint Fiacre
75002 Paris - France

T. (33) 01 77 45 46 23
E. contact@cpa-france.org
www.cpa-france.org
Twitter : @CPA_Performance

Noella Boullay : Déléguée Générale - nboullay@cpa-france.org
Marion Vittadello : Chargée de Communication - mvittadello@cpa-france.org

AVEC NOS REMERCIEMENTS POUR LA PARTICIPATION À LA RELECTURE ET À LA RÉALISATION DES FICHES :

MEMBRES DU COLLÈGE JURIDIQUE :

AWIN	Daniel LOURENCO Margarita ZLATKOVA	elixis	Augustin VATUS	PRISMA MEDIA	Yoann DENEE Fatima KHODRI
BEYABLE	Julien DUGARET	Gamned!	Damien MORA	PRM FACTORY	Oualid BARBOUCHI
brm AVOCATS	Caroline BELOTTI	HARLAY	Fabrice PERBOST	Tagada media	Adams MIMOUNI
CALOA	Stéphane LANDRY	KWANKO	Bruno DE LONGUEIL	WebRivage	Julien IMBERT
COMPANEO	Denis RIOLS	MARCEAU AVOCATS	Yves SEXER Marion LECARDONNEL	welcoming	Anne DUMON
EASY VOYAGE	Hervé SEVESTRE	Perspectives AVOCATS	Jean-Jacques BENATTAR Grégory MARGOLINE		

À propos du CPA :

Créé en 2008, le CPA (Collectif de la Performance et de l'Acquisition) est le syndicat professionnel des acteurs du marketing digital à la performance, secteur d'activité constituant le socle de toute stratégie d'acquisition digitale.

Le CPA représente des Editeurs et Prestataires experts, offrant des solutions indépendantes et sur mesure aux décideurs du marketing digital (annonceurs et e-marchands) afin de soutenir leur développement.

Par son action (Livres blancs, Chartes de qualité, Recommandations, Evènements & Networking), le CPA répond à quatre objectifs principaux :

- Réguler un marché foisonnant et en mutation permanente,
- Informer sur les meilleures pratiques de l'acquisition digitale,
- Assurer leur mise en oeuvre dans l'application du cadre légal,
- Représenter les droits et intérêts de ses membres.

Face à la multiplication des modèles d'acquisition et aux parcours utilisateurs toujours plus complexes, les membres du CPA s'engagent à mettre leur expertise, leur compréhension du secteur et leur esprit d'innovation au service de leurs clients. Le CPA fédère les principaux acteurs du marché du marketing digital à la performance qui représente 10 000 emplois et un chiffre d'affaires de 600 millions d'euros.

Conseil d'Administration du CPA

AWIN · CALOGA · COMMANDERS ACT · COMPANEO · DIGITAL KEYS · effinity · EULERIAN · HARLAY · KWANKO · marketSHOT · nano INTERACTIVE · PM PRISMA MEDIA

ADBACK · AdStead · ADVERLINE · AFILIZA · Marcel · antevenio · AntVoice · appvizer · arkeero · BEYABLE · BONS BONS · brm · CAR DATA · CFC · Cup Of Media · DARWIN · devis · DevisProx · EASY VOYAGE · EFFINET · elixis · esv digital · Graphinium · GROUPON · IGNITION ONE · INFOPRO · kelbroma · Lagardère · Lead'in · leadvalue · MADE IN FUTURA · makazi · mapp · MARCEAU AVOCATS · MEDIAMOOV · mediarithmics · Oath · coreka · Perspectives · PRM FACTORY · Quantcast · quantum · Rakuten Marketing · reduc.fr · REMAILME · RetailMeNot · SQUADATA · Studio's Mercurya · Tagada · TARGET2SELL · TimeOne · The Reach Group · uzer · WannaSpeak · WebRivage · welcoming · WIZALY