LSIX
LAW FIRM

DONNES PERSO. & CSI

Licence professionnelle Sécurité des biens et des personnes
2023 - 2024

Monsieur KARPIEL

Les données personnelles que je traite dans mon quotidien ?

Me concernant (à titre privé) : ……

……

Dans le cadre de mon travail (à titre professionnel) :

……

Pourquoi protéger les données personnelles ? (si je n'ai rien à me reprocher ?)

. . . . . .

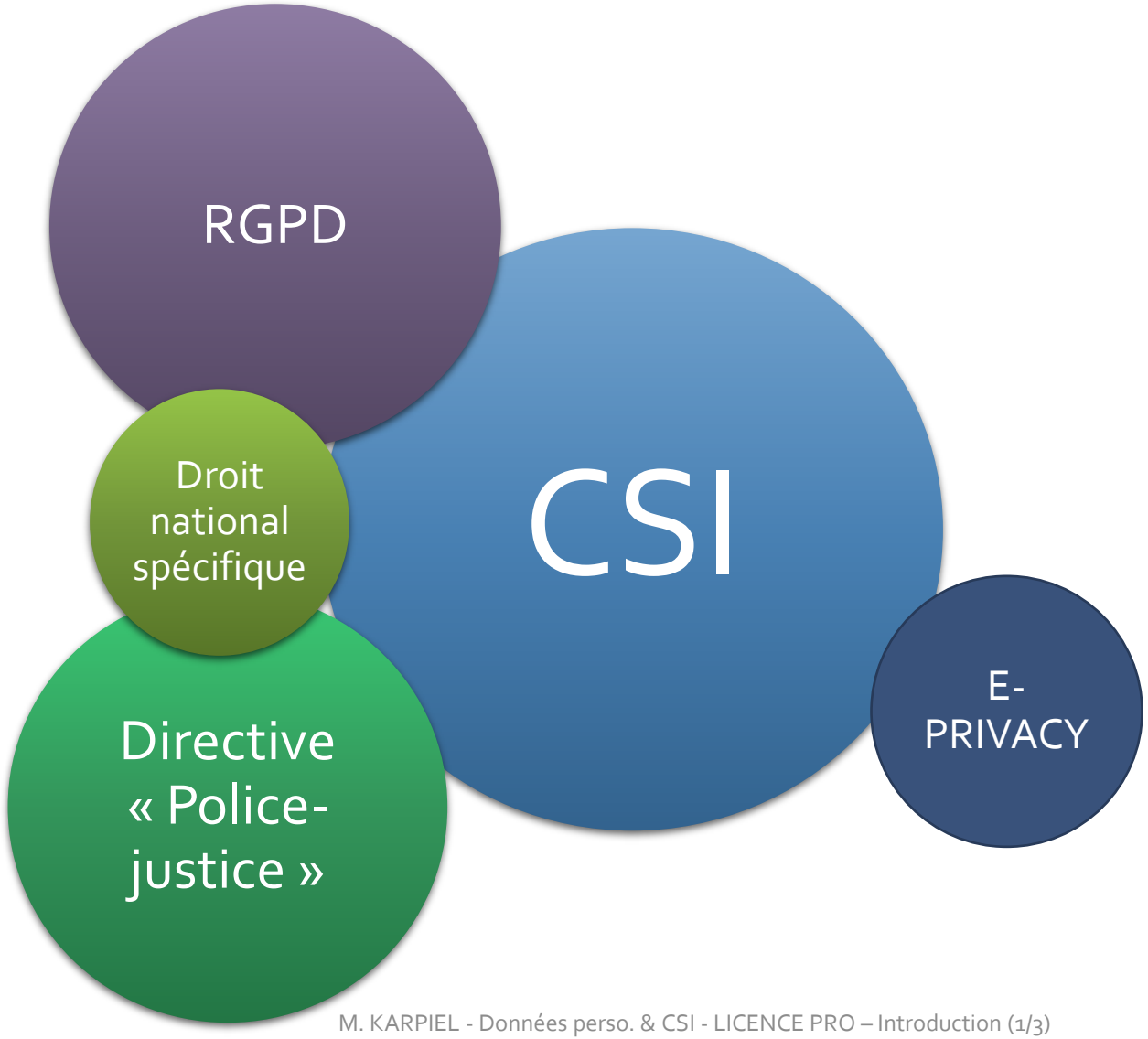
. . . . . .

. . . . . .

. . . . . .

CSI & données personnelles

Introduction 1/3



INTRODUCTION.

- La France premier état européen à se doter d'une législation spécifique en protection des données à caractère personnel.
  → Polémiques autour du projet SAFARI d'interconnexion des fichiers (Le Monde, mars 1974)
- Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive européenne n°95/46/CE du 24 octobre 1995
- **Une évolution nécessaire ?**

  ……

  …… → RGPD

4 principales sources de textes

- **RGPD** = Règlement 2016/679 adopté le 27 avril 2016 & abroge la directive 95/46
  → Harmonisation des législation nationales car **directement applicable** dans l'ordre interne depuis le 25 mai 2018

- DPJ : traitement des DP par les autorités compétentes à des fins prévention et de détection des infractions pénales / enquêtes / poursuites / d'exécution de sanctions pénales / menaces sécurité publique / prévention des menaces.

