Deloitte. Legal | Taj Société d'avocats

Le RGPD et la gestion de flotte automobile

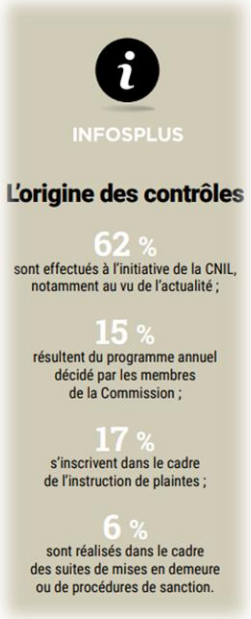
AMRAE, le jeudi 4 avril 2019

Hervé Gabadou, Deloitte Legal l Taj

Protection des données - préambule

Les contrôles, les plaintes, les sanctions

- **Les contrôles**

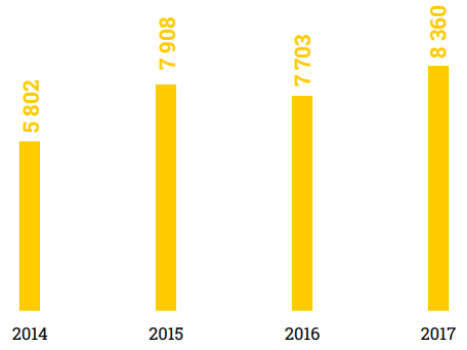


- En 2017, la CNIL a procédé à 65 contrôles en ligne et à près d'une vingtaine de contrôles sur pièces.
- La CNIL a réalisé une cinquantaine d'audits à l'occasion du Sweep Day.

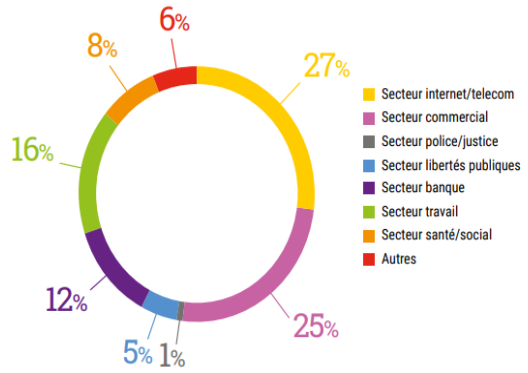
- **Les plaintes**

- En 2017, la CNIL a reçu 8 360 plaintes : un nombre record.
- Les plaintes concernent principalement les secteurs internet/ téléphonie et commerce qui représentent à eux deux 52 % des plaintes reçues.

Évolution du nombre de plaintes depuis 2014



Répartition des plaintes par secteur d'activité 2017



- **Les sanctions**

© 2019 Deloitte Legal I Taj

Sommaire

01 **Les changements**

02 **Les principaux repères**

03 **Q&A**

© 2019 Deloitte Legal I Taj

01

Les changements

© 2019 Deloitte Legal l Taj

Panorama des principaux changements

Pour les individus l'empowerment

Pour les entreprises, l'accountability

Renforcement des droits des individus

Le consommateur devient « ***Consom'acteur*** »

Suppression des formalités déclaratives

Les entreprises doivent être en mesure de **rendre compte** à tout moment de l'effectivité de la protection

Renforcement des pouvoirs de sanctions

Amende d'un montant de 2% du CA HT mondial ou 10 millions d'euros voire, dans les cas les plus graves, une amende pouvant atteindre 4% du CA HT mondial ou 20 millions d'euros

Premières sanctions: les cas Google et Facebook

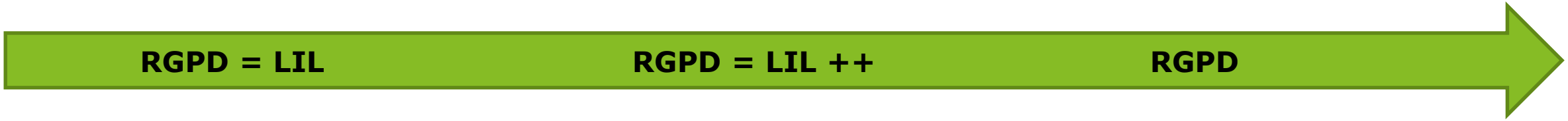
Un changement de paradigme!

