avanci

Agence Conseil Data & Marketing

LE GUIDE COMPLET

Comment être **compatible RGPD** ?

Solutions Data & CDP | Data intelligence | Stratégie & Activation CRM

Sommaire

Introduction ____ 3

1 RGPD : une réglementation pour quoi faire ? ____ 4

2 Les 5 points essentiels du RGPD ____ 9

3 Rôle et missions du DPO ____ 11

4 Sous-traitant et RGPD, qui est responsable ? ____ 16

5 Les 6 étapes liées à la mise en conformité ____ 19

Conclusion ____ 23

À propos d'Avanci ____ 25

À propos de MV Group ____ 26

Introduction

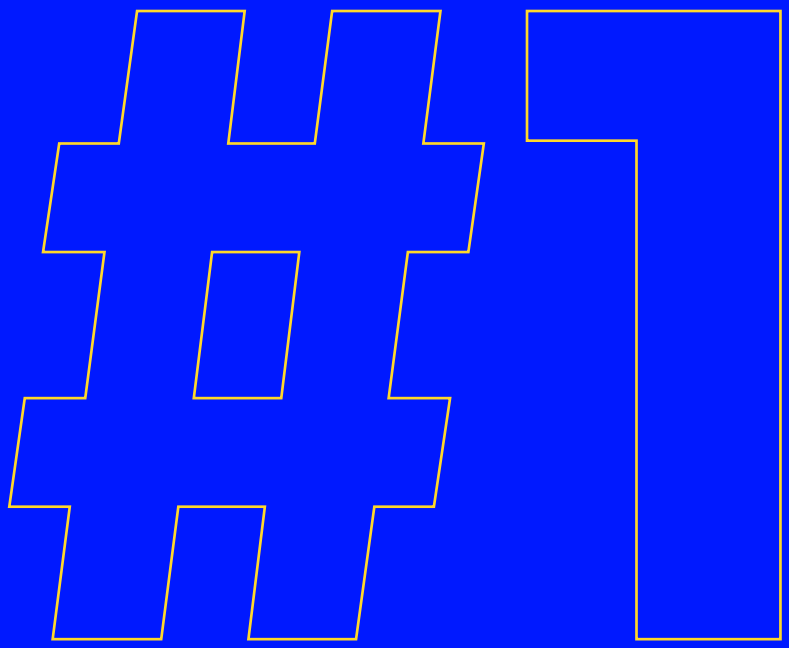
Depuis le 25 mai 2018, le Règlement Général sur la Protection des données, ou RGPD, est entré en vigueur dans les pays membres de l'Union européenne.

Ce texte, également connu sous le nom de General Data Protection Regulation, ou GDPR en anglais, a été adopté par le Parlement européen.

Il s'agit d'une réglementation concernant la protection, le stockage, le traitement et la diffusion des données personnelles des résidents européens qui impactera notamment les entreprises B2B et B2C.

Nous avons conçu ce guide, qui n'est pas un document juridique et n'a pas la prétention d'être exhaustif, afin de vous aider à prendre conscience des obligations et enjeux liés à ce règlement. Il vous guidera dans les principales étapes pour vous aider à mettre votre entreprise en conformité avec le RGPD.

Disclaimer : ce guide partage des informations à titre indicatif. Il ne saurait nullement engager la responsabilité de la société Avanci. Il vous appartient de vous renseigner auprès de professionnels du droit quant à vos obligations relatives à la protection des données à caractère personnel.



RGPD : une réglementation pour quoi faire ?

Le RGPD permet notamment de renforcer la protection des données personnelles des utilisateurs sur internet.

Jusqu'à présent, en France, ces éléments étaient régis par la Loi informatique et liberté. C'est à la suite de ce texte de loi que nous avons notamment vu apparaître les bandeaux suivants en bas des sites internet français.

Mais la mise en pratique de la protection des données restait malgré tout complexe à comprendre pour les utilisateurs. De plus, elle ne s'appliquait que sur le territoire français et n'était pas spécialement adaptée aux récentes innovations technologiques.

Le Parlement européen a donc établi le Règlement Général sur la Protection des Données qui a 3 objectifs :

- **Créer un cadre harmonisé pour la protection des données** en s'adaptant aux dernières évolutions technologiques (intelligence artificielle, big data, etc.) ;
- **Renforcer les droits des individus** quant à la diffusion, la gestion et le traitement de leurs données personnelles ;
- **Responsabiliser les entreprises** qui collectent et traitent ces données individuelles.

