Le RGPD

TON GUIDE PRATIQUE EN TOUTE SIMPLICITÉ

WWW.CAPTURE-COMMUNICATION.FR

Sommaire

Introduction

Il y a encore quelques années, le web se limitait à nous délivrer les informations que nous recherchions. Désormais, ce sont nos comportements, associés ou non à des objets, qui permettent de fournir des services toujours plus gourmands en données personnelles. **Chaque individu est devenu un générateur de données, parfois même, sans le savoir clairement.**

En 2013, les révélations d'Edward Snowden font l'effet d'une bombe, le monde entier découvre que **les données personnelles collectées par les géants d'Internet sont utilisées par les services de renseignements américains.** Le monde entier est sur écoute.

C'est dans ce contexte qu'est né en 2016 le Règlement Général sur la Protection des Données, plus connu sous son acronyme, le **RGPD** ou GDPR en anglais. Ce règlement est **applicable depuis le 25 mai 2018.**

Son objectif premier est de proposer un cadre protecteur pour les données des personnes situées sur le territoire de l'Union Européenne. Il s'inscrit dans la continuité de la Loi Française Informatique et Libertés de 1978 et renforce le contrôle que les citoyens peuvent avoir sur l'utilisation de leurs données.

1- Qu'est-ce que le RGPD ?

Le RGPD (Règlement Général sur la Protection des Données ou GDPR en anglais) est là pour renforcer les actions mises en place depuis **la loi Informatique et Liberté de 1978**. Le but est d'augmenter la protection, la traçabilité et le respect des données des utilisateurs d'Internet, donc les vôtres.

Avec le RGPD, de nombreuses formalités issues de la loi de 1978 et de 28 législations vont disparaître pour laisser la place à une nouvelle manière de **collecter, stocker, utiliser et sécuriser les données personnelles**, plus maîtrisée, plus pérenne et plus logique. Il est important de savoir que le **RGPD** s'applique au traitement de données qu'il soit informatisé ou en version papier. Cette réglementation a été votée au **Parlement Européen en 2016** et entrera en vigueur le **25 mai 2018** au niveau mondial après quatre ans de négociations.

À l'heure actuelle, nos données sont partout et, bien utilisées, elles nous permettent de recevoir les informations qui nous intéressent, d'améliorer nos produits et services, de connaître et comprendre notre cible...
Malheureusement, il arrive que celles-ci soient **mal utilisées, revendues, prises à notre insu pour nous proposer des contenus abusifs.** C'est là que le **RGPD** entre en jeu afin de protéger les utilisateurs et leur rendre les droits, obligeant à plus de transparence et de respect entre les entreprises et les utilisateurs. Le but du RGPD est également d'unifier la réglementation au niveau européen avec un cadre juridique unique.

Les points fondamentaux à comprendre pour respecter cette nouvelle réglementation sont :

01	02	03	04	05	06
Ne collectez que les données vraiment nécessaires	Soyez transparent	Pensez aux droits des personnes	Gardez la maîtrise de vos données	Identifiez les risques	Sécurisez vos données

Qu'est-ce que les données ?

Les données personnelles sont **les informations qui permettent d'identifier, directement ou indirectement, une personne**, telles que ses nom, prénom, photo, date de naissance, statut matrimonial, adresse postale, e-mail, adresse IP d'ordinateur, n° de téléphone et bien d'autres.

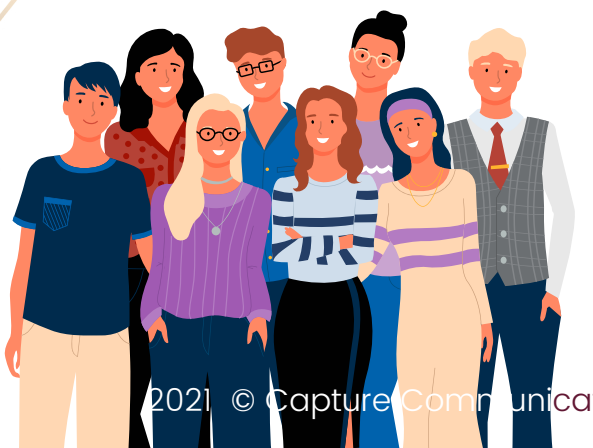
Avec l'utilisation actuelle d'Internet, ce genre d'information sur nous circule partout. Très souvent, ces données sont collectées, puis exploitées commercialement notamment dans le cadre de campagnes publicitaires.

Il est important de distinguer le type de données personnelles. Il existe aussi les données dites « **sensibles** » qui doivent être traitées différemment (informations concernant la **santé, l'origine raciale ou ethnique, les opinions politiques, religieuses, l'appartenance syndicale, etc...**).

Qui est concerné ?

C'est là qu'il est important de se pencher sur la question, car **pratiquement tout le monde est concerné.** La réglementation s'applique à tout organisme public ou privé qui traite des données de personnes sur informatique (client, prospects, utilisateurs, fournisseurs…) installé dans l'UE et aux organismes internationaux amenés à traiter les données personnelles de personnes de l'UE. Le principe d'engagement responsable des acteurs (accountability) signifie que chaque acteur doit connaître et appliquer la réglementation. Le responsable du traitement doit pouvoir démontrer sa conformité.