© 2019 Deloitte Legal I Taj

RGPD : panorama des principaux changements

Les obligations du RT préexistantes renforcées

→ **Encadrer les transferts de données**
→ **Assurer la sécurité du traitement**
→ **Garantir les droits des personnes**
→ **Recueil du consentement** (mais nouvelle définition)



Les obligations du RT maintenues

→ **Respect du principe de finalité**
→ **Respect du principe de proportionnalité** (= minimisation)
→ **Limitation de la durée de conservation des données**
→ **Obligation d'information des personnes**

Création de nouvelles obligations pour le RT et le ST

→ **Garantir les nouveaux droits des personnes concernées** (droit à l'effacement, droit à la limitation du traitement, droit à la portabilité des données)
→ **Notifier les failles de sécurité dans les 72 heures**
→ **Etablir un registre des activités de traitement**
→ **Désigner un DPO**
→ **Mener une étude d'impact**
→ **Documenter sa conformité** (accountability)

© 2019 Deloitte Legal I Taj

02

Les principaux repères

- Qui ?
- Quoi ?
- Pourquoi faire ?
- Où ?
- Jusqu’à quand ?
- Comment ?

© 2019 Deloitte Legal l Taj

Qui sont les principaux acteurs ?

Qui ?

Gestionnaire de flotte

Loueur de véhicules

Courtier

Assureur

Autres partenaires (expert, gestionnaire de sinistres, avocat…)

Qualification juridique des acteurs

- ✓ Responsables de traitement
- ✓ Sous-traitants
- ✓ Destinataires
- ✓ Responsables de traitement conjoint

Qualification !

© 2019 Deloitte Legal I Taj

Quelles sont les obligations des acteurs ?

Obligations des responsables de traitement

- **Obligation de mise en œuvre des mesures techniques et organisationnelles appropriées** pour s'assurer et être en mesure de démontrer la conformité au RGPD

Obligations des sous-traitants

- **Obligation de transparence et de traçabilité**
- **Obligation de la protection des données dès la conception ou par défaut**
- **Obligation de garantir la sécurité des données** traitées
- **Obligation d'assistance, d'alerte et de conseil**

Obligations des responsables de traitement et des sous-traitants

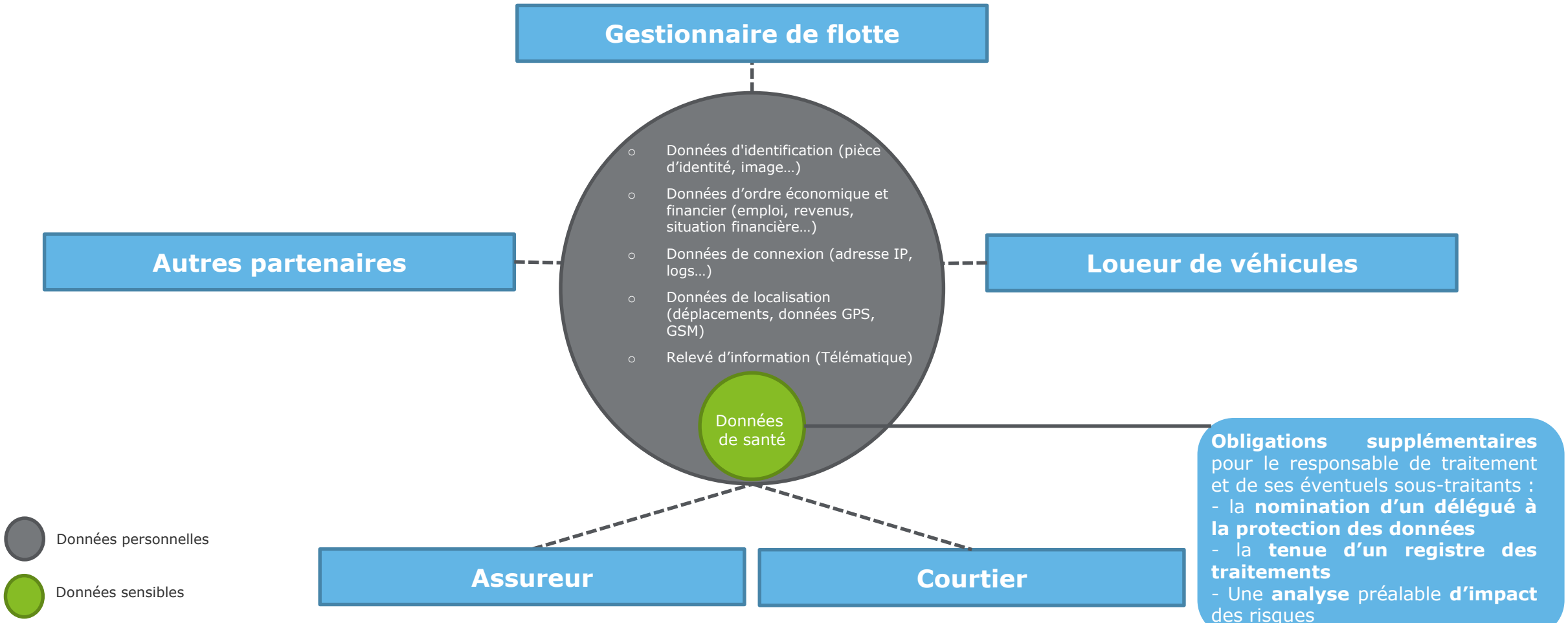
- Principe d'accountability
- Principe de minimisation
- Privacy by design/by default
- Principe de transparence
- Principe d'intégrité, de confidentialité et de résilience

