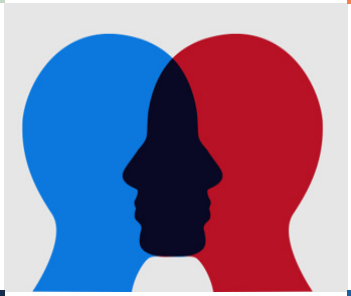
Sourire



Empathie

MIDRANGE Group

Intuition

BONNE Philippe
Président

philippe.bonne@midrange-group.com

VUTI Kozi
Directeur Conseil et Innovation

kozi.vuti@midrange-group.com

MAITRE Pascal
Directeur Commercial

pascal.maitre@midrange-group.com

MIDRANGE Group relève au quotidien les défis de transformations des entreprises grâce à l'innovation et l'expertise sectorielle.

Stratégie, Conseil, Digital, Technologies,
nous vous accompagnons dès maintenant

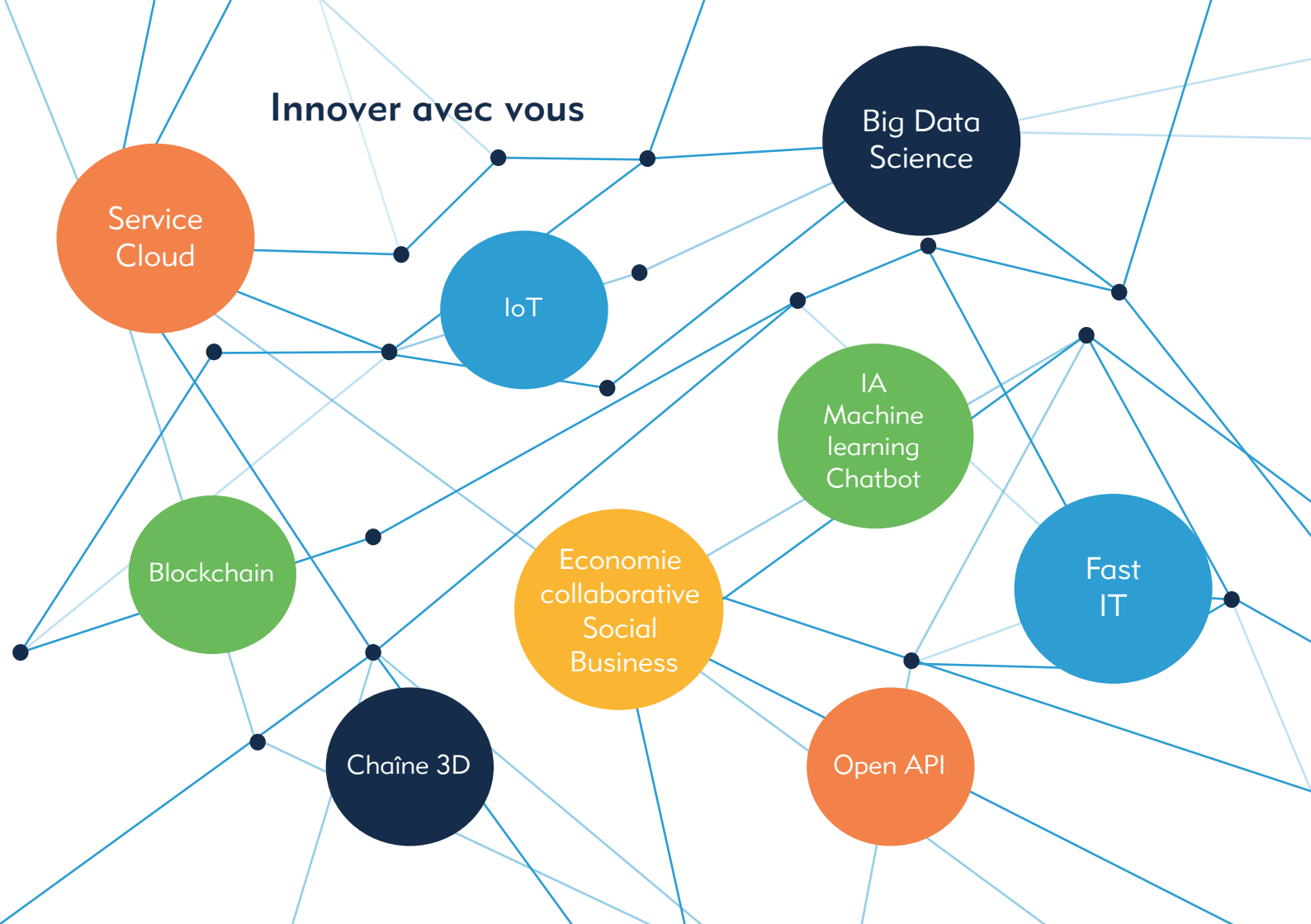
Valorisation de la donnée
Tableaux de bord décisionnels, Statistiques descriptives, Analyses prédictives

Innovation service
Optimisation de la relation client, E-commerce, Pricing VO, Lead Management

MIDRANGE Group

Performance opérationnelle
Digitalisation de l'après-vente, DMS Management, Efficience des systèmes d'information, Pilotage des décisions stratégiques

Collaboration Office 365
Amélioration de la productivité, Augmentation de l'expérience collaborateur : travail collaboratif en interne, avec les clients, avec les fournisseurs


Innover avec vous
Big Data Science
Service Cloud
IoT
IA Machine learning Chatbot
Blockchain
Economie collaborative Social Business
Fast IT
Chaîne 3D
Open API

CNPA

AGIR POUR VOTRE AVENIR

EDITO

Une des missions fondamentales du CNPA consiste à vous accompagner face aux incidences des évolutions règlementaires. De nombreux guides de mise en conformité au RGPD ont été publiés au cours des derniers mois : génériques, théoriques, inadaptés aux réalités d'une entreprise.

Le CNPA a choisi une autre démarche. En s'entourant d'experts, à la fois technique (Midrange Consulting) et juridique (Me Dedieu du Cabinet 3DTIC), nous avons rédigé ce guide qui s'adresse spécifiquement aux professionnels de l'automobile.
Vous y trouverez des outils, une méthodologie, les réponses concrètes aux questions que vous avez soulevées lors d'ateliers participatifs, et je tenais à vous remercier ici pour votre implication.

Proposer des modèles génériques de registres de traitement, ou de chartes, n'était pas dans l'esprit de ce guide, qui se veut sur-mesure. Il n'aurait pas permis de répondre à la diversité de vos entreprises, ni à la diversité de vos activités.
Ainsi, pour ceux qui souhaitent un accompagnement approfondi, un partenariat a été mis en place avec nos experts, et vous permettra d'obtenir des modèles sur-mesure pour votre entreprise, à des tarifs préférentiels.

En espérant que notre démarche s'adapte au mieux à votre gestion quotidienne de vos affaires.

Bonne lecture.

Xavier Horent

SOMMAIRE

RGPD, KÉZACO ?

Règlement Général Protection des Données

ou General Data Protection Regulation **(GDPR)**

DATES CLÉS

27 avril 2016
Adoption du texte européen

25 mai 2018
Entrée en vigueur

Les Données Personnelles de chaque citoyen européen relèvent de sa vie privée, comme son droit sur son image

> Le RGPD concerne chacun de nous, **personne physique** : nous sommes tous **intéressés à titre individuel** car nous fournissons nos Données Personnelles tous les jours à de nombreux opérateurs : **démarche active et collaborative des Personnes Concernées**

> Le RGPD **se préoccupe avant tout des droits de chacun sur ses Données Personnelles**

> Le RGPD considère que la valeur et la richesse de **nos Données Personnelles** rendent absolument nécessaire leur **protection** maximale et sérieuse

« Préoccupation essentielle du législateur européen : **faire respecter les droits de l'Homme et leurs libertés fondamentales dont leur vie privée** »

Principe posé par le RGPD : **les citoyens européens sont souverains sur leurs Données Personnelles**

> Nul ne peut les en déposséder et les maltraiter

> Nul ne peut collecter et traiter des Données Personnelles sans l'aval de la Personne Concernée, sauf raisons légitimes et légales

L'APPLICATION DU RGPD

Réglementation européenne s'applique de façon uniforme dans tous les Etats membres de l'Union Européenne (UE)

> Les Etats de l'UE ne peuvent qu'adapter par une loi locale certains des principes posés par le RGPD

> En France, c'est la loi du 20 juin 2018 modifiant la loi Informatique et Libertés

Champ d'application du RGPD

Pour les Personnes Concernées,
le RGPD s'applique à :
> Toute personne de nationalité de l'un des États européens dont données traitées en Europe
> Toute personne située/établie dans un État européen
> Tous ceux dont le droit reconnaît l'application du RGPD (exemple : Suisse)

Pour les entités Responsables de Traitement,
le RGPD s'applique à
> toute entité ayant à traiter des Données Personnelles de ressortissants ou personnes établies dans un État de l'UE, quel que soit le lieu d'établissement de l'entité

Personnes Concernées
→ page 14

Données Personnelles
→ page 13

Responsables de Traitement
→ page 16

/1

UNE OPPORTUNITÉ *BUSINESS*

MIXER LA PERFORMANCE OPÉRATIONNELLE ET LA CONFORMITÉ RÈGLEMENTAIRE N'EST PAS ANTINOMIQUE, DÉCOUVREZ COMMENT LE FAIRE

Le XXI[e] siècle sera plus que tout autre marqué par une **économie de confiance** où les acteurs sont co-créateurs de valeur ajoutée.

Cette co-création de valeur **se fonde sur la croyance spontanée ou acquise en la valeur morale, affective, professionnelle de l'autre,** qui fait que l'on est incapable d'imaginer de sa part tromperie, trahison ou incompétence.

Le RGPD permet à chacun de construire de manière légale et certifiée ce baromètre de confiance, fondé sur le niveau d'autorisation que chaque acteur de son écosystème business est disposé à lui accorder.

L'entreprise a des données, et doit être capable d'inspirer suffisamment confiance pour que l'individu l'autorise à l'intégrer dans **son patrimoine *business* : la data.**
Ce qui fait du RGPD une véritable opportunité *business*.

Créer et pérenniser la relation avec le client oblige à **une transparence** sur l'exploitation de ses données dont il est propriétaire.

Une relation co-créatrice de valeur ou co-engageante, où chaque acteur du partenariat doit pouvoir **répondre aisément à la question du client :** *est-ce que vous respectez la finalité pour laquelle je vous ai autorisé à exploiter ma donnée ?*

CRÉATION DE VALEUR : COMMENT ?