> **Attention, les sanctions prévues si vous n'êtes pas en règle sont très élevées pouvant atteindre 10 à 20 millions d'euros ou 2 à 4% du chiffre d'affaires annuel de l'entreprise.**



2- Les 8 règles d'or

Le RGPD encadre la collecte, l'utilisation et la conservation des données personnelles par **8 règles d'or auxquelles tout organisme privé ou public doit se conformer.**

1- Licéité du traitement
Un traitement ne peut être mis en œuvre que s'il est fondé sur une des 6 conditions de licéité

2- Finalité du traitement
Les données personnelles collectées ne peuvent être traitées que pour une finalité définie précisément et légitime

3- Minimisation des données
Seules les données strictement nécessaires pour atteindre la finalité peuvent être collectées et traitées

4- Protection particulière des données sensibles
Les données sensibles ne peuvent être collectées et traitées que dans certaines conditions

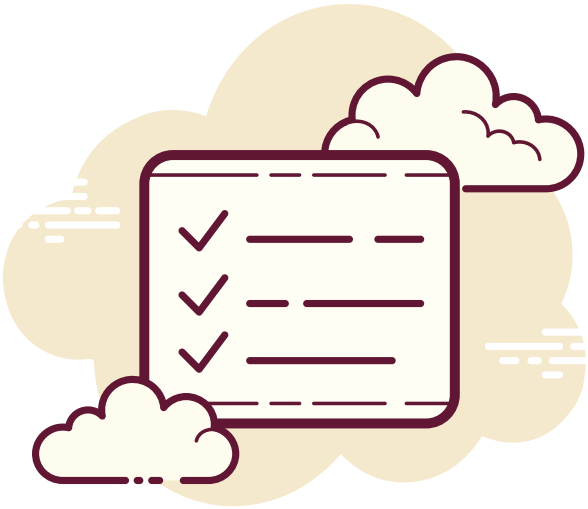
5- Conservation limitée des données
Les données doivent être archivées, supprimées ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte

6- Obligation de sécurité
Au regard des risques, des mesures doivent être mises en œuvre pour s'assurer de la sécurité des données traitées

7- Transparence
Les personnes doivent être informées de l'utilisation des données les concernant et de la manière d'exercer leurs droits

8- Droit des personnes
Les personnes bénéficient de nombreux droits qui leur permettent de garder la maîtrise de leurs données

Ces règles constituent à la fois un gage de sécurité juridique pour les responsables de traitements et un facteur de transparence et de confiance à l'égard des personnes concernées, à savoir les usagers, les clients, les consommateurs, les salariés, les agents et les administrés.



Les informations que le responsable du traitement doit particulièrement mettre en avant sont :

- **L'identité** du responsable du traitement
- Les **finalités** du traitement
- Les **catégories** de données collectées
- L'existence d'un **droit de retrait du consentement**
- Selon les cas : le fait que les données collectées seront utilisées dans **le cadre de décisions individuelles automatisées** ou qu'elles feront l'objet d'un **transfert hors UE**

3- Les risques liés à l'utilisation des données personnelles

95% des possesseurs de smartphones peuvent être ré-identifiés par le croisement d'au moins quatre de leurs positions géographiques, telles que celles contenues dans les métadonnées des photos prises sur mobile.

En se basant sur deux localisations, comme le trajet récurrent domicile-travail, 50% des gens seraient identifiables

***Source** : Arvind Narayanan citant l'étude "Unique in the Crowd : the privacy bounds of human mobility", Yves-Alexandre de Montjoye*

La profusion des données personnelles

Leur granularité, leur exposition et accessibilité, combinées à l'essor sans précédent des puissances de calcul et techniques de recoupement algorithmiques, ainsi qu'à la multiplication des cyberattaques, **représentent un réel risque pour nos droits et libertés.**

Ainsi, par exemple, nos habitudes de vie peuvent facilement être déduites grâce à l'historique de nos localisations enregistrées par notre smartphone.

Une série de données spatio-temporelles de qualité permet de déterminer nos lieux d'habitation et de travail, notre identité et nos centres d'intérêts.

Certaines données comme l'état de santé d'une personne, sa religion ou ses opinions politiques sont confidentielles et doivent le rester.

Dès 2001, **Latanya Sweeney**, alors doctorante au sein du MIT, **prouve que garantir la confidentialité de telles données n'est pas chose aisée.**

En croisant une liste électorale avec une base de données médicales pseudonymisée, c'est à dire purgée de tous ses éléments directement identifiants, mais contenant des codes postaux, dates de naissance et sexes, **elle parvint à ré-identifier 90% des individus et à prendre connaissance des données médicales du Gouverneur de l'Etat du Massachusetts de l'époque.**

En cas de faille de sécurité, vous êtes dans l'obligation d'avertir la CNIL dans les 72H si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la CNIL.

4- Cas pratique, votre site internet

Vérifier & mettre en conformité votre site internet

Sur votre site internet, **vous collectez forcément des données.**

Le simple fait **d'analyser vos visites avec Google Analytics** fait que vous collectez des données. Vous avez un formulaire de contact ? Un blog ? Une newsletter ? **Toutes ces fonctionnalités récoltent les données de vos utilisateurs.**