4 principales sources de textes

- Droit national

→ Les traitements mis en œuvre pour assurer la sûreté de l'Etat ou encore la défense nationale ne relèvent pas du champ d'application de l'Union européenne et restent régis par les dispositions de la seule loi « **Informatique et Libertés** ».

.....

.....

.....

.....

4 principales sources de textes

- Le 10 janvier 2017, la Commission européenne publie une proposition de règlement **« E-Privacy »**

→ Objectif abroger la directive 2002/58 du 12 juillet 2002 et harmoniser la législation des États membres en matière de confidentialité des communications électroniques.

→ « *faire en sorte que les services numériques soient plus sûrs et suscitent davantage de confiance* »

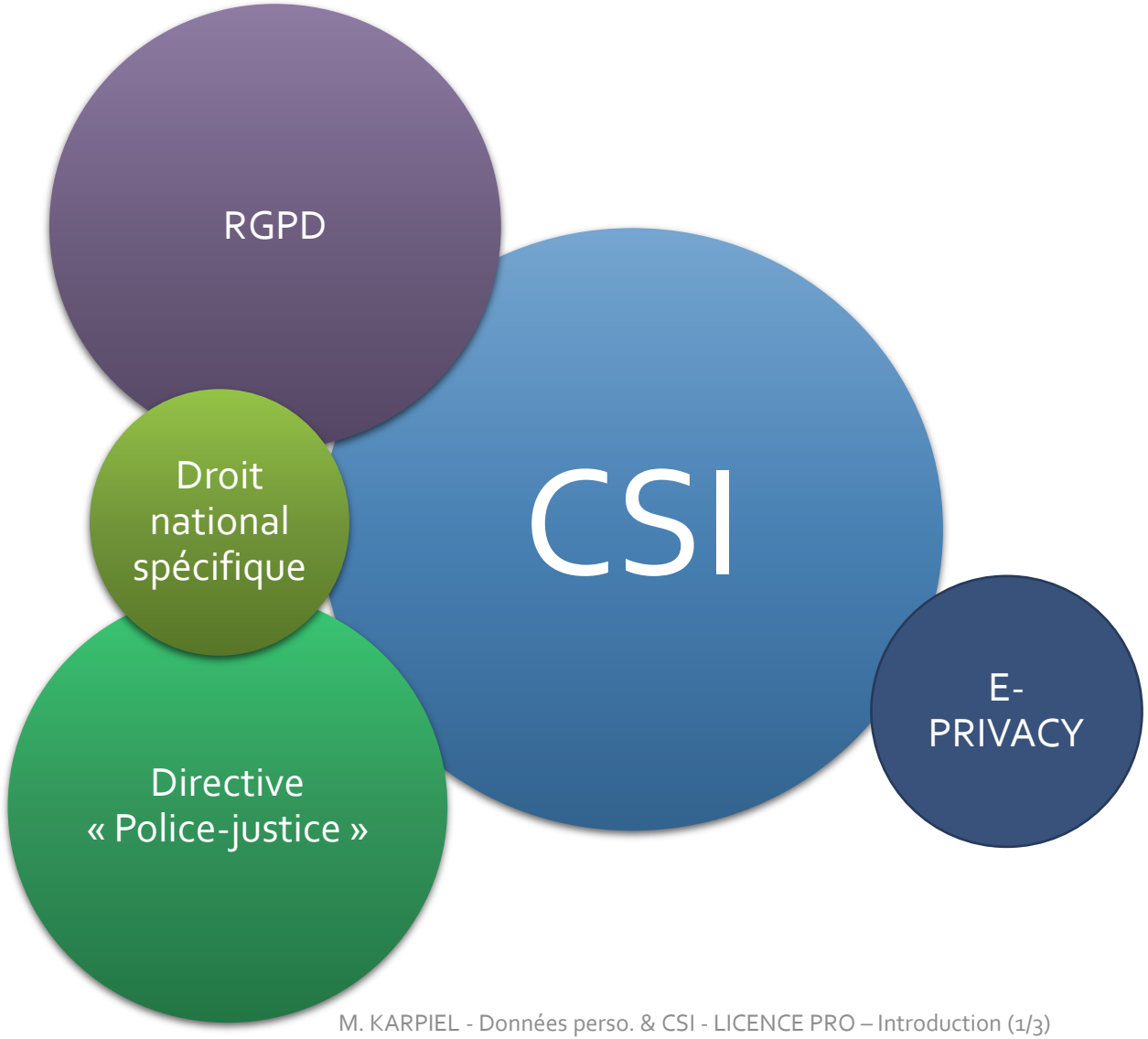
……

……

……

CSI & données personnelles

Introduction 1/3



DEF : Donnée personnelle

- Toute information se rapportant à une personne physique <u>identifiée</u> :
  - ❖ **Directement**

  ……

  - ❖ **Indirectement**

  voix, image, adresse postale, ……

  ……

DEF : Donnée personnelle

- Toute information se rapportant à une personne physique <u>identifiable</u> :
  - ❖ **à partir d'une seule donnée**

  .....