Au niveau microéconomique, « créer de la valeur » signifie faire du profit.

Aujourd'hui, on constate une nouvelle répartition du profit entre les entreprises : celles qui mettent la multitude au cœur du *business model*, et les autres. La communauté des utilisateurs constitue la « multitude ».

Créer de la valeur ne consiste **pas à se réorganiser** mais à se **transformer.**

L'acteur central dans la création de valeur, c'est la **data client**.

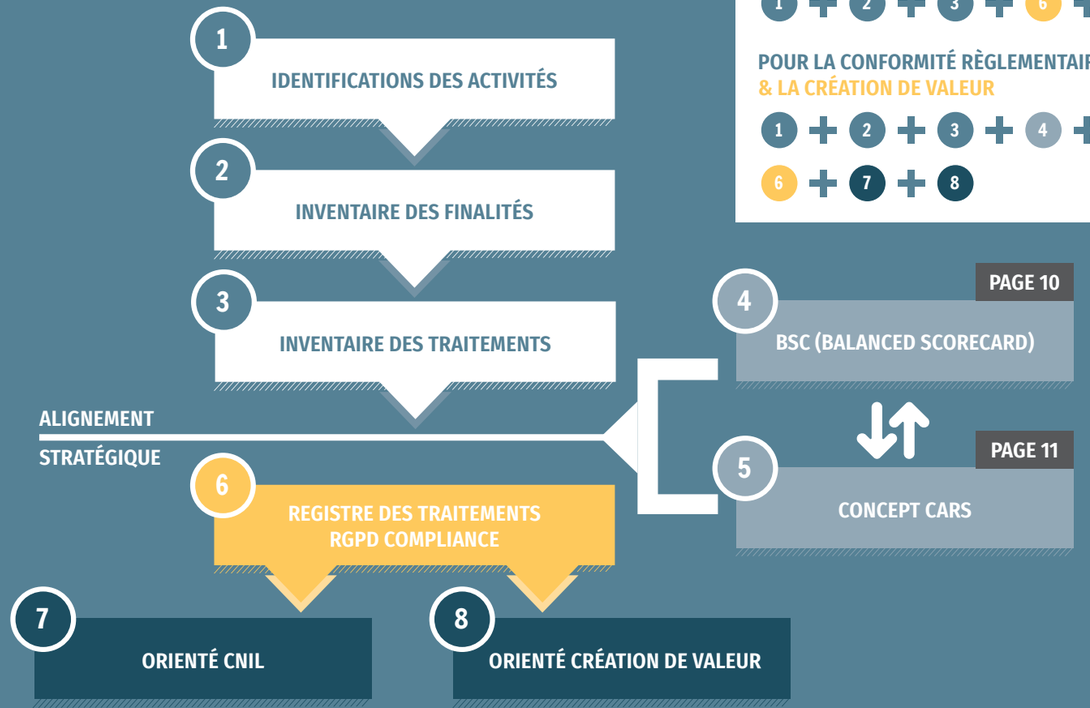
Se transformer c'est donc exploiter le RGPD non pas comme une contrainte mais au contraire comme une excellente opportunité pour une **meilleure gouvernance de la data** au sein de son entreprise.

Nous vous proposons d'utiliser **deux outils** pour transformer votre gouvernance de la **DATA** au sein de votre entreprise :

1 LE BUSINESS BALANCED SCORECARD (BSC) [page 10]

2 LE CONCEPT CARS *(outil Blue Ocean Strategy adapté à l'automobile et la mobilité par Midrange Consulting)* [page 11]

LES ÉTAPES DE LA CRÉATION DE VALEUR



POUR LA CONFORMITÉ RÈGLEMENTAIRE

1 + 2 + 3 + 6 + 7

POUR LA CONFORMITÉ RÈGLEMENTAIRE & LA CRÉATION DE VALEUR

1 + 2 + 3 + 4 + 5 + 6 + 7 + 8

LE BSC (BUSINESS BALANCED SCORECARD)

Le BSC (Business Balanced Scorecard) vous permettra de voir si les Traitements :

> sont bien cartographiés dans le but de répondre aux enjeux stratégiques de l'entreprise
> sont bien positionnés afin de participer à la performance de l'entreprise

Perspective Client

Les Traitements réalisés par mes partenaires et les données collectées par mes collaborateurs

>>> **prennent-ils en compte la satisfaction et l'analyse des besoins de ma clientèle ?**

Perspective Finance

Les finalités, les Traitements de mon entreprise

>>> **participent-ils à la performance financière ?**

Perspective Collaborateur

Le niveau de sensibilisation de mes collaborateurs à la valeur du patrimoine de la data et l'organisation humaine

>>> **me permet-il d'être une organisation innovante pour les enjeux de demain ?**

Perspective Processus interne

Les Traitements métiers réellement exécutés

>>> **me permettent-ils alors d'avoir un réel avantage concurrentiel ?**

LE CONCEPT CARS

Le concept CARS est une grille des quatre actions opérationnelles permettant de redéfinir les Traitements de valeur pour le client.

NOTA : le concept CARS est un outil Blue Ocean Strategy adapté à l'automobile par Midrange Consulting

Créer

Quelles sont les finalités ?
Quels sont les Traitements ?
qui sont jusque-là négligés par mon entreprise, qui doivent être créés.

>>> **création des finalités et Traitements pour répondre à la perspective Client (BSC)**

Réduire

Quelles sont les finalités ?
Quels sont les Traitements ?
qui sont jusque-là perçus comme nécessaires mais qui en réalité ne participent pas de manière significative à la création de valeur client.

>>> **réduction de finalités et Traitements pour répondre à la perspective Finance (BSC)**

Augmenter

Quelles sont les finalités ? Quels sont les Traitements ? qui sont jusque-là considérés comme normaux par mon entreprise pour lesquels l'entreprise doit augmenter les mesures car ils produisent plus de résultats qu'il n'y parait.

>>> **augmentation des finalités et Traitements afin de renforcer leur utilité pour alimenter les 4 perspectives de la Balanced Business Scorecard (BSC)**

Supprimer

Quelles sont les finalités ? Quels sont les Traitements ? qui sont jusque-là acceptés sans réelle réflexion, n'apportent plus rien de positif, au regard de l'évolution des exigences des clients, par conséquent ne participent plus à la création de valeur client.

>>> **suppression des finalités et Traitements au regard des 4 perspectives de la Balanced Business Scorecard (BSC)**

/ 2

UN CLIENT SOUVERAIN ET COLLABORATIF

DÉFINITIONS ET PRINCIPES FONDAMENTAUX POSÉS PAR LE RGPD - DROITS DES PERSONNES CONCERNÉES SUR LEURS DONNÉES PERSONNELLES

DÉFINITION

DONNÉES PERSONNELLES OU DONNÉES À CARACTÈRE PERSONNEL

Toute information se rapportant directement ou indirectement à une personne physique identifiée ou identifiable quel que soit le support : écrit (mail, sms, etc.), voix (enregistrement, écoutes téléphoniques), image (photographie, vidéo, etc.) si le rapprochement image/données permet une identification

- Données de localisation/ géolocalisation
- Carte grise
- Numéro de série
- Numéro de châssis
- Toutes données liées à l'immatriculation du véhicule
- Codes véhicules (accès, vitres, etc.)

- Clients
- Salariés (vie privée)
- Candidats
- Collaborateurs : informations sur la vie professionnelle (CV, coordonnées professionnelles, certificats, etc.)

+ de précisions P. 49

DONNÉES SENSIBLES/PARTICULIÈRES

Certaines données sont dites « sensibles » ou « particulières ».

C'est le cas par exemple des origines ethniques ou raciales, de la santé, y compris mentale, des opinions politiques et/ou philosophiques, de l'appartenance syndicale, du numéro de sécurité sociale, des données relatives aux infractions, notamment au Code de la route, des données comportant appréciation sur difficulté sociale de personnes ou encore ayant pour objet l'interconnexion de fichiers.

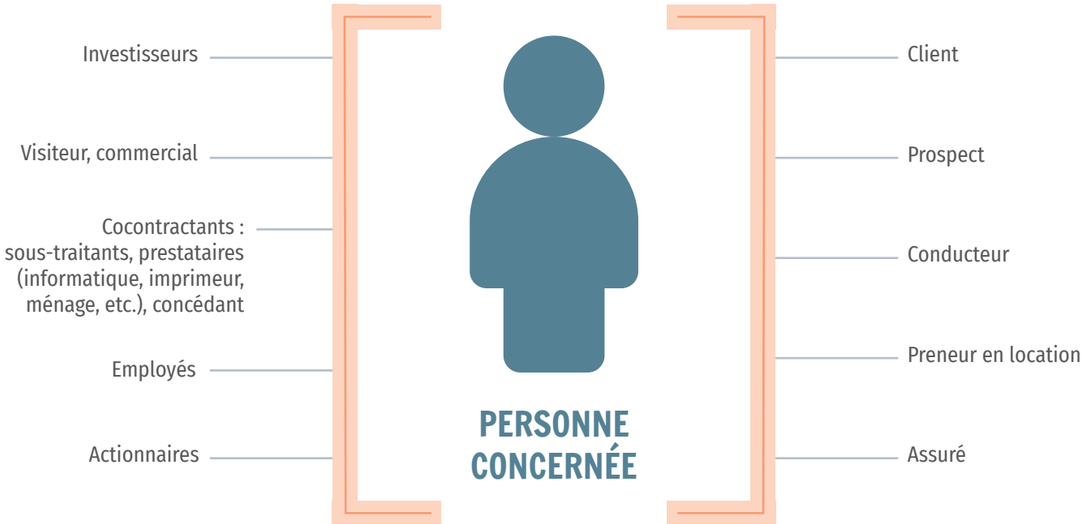
Le Traitement de ces données génère des obligations complémentaires

- Sécurité renforcée du Traitement des données
- Désignation d'un Délégué à la Protection des Données (DPO)
- Analyse d'Impact sur la vie privée