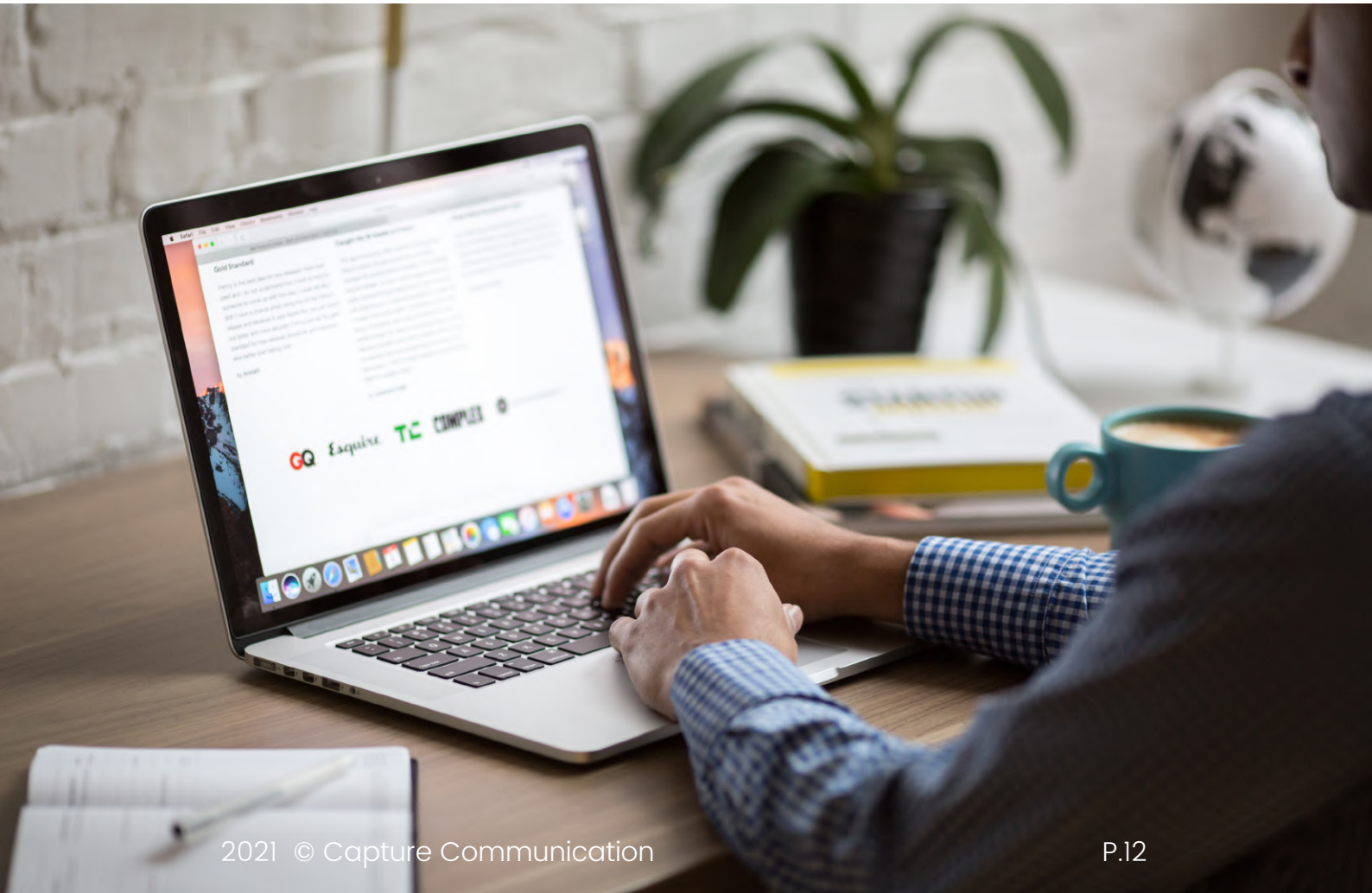
Quelques points essentiels à vérifier :

- Votre **site internet doit être en HTTPS**
- Il doit être le plus **sécurisé** possible et vous devez **limiter le nombre de personnes** ayant accès à votre backoffice (tableau de bord)
- Votre **site est bien à jour** et vous limitez le nombre de plugins en place
- Votre page de **mentions légales** est à jour ainsi que votre page de **politique de confidentialité**
- Et en bonus des **CGU** (Conditions Générales d'Utilisation), pas obligatoire, mais fortement recommandé

> Ces 3 pages doivent être accessibles sur chaque page et la **politique de confidentialité sur chaque formulaire**, en expliquant clairement quelles données vous récoltez, pourquoi, comment, dans quel but et pour combien de temps (et oui, nous n'avons plus le droit de garder des informations personnelles indéfiniment).
>
> Il est également important d'expliquer comment vous protégez les données de votre communauté et comment l'utilisateur peut y **accéder, les modifier, voir les supprimer**. Votre utilisateur a désormais le **droit à l'effacement, à la limitation du traitement et à la portabilité des données**, comme nous le verrons plus tard dans ce guide.

- Sur chacun de vos **formulaires** (contact, commentaire, newsletter, ...) votre utilisateur doit cocher une petite **case de consentement** (non pré-cochée) avec un lien vers votre **politique de confidentialité**

- Votre **bandeau d'acceptation des cookies** doit permettre à votre utilisateur d'**accepter, refuser ou choisir les cookies** utilisés sur votre site. En plus, il doit pouvoir voir exactement les cookies mis en place sur votre site et votre politique de confidentialité. Enfin, il doit pouvoir revenir sur ses choix à tout moment.



5- Responsable de traitement et sous-traitant

Un traitement de données peut être mis en œuvre par un organisme soit pour son propre compte, soit pour le compte et sur instruction d'un autre organisme.

Cette question joue un rôle central dans le partage des responsabilités entre les acteurs et impacte significativement leurs obligations respectives.

Un organisme peut donc être :
- Responsable de traitement (RT) s'il détermine le "pourquoi" et le "comment" du traitement des données, c'est à dire sa finalité et ses moyens (condition de mise en œuvre, notamment sur le plan technique, matériel et organisationnel)

OU

- Sous-traitant (ST) s'il traite des données personnelles pour le compte et sur instruction d'un autre organisme

Responsable de traitement :
De façon générale, le responsable de traitement, qui doit être porté à la connaissance des personnes concernées, **est considéré comme étant l'organisme pour lequel le traitement est mis en œuvre** : c'est donc sur lui que pèsera la responsabilité du respect des obligations.