Obligation de sécurité des données à la charge du responsable de traitement y compris lorsque les données sont confiées à des sous-traitants, tous deux étant **solidairement responsables**

© 2019 Deloitte Legal I Taj

Quelles sont les catégories de données traitées ?

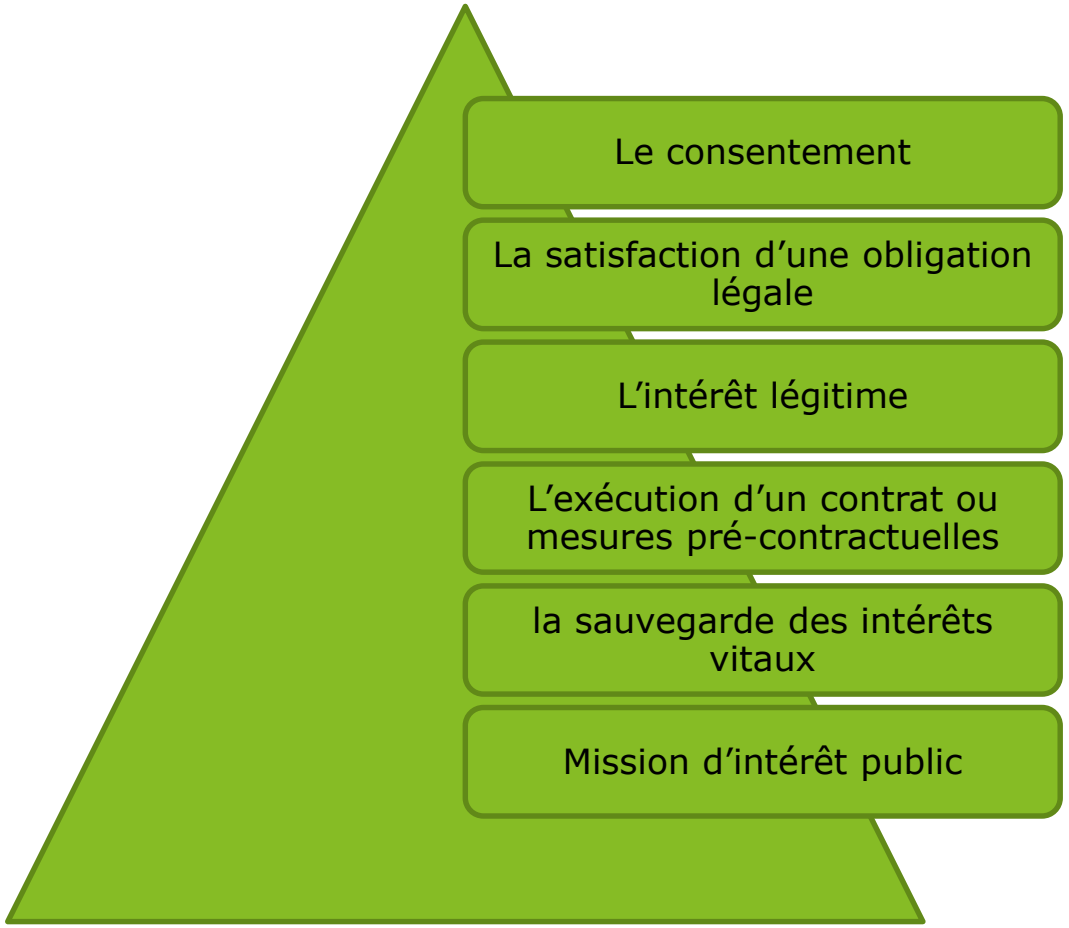
Quoi ?