DÉFINITION

PERSONNE CONCERNÉE

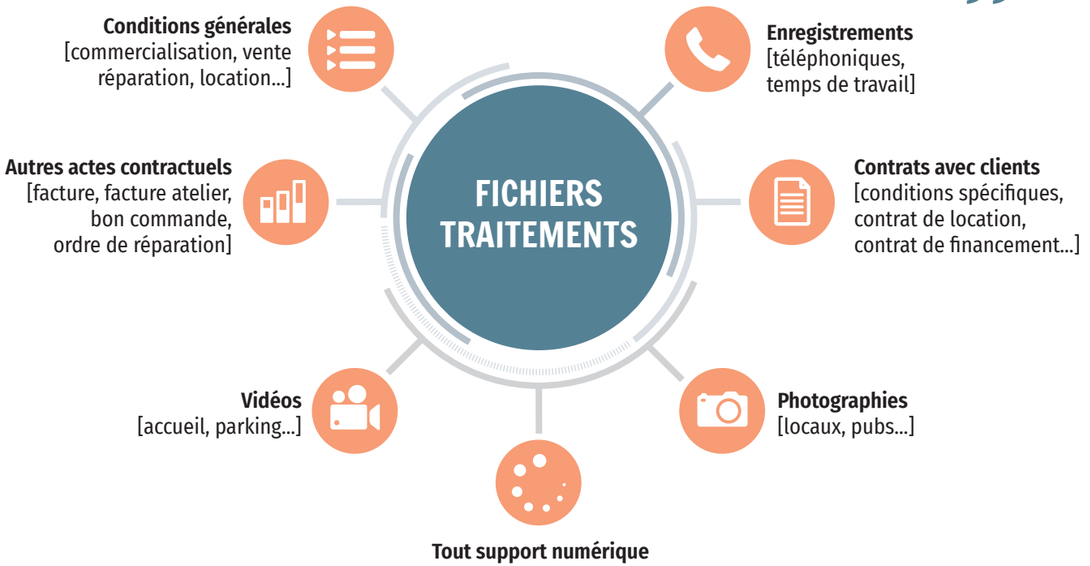
Personne physique à laquelle se rapporte les **Données Personnelles** ou sur **qui peuvent porter** des données collectées et traitées



DÉFINITION

TRAITEMENT DE DONNÉES PERSONNELLES

Toute opération ou ensemble d'opérations portant sur des données ou des ensembles de Données Personnelles, quel que soit le procédé utilisé et que l'opération soit effectuée ou non à l'aide de procédé informatisé



DÉFINITION

RESPONSABLE DE TRAITEMENT DE DONNÉES

Personne physique ou morale, autorité publique, service, ou autre organisme qui, seule ou conjointement avec d'autres, détermine les finalités et moyens de Traitements

> Le Responsable de Traitement est l'entité pour laquelle sont collectées les données et qui les traite comme par exemple :

- La société qui détient le garage, la concession...
- L'entité qui exerce l'activité de contrôles techniques, d'auto-école, de station-service, de station de lavage, de carrosserie, de dépannage, de recycleur, de parking, de loueur véhicules, de réparations...

> Hormis dans le cas de l'exercice d'une activité professionnelle individuelle, le Responsable des Traitements n'est pas une personne physique

IMPORTANT

Le Responsable de Traitement **n'est pas « propriétaire »** des Données Personnelles qui restent la seule propriété de la Personne Concernée.

AUTRES ACTEURS DES DONNÉES

Sous-traitant : personne physique ou morale, autorité publique, service ou tout autre organisme **traitant des données à caractère personnel** au nom et **pour le compte du Responsable du Traitement**

Exemple : prestataire informatique logeant les serveurs ; parfois le concessionnaire selon accords avec constructeur

Cotraitant ou coresponsable de Traitement : personne physique ou morale, autorité publique, service ou tout autre organisme qui **détermine conjointement les finalités et les moyens de Traitements** des Données Personnelles

Exemple : parfois le concessionnaire selon accords avec constructeur

Destinataires des données : personne physique ou morale, autorité publique, service, ou tout autre organisme, **tiers au Responsable ou non**, qui reçoit communication de Données Personnelles

> Tiers : personne physique ou morale, autorité publique, service ou organisme autre que la Personne Concernée, le Responsable de Traitement, le sous-traitant et les personnes qui, placées sous autorité directe du Responsable de Traitement ou sous-traitant, sont autorisées à traiter les Données Personnelles

> Tout **collaborateur, salarié, personne membre** d'une entreprise, entité, groupe qui accède ou à laquelle sont transférées des Données Personnelles en est « destinataire »

+ de précisions P. 51

PRINCIPES ESSENTIELS POSÉS PAR LE RGPD

PROTECTION RENFORCÉE DES DROITS DES PERSONNES CONCERNÉES
> **Renforcement et nouveaux droits des Personnes Concernées** sur leurs Données Personnelles
> **Consentement** des Personnes Concernées : conditions renforcées pour obtention et conservation

OBLIGATIONS ET RESPONSABILISATION RENFORCÉES DES RESPONSABLES DE TRAITEMENT
> **Renforcement de leurs obligations, des mesures** à mettre en place et de leur **responsabilité**
> Obligation de faire une **Étude Impact sur la vie privée** pour les Traitements de données à risques
> **Obligation de sécurité et de notification de toute violation** de Données Personnelles

RESPONSABILISATION ET CONFORMITÉ IMMÉDIATE
> Obligations à respecter dès la collecte des données et la création du Traitement = *« privacy by design »*
> Remplacement des formalités par la mise en place d'outils de « conformité » = *« accountability »*

PARTAGE DE RESPONSABILITÉS
> **Obligations nouvelles pour les sous-traitants** de Traitements de Données Personnelles
> **Partage de responsabilités** entre le Responsable et le sous-traitant

DURCISSEMENT DU RÉGIME DE SANCTIONS
> **Renforcement des pouvoirs de contrôle et de sanctions** de la CNIL
> **Augmentation des sanctions et amendes** administratives

EFFICACITÉ ET UNICITÉ DE LA RÉGLEMENTATION
> **Une loi uniforme** pour tous les Etats de l'Union Européenne adaptée par chaque Etat
> **Un guichet unique/autorité** de contrôle par Etat = *« one stop shop »*
> Une autorité de contrôle européenne : le **Comité Européen à la Protection des Données** (G29)

DROITS DES PERSONNES CONCERNÉES SUR LEURS DONNÉES PERSONNELLES

Il s'agit des droits des clients, prospects, collaborateurs et autres interlocuteurs des professionnels de l'automobile/membres du CNPA

DROITS RENFORCÉS

> **Droit d'accès**
- Droit de **savoir si et comment sont traitées ses données**
- Droit **d'obtenir toutes les informations** devant être communiquées par le Responsable de Traitement
- Droit d'obtenir une **copie** des données collectées

De nombreuses personnes ont commencé à solliciter ce droit d'accès : nécessité de toujours y répondre et de satisfaire la demande après une vérification d'identité

> **Droit d'opposition**
- Droit de s'opposer à tout Traitement de ses données **pour raisons tenant à situation particulière** (sauf exceptions légales et motif légitime et impérieux du Responsable de Traitement)

+ de précisions P. 58

NOUVEAUX DROITS

> **Droit à la portabilité des données**
Droit d'obtenir ses données dans un format structuré et usuel et de les transmettre ou faire transmettre à un autre Responsable de Traitement

> **Droit de notification**
Obligation pour le Responsable de Traitement de **notifier à chaque Personne Concernée toute faille de sécurité et atteinte à ses données** susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques

> **Décision individuelle automatisée et profilage**
Droit de refuser de faire l'objet d'une décision de « profilage » : toute forme de Traitement automatisé utilisant les Données Personnelles pour évaluer certains aspects personnels, dont la collecte de pratiques et usages pour ciblage promotionnel et commercial

NOTA sur le droit à la portabilité des données.
Attention aux abus dans les demandes de portabilité déjà constatés : ce droit porte sur les Données Personnelles et non sur les véhicules
→ la demande de portabilité ne justifie pas toute demande d'informations sur un véhicule
Par exemple, le droit à la portabilité ne permet pas de solliciter toutes les données sur toute intervention et réparation subie par un véhicule qui pourrait conduire à fournir des informations et données d'autres personnes (par exemple un précédent propriétaire)
Il est absolument nécessaire pour chaque demande de portabilité de vérifier l'identité et les informations de la Personne Concernée.
Attention à ne pas transmettre des Données Personnelles d'autres personnes que celle qui exerce son droit à la portabilité de ses données.

D'autres droits ont été renforcés par le RGPD : droit de rectification, droit à l'effacement / droit à l'oubli.

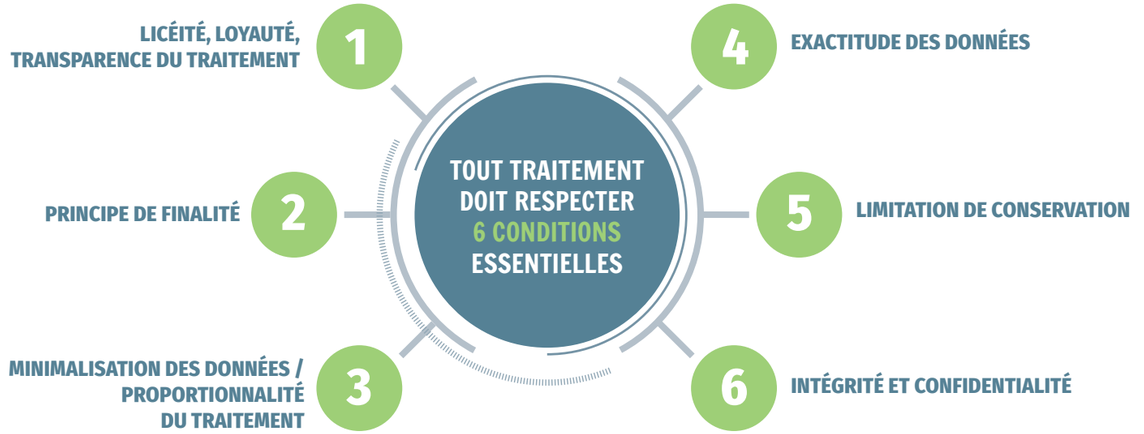
Un autre nouveau droit a été apporté par le RGPD : le droit à limitation du Traitement.