En principe, ce sera au représentant légal de veiller à la bonne prise en compte par l'organisme des principes "Informatique et Libertés"

- **Pour le secteur privé** ; Président, directeur général, PDG, gérant, ...

- **Pour le secteur public** ; Ministre, maire, président de l'EPCI, du conseil départemental, ...

Sous-traitant :
Un organisme est sous-traitant lorsqu'il traite des données personnelles pour le compte et sur l'instruction d'un autre organisme ayant la qualité de responsable du traitement. Ces activités de sous-traitant peuvent concerner une tâche bien précise (envoi de courriers de prospection commerciale) ou être plus générales et étendues (gestion de l'ensemble d'un service d'un autre organisme comme la gestion de la paie).

6 - Le registre de traitement des données

Un registre des activités de traitement **doit être mis en place par tout responsable de traitement ou sous-traitant**. Outil essentiel dans les opérations de conformité, il permet de **recenser les traitements**, et par la même occasion, de disposer d'une vue d'ensemble sur ce qui est fait des données personnelles dans les organisations.

Le registre permet de se poser les bonnes questions :

- À quoi sert précisément cette collecte de données ?
- Ai-je vraiment besoin de cette donnée en particulier dans le cadre de mon projet ?
- Est-il pertinent de conserver toutes les données aussi longtemps ?
- Les données sont-elles suffisamment protégées ?
- Etc.

Organismes concernés

L'obligation de tenir un registre des traitements concerne tous les organismes, publics comme privés, quelle que soit leur taille, dès lors qu'ils traitent des données personnelles.

Le registre doit être tenu par les responsables de traitement et les sous-traitants eux-mêmes.

Cette mission peut être confiée au délégué à la protection des données, même s'il est externalisé, ou à une autre personne en interne.

Forme et contenu

Le RGPD impose que le registre se présente sous forme écrite. Son format est libre et peut être constitué au format papier ou électronique.

Contenu

Le registre est un document de recensement et d'analyse, il doit refléter la réalité des traitements et permettre d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données
- les catégories de données traitées
- à quoi servent les données
- qui accède aux données et à qui elles sont communiquées
- combien de temps elles sont conservées
- comment elles sont sécurisées

La liste détaillée des éléments à intégrer au registre du responsable de traitement et du sous-traitant est disponible sur le site de la CNIL.

Le sous-traitant doit tenir un registre spécifique pour les activités de traitements réalisées pour le compte de ses clients (ex : hébergement de base de données, maintenance, etc.).

Le registre du responsable de traitement et celui du sous-traitant ne sont donc pas les mêmes.

Si l'organisme agit à la fois en tant que sous-traitant et responsable de traitement, il doit clairement distinguer les deux catégories d'activités.

Dérogation

Les entreprises de **moins de 250 salariés** bénéficient d'une dérogation. Elles sont autorisées à n'inscrire dans le registre que les traitements suivants :

- les **traitements récurrents** (ex: gestion de la paie, gestion des clients, des prospects et des fournisseurs, etc.)
- les traitements **susceptibles de comporter un risque** pour les droits et libertés des personnes (ex: systèmes de géolocalisation, de vidéosurveillance, etc.)
- les traitements qui portent sur des **données sensibles** (ex: données de santé, infractions, etc.).
-

Exemple : Un concessionnaire automobile décide de lancer une campagne de communication à l'occasion de l'ouverture d'un nouvel établissement.
Les traitements liés à cette campagne n'ont pas besoin d'être intégrés au registre puisqu'il s'agit d'un événement ponctuel dont le traitement ne représente aucun risque pour les personnes concernées.

En cas de doute sur l'application de cette dérogation, la CNIL recommande d'intégrer le traitement au registre.

Modèle de registre

Pour faciliter la tenue de ce registre, la CNIL propose sur son site internet un modèle de registre destiné à répondre aux besoins les plus courants en matière de traitement de données, en particulier pour les petites structures (TPE-PME, associations, petites collectivités, etc.).

Méthode

Pour mettre en place ce registre, la CNIL conseille de procéder en trois étapes :

Étape 1 : rassembler les informations disponibles

- identifier et rencontrer les responsables opérationnels des différents services susceptibles de traiter des données personnelles utiliser la liste des traitements déclarés à la CNIL.
- analyser le site internet (ou les applications)
- identifier les données collectées dans les formulaires en ligne
- Utiliser la listes des traitements déclarés à la CNIL
-

Étape 2 : élaborer la liste des traitements

- lister les différentes activités impliquant un traitement de données personnelles
- exploiter les informations collectées lors des entretiens avec les responsables opérationnels
- remplir une fiche de registre par activité.
-

Étape 3 : affiner

Sur la base de ce registre :

- identifier et analyser les risques qui peuvent peser sur les traitements de données mis en œuvre
- élaborer un plan d'action de mise en conformité RGPD

Suivi

Le registre doit être mis à jour régulièrement pour suivre les évolutions des activités et des traitements de données.
En pratique, toute modification apportée aux conditions de mise en œuvre d'un traitement doit être mentionnée dans le registre : nouvelle catégorie de données collectées, etc.

Communication

Le registre doit pouvoir être communiqué à la CNIL lorsqu'elle le demande. Elle l'utilise dans le cadre de sa mission de contrôle des traitements de données. Les organismes du secteur public sont tenus de transmettre le registre à toute personne qui en fait la demande, car il s'agit d'un document administratif, communicable à tous, au sens du code des relations entre le public et les administrations.

Le registre doit être communiqué après avoir retiré toutes les informations dont la divulgation pourrait en particulier porter atteinte aux secrets protégés par la loi, et notamment à la sécurité des systèmes d'information.