© 2019 Deloitte Legal I Taj

Quelle est la base juridique du traitement ?

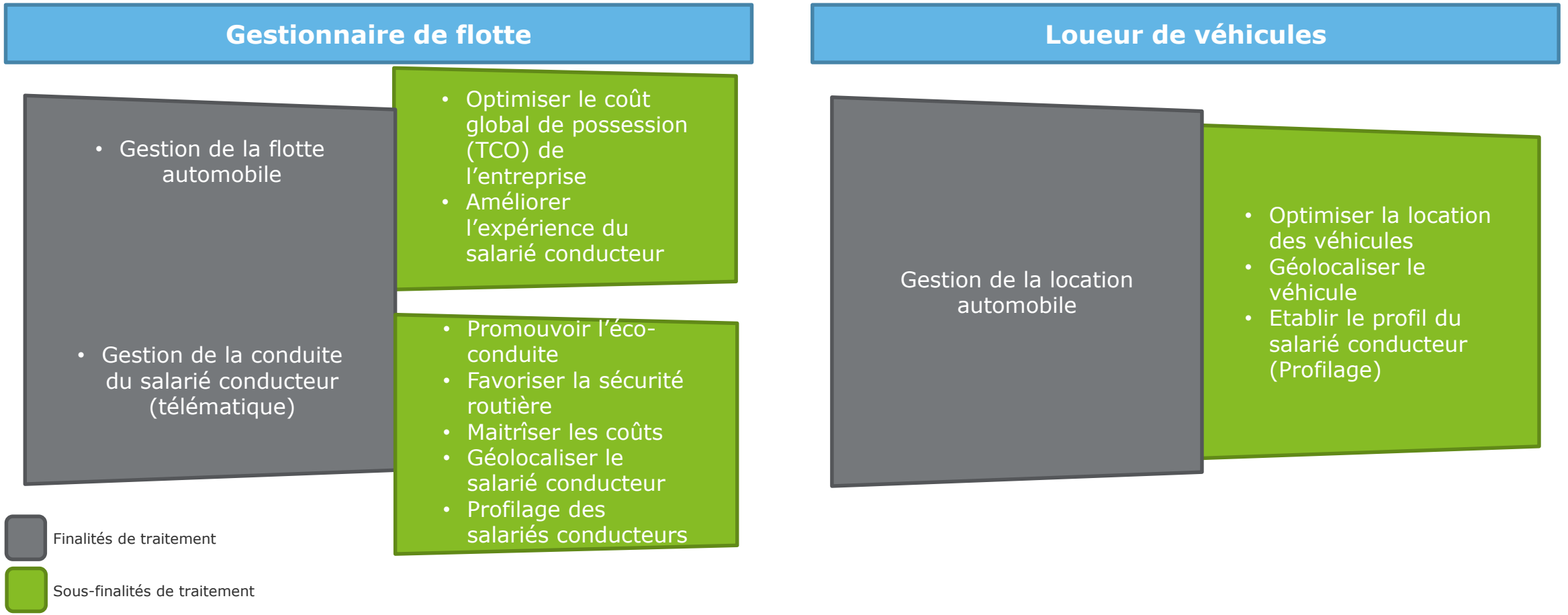
Quoi ?