/ 3

L'ENTREPRISE, SES DROITS ET DEVOIRS

DROITS, DEVOIRS ET OBLIGATIONS
DES PROFESSIONNELS DE L'AUTOMOBILE
ET MEMBRES DU CNPA LORS DE LA COLLECTE
ET DU TRAITEMENT DES DONNÉES PERSONNELLES

CONDITIONS DE LICÉITÉ D'UN TRAITEMENT DE DONNÉES PERSONNELLES PAR LES PROFESSIONNELS DE L'AUTOMOBILE



TRAITEMENT LICITE

Obligation de Traitement de manière licite, transparente et loyale

→ obligation d'information préalable de la Personne Concernée

[→page 23 sur les informations préalables]

FINALITÉ

Principe de finalité

→ obligation de déterminer des finalités légitimes et explicites du Traitement et de les respecter

> Définir clairement l'**objectif** du Traitement : il doit être **compatible avec les missions et activités du Responsable de Traitement**
Exemples : collecte à des fins de prospection commerciale, pour entretien du véhicule, etc.

> Définir précisément les **destinataires** du Traitement
Exemples : sous-traitant, prestataire marketing, collaborateurs, constructeur, etc.

MINIMALISATION

Obligation de « minimalisation des données » et proportionnalité du Traitement

> Données collectes **adéquates, pertinentes, non excessives et limitées à ce qui est nécessaire au regard de la finalité** du Traitement
Exemple : inutile de connaître les orientations politiques pour finalité de prospection commerciale

> **Documenter le respect de cette obligation** avec des preuves : contrôle strict des juridictions et de la CNIL
Exemple : vidéosurveillance dans les locaux des salariés, dans les garages, etc. très encadrée

EXACTITUDE

Obligation d'exactitude des données

→ obligation de moyen renforcée

> Obligation de traiter des **données exactes et à jour**
Exemple : assurer et mettre à jour des données de facturation/bon de réparation

> Toute mesure raisonnable doit être prise pour **effacer ou corriger** des données inexactes ou périmées

CONSERVATION

Limitation de la conservation

→ obligation de conservation adéquate, proportionnelle et raisonnable // droit à l'oubli et à l'effacement

> **Délai de conservation limité par les finalités** du Traitement

> Délais de conservation définis et annoncés pour chaque finalité

INTÉGRITÉ

Obligation d'intégrité et de confidentialité

→ obligation de résultat

> **Mesures techniques et organisationnelles appropriées en particulier de sécurité**

> **Pour garantir**
- **Sécurité** appropriée aux données collectées
- Protection contre le **Traitement non autorisé, la perte, la destruction, les accidents**

+ de précisions P. 50

FOCUS

OBLIGATION ESSENTIELLE DE LICÉITÉ DE TRAITEMENT
INFORMATIONS PRÉALABLES OBLIGATOIREMENT FOURNIES PAR LE RESPONSABLE DU TRAITEMENT

Avant de traiter les données, le Responsable doit délivrer **à la Personne Concernée, de façon claire, concise et compréhensible, par tout moyen (penser à en conserver la preuve), des informations précises.**

Identité et coordonnées du Responsable du Traitement (l'entité)

Coordonnées du Délégué à la Protection des Données (DPO) le cas échéant

Finalités et base juridique du Traitement

Destinataires de la collecte (salariés, constructeur, etc.)

Durée de conservation

Caractère réglementaire ou contractuel de la collecte de données

En cas de conclusion d'un contrat, conséquences sur la non-fourniture des données

Existence d'une prise de décision automatisée (profilage)

Pour Traitement ultérieur : informations sur de nouvelles finalités

Droits de la Personne Concernée sur ses Données collectées [→ page 19]

FOCUS

OBLIGATION ESSENTIELLE DE LICÉITÉ DE TRAITEMENT
LE CONSENTEMENT DE LA PERSONNE CONCERNÉE

Principe : Avant la mise en œuvre d'un Traitement licite, le Responsable doit obtenir le **consentement libre, spécifique, éclairé et univoque de la Personne Concernée**

Libre Garanties données aux Personnes Concernées du respect de leurs droits [→ page 19 sur les droits des Personnes Concernées]

Éclairé Informations préalablement fournies par l'entreprise [→ page 23 sur les informations préalables]

Spécifique Consenti pour la ou les seule(s) finalité(s) précise(s) annoncées par l'entreprise

Univoque action positive sans contrainte : la Personne Concernée coche la case elle-même = opt in (et non case déjà cochée : opt out)

Exception à l'obligation du consentement pour les données nécessaires à l'exécution :

> **d'un contrat ou précontrat**

Exemple : le contrat de vente du véhicule comporte les Données Personnelles

> **d'une obligation légale**

Exemple : la loi impose la collecte de données comme par exemple pour l'établissement d'une facture

> **d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique**

Exemple : transmission de données sur les condamnations au Code de la route ou carte grise par application d'une loi dans tous documents destinés au public

> **d'un intérêt légitime du Responsable de Traitement**

Conserver les preuves des consentements obtenus

> **Formulaires de consentement** à faire remplir/signer et penser à garder une trace écrite des consentements donnés oralement

> **Créer un registre ou fichier de consentements permettant à tout moment de démontrer le consentement libre, éclairé, spécifique et univoque**

> **Organiser une conservation sécurisée permettant la gestion de l'exercice de tous droits des Personnes Concernées**

? + de précisions P. 56

FICHE PRATIQUE SUR LE CONSENTEMENT ET LA PROSPECTION COMMERCIALE

PRINCIPE
consentement obligatoire pour toute prospection commerciale

Exception, consentement préalable non obligatoire :

> Si la Personne Concernée est déjà cliente du Responsable de Traitement
ET
> Si la prospection porte sur des **produits ou services analogues à ceux déjà fournis par ce dernier**
Exemple : opération promotionnelle sur des véhicules organisée par un garage pour ses clients

À condition de respecter les 3 conditions suivantes :

> **Informer** la Personne Concernée que son adresse électronique sera utilisée à des fins de prospection commerciale

> Informer la Personne Concernée des **conditions et mesures mises en place pour respecter ses droits**

> **Permettre à la Personne Concernée d'exercer effectivement ses droits et de s'opposer à tout moment** à cette utilisation de manière simple et gratuite

MISE EN ŒUVRE POUR LA PROSPECTION COMMERCIALE

Voie électronique : e-mail, SMS, MMS, automate d'appels, fax, etc.
Opt in = action positive claire et non conditionnée
→ Pas d'action = NON = refus
! la Personne Concernée doit cocher elle-même la case

Voie postale, courrier
→ Pas d'action = OK/acceptation MAIS possibilité laissée à la Personne Concernée de s'opposer de façon simple et dénuée d'ambiguïté
(exemple : retour de courrier)

Téléphone
Opt in = action positive claire et non conditionnée
→ Pas de oui = NON = refus
Impossible si la Personne Concernée est inscrite sur liste d'opposition au démarchage téléphonique
(exemple : Bloctel)

/ 4

ORCHESTRER LA MISE EN ŒUVRE

À PARTIR DE LA RICHESSE D'INFORMATIONS FOURNIES PAR LA CNIL, COMMENT ORGANISER LA MISE EN ŒUVRE DANS UN UNIVERS AUTOMOBILE ET MOBILITÉ

OBLIGATIONS ET RECOMMANDATIONS

Le RGPD impose aux Responsables de Traitement la mise en place et en œuvre d'un **programme de conformité** comportant les **mesures obligatoires selon le RGPD** et les **mesures vivement recommandées (induites par les mesures obligatoires)** suivantes :

OBLIGATOIRES

Créer un **registre de ses Traitements de données** (→ pages 28 à 33)

Désigner un pilote des Traitements ou un **Data Protection Officer (DPO)**/Délégué à la Protection des Données (→ page 34)

Mettre en place une procédure de **sécurisation des données** et des Traitements

Mettre en place une procédure de **notification des incidents** et failles de sécurité

Mettre en place un système d'évaluation des risques et conduite **d'Analyses d'Impact** pour les cas de risques d'atteinte à vie privée (→ page 36)

RECOMMANDATIONS ADDITIONNELLES

Charte et politiques de Données Personnelles (→ page 35)

Programme de formations (sensibilisation) des personnes amenées à traiter des Données Personnelles

Mise en harmonie et conformité des documents contractuels avec tous les partenaires de l'entité / de toutes les entités / du groupe (→ pages 37 à 39)

RECOMMANDATION *BUSINESS*

Créer un **registre de ses Traitements de données orienté création de valeur :** augmenter l'expérience client, collaborateur, partenaire

LE REGISTRE DES TRAITEMENTS

Les travaux, produits avec les groupes de travail du CNPA, ont permis de mettre en exergue l'importance d'engager toutes les parties prenantes de l'entreprise, et de mener les actions d'évolution du système d'informations (SI), en collaboration entre clients et partenaires selon les responsabilités de chacun.

Il ne s'agit pas d'une option au sein de l'entreprise, mais d'un impératif, soutenu au plus haut niveau de l'entreprise et devant faire l'objet d'un budget spécifique et adéquat, dont la partie SI peut représenter une large partie sinon la majeure.

2 approches méthodologiques ont été identifiées :

APPROCHE A

Pour les **entreprises de petite taille** ou dont plus de 50% de leurs activités sont externalisées

illustrée aux pages 30-31

APPROCHE B

Pour les **entreprises de moyenne et grande taille** ou les entreprises dont la majorité des activités sont internalisées.

illustrée aux pages 32-33

Quelle que soit la taille de l'entreprise, son organisation juridique, il faut démarrer par la cartographie des activités et des Traitements.

→ page 29

CARTOGRAPHIER LES ACTIVITÉS ET TRAITEMENTS

Pour bien orchestrer la mise en œuvre, il faut commencer par lister les activités pour la classification des Traitements, et identifier au sein de son entreprise les 3 sources de collecte des Traitements.

LES 3 CATÉGORIES DE SOURCES DE COLLECTE

Les Traitements internes

Les Traitements métiers, qui sont issus des partenaires comme un constructeur, un franchiseur, un expert comptable, un RH externalisé, etc.

Les Traitements digitaux, qui font souvent appel à des systèmes de traitement hors Union Européenne

LISTE DES 15 ACTIVITÉS RETENUES

1 / Direction
2 / Comptabilité
3 / RH
4 / Administratif & Services généraux
5 / PR et magasin
6 / APV (Après Vente)
7 / Carrosserie
8 / Relation client
9 / Marketing
10 / Location
11 / Ventes VN
12 / Ventes VO
13 / Vente en Ligne
14 / Formation (Organisme)
15 / Informatique

En prenant en considération les métiers suivants : Agent de marque, Carrossier, Centre de lavage, Collecteur de pneumatiques usagés, Concessionnaire VI et VP, Contrôle technique, Cycles-Motocycles, Dépanneur, Remorqueur-Fourrière, Détaillant en carburants, Education routière et professions liées, Installateur agréé GPL, métiers de la mobilité partagée, Négociant en produits pétroliers, Négociant VO, Parc de stationnement, Pneumatique, Ramasseur agréé d'huiles usagées, Recycleur, Réparateur indépendant, Service Multimarque de l'Après-vente, Véhicules historiques.