Les organismes privés (non chargés d'une mission de service public) ne sont pas tenus de communiquer le registre au public. Toutefois, s'ils l'estiment opportun, ils peuvent le communiquer aux personnes qui en font la demande.

Bonne pratique

Il peut être utile d'enrichir le registre avec des informations complémentaires afin qu'il devienne un véritable outil de pilotage de la conformité en rassemblant dans un même document les exigences du RGPD et toutes les informations relatives aux traitements qui sont mis en œuvre.

Exemples : historique des violations de données, les documents liés aux sous-traitants, etc. Cela permet d'identifier les actions à mener et de les prioriser.

En Bref

Le registre permet d'avoir une vue d'ensemble des traitements pour piloter la conformité. Les registres du sous-traitant et du responsable de traitement ne sont pas les mêmes : ils doivent être bien distincts et toujours être tenus régulièrement à jour.

7 - Droits des personnes sur leurs données

L'un des objectifs majeurs du RGPD est de renforcer les droits des personnes et de faciliter leur exercice. Aux droits d'accès, de rectification, d'effacement et d'opposition qui se voient renforcés viennent s'ajouter de nouveaux droits. Ces nouveaux droits sont le droit à la portabilité, le droit à la limitation du traitement et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé.

RGPD - Considérant 11

Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel [...]

RGPD - Considérant 7

Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant.

Le droit d'accès

L'exercice du droit d'accès permet aux personnes de savoir si des données les concernant sont traitées et d'en obtenir la communication dans un format compréhensible.

Le droit d'accès permet également de contrôler l'exactitude des données et, si nécessaire, de les faire rectifier ou effacer.

Lorsqu'une personne exerce son droit d'accès, le responsable de traitement doit lui fournir une copie des données la concernant ainsi que les informations suivantes :

- les finalités du traitement
- les catégories de données concernées
- la durée de conservation des données
- l'existence du droit de rectification, d'effacement, de limitation ou d'opposition au traitement des données
- l'origine des données quand elles n'ont pas été collectées auprès de la personne concernée
- l'existence éventuelle d'une prise de décision automatisée, y compris un profilage
- le droit d'introduire une réclamation auprès d'une autorité de contrôle
- les destinataires auxquels les données ont été ou seront communiquées, en particulier les destinataires
- qui sont établis dans des pays tiers.

Le droit de rectification

Le droit de rectification permet de corriger des données inexactes concernant la personne (âge ou adresse erronés) ou de compléter des données (adresse sans le numéro de l'appartement) en lien avec la finalité du traitement.

Le droit d'opposition

Les personnes peuvent s'opposer au traitement de leurs données. Ce droit d'opposition peut être exercé à tout moment pour des raisons tenant à la situation particulière de la personne. Dans le cas de la prospection, la personne n'a pas besoin de fournir de motif pour exercer son droit d'opposition.

Le droit d'opposition n'est pas un droit à la suppression simple et définitive de toutes les données ou du compte qui est rattaché à une personne. Par exemple, seule une rupture de contrat permet la suppression d'un compte chez un opérateur mobile ou un site de e-commerce.

Si une demande d'opposition ne concerne pas la prospection, l'organisme pourra justifier son refus au motif que :

- il existe des motifs légitimes et impérieux à traiter les données ou que celles-ci sont nécessaires à la constatation, l'exercice ou la défense de droits en justice
- la personne a consenti (elle doit alors retirer son consentement)
- un contrat lie la personne avec l'organisme (la personne peut mettre fin au contrat)
- une obligation légale impose à l'organisme de traiter les données
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Le droit à l'effacement ("droit à l'oubli")

Les personnes peuvent demander à un organisme l'effacement des données personnelles les concernant.

Ce droit s'applique seulement dans l'une de ces six situations :

- les données ne sont plus nécessaires au regard des finalités pour lesquelles elles sont collectées ou traitées
- la personne retire son consentement au traitement de ses données
- la personne s'oppose au traitement et il n'existe pas de motif légitime impérieux
- le traitement est illicite (ex : le traitement s'effectue en violation d'une disposition du code de la santé publique)
- les données doivent être effacées pour respecter une obligation légale
- les données ont été collectées auprès de mineurs dans le cadre de l'offre de services de la société de l'information.

En revanche, le droit à l'effacement ne peut pas s'appliquer s'il va à l'encontre :

- de la liberté d'expression et d'information
- du respect d'une obligation légale
- d'un motif d'intérêt public dans le domaine de la santé publique
- des fins archivistiques dans l'intérêt public, des fins statistiques, de recherche scientifique ou historique
- de la constatation, de l'exercice ou de la défense de droits en justice.

Les nouveaux droits

Le droit à la portabilité

RGPD - Art 20

L'objectif du droit à la portabilité est de permettre aux personnes de gérer leurs données en les réutilisant par exemple pour un usage personnel. Il s'agit également de faciliter la libre circulation des données d'un prestataire à un autre afin de stimuler la concurrence entre responsables de traitement.
Ce droit permet à toute personne de récupérer les données personnelles qu'elle a fournies à un responsable de traitement. Ces données doivent être transmises à la personne qui les demande dans un format structuré, couramment utilisé et lisible par une machine.
Ce droit inclut aussi la possibilité de transmettre ces données à un nouveau responsable de traitement, en demandant au responsable initial de procéder au transfert, si cela est techniquement possible.
L'existence de ce nouveau droit implique que les responsables de traitement travaillent ensemble à l'élaboration de formats interopérables pour permettre l'exercice effectif de ce droit.