RGPD : quelques définitions pour mieux comprendre le règlement

Avant d'aller plus loin, il est important de revenir sur quelques définitions importantes pour comprendre les impacts du RGPD et les noms donnés aux différents acteurs du règlement.

Une donnée à caractère personnel

est constituée par toute information qui se rapporte à une personne physique identifiée ou identifiable. Il peut s'agir de son identité, ses coordonnées, ses données GPS… Mais aussi de ses habitudes de consommation, son adresse IP, son ID de cookie, ou encore un trombinoscope, un annuaire d'entreprise… Sont exclues les données réellement anonymisées (mais pas les données pseudonymisées).

Un traitement de données

est défini comme toute opération ou ensemble d'opérations réalisées manuellement ou à l'aide de procédés automatisés. Comme par exemple : la collecte, l'enregistrement, la structuration, la modification, l'extraction, la mise à disposition… Qu'il s'agisse d'un traitement informatique ou papier.

Un Data Privacy Officer (DPO), ou Délégué à la Protection des Données (DPD)

est la personne en charge de l'application et du respect de la RGPD pour une entreprise. Il peut être un salarié de cette dernière, travailler en tant que prestataire de service ou être employé d'un sous-traitant.

Le responsable de traitements des données

est l'entité (personne, entreprise ou organisme) qui détermine pourquoi et comment effectuer un traitement. Il peut donc s'agir par exemple d'une personne décidant de faire appel à un sous-traitant pour réaliser une prestation d'emailing ou encore la personne qui décide de faire effectuer cette tâche au sein de son entreprise.

Le sous-traitant

est une personne ou une entreprise qui effectue une prestation de services impliquant un traitement de données au nom d'une autre personne ou d'une autre entreprise responsable de traitement. Peuvent être qualifiées de sous-traitants les sociétés de services informatiques, les agences marketing et de communication, comme Avanci, ou encore les organismes publics et associations effectuant un service ou une prestation impliquant un traitement de données personnelles pour une autre entité. Les éditeurs de logiciels ne sont pas considérés comme des sous-traitants au sens du RGPD.

RGPD Qui, quoi, où, quand, comment ?

Qui est concerné par le RGPD ?

Toutes les entreprises et organismes qui collectent ou traitent les données personnelles de résidents européens ou qui sont établies sur le territoire de l'Union européenne relèvent du RGPD .

Ce règlement impacte donc les entreprises B2B et B2C qui utilisent des bases de données à des fins de marketing publicitaires et toutes celles qui collectent des données en vue de créer des profils marketing. C'est donc un grand changement pour les entreprises B2B !

Date limite de mise en conformité

Vous aviez jusqu'au **25 mai 2018** pour être au diapason. Désormais, vous risquez des sanctions en cas de non-respect allant du simple rappel à l'ordre à des amendes pouvant atteindre 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires de l'entreprise.

Que faut-il faire pour être conforme ?

Pour être conforme, votre entreprise devra être en mesure de renseigner précisément :

- Quels types de données sont collectées ?
- Pour quel usage ?
- Comment et où sont-elles stockées ?

Pour y arriver, les entreprises devront notamment nommer un Data Privacy Officer (DPO) ou, en français, un Délégué à la Protection des Données (DPD) et constituer un registre de données. Les obligations sont à la charge des organismes responsables de traitements (personne physique ou morale qui seule ou conjointement détermine les finalités et les moyens du traitement) mais aussi applicable aux entités qui traitent les données en qualité de sous-traitant, pour le compte d'un tiers.

Les 5 points essentiels du RGPD

On vient de le voir, l'objectif du RGPD est de renforcer la protection des données personnelles de tous les individus résidant dans l'Union européenne. Les entreprises qui traitent des données personnelles devront donc travailler dans un cadre précis où la protection des données se fait « par défaut ».

En voici, les 5 grands principes :

1

La base légale du traitement

Selon le type de traitement de données envisagé, il convient de définir la base légale adaptée parmi: le consentement, l'exécution d'un contrat, l'intérêt légitime, une obligation légale, la sauvegarde des intérêts vitaux de la personne, une mission d'intérêt public.