© 2019 Deloitte Legal I Taj

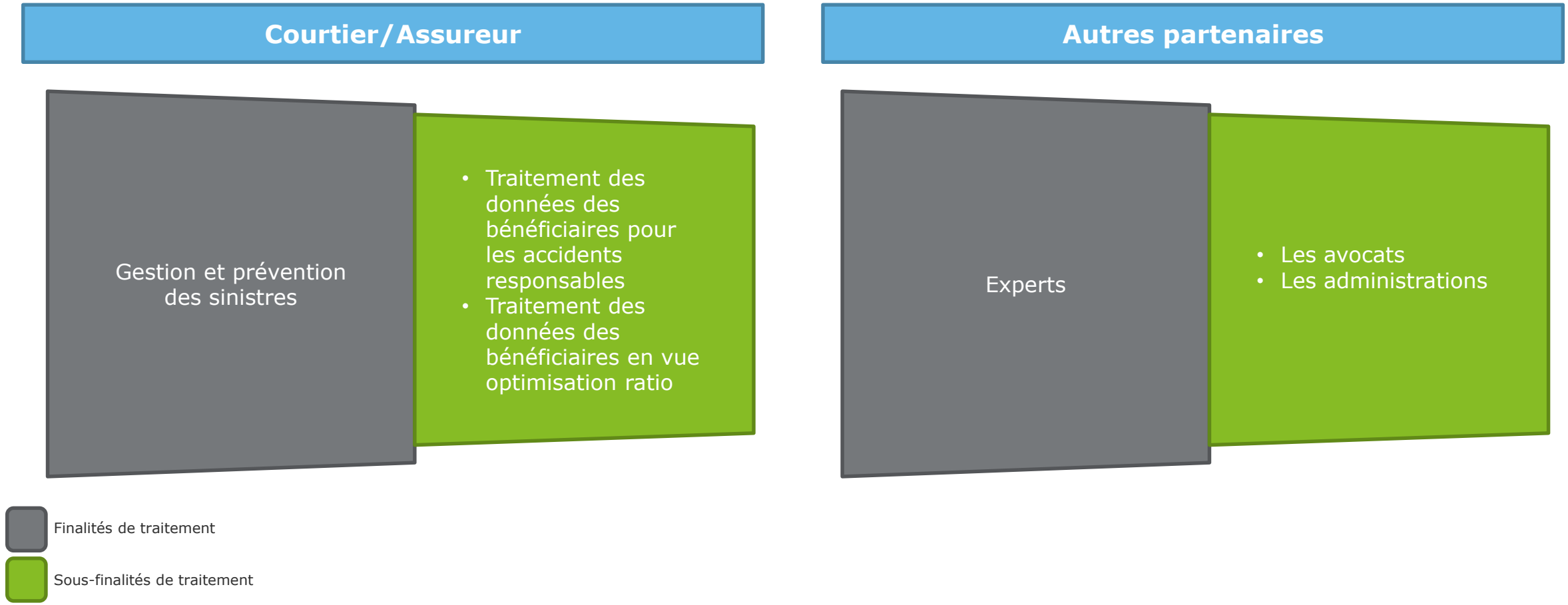
Quelles sont les finalités de traitement de données ?

Pourquoi faire ?



© 2019 Deloitte Legal I Taj

Quelles sont les finalités du traitement des données ?



© 2019 Deloitte Legal I Taj

Où sont hébergées les données ?

Où ?

Pays membres de l'Union Européenne ou de l'Espace Economique Européen, pays adéquat ou présentant des garanties appropriées

Pays tiers

© 2019 Deloitte Legal I Taj

Quelle est la durée de conservation des données ?

Jusqu'à quand ?

Données d'identification, d'ordre économique et financier et de connexion : **5 ans à compter du terme du contrat de prêt du véhicule**

Données de localisation : **2 mois à compter de la collecte de ces données**

Données de profilage : **durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**

Données de santé : **durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées**

Données personnelles

Données sensibles

© 2019 Deloitte Legal I Taj

Comment documenter la mise en conformité ?

Comment ?

LA DOCUMENTATION SUR LES TRAITEMENTS DE DONNÉES PERSONNELLES

- ✓ **Le registre des traitements**
- ✓ **Les analyses d'impact sur la protection des données** (DPIA)
- ✓ **L'encadrement des transferts de données** hors de l'Union Européenne

L'INFORMATION DES PERSONNES

- ✓ Les **mentions d'information**
- ✓ Les **modèles de recueil du consentement** des personnes concernées
- ✓ Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- ✓ **Les contrats avec les sous-traitants et les co-responsables de traitement**
- ✓ **Les procédures internes en cas de violations de données**
- ✓ **Les preuves que les personnes concernées ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base
- ✓ **Les flux de données** en dehors de l'Union Européenne

© 2019 Deloitte Legal I Taj

Que faire en cas de faille de sécurité ?