Ce droit est applicable seulement si les deux conditions cumulatives suivantes sont réunies :
- le traitement est fondé sur le consentement de la personne ou sur un contrat.
Sont donc exclus les traitements fondés sur l'intérêt public, l'intérêt légitime du responsable de traitement ou une obligation légale. Le droit à la portabilité ne peut donc pas s'appliquer à la vidéosurveillance, à la lutte contre la fraude ou au contrôle d'accès à des locaux
- le traitement est effectué à l'aide de procédés automatisés.

Les nouveaux droits

Le droit à la limitation du traitement

RGPD - Art 18

Le droit à la limitation vient compléter les cinq autres droits que nous venons de voir. Lorsqu'une personne souhaite rectifier des informations ou s'opposer à ce qu'elles soient traitées, l'organisme dispose d'un délai d'un mois pour traiter la demande. Pendant ce délai, cette personne peut faire valoir son droit à la limitation pour geler l'utilisation de ces données. Concrètement, l'organisme ne devra plus utiliser les données, mais devra les conserver. Inversement, il est possible de demander la limitation du traitement de certaines données lorsque l'organisme souhaite lui-même les effacer.

Le responsable de traitement doit informer la personne concernée qui a obtenu la limitation du traitement avant la levée d'une telle limitation.

La limitation entraîne **le gel temporaire du traitement des données**, sauf si :
- la personne **donne son consentement à une autre forme de traitement**
- le traitement de ces données **est nécessaire** à la constatation, l'exercice ou la défense de droits en justice, à la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

Les nouveaux droits

Le droit de ne pas faire l'objet d'une décision exclusivement fondée sur un traitement automatisé

RGPD - Art 22

Le profilage consiste à utiliser les données personnelles d'un individu en vue d'analyser et de prédire son comportement, comme par exemple déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc. Toute personne a le droit de ne pas faire l'objet d'une décision entièrement automatisée - souvent basée sur un profilage - qui a un effet juridique ou qui l'affecte sensiblement.

Un organisme peut néanmoins automatiser ce type de décision si l'une de ces conditions est remplie : - la personne concernée a donné son consentement explicite - la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne et l'organisme - la décision automatisée est autorisée par des dispositions légales spécifiques.

Dans tous les cas, la personne doit pouvoir :
- **être informée** qu'une décision entièrement automatisée a été prise à son encontre
- **demander à connaître** la logique et les critères employés pour prendre la décision
- **contester** la décision et **exprimer** son point de vue
- **demander l'intervention** d'un être humain qui puisse réexaminer la décision

Possibilité de ne pas donner suite à la demande de la personne concernée

Le responsable de traitement est tenu de faciliter l'exercice des droits et ne peut en aucun cas refuser de donner suite à une demande sans le justifier auprès de la personne concernée.

Le RGPD autorise ainsi les responsables de traitement à ne pas donner suite à une demande dans les cas suivants :

- S'agissant du droit d'opposition, lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée ou pour la constatation, l'exercice ou la défense des droits en justice.
- S'agissant des droits d'accès et à la portabilité, lorsque sa mise en œuvre porte atteinte aux droits ou libertés d'autrui (notamment secret des affaires, propriété intellectuelle, droit d'auteur protégeant un logiciel).
- S'ils peuvent démontrer qu'ils ne sont pas en mesure d'identifier la personne concernée.
- S'ils peuvent démontrer que les demandes d'une personne sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif (dans ce cas, le responsable pourra choisir de répondre en exigeant le paiement de frais raisonnables).

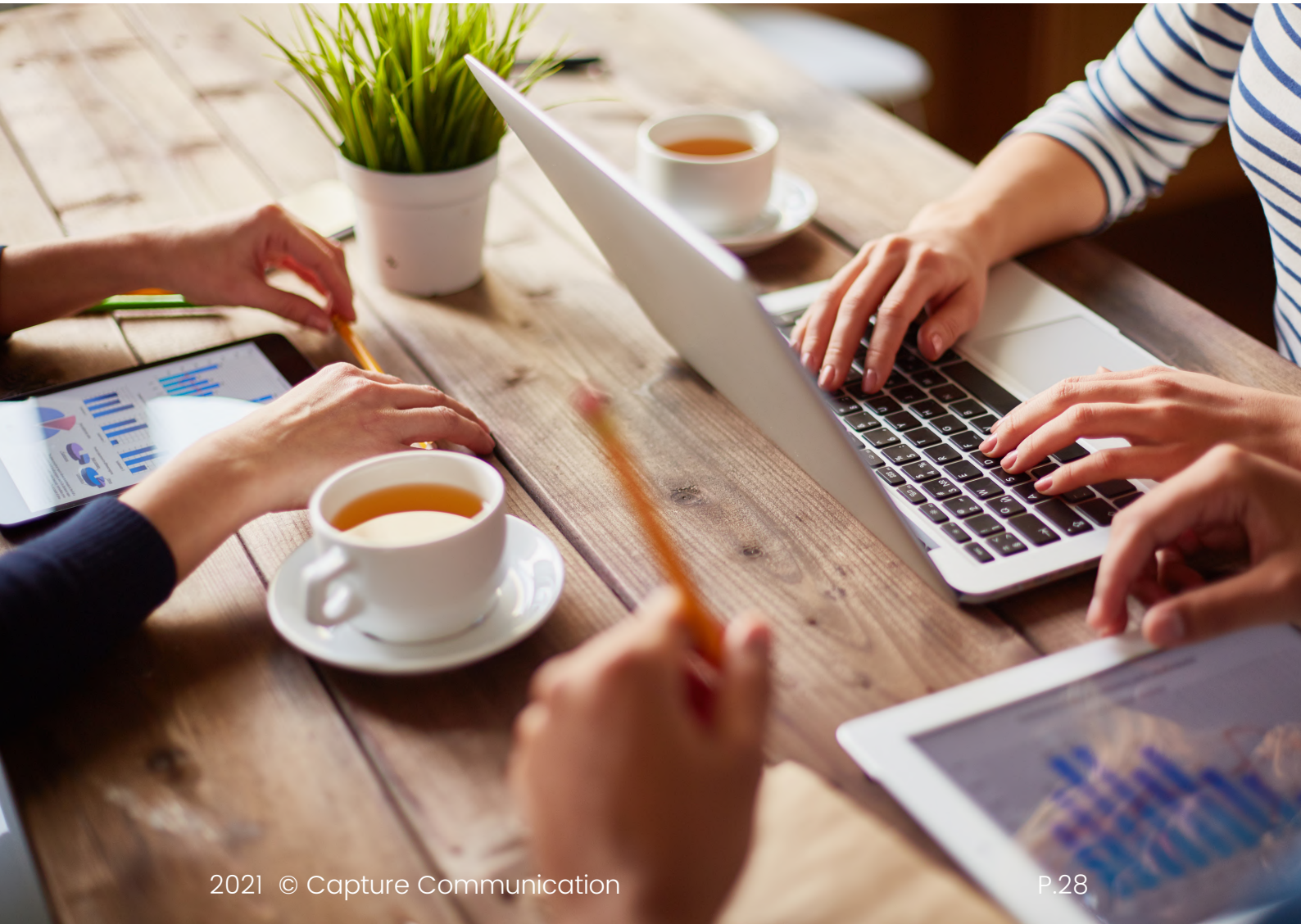
Dans chaque cas, le responsable du traitement doit informer la personne de cette décision sans tarder. Il dispose d'un mois à compter de la réception de la demande pour lui indiquer le motif de son inaction, ainsi que la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel.