2

L'exercice des droits sur les données doit être facilité

Un individu doit être en mesure de pouvoir exercer des droits sur ses données, et ainsi notamment: y accéder, les corriger, les supprimer, ou encore s'opposer au traitement. De plus, pour tout service en ligne, un individu doit être en mesure de télécharger l'intégralité de ses données personnelles pour les transférer chez un autre prestataire.

3

Une durée de conservation limitée

Il n'est plus possible de conserver les données des personnes indéfiniment. Le responsable de traitement doit définir pour chaque traitement une durée de conservation adaptée à la finalité du fichier et au type d'information concernée.

4

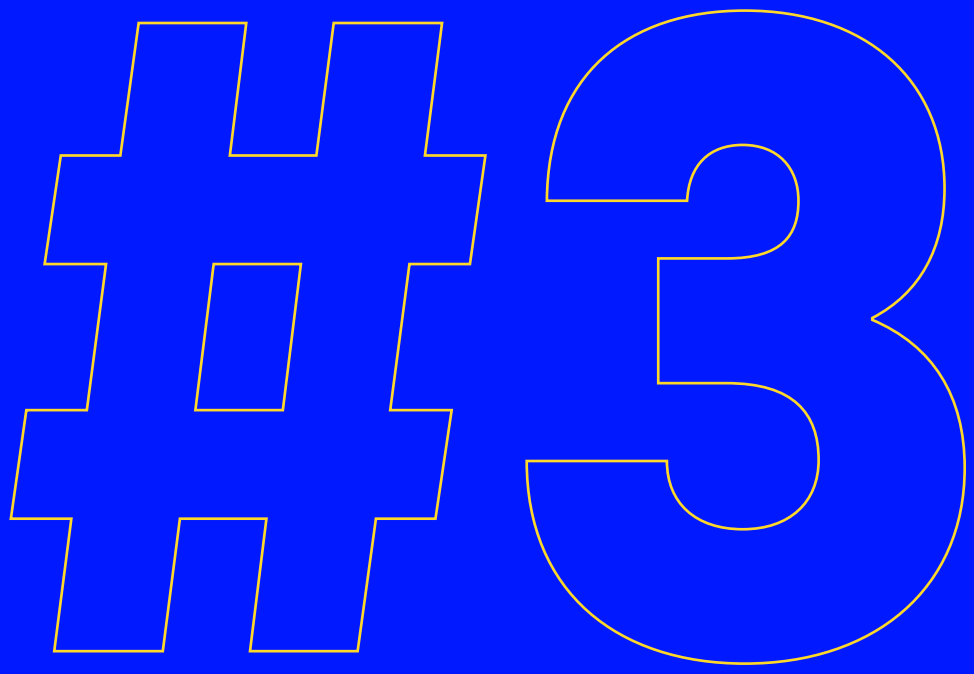
La sécurisation et la confidentialité

Le responsable de traitement est le garant de la sécurité des données à caractère personnel qu'il détient. Cette sécurisation passe par des méthodes techniques, méthodologiques et juridiques.

5

L'obligation d'information en cas de fuite de données

Le délai d'information est désormais très court. Le DPO doit en informer la Cnil de son pays sous 72h, sous peine de sanction.



Rôle et missions du DPO

La nomination d'un DPO est rendue obligatoire par le RGPD dans certaines conditions. Jusqu'à présent, il s'agissait du Correspondant Informatique et Liberté (Cil). Avec le nouveau règlement, son rôle évolue.

Il a désormais 4 missions principales :

- Informer et conseiller le responsable du traitement des données et/ou son sous-traitant à propos de l'usage et la protection des données personnelles.
- S'assurer du bon respect du RGPD et notamment constituer le registre des données de l'entreprise.
- Réaliser une analyse d'impact si cela est nécessaire.
- Communiquer avec la Cnil en cas de besoin ou de contrôle

Le DPO n'est pas personnellement responsable en cas de non-conformité de son entreprise au RGPD. Mais il est la personne référente dans l'application du règlement.