LE REGISTRE DES TRAITEMENTS APPROCHE A

Cette première approche concerne **les entreprises de petite taille** ou dont plus de 50% de leurs activités sont externalisées.

Définir les activités qui décrivent le mieux votre entreprise

Inventorier l'ensemble des prestataires qui sont susceptibles d'exploiter des données

Inventaire complet de tous les Traitements (numérique, papier, audio, vidéo)

Validation juridique des Traitements à intégrer au registre de Traitements

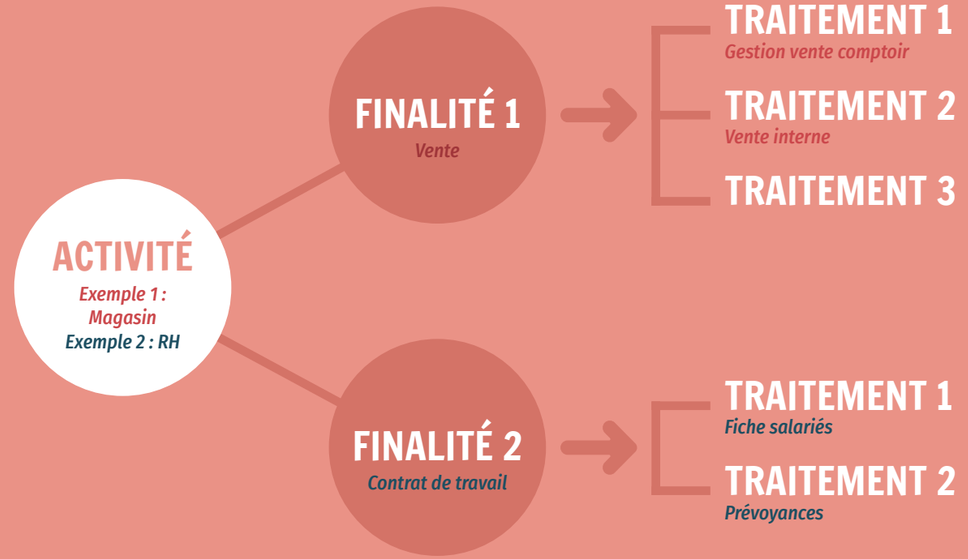
REGISTRE DES TRAITEMENTS

Réalignement juridique des contrats, de la demande de consentement

Réalignement technique des règles basiques de sécurité*

** (Contrôle d'accès des utilisateurs, journalisation des accès des utilisateurs, mesures de protection des logiciels, sauvegarde des données, chiffrement des données)*

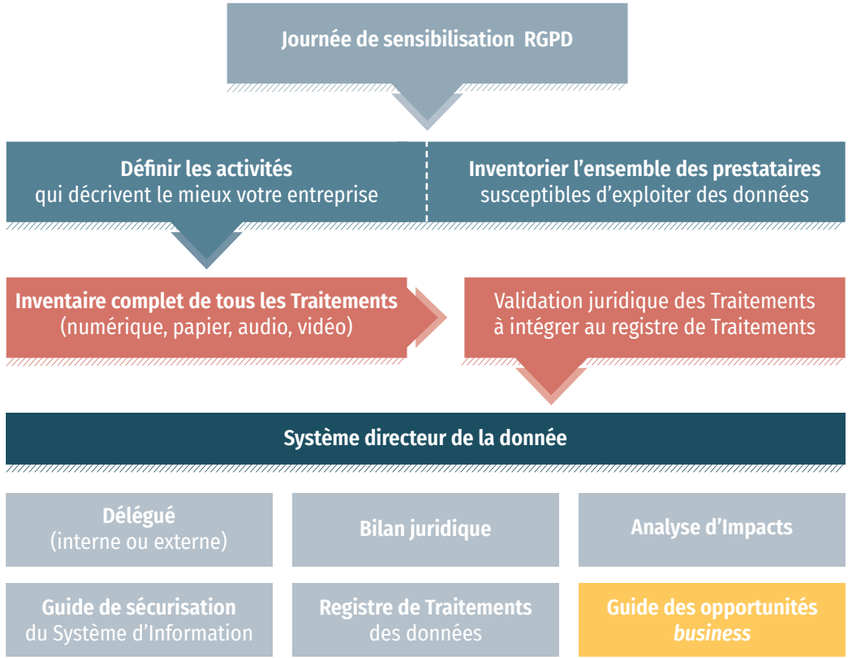
MODÈLE D'ORGANISATION PROPOSÉ APPROCHE A



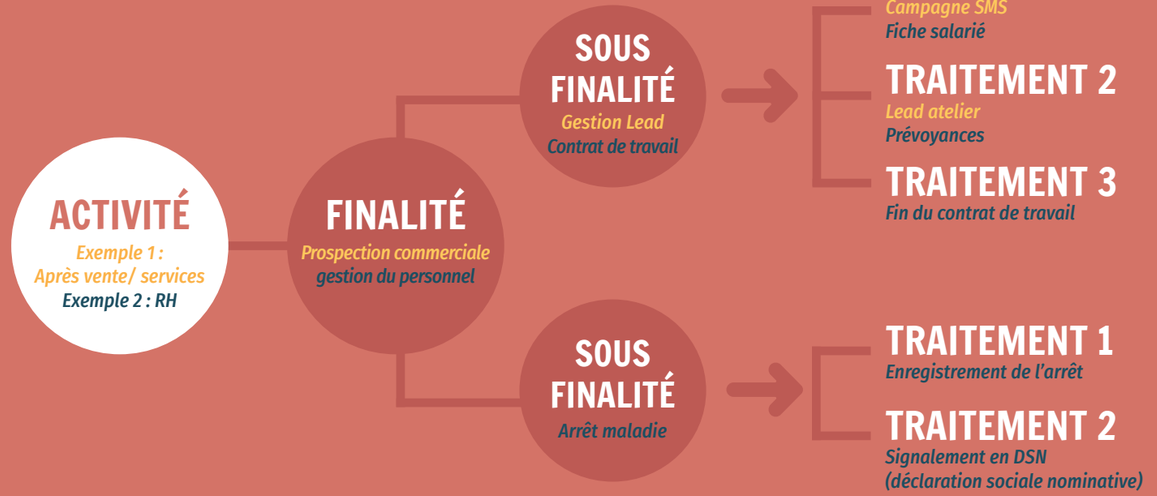
LE REGISTRE DES TRAITEMENTS APPROCHE B

Cette seconde approche concerne les **entreprises de moyenne et grande taille** ou les entreprises dont la majorité des activités sont internalisées.

Cette approche permet de disposer d'un plan d'investissement pluriannuel avec pour finalité de construire un profit total mixant les 2 modes de calcul :
1/ revenu par client x nombre de clients
2/ prix unitaire x quantité vendue.



MODÈLE D'ORGANISATION PROPOSÉ APPROCHE B



DÉSIGNATION D'UN PILOTE DES TRAITEMENTS DES DONNÉES ET/OU D'UN DATA PROTECTION OFFICER (DPO) /DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Dans tous les cas, **déterminer la personne « pilote » qui est responsable de la mise en œuvre et de la gestion des mesures RGPD,** et le cas échéant une équipe-projet

Dans les cas fixés par le RGPD, **désigner un Data Protection Officer (DPO) / Délégué à la Protection des Données**

> **Obligatoire pour :**
- Traitement à grande échelle (en nombre de Personnes Concernées)
  Exemple : Traitement de géolocalisation de tous ses clients
  Exemple : Traitement des données à caractère personnel par un moteur de recherche à des fins de publicité.
- Traitement de données sensibles/particulières

> Exigence de qualifications et compétence en droit et en pratique ; professionnalisation de la fonction

> Mission centrale **MAIS la responsabilité de conformité demeure à la charge de l'entité et de ses dirigeants**

> **Possibilité d'externaliser la fonction de DPO**

> Pour les petites entités soumises à l'obligation de désigner un DPO (Traitement de données sensibles/particulières de ses salariés ou de condamnations au Code de la route par exemple) : **possibilité d'envisager la mutualisation du DPO par plusieurs entités**

CODE OU CHARTE DE DONNÉES PERSONNELLES ET POLITIQUE DE CONFIDENTIALITÉ

Le code ou la charte des données doit prévoir a minima :

> **Politique de confidentialité et de bonnes pratiques pour la collecte et le Traitement des Données Personnelles :** finalités, destinataires, durée de conservation, modes de gestion de Traitement

> **Information des Personnes Concernées**
- Mentions obligatoires dont identité du Responsable de Traitement et le cas échéant du DPO

> **Règles d'exercice de leurs droits par les Personnes Concernées. Consentement des Personnes Concernées**
- Modalités, recueil et conservation

> **Procédure de transfert de données hors UE**
- Interdiction de transfert de données hors UE, sauf pays tiers avec un niveau protection adéquat : Argentine, Canada, Suisse, Nouvelle-Zélande, etc.
- Transfert moyennant des garanties appropriées comme par exemple la signature de contrats
– Binding Corporate Rules (BCR) approuvés par la CNIL et information + consentement exprès éclairé de la Personne Concernée

Pour un accompagnement sur la création d'une charte personnalisée, voir page 58 pour contacter des spécialistes.