Notification de l'exercice des droits

Lorsqu'une personne exerce son droit de rectification, d'effacement ou de limitation, le responsable de traitement doit en informer tous les organismes à qui il a transmis les données personnelles en question. Cette communication doit impérativement être effectuée à moins qu'elle ne se révèle impossible ou n'exige des efforts disproportionnés.

En Bref :

Les personnes concernées sont placées au cœur de la réglementation en matière de protection des données. Les droits dont elles bénéficient leur permettent de garder la main sur leurs données et de pouvoir réagir en cas d'atteinte à leurs droits, voire en cas de préjudice.



8 - Le délégué à la protection des données

Le mot d'ordre du RGPD est la responsabilisation des acteurs des traitements de données personnelles : ils doivent s'inscrire dans une démarche de prise en compte permanente et dynamique des principes protecteurs.
Les organismes doivent ainsi recourir de façon obligatoire ou volontaire :

- à différents instruments de conformité :

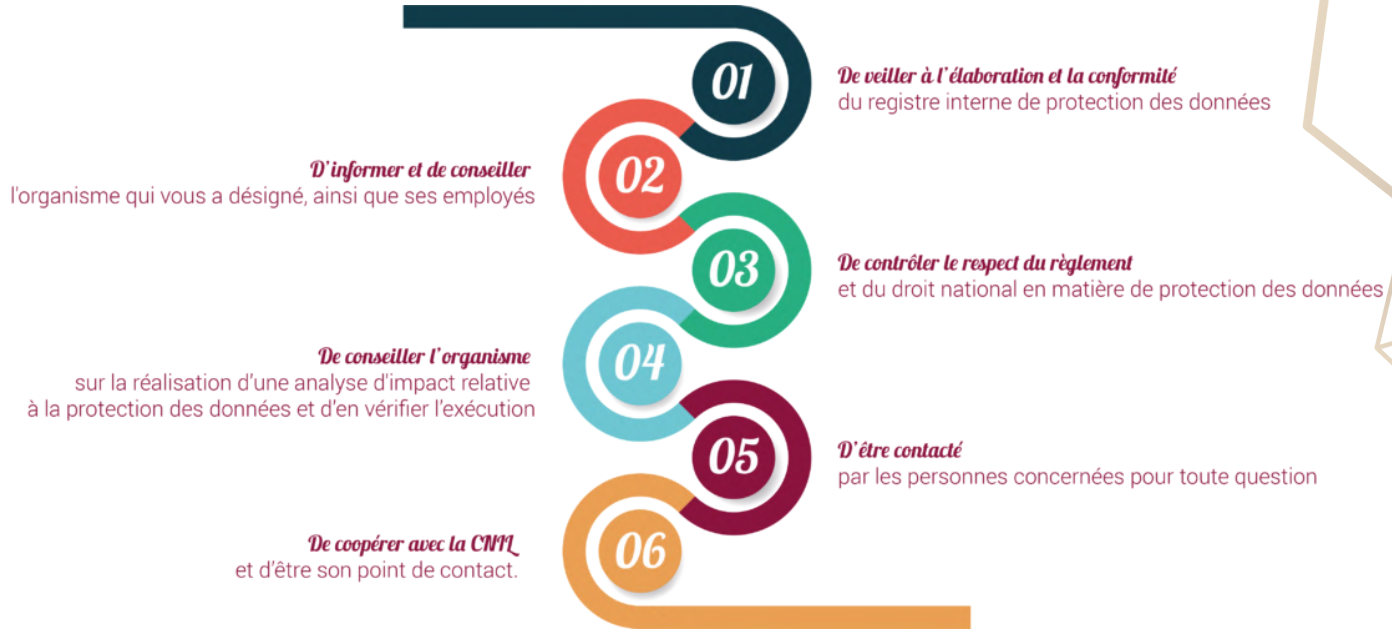
registre des activités de traitement, analyse d'impact sur la protection des données, etc.