Les missions du DPO se concrétisent par la réalisation de 2 documents

1. Le registre des données

Le DPO est chargé de documenter les données personnelles. Il s'agit de produire un Registre des données qui liste toutes les données personnelles stockées par une entreprise. Il indique où elles sont stockées (CRM / Fichier Excel / chez un sous-traitant), qui peut y avoir accès ou encore quelle est la finalité de leur traitement. En cas de contrôle, c'est ce document qui sera demandé en premier lieu. Il est d'autant plus important puisqu'il servira de base à la mise en place des consentements des utilisateurs. En effet, en énumérant précisément la finalité de vos traitements, vous serez en mesure de rédiger des demandes de consentements claires et précises.

Le registre doit répondre à 7 questions :

- Quel type de données personnelles est traité ?
- Qui gère ou a accès à ces données ?
- Où sont stockées les données ?
- Identifier les flux de données : d'où viennent-elles ? où vont-elles ?
- Quel est l'objectif du traitement de ces données ?
- Combien de temps les données sont-elles stockées ?
- Quelles sont les mesures de sécurité mise en place pour les protéger ?

Pour répondre aux 3 premières questions

La constitution d'une cartographie des données sera nécessaire, il s'agit d'identifier toutes les données collectées par une entreprise, par qui et sur quel support. Généralement, on identifie 3 types de données : les données sur les clients et les fournisseurs, les données sur les salariés et, pour un sous-traitant, les données collectées et/ou traitées pour les clients.

2. L'étude d'impact sur la vie privée

L'étude d'impact sur la vie privée, ou Privacy Impact Assessment (PIA), est requise dès lors que les données traitées sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

C'est le cas si vos données concernent un public vulnérable (personnes âgées, mineurs), ou si elles sont en rapport avec une décision légale ou financière (demande de crédit par exemple) ou encore si les personnes font l'objet d'une surveillance systématique (contrôle de l'activité des salariés par exemple). C'est également le cas si l'entreprise effectue des opérations marketing consistant à envoyer des messages et informations ciblées en fonction du profil d'un individu, ou bien en cas de collecte de données à large échelle.

Ce document est composé de 4 volets :

- L'étude du contexte : qui précise le contexte et les enjeux du traitement des données;
- L'étude des mesures : pour indiquer les mesures à la fois techniques et organisationnelles pour respecter la règlementation et gérer les risques relatifs à la vie privée ;
- L'étude des risques : pour mesurer les risques liés à la sécurité des données et quel pourrait être leur impact sur la vie privée ;
- La validation du respect de réglementation et de la gestion des risques identifiés. S'il n'est pas possible de réaliser cette étape. Il faut donc recommencer les étapes précédentes.

Vous comprenez ainsi que ce document est essentiel pour être en parfaite conformité avec la réglementation.

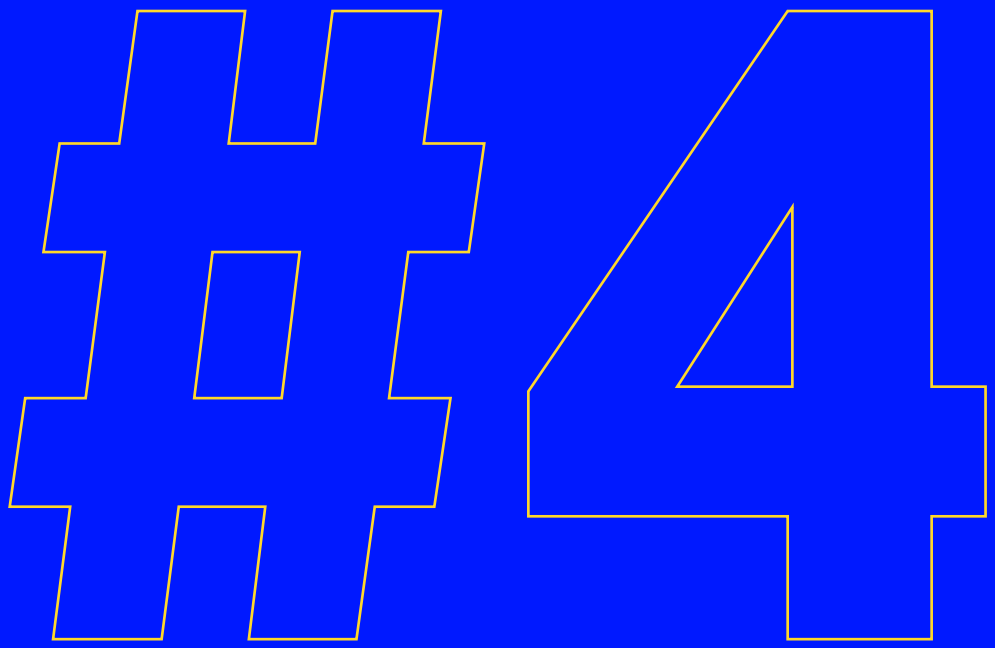
Faut-il nommer un DPO en interne ou en externe ?