CONDUIRE UNE ANALYSE D'IMPACT

> Obligation d'évaluer les risques d'affecter la vie privée des Personnes Concernées
→ **Analyses d'Impact pour les cas de risques d'atteinte à la vie privée**
/ *Data Protection Impact Assessment -DPIA- ou Privacy Impact Assessment -PIA-*

> Avant la mise en œuvre de Traitement, pouvant emporter risques élevés sur les droits et libertés des Personnes Concernées :
- Évaluation systématique d'aspects personnels (comportement, etc.) fondée sur un **traitement automatisé**
- **Collecte** de données à grande échelle
Exemple : traitement des données de géolocalisation en temps réel des clients
- Données sensibles
- Croisement de données
- Surveillance systématique *Exemple : système de contrôle des salariés*

> **Approche des Données Personnelles par les risques :** évaluer les **risques sur la vie privée** et déterminer les **mesures adéquates** pour y parer

> Méthodes diverses, comprenant a minima 4 étapes :
1 - Délimitation/description du contexte et des finalités du Traitement
2 - Analyse de nécessité et proportionnalité du traitement requises
3 - Évaluation des risques sur la vie privée
4 - Mesures d'adaptation requises pour assurer la protection

> Mise en œuvre des mesures adéquates

> Transmission de l'Analyse d'Impact à la CNIL

CONFORMITÉ DE SES PARTENAIRES AU RGPD ADAPTER LES CONTRATS

Nécessité de s'assurer que les partenaires avec lesquels des Données Personnelles sont partagées/échangées/transférées observent toutes les obligations du RGPD et les mêmes règles rigoureuses notamment de sécurité et confidentialité de Traitement des données

Le RGPD ne doit pas être l'occasion d'imposer des obligations injustifiées ou déséquilibrées à son cocontractant : « la loi rien que la loi »

> **Dans tout contrat important partage ou transfert ou échange de Données Personnelles, nécessité de sécuriser techniquement et juridiquement la relation contractuelle**
→ **Insérer des clauses protectrices des intérêts des professionnels de l'automobile et des Personnes Concernées** portant par exemple sur la politique de protection des Données Personnelles et le respect des droits des Personnes Concernées, la sécurité physique des données et locaux, les droits respectifs de chaque partie de chacun sur les données stockées, collectées, traitées : conditions d'accès des salariés et autres personnes physiques appelées à en connaître ou les traiter (comptables, accueil des clients, réparateurs, moniteur d'auto-école, etc.), durée de conservation, modalités de suppression, sort des données à l'issue du contrat etc.

> **Dans tous les documents contractuels commerciaux avec les clients tels que CGV, CGU, CGA, contrat de commercialisation, mentions obligatoires claires, complètes et accessibles pour les Personnes Concernées sur les informations essentielles**
Exemple : finalités des Traitements, types de données collectées, identité/coordonnées du Responsable de Traitement, de la personne/pilote et du DPO le cas échéant, etc.

Pour une assistance sur la rédaction, l'adaptation et la négociation des contrats, voir page 58 pour contacter des spécialistes.

+ de précisions P. 53

ORGANISER LA SOUS-TRAITANCE
DU TRAITEMENT DES DONNÉES PERSONNELLES

> Sous-traitant = tout prestataire qui collecte, héberge ou traite des données **pour le compte du Responsable**

> Le sous-traitant a les **mêmes obligations au regard du RGPD que le Responsable du Traitement.** Il doit présenter des **garanties suffisantes quant à la mise en œuvre de mesures techniques/organisationnelles appropriées** (sécurité technique, mesures respect RGPD, etc.). **C'est la responsabilité du Responsable du Traitement de s'assurer des garanties présentées par son ou ses sous-traitant(s)** : cahier charges, label, certification ...

> **Un contrat écrit entre le sous-traitant et le responsable est obligatoire.**

> Il prévoit a minima :
- Objet et durée du Traitement
- Nature et finalité du Traitement
- Type de données à caractère personnel
- Catégories de Personnes Concernées

> Il précise les **devoirs du sous-traitant,** comme par exemple :
- Ne traite des Données Personnelles que sur instructions du Responsable
- Garantit le respect de la confidentialité par tous ses membres
- Détruit toutes données et copies dans les délais prévus
- Permet les audits et fournit les éléments de preuve requis par le Responsable

+ de précisions P. 51

> Il précise le sort des données et de la base après cessation : **le sous-traitant peut négocier la conservation de la base de données qu'il collecte à l'issue du contrat de sous-traitant**

> **Le Responsable du Traitement partage la responsabilité avec le sous-traitant, mais demeure le premier responsable (et peut se retourner contre le sous-traitant pour un partage ou un transfert de responsabilité)**

ORGANISER LA COTRAITANCE
DU TRAITEMENT DES DONNÉES PERSONNELLES

> « Co-Responsables de Traitement » ou « Cotraitants » : lorsque deux Responsables de Traitement ou plus **déterminent conjointement les finalités et moyens du Traitement.**

> Un contrat écrit est obligatoire dont les grandes lignes doivent être mises à disposition des Personnes Concernées par les Données Personnelles partagées
- Il y a une certaine liberté contractuelle : plusieurs degrés de co-responsabilité sont possibles
- Le contrat doit prévoir toutes les clauses de nature à organiser la répartition des tâches, des rôles et des responsabilités

Exemples : stipulations portant sur les obligations respectives des cotraitants, partage des risques et des responsabilités entre les Responsables conjoints (responsabilité conjointe), politique de confidentialité applicable à tous les membres de chacun des cotraitants, etc.

IMPORTANT

Le contrat doit absolument prévoir le sort de la propriété du Traitement et des bases de données à l'issue du contrat de cotraitance des Données Personnelles : **celui qui collecte les données doit s'assurer qu'il pourra continuer à les traiter**

Pour une une assistance sur la rédaction, l'adaptation et la négociation des contrats, voir page 58 pour contacter des spécialistes.

/5

LA SÉCURISATION DES DONNÉES

ÉVITER LES RÉPERCUSSIONS SÉVÈRES EN TERMES DE PERTES ÉCONOMIQUES ET FINANCIÈRES, ET DE DÉGRADATION DE L'IMAGE DE L'ENTREPRISE LIÉES À UNE MAUVAISE SÉCURISATION DES TRAITEMENTS

POLITIQUE DE SÉCURITÉ DES DONNÉES ET TRAITEMENTS

Le RGPD requiert la **mise en place des « mesures techniques et organisationnelles appropriées »** et d'une **procédure de sécurité** des données et des Traitements afin de garantir un niveau de sécurité adapté au risque.

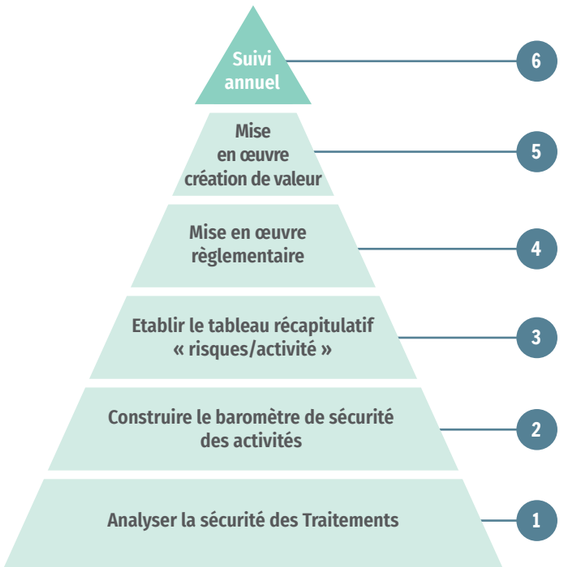
La **sensibilisation des utilisateurs** manipulant les données avec une charte informatique est **obligatoire**.

- **Authentifier les utilisateurs**
  Exemple : un login/mot de passe individuel
- **Gérer les habilitations**
  Exemple : supprimer les permissions d'accès obsolètes
- **Tracer les accès et gérer les incidents**
  Exemple : prévoir la procédure pour les notifications de violation
- **Sécuriser les échanges avec d'autres organismes**
  Exemple : transmettre le code secret lors d'un envoi de donnée via un canal différent
- **Sécuriser l'informatique mobile**
  Exemple : chiffrement, sauvegardes, etc.
- **Protéger le réseau informatique interne**
  Exemple : accès distants par VPN, réseaux Wi-Fi en WPA2 ou WPA2-PSK
- **Sécuriser les serveurs**
  Exemple : limiter l'accès, installer sans délai les mises à jour critiques
- **Archiver de manière sécurisée**
  Exemple : détruire les archives obsolètes de manière sécurisée
- **Sauvegarder et prévoir une continuité d'activité**
  Exemple : prévoir et tester régulièrement la continuité d'activité
- **Gérer la sous-traitance**
  Exemple : conditions de restitution et de destruction des données
- **Encadrer les développements informatiques**
  Exemple : encadrer le contenu des zones de commentaires
- **Protéger les locaux**
  Exemple : installer des alarmes anti-intrusion et les vérifier périodiquement
- **Encadrer la maintenance et la destruction des données**
  Exemple : effacer les données de tout matériel avant sa mise au rebut
- **Sécuriser les sites web**
  Exemple : gestion des cookies, sécuriser les accès aux URL, etc.
- **Sécuriser les postes de travail**
  Exemple : un antivirus, un firewall, etc.
- **Utiliser des fonctions cryptographiques**
  Exemple : conserver les codes secrets et les clés cryptographiques de manière sécurisée

Source : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

SÉCURITÉ UNE DÉMARCHE PRAGMATIQUE

Les différentes actions opérationnelles sont :



6 **Évaluer** concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps :
1 - au moins une fois par an pour les petites entreprises
2 - au moins deux fois par an pour les moyennes et grandes entreprises

5 **Réaligner** son système d'information sur la stratégie d'entreprise *(schéma directeur système d'information)* à partir des recommandations des organes de l'Etat que sont :
1 - Guide des bonnes pratiques de l'informatique www.cybermalveillance.gouv.fr
2 - Guide d'Hygiène Informatique www.ssi.gouv.fr

4 **Exécuter** les 17 mesures techniques recommandées par la CNIL www.cnil.fr

3 **Disposer** d'un outil de pilotage stratégique et d'investissement pour préserver le patrimoine *business* de l'entreprise

2 **Etablir** un baromètre de sécurité par activité

1 **Mesurer** le niveau de maturité de chaque Traitement par rapport aux trois évènements redoutés :
1 - accès illégitime à des données
2 - modification non désirée de données
3 - disparition de données

UN OUTIL DE PILOTAGE

Le tableau modèle suivant suggéré par la CNIL et réadapté par les groupes de travail CNPA peut être utilisé pour

> formaliser les menaces réalisables
> déterminer les mesures existantes ou prévues
> estimer la gravité et la vraisemblance des risques

Il permet d'établir les plans d'actions (techniques, organisationnelles), de déterminer le budget d'investissement et de **prioriser les actions pour préserver son patrimoine *business*.**

Risques /données de l'activité	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime à ces données						
Modification non désirée des données						
Disparition des données						

QUELQUES BONNES PRATIQUES

BONNE PRATIQUE

Rédiger et mettre en œuvre une procédure de suppression sécurisée des données

Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin du contrat de location

Est-ce que vous utilisez un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers, par exemple sftp ou https ?