- aux services d'un nouvel acteur :

le délégué à la protection des données (DPO).

Le délégué à la protection des données constitue un acteur clé du système de gouvernance des données personnelles à mettre en place. Par ses missions d'information, de conseil, de contrôle et d'interface, il va impulser, piloter, coordonner les actions de mise et de maintien en conformité de l'organisme.

Ces missions principales ? Les voici :



Conclusion

La mise en conformité RGPD est un gros chantier, mais c'est aussi une démarche essentielle pour toi et ton entreprise.

Aujourd'hui, il est indispensable d'être aux côtés de votre communauté de manière authentique, éthique et transparente. Cela passe donc aussi par le respect de leurs données et la confiance que vous donnez à votre audience. Et si besoin, n'hésitez pas à faire appel à un professionnel.

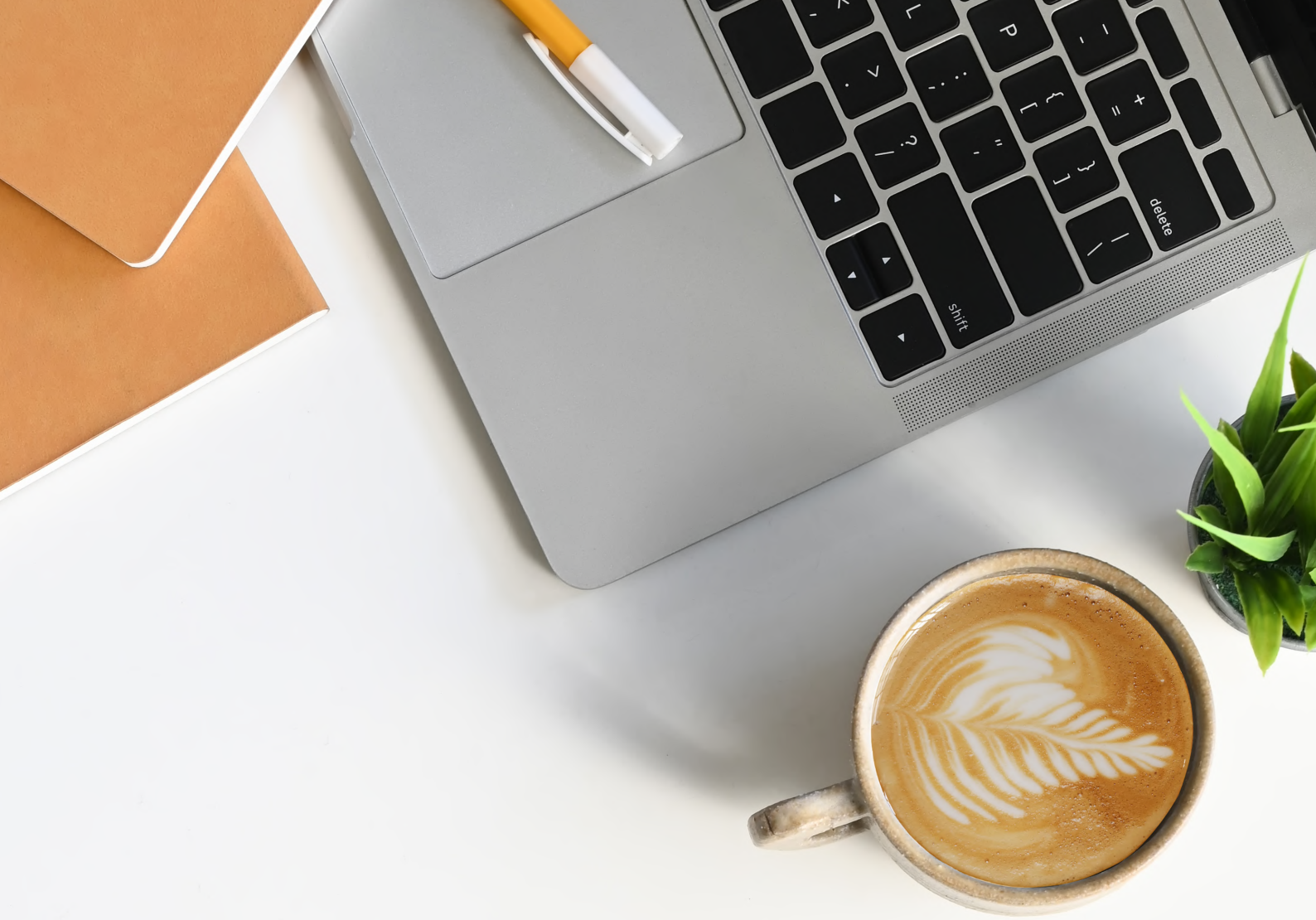
Vous souhaitez aller plus loin ?
N'hésitez pas à visiter le site de la CNIL qui est très complet ainsi que celui de BPI France. Plus précisément, vous pouvez lire cet article très complet de WEBRankInfo, l'article Nouvelles règles pour les cookies et autres traceurs de la CNIL et suivre la formation très complète de la CNIL : "L'atelier RGPD".

Vous pouvez aussi retrouver nos articles :
RGPD, vous êtes aussi concerné !
Nouveautés RGPD 2021, êtes-vous en conformité ?
Les 8 règles d'or du RGPD (article à venir)

"

Nous ne sommes ni avocates, ni spécialistes de la protection des données. Ce guide vise à vous permettre d'y voir plus clair et de comprendre l'importance de respecter cette réglementation.
Si nous pouvons vous aider & vous conseiller,
n'hésitez pas à nous contacter.

"



Capture

Agence de communication visuelle & digitale

Contactez-nous

06.72.41.02.30

contact@capture-communication.fr

www.capture-communication.fr