Du fait de ses fonctions, le DPO doit être exempt de tout conflit d'intérêt. Il doit aussi avoir d'excellentes connaissances sur la législation relative à la protection des données ainsi que sur le secteur d'activité de l'entreprise qui requiert ses services.

Il existe 2 façons de recourir aux services d'un DPO :

- **Pour les grandes entreprises**, il est recommandé de nommer un DPO en interne (qui sera donc un salarié de l'entreprise) du fait du volume de données et d'une grande variété de finalités dans le traitement.
- **Pour les entreprises de plus petites tailles**, qui font du traitement de données de manière ponctuelle, il est possible de faire appel à un DPO externe, qui sera donc un prestataire de services. Sous certaines conditions, il est envisageable de mutualiser les services d'un DPO pour un regroupement d'entreprises.

En tant que sous-traitant, Avanci a engagé depuis début 2018 un DPO.



Sous-traitant et RGPD, qui est responsable ?

Le but du RGPD est de responsabiliser tous les acteurs de la collecte et du traitement de données personnelles. Ainsi, si vous avez affaire avec une agence digitale pour vos opérations de webmarketing par exemple, chacun de vous aura des responsabilités spécifiques.

Dans le cadre de votre collaboration avec Avanci, quelles sont nos obligations en tant que sous-traitant ?

Pour être conforme avec le RGPD, votre sous-traitant doit vous offrir 4 types de garanties :

1

L'obligation de transparence et de traçabilité

Cela implique plusieurs actions :

- Rédiger un contrat entre vous et le sous-traitant pour définir les rôles et obligations de chacun ;
- Recenser vos instructions par écrit afin d'être en mesure de prouver que votre sous-traitant agit pour le compte de votre entreprise ;
- Donner votre autorisation écrite si votre sous-traitant fait lui-même appel à un autre sous-traitant ;
- Obtenir de votre sous-traitant toutes les informations nécessaires pour prouver qu'il respecte ses obligations et pour vous permettre de réaliser un audit.

2

La prise en compte des principes de protection

Le sous-traitant doit vous garantir qu'il respecte toutes les exigences du RGPD dès la conception des outils, services ou produits et que, par défaut, seules les données nécessaires à la finalité du traitement sont collectées.

3

L'obligation de garantir la sécurité des données traitées

Un niveau adéquat de sécurité doit être garanti par le sous-traitant en fonction de la nature des données. Il doit également s'assurer que ses employés traitant les données sont soumis à une obligation de confidentialité.

4

L'obligation d'assitance, d'alerte et de conseil

Votre sous-traitant doit rapidement vous avertir en cas de violation de ses données. Mais, il doit également vous informer si une de vos instructions constitue une violation du RGPD ou si une personne fait exercer son droit d'accès, de rectification ou encore de suppression de données.

Quelles sont les obligations d'un sous-traitant ?

Un sous-traitant doit remplir trois obligations :

1.

Il devra nommer un DPO en interne :

- S'il est un organisme ou une autorité publique ;
- Si son activité de base le conduit à effectuer un suivi régulier et systématique de personnes à grande échelle pour le compte de ses clients, c'est le cas de la plupart des agences de marketing ou de communication, comme Avanci par exemple ;
- Si son activité de base le conduit à traiter à grand échelle des données sensibles ou relatives à des infractions ou condamnations pour le compte de ses clients.