À NE PAS FAIRE

Réutiliser, revendre ou jeter des supports ayant contenu des données à caractère personnel sans que les données n'aient été supprimées de façon sécurisée

BONNE PRATIQUE

Créer un mot de passe solide :

1 - la méthode des premières lettres « Un tien vaut mieux que deux tu l'auras » : 1tvmQ2tl'A

2 - la méthode phonétique « J'ai acheté huit CD pour cent euros cet après-midi » : ght8CD%E7am

3 - Inventez votre propre méthode connue de vous seul !

Est-ce que l'environnement des salles informatiques (climatisation, onduleur, etc.) est sous-dimensionné et avec un entretien négligé ? Et accessible à tout le personnel ?

À NE PAS FAIRE

Conserver les sauvegardes au même endroit que les machines hébergeant les données

POLITIQUE DE GESTION DES FAILLES DE SÉCURITÉ

Mettre en place la procédure de notification des incidents/failles de sécurité/violation des données et des mesures appropriées pour :

> La gestion, le traitement et la résolution de tout incident de sécurité

> La notification de toute violation de données :
- À la CNIL dans les 72h
- À la Personne Concernée si risque élevé, dans les meilleurs délais

> La tenue d'un registre d'incidents toujours à jour

/ 6

LE RGPD ET LE FUTUR

EN PLAÇANT LE CONSOMMATEUR
AU CŒUR DE LA CHAÎNE DE VALEUR,
LES NOUVEAUX *BUSINESS MODELS* RENDENT
CADUQUES LES ANCIENS, FONDÉS SUR LA SEULE
AMÉLIORATION DE L'OFFRE AU CONSOMMATEUR

LE RGPD EST UN OUTIL QUI PERMET D'ANTICIPER L'ÈRE DE L'ULTRA-CLIENT

L'INTERNET DES OBJETS / IOT

Un univers d'objets intelligents et connectés

Il représente l'extension d'Internet à des choses et à des lieux du monde physique. L'IoT est une solution d'opportunités pour l'e-santé, le sport connecté, la ville connectée, l'usine du futur, l'agriculture connectée, etc.

> Ce qui veut dire une augmentation exponentielle du flux de données avec des incidences sur l'exploitation des données de la vie privée des personnes

Impact pour l'individu

> Collecter les Données Personnelles pour avoir une meilleure connaissance de l'usage d'un produit ou d'un service

> Collecter les Données Personnelles pour la médecine préventive

LA BLOCKCHAIN

« Machine à générer de la confiance »

Il s'agit d'un système de registre distribué et réputé inviolable dans lequel sont enregistrées toutes les transactions effectuées entre ses utilisateurs.

Les échanges sont effectués sans organe central de contrôle. Les deux entités impliquées dans une transaction (personnes ou organisations) sont représentées par leurs clefs numériques.

Impact pour l'individu

> Collecter les Données Personnelles pour la signature électronique et l'horodatage dans les processus métier

> Collecter les Données Personnelles pour enregistrer et conserver toutes les informations concernant son véhicule dans un carnet d'entretien dématérialisé, unique et sécurisé

FOIRE AUX QUESTIONS

DONNÉES CONCERNÉES

Les données du véhicule sont-elles des données à caractère personnel ?

Sont des Données Personnelles toutes les informations permettant l'identification d'une personne physique :

> Toute donnée se rapportant à un véhicule qui permet une identification d'une Personne Concernée qui est
  - Propriétaire
  - Locataire
  - Utilisatrice
  - Assuré
  - Titulaire de la carte grise
> Et toute donnée du véhicule permettant l'identification d'une personne physique
  - Toute donnée liée à l'immatriculation du véhicule
  - Numéro de châssis
  - Codes du véhicule comme celui des vitres ou de l'accès au véhicule
  - Données de localisation grâce au GPS du véhicule

Traitons-nous des données sensibles ou particulières dans nos concessions, garages, entités ?

Sont des données sensibles ou particulières :

> Toutes les informations recueillies pour les salariés et collaborateurs comme le numéro de sécurité social pour traitement des congés maladie, sur leur appartenance syndicale pour les représentants du personnel, etc.
> Les informations relatives aux infractions au Code de la route

Les documents papier sont-ils concernés par le RGPD ?

Tous les Traitements de Données Personnelles sont concernés, que le support soit en format :

> Papier : formulaire écrit, carte de fidélité, etc.
> Oral : conversation, enregistrement, messages vocaux, etc.
> Pictural/image : photographie, vidéo

Dès que l'identification de la Personne Concernée est possible.

CONSERVATION DES DONNÉES

Quelle est la durée de conservation des données ?

> Principe de conservation posé par le RGPD = les données doivent être conservées sous une forme permettant l'identification des Personnes Concernées **pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**

> Les durées varient selon les données et les Traitements ; exemples de durées de conservation recommandées par la CNIL (et textes antérieurs au RGPD) :

- **Client : 3 ans** après la dernière relation commerciale
- **Prospect : 3 ans** après la dernière sollicitation restée sans réponse
- Dispositif de **vidéosurveillance** pour la sécurité des biens et personnes : **1 mois**
- Données des **collaborateurs pour paie**, horaires : **5 ans**
- Données de **santé des collaborateurs : 10 ans**
- **Carte d'identité : 1 an**
- Données de **cartes bancaires : dès la transaction réalisée** = paiement effectif (mais penser et rajouter le délai de rétractation)

> **Attention toutefois aux conflits de lois : ces durées de conservation doivent être combinées avec d'autres lois qui imposent des durées plus longues comme par exemple la prescription pour une action judiciaire**
(exemple : action judiciaire sur un contrat commercial)

> **Exemple de prescription en matière commerciale : 5 ans**

Faut-il informer nos clients sur la date de conservation des données ?

> Obligation de principe d'informer les Personnes Concernées sur le délai de conservation de ses données (→ page 23 sur les informations préalables)

Quand dois-je effacer les Données Personnelles dans mes bases ?

> À l'expiration du délai de conservation annoncé à la Personne Concernée

> Possibilité de prévoir un archivage ; 2 formes d'archivage envisageables : intermédiaire et définitif (qui implique suppression/anonymisation des données)

Que faire de mes données obsolètes ?

> Obligation de détruire les données erronées et de les corriger

> Obligation de détruire les données après délai de conservation annoncé

RESPONSABILITÉ

Qui est Responsable du Traitement : le constructeur ou le concessionnaire ? (Exemple : base de données via le CRM/DMS)

> **Dans le cas de partage et/ou transfert de données, un contrat écrit doit impérativement organiser la répartition et les modalités d'exécution des obligations** *(exemple : détermination de l'entité et la personne physique en charge de recueillir et exécuter les droits d'accès des Personnes Concernées)*, **des relations et des responsabilités sur les données.**

> Les parties **définissent ensemble,** dans le cadre de leurs relations et négociations commerciales, si elles entendent se soumettre au **régime de la sous-traitance ou à celui de la cotraitance**. Dans les 2 cas, les responsabilités, en particulier quant à la sécurité et la confidentialité sur les données, sont partagées. Le contrat doit définir précisément le rôle de chaque partie.

> **Ne pas confondre la notion de « Responsable de Traitement »** du RGPD (→ page 16) **et le propriétaire des bases de données** (le propriétaire des données ne peut être que la Personne Concernée) : le contrat doit prévoir le sort des données et de la base de données après cessation des relations contractuelles.

→ **Il est essentiel de négocier et rédiger un contrat précis et le plus équilibré possible**

Qui est Responsable du Traitement : le sous-traitant, le constructeur, un autre acteur ? (Exemple : site Web)

> Le sous-traitant agit pour le compte du Responsable de Traitement ; il n'en demeure pas moins responsable d'un Traitement conforme au RGPD et aux instructions du Responsable de Traitement.

> Une cascade de sous-traitants est possible avec l'accord du Responsable de Traitement
Exemple : le constructeur peut être Responsable de Traitement et le concessionnaire sous-traitant ; le prestataire informatique fournisseur du DMS est également un sous-traitant avec lequel le concessionnaire doit s'organiser par la voie d'un contrat clair pour la répartition des responsabilités sur le Traitement des données

> Le RGPD prévoit expressément un partage de responsabilités du sous-traitant avec le Responsable de Traitement ; mais le Responsable de Traitement reste primo garant

→ **Nécessité de circonscrire précisément les rôles et responsabilités dans le contrat**

INCIDENCE SUR LES CONTRATS

Faut-il revoir tous nos contrats prestataires ?

> Pour les partenaires avec lesquels un professionnel de l'automobile échange/partage des Données Personnelles sur toute personne physique (clients, prospects, collaborateurs, etc.), il est impératif de compléter les contrats avec toutes les clauses relatives aux Données Personnelles traitées afin de s'assurer que chaque partie respecte toutes les obligations RGPD (→ pages 37 à 39 sur l'adaptation des contrats)

Quelles nouvelles clauses sont à intégrer dans les contrats de sous-traitance ?

> Le RGPD impose d'insérer un certain nombre de clauses pour fixer précisément les missions et obligations du Sous-Traitant a minima (→ page 38 sur la sous-traitance du Traitement des Données Personnelles)

> Penser à prévoir le sort des bases de données et données à l'issue du contrat de sous-traitance

Doit-on revoir les contrat de travail de nos collaborateurs ?

> Comme toute Personne Concernée, les collaborateurs et salariés doivent être informés de la nature des données collectées les concernant, de la finalité du Traitement de leurs données et de l'intégralité de leurs droits sur leurs Données Personnelles. Leur consentement doit être préalablement obtenu pour toute collecte de données sauf si elles sont nécessaires pour exercer toutes les obligations et droits que génère pour l'employeur le lien de dépendance *(exemple : informations nécessaires pour établir le bulletin de paie ou pour gérer les congés maladie, etc.)*

→ **nécessité de conserver les preuves des consentements sollicités des collaborateurs**

> Chaque entité est responsable de ses collaborateurs et doit leur faire respecter toutes les nouvelles obligations RGPD lorsqu'ils sont amenés à connaître et/ou traiter des Données Personnelles de tiers, en particulier l'obligation de confidentialité

→ **nécessité de leur rendre applicable et obligatoire la charte des Données Personnelles/politique de confidentialité par une clause insérée dans le contrat de travail + clauses Données Personnelles insérées dans le règlement intérieur de l'entreprise**

MENTIONS OBLIGATOIRES

Quelles sont les mentions obligatoires RGPD à intégrer aux CGV ?