Documenter en interne la faille en déterminant :

- la **nature de la violation**;
- si possible, les **catégories** et le nombre approximatif **de personnes concernées** par la violation;
- les **catégories** et le nombre approximatif **d'enregistrements de données** à caractère personnel concernés;
- décrire les **conséquences** probables **de la violation de données** ;
- décrire les **mesures prises** ou que vous envisagez de prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Si la faille présente un **risque** :
obligation de notifier à la CNIL

Si la faille présente un **risque élevé** :
obligation de notifier à la CNIL et à la personne concernée

Notification de la faille de sécurité à la Cnil dans les **72 heures** à compter de la constatation de la violation et à la **personne concernée** dans les **meilleurs délais**

Le **sous-traitant informe immédiatement** le **responsable de traitement si** les **instructions documentées constituent** selon lui une **violation du RGPD ou si** une **faille de sécurité se produit**

© 2019 Deloitte Legal I Taj

Les nouveaux droits

© 2019 Deloitte Legal I Taj

03

Q&A

© 2019 Deloitte Legal l Taj

Vos contacts

Hervé Gabadou

Avocat Associé

+33 1 55 61 65 56

hgabadou@taj.fr

Hervé assiste ses clients dans la structuration juridique de leur informatique et de leurs projets numériques (politique contractuelle, sécurisation juridique des actifs immatériels, réflexes en matière de sécurité et de confidentialité des données personnelles, spécifications juridiques d'un projet informatique pour un secteur réglementé).

Il maîtrise également les questions associées à la protection des données personnelles dans un contexte national et international, gère les relations auprès de la CNIL et fournit toute son assistance dans le cadre d'audits de conformité à la loi Informatique, fichiers et libertés et au Règlement Européen en matière de Protection des Données personnelles (RGPD).

Hervé a été chargé d'enseignement en DESS de Méthodes expertales et arbitrales en informatique et techniques associées à Paris II.

Il a également été en charge d'un groupe de travail e-santé au sein d'une association qui regroupe les industries de santé.

Enfin, il a présidé le comité Outsourcing de l'association internationale ItechLaw et a été un des membres fondateurs de l'Outsourcing Law Group regroupant des cabinets d'avocats indépendants étrangers, leaders dans ce domaine.

Droit de l'informatique : les expertises de Taj

Contrats et marchés informatiques

Signature électronique, Informatique et Libertés

Réseaux et Internet

© 2019 Deloitte Legal I Taj

Deloitte. Legal | Taj Société d'avocats

A propos de Taj
Taj est l'un des premiers cabinets d'avocats français, spécialisé en stratégies fiscales et juridiques internationales. Il compte aujourd'hui 545 professionnels parmi lesquels 62 associés, basés à Paris, Bordeaux, Lille, Lyon et Marseille. Ses expertises les plus réputées couvrent la fiscalité internationale et les prix de transfert, les fusions acquisitions, la fiscalité indirecte, le contrôle fiscal et contentieux, la fiscalité de la mobilité internationale, le droit social, le droit des affaires et des entreprises en difficulté. Taj est une entité du réseau Deloitte et s'appuie sur l'expertise de 44 000 juristes et fiscalistes de Deloitte situés dans 150 pays.
Pour en savoir plus, www.taj.fr ou www.taj-strategie.fr

A propos de Deloitte
Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited, société de droit anglais (« private company limited by guarantee »), et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes. Pour en savoir plus sur la structure légale de Deloitte Touche Tohmatsu Limited et de ses cabinets membres, consulter www.deloitte.com/about. En France, Deloitte SA est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.
Pour en savoir plus, www.deloitte.com/about

© 2019 Deloitte Legal I Taj

Annexe I

Glossaire

- **Responsable de traitement** : personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

- **Sous-traitant** : personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

- **Destinataire** : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

- **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

© 2019 Deloitte Legal I Taj

Annexe I

Glossaire

- **Données sensibles** : informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

- **Données de santé** : données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

- **Consentement** : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

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

- **Limitation du traitement** : le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

© 2019 Deloitte Legal I Taj

Annexe I

Glossaire

- **Traitement transfrontalier** :

plusieurs

a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans États membres;

b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

- **Violation de données à caractère personnel** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

© 2019 Deloitte Legal I Taj