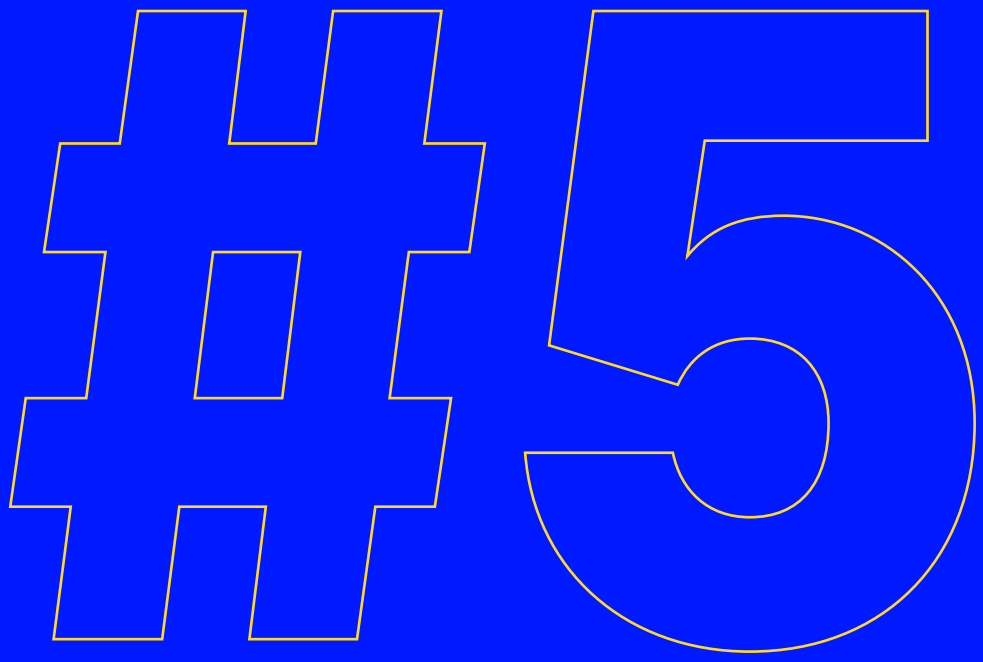
2.

Il devra **établir un contrat avec chacun de ses clients** stipulant, l'objet et la durée de la prestation, la nature et la finalité du traitement, le type de données traitées, les catégories de personnes concernées, les obligations et les droits de chacun des clients en tant que responsables de traitement, ainsi que les obligations et droits en tant que sous-traitant.

3.

Enfin, c'est au sous-traitant de **veiller à la sécurité des données traitées.** Les employés doivent être soumis à une obligation de confidentialité et il est nécessaire de prendre des mesures techniques et organisationnelles pour garantir la sécurité des données.

Certaines prestations d'Avanci sont désormais régies par le RGPD. Aussi, un DPO a été nommé en 2018 afin de nous accompagner. De plus, nous sommes soucieux de toujours vous fournir des prestations de qualité et performantes. Aussi, nous travaillons avec des prestataires qui ont pu nous confirmer leur mise en conformité avec le RGPD. Enfin, nos collaborateurs dont les missions sont régies par le RGPD sont formés aux impératifs du RGPD et seront régulièrement conseillés et accompagnés par notre DPO.



Les 6 étapes liées à la mise en conformité

01

Désigner un Data Privacy Officer (DPO)

La nomination d'un Data Privacy Officer (DPO) est obligatoire pour les organismes publics (collectivités locales, hôpitaux, universités...) et certaines entreprises en fonction de leur activité :

- Si leur activité de base les conduit à effectuer un suivi régulier et systématique de personnes concernées par les traitements ;
- Si leur activité de base les conduit à traiter à grande échelle des données sensibles ou relatives à des infractions ou condamnations.

Cela concerne les acteurs spécialisés dans le profiling, les acteurs de l'e-commerce ou de marketing digital comme Avanci, les banques, les assurances, ou encore les opérateurs télécoms.

Le DPO sera garant de la conformité en matière de protection des données au sein de son organisme. De plus, en cas de contrôle, il sera la personne référente dans l'entreprise.

02

Cartographiez vos traitements de données

Cette étape est essentielle et consiste à réaliser un registre de traitements de données. L'objectif est de recenser les types de données que vous traitez, l'emplacement où elles sont stockées ainsi que les personnes qui y ont accès. Vous pourrez ensuite mettre en place et tenir à jour le « registre des activités de traitements » qui inclut les flux et la typologie d'utilisation des données en plus de la cartographie. Pour mesurer concrètement l'impact du règlement sur la protection des données traitées, il faut donc recenser de façon précise les traitements effectués sur les données personnelles. Voici quelques exemples d'informations à recenser : finalités du traitement, catégories de personnes concernées, catégories de données traitées, catégories de destinataires des données, durée de conservation des données...