> Voir pages 37 à 39 sur l'adaptation des contrats

Quelles sont les mentions obligatoires RGPD à intégrer aux formulaires de mes sites web ?

> **Entrepreneur individuel :** nom, prénom, domicile ; **pour une société :** raison sociale, forme juridique, adresse de l'établissement ou siège social, montant du capital social

> Activité commerciale : numéro d'inscription au registre du commerce et des sociétés (RCS) et numéro individuel d'identification fiscale, numéro de TVA intracommunautaire ; pour activité artisanale : numéro d'immatriculation au répertoire des métiers (RM)

> Adresse de courrier électronique joignable et consultée et numéro de téléphone

> Nom du « directeur de la publication » (entité/société pour le compte de laquelle est créé le site) et coordonnées de l'hébergeur du site (nom, dénomination ou raison sociale, adresse et numéro de téléphone du prestataire hébergeur)

> Pour site marchand (vente en ligne, etc.) : conditions générales de vente (CGV), prix (exprimé en euros et TTC), frais et date de livraison, modalités de paiement, service après-vente, droit de rétractation, durée de l'offre, coût de la technique de communication à distance

> + informations sur la politique de cookies le cas échéant

Quelles sont les mentions obligatoires RGPD à intégrer aux emails prospects ?

> Nécessité d'obtenir le consentement de la personne sollicitée par un acte positif clair :

→ **Nécessité de faire cliquer ou cocher une case pour poursuivre la prospection et les sollicitations + mention du droit au retrait du consentement à tout moment**

> **Identité et coordonnées** de l'organisme Responsable du Traitement + **coordonnées du pilote/point de contact pour les données ou délégué à la protection des données** de l'organisme s'il a été désigné

> **Finalités** : prospection commerciale

> **Rappel des tous les droits des Personnes Concernées** (accès, opposition, rectification, effacement, limitation, portabilité) + **droit d'introduire une réclamation** (plainte) auprès de la CNIL

> **Destinataires ou catégories de destinataires des données** : pour les concessionnaires qui collectent des données pour le constructeur, ne pas oublier de le mentionner

> **Durée de conservation des données** ou critères permettant de la déterminer

> **Existence d'une prise de décision automatisée ou d'un profilage** et informations utiles à compréhension de l'algorithme et sa logique + conséquences pour la personne

> **Renvoi à la charte des données/politique de confidentialité de l'entité**

Quelles sont les mentions obligatoires RGPD à intégrer aux emails clients ?

> Les mêmes que pour la question précédente, sauf pour le consentement :

- Pour un client auquel sont proposés des produits ou services similaires, **l'obtention du consentement n'est pas nécessaire ; mais il est obligatoire de l'informer qu'il peut retirer son consentement à tout moment**

CONSENTEMENTS

Les consentements obtenus avant le 25 mai 2018 sont-ils caducs ?

> Les consentements obtenus avant le 25 mai 2018 restent valables s'ils ont été sollicités avec les informations minimales préalables requises et si la Personne Concernée a été informée de ses droits. À défaut, il est recommandé de solliciter le consentement dès le premier contact après le 25 mai 2018.

La CNIL préconise-t-elle des modalités d'archivage des preuves obtenues ?

> Pas de modèle particulier préconisé par la CNIL pour l'archivage des consentements

> Un registre ou un espace dédié collectant tous les consentements est nécessaire et doit pouvoir être facilement consultable et régulièrement mis à jour

Peut-on/doit-on rajouter sur l'ordre de réparation/ ordre de travail un consentement ?

> Il est préférable de prévoir sur chaque document comportant mention de Données Personnelles, un paragraphe rappelant que le consentement est nécessaire et tous les droits de la Personne Concernée ainsi qu'un renvoi à la charte des données/politique de confidentialité de l'entité

Peut-on rajouter un consentement en annexe d'une facture ou d'un devis ?

> Il est toujours possible de faire figurer les mentions sur les données en annexe à un document mentionnant des Données Personnelles à la condition que l'annexe soit identifiée et attachée au document de façon claire

> Il est judicieux de faire mention et renvoi dans ses documents contractuels à la charte de Donnée Personnelles/ politique de confidentialité de son entité, voire de l'annexer

ET MOI DANS TOUT ÇA ?

La CNIL a-t-elle le droit de « fouiller » chez nous ?

> Les agents habilités de la CNIL peuvent, sur autorisation du juge des libertés et de la détention du tribunal de grande instance, accéder de 6 heures à 21 heures aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un Traitement de données à caractère personnel, à l'exclusion des parties de ceux-ci affectées au domicile privé pour l'exercice de leurs missions

> Lors d'un tel « contrôle sur place », l'objectif des agents contrôleurs est d'obtenir **« copie du maximum d'informations, techniques et juridiques, pour apprécier les conditions dans lesquelles sont mis en œuvre des Traitements de données à caractère personnel. »** Ils demandent donc des documents et ce de façon très large puisqu'il peut s'agir de tout document ayant trait aux Traitements des Données Personnelles: le registre des Traitements, tous contrats (locations de fichier, sous-traitance informatique, etc.), tous formulaires, tous dossiers papiers, toutes bases de données. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

> La CNIL peut aussi librement effectuer des contrôles en ligne sur les services accessibles au public et faire des constats à distance.

Quels sont les impacts RGPD sur l'emailing, le *marketing automation*, les *call centers* externes ?

> Dans tous les cas, *BtoB, BtoC,* le Responsable du Traitement doit faire respecter par tous ses prestataires, toutes les obligations et toutes les règles imposées par le RGPD et s'assurer de leur respect effectif

> **Nécessité de conclure un contrat précis par lequel il sera par exemple prévu que les prestataires vérifieront et respecteront toutes les règles de consentement, de blocage (Bloctel, etc.) et plus généralement toutes les dispositions du RGPD**

Je reçois de nombreux mails RGPD à titre personnel : pourquoi ?

> Attention à bien faire la distinction entre :

- Les mails et demandes légitimes tels que ceux tendant par exemple à l'obtention de votre consentement ou à vous informer sur la nouvelle politique de données et confidentialité mise en place dans leur organisme
- Les mails et demandes opportunistes, filous, voire arnaqueurs : certains usent et abusent du RGPD pour former des demandes ou imposer des obligations non prévues et non inscrites dans le RGPD et la législation française

➔ dans tous les cas, vérifiez et assurez-vous toujours de l'identité de l'expéditeur

Le RGPD impose des règles en matière de Données Personnelles, et non en matière de données de véhicule : ne pas transférer de Données Personnelles qui ne concernent pas la personne sollicitant ses propres Données Personnelles

POUR ALLER PLUS LOIN

Si vous souhaitez aller plus loin, et parce que l'applicabilité du RGPD est propre à chaque entreprise, le CNPA a négocié pour vous un accompagnement sur-mesure avec Midrange Consulting et le cabinet d'avocat 3DTIC, qui ont rédigé en collaboration ce guide.

L'incontournable

Des services clés en main à forfait minimal pour faciliter la conformité RGPD

> Registre de Traitements
- Fourniture d'un outil et/ou d'un modèle de cartographie
- Accompagnement technique et juridique

> Formation/sensibilisation à distance aux principaux concepts du RGPD

> Webinars d'actualités RGPD (conférence en ligne) semestriels

> Clauses juridiques « Données Personnelles » de base à intégrer dans les actes juridiques

> Guide des modes opérationnels de démarrage pour la mise en œuvre du RGPD

Contactez Midrange Consulting (demandez Natacha MONTROT)
au 01 34 40 95 00 ou par mail : rgpd@midrange-group.com
Contactez le cabinet 3DTIC avocats (Dominique DEDIEU)
au 06 78 69 69 38 ou par mail : dominiquededieu@3dtic.com

À la carte

Des services experts pour vous accompagner à tout moment et pour toutes mesures requises par la mise en conformité au RGPD

> Formations
- Formations au RGPD à la demande pour toutes problématiques

> Registre
- Assistance à l'élaboration et accompagnement dans l'inventaire de vos Traitements de Données Personnelles
- Audit technique et juridique du Registre élaboré

> Analyse de l'existant
- Examen de toute mesure RGPD technique et juridique existante
- Mesures des écarts techniques et juridiques
- Recommandations pour mise en conformité

> Mise en Conformité interne et externe
- Conseils et élaboration des documents juridiques RGPD :
  > *Politiques/charte Données de l'entreprise/du groupe*
  > *Documents relatifs aux salariés*
  > *Mentions obligatoires sur les Données figurant dans documents destinés au public (Conditions Générales, site Internet ...)*
  > *Élaboration/harmonisation de tous contrats (sous-traitance, cotraitance, partage, transfert de Données ...)*
- Guide de sécurisation des Données et Traitements

> Assistance et conseils permanents
- Hotline juridique et technique spécialisée RGPD *(selon plusieurs formules de hotline/abonnement)*
- Point de contact unique : prise en charge technique et juridique des demandes des Personnes Concernées par leurs Données, mise en œuvre du plan d'action adéquat

Les contributeurs

Ce guide a été rédigé sur la base d'ateliers participatifs, pour vous fournir des outils, une méthodologie, et des réponses concrètes aux questions que vous avez soulevées.

Ont contribué à ces ateliers : pour les concessionnaires VP, les groupes Gémy, Maurel, Jallu-Berthier, Nomblot, Féline Auto, Duffort ; pour les concessionnaires VI, le groupe Lenormant ; pour les loueurs, le groupe Sixt ; pour le contrôle technique, le groupe Autovision.
Les Métiers Carrossiers, Auto-écoles, Agents, SMAVA, 2 Roues, Recycleurs, Dépanneurs, Parcs de stationnement, ont également participé ou été sollicités.

Dominique DEDIEU
Avocate
+ 33 (0) 6 78 69 69 38
dominiquededieu@3dtic.com

Kozi VUTI
Directeur Général
+33 (0)6 21 28 43 72
kozi@vuti.fr

Création : Plotfox Production
Rédaction : Dominique Dedieu & Kozi Vuti
Crédits photos : Adobe Stock
Impression : Le Réveil de la Marne

CNPA

AGIR POUR VOTRE AVENIR

www.cnpa.fr