Prioriser les actions

Le DPO doit mettre en place et prioriser les actions correctives pour être en conformité avec le RGPD. Il doit ainsi déterminer le rôle des tiers avec qui vous partagez vos données et mettre en place des garanties adaptées (contrats) permettant de préciser les rôles respectifs de chacun, ou encore revoir les process de traitements des données si nécessaire. Il doit aussi s'assurer que les personnes concernées sont informées du traitement de leurs données à caractère personnel : les modalités et le contenu diffèrent en fonction de la nature de la collecte (directement ou via un tiers). Différents supports peuvent être utilisés pour communiquer cette information.

Le DPO doit également mettre en place la procédure de récupération du consentement des visiteurs quant au traitement de leurs données personnelles. Ainsi, les « cases pré-cochées » ne seront plus considérées comme suffisantes pour recueillir le consentement.

Gérer les risques

Le responsable du traitement et le sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté, en se basant sur les recommandations du DPO.

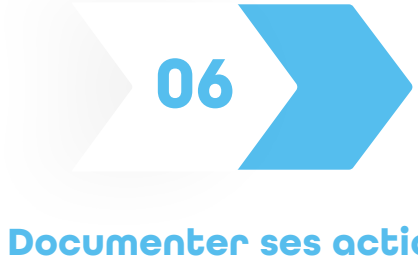
Sur la base du registre, identifiez les actions à mener pour se conformer aux obligations actuelles et à venir. Puis, priorisez par rapport aux risques relatifs aux traitements sur les libertés des personnes concernées. S'il y a des traitements à "risques élevés", réalisez une étude d'impact sur la vie privée (PIA) et prenez les mesures pour faire face à ces risques. Par exemple, il peut s'agir de traitement d'informations « particulières » ou relatives à des infractions, des condamnations, des opinions politiques, des données de santé, de traitements de surveillance systématique à grande échelle, de profilage, etc. Les risques peuvent être en termes de confidentialité, d'intégrité... Les violations de données personnelles doivent être notifiées à l'autorité de contrôle (CNIL) si possible dans les 72h.

Organiser des processus internes

Les entreprises doivent s'assurer que leurs process garantissent la sécurisation des données traitées et le respect du RGPD à tout moment. Elles doivent ainsi prendre en compte tous les évènements qui peuvent survenir au cours de la vie d'un traitement.

Cela consiste à :

- Déployer un processus permanent et dynamique de mise en conformité ;
- Apporter la preuve que les mesures appropriées ont été prises ;
- Auditer les mesures prises dans le cadre d'un contrôle continu.



Documenter ses actions

Déployez et publiez les mentions d'information et formulaires de consentement nouvellement créés ou révisés. Pour prouver votre conformité au règlement, vous devez regrouper au sein d'un document les actions réalisées et le tenir à jour.
Pour la mise en œuvre, il est recommandé de vous assurer que vos sous-traitants connaissent leurs nouvelles obligations et responsabilités et qu'elles sont formalisées contractuellement.

Si plusieurs acteurs interviennent dans la mise en œuvre d'un traitement de données à caractère personnel, les relations entre ces acteurs doivent être encadrées avec les responsabilités de chacun, notamment dans le cadre de responsabilité conjointe ou entre un responsable de traitement et le sous-traitant. Il sera nécessaire d'établir un contrat.

Conclusion

Le RGPD n'est pas une fatalité

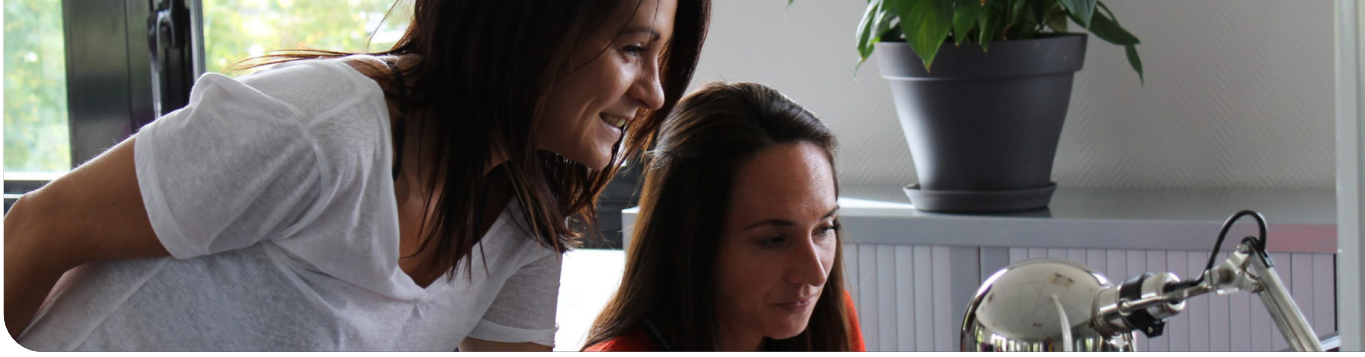
Entre les obligations, les garanties ou encore la mise en application... le RGPD apparaît comme une véritable contrainte pour de nombreuses entreprises.

Mais quitte à prendre le taureau par les cornes, autant voir les choses du bon côté !

Tout d'abord, le grand public (et c'est encore plus fort chez les jeunes générations) devient de plus en plus conscient et soucieux du traitement de leurs données personnelles sur le web.

De nouvelles méthodes apparaissent chaque jour pour permettre une communication plus personnalisée pour les annonceurs. Il était donc normal qu'une législation se mette en place. Prenez les devants ! Faîtes les choses bien et de façon transparente : votre image de marque n'en sera que valorisée.

Enfin, la mise en place du RGPD est aussi l'occasion de faire le point sur vos process, vos normes de sécurité en interne. En plus de cibler des failles potentielles, la constitution du registre de données vous aidera à avoir une approche plus stratégique de votre façon de travailler et d'avoir une meilleure maîtrise sur votre data.



À propos d'

avanci
Agence Conseil Data & Marketing

Avanci amplifie la valeur de vos clients

- Associer le savoir-faire d'une agence conseil en marketing relationnel à celui d'une agence spécialisée en DataMarketing
- Couvrir l'ensemble de la chaîne de valeur du marketing client en mettant la Data et la connaissance client au coeur de nos recommandations
- Vous accompagner dans la mise en oeuvre de votre stratégie relationnelle
- Créer des liens émotionnels et durables entre vos clients et votre marque
- Créer des outils performants de DataMarketing et de pilotage de la phase de recrutement à la fidélisation

Pourquoi choisir Avanci ?

Chez Avanci, nous vous accompagnons pour vous aider à y voir plus clair.
Nos équipes d'experts Data auditent votre architecture technique et identifient vos sources de données pour vous proposer la meilleure solution en fonction de vos objectifs.

Nos partenaires

upland BlueVenn · actito · data iku · Adobe · selligent · DATA LEGAL DRIVE · tableau · Kameleoon · tinyclues · mediarithmics

À propos de

MV GROUP
LE DIGITAL AVEC DU COEUR

MV Group est un groupe de marketing digital composé de 100 expertises réunies dans 11 filiales aux compétences data et digitales complémentaires.
Notre ambition ? Assurer la réussite de nos clients et faire grandir leur business grâce au digital.

Réussir sa stratégie digitale autrement

Pour simplifier les process et vous donner une meilleure compréhension de notre savoir-faire, nous vous assurons un interlocuteur unique. Il vous garantira efficacité et cohérence dans la mise en place de votre stratégie et la synergie des équipes. Travailler avec MV Group, c'est avoir la puissance de pôles d'expertises collaborant en synergie pour un effet incrémental :

- Branding
- Acquisition
- Conversion
- Fidélisation
- Stratégie
- Valeur client
- Valeur produit
- Engagement
- Formation

avanci

Agence Conseil Data & Marketing

Solutions Data & CDP

Data intelligence

Stratégie & Activation CRM

Vous souhaitez échanger sur votre projet ?

09 70 14 38 07 avanci.fr contact@avanci.fr

MV GROUP

ebit-data GBM Graphi Sweet yumens winbound NM DATA avanci euroleads TRIBU we feel good. 501

BORDEAUX – LILLE – LYON – MARSEILLE – NANTES – NICE – PARIS – RENNES – STRASBOURG – TOULOUSE – TOURS