  - ❖ **à partir du croisement d'un ensemble de données**

  .....

DEF : Traitement de données personnelles

- Opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (*collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement*). :

❖ **Exemple**

Tenue d'un fichier des mains courantes, ……

Collecte……

Mise à jour……

Informatisé ou papier ?

DEF : Traitement de données personnelles

- Doit avoir un objectif, une **finalité**.
- Doit être **légal, légitime et proportionné** au regard de votre activité professionnelle.

- **Impossible de collecter ou traiter des données personnelles :**

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

DEF : Traitement de données personnelles

Exemple : *dans l'entreprise CONFORME_DP un service s'occupe de la paie.*

- Finalité principale : ……
  - ❖ Sous-finalité 1 : ……
  - ❖ Sous-finalité 2 : ……
  - ❖ Sous-finalité 3 : ……

DEF : Responsable de traitement

Celui qui détermine les finalités et les moyens du traitement.
Il décide du « pourquoi » les données sont traitées.
Il a des obligations :

.....

.....

.....

.....

.....

Registre des activités de traitement (Art. 30 du RGPD) ?

1. Chaque responsable du traitement «…» tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, « … », du représentant du responsable du traitement et du délégué à la protection des données;
b) les finalités du traitement;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;
e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, « … »
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

2. Chaque sous-traitant «…» tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) b) c) d) …

3. Les registres « …» sous une forme écrite y compris la forme électronique.

4. « *doit être* …» à la disposition de l'autorité de contrôle sur demande.

5. Les obligations visées aux paragraphes 1 et 2 ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données « … »

Registre des activités de traitement – responsable Traitement

I. RGPD

I.1. Périmètre du RGPD?

S'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne,
- ou que son activité cible directement des résidents européens.

Exemple :

.....

.....

.....

.....

.....

I.2. Les grands principes du RGPD

- Finalité : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime.

Ce principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur.

Exemples de finalité : gestion des recrutements, gestion des paies, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

I.2. Les grands principes du RGPD

- Proportionnalité et pertinence : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;

Exemples de données non pertinentes ou excessives au regard de la finalité :

- Le recueil d'informations sur la situation professionnelle de l'entourage d'un candidat n'est pas pertinent dans un fichier de recrutement
- Le numéro de carte d'identité n'est pas nécessaire pour la délivrance d'un extrait d'acte d'état civil
- Le numéro de sécurité sociale n'est pas utile pour l'inscription à l'école ou aux activités périscolaire

Attention aux champs libres et aux zones commentaires

I.2. Les grands principes du RGPD

- Durée de conservation limitée : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité ;

Le cycle de vie de la donnée en 3 phases (diapo suivantes) :

1. Conservation en base active
2. Archivage intermédiaire
3. Archivage définitif

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée

1. Conservation en base active

Il s'agit de la durée nécessaire à la réalisation de l'objectif (finalité du traitement) ayant justifié la collecte/enregistrement des données. Par exemple, dans une entreprise, les données d'un candidat non retenu seront conservées pendant 2 ans maximum (sauf s'il en demande l'effacement) par le service des ressources humaines.

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée

2. Archivage intermédiaire

Les données personnelles ne sont plus utilisées pour atteindre l'objectif fixé (« dossiers clos ») mais présentent encore un intérêt administratif (ex : gestion d'un éventuel contentieux, etc.) ou doivent être conservées pour répondre à une obligation légale (par exemple, les données de facturation doivent être conservées dix ans même si la personne concernée n'est plus cliente). Les données peuvent alors être consultées de manière ponctuelle et motivée par des personnes spécifiquement habilitées ;

I.2. Les grands principes du RGPD

Le cycle de vie de la donnée

3. Archivage définitif

En raison de leur « valeur » et intérêt, certaines informations sont archivées de manière définitive et pérenne.

À la différence de la conservation en base active, les deux dernières étapes ne sont pas systématiquement mises en place. Leur nécessité doit être évaluée pour chaque traitement, et, pour chacune de ces phases, un tri sera opéré entre les données.

I.2. Les grands principes du RGPD

Exemple de durées de conservation

Durées de conservation des données à caractère personnel

(Maj mars 2018)

Le présent document a pour objet de référencer les différentes durées de conservation des données à caractère personnel traitées dans le cadre des activités de l'entité.

Ces durées de conservation peuvent être déterminées par la loi (code du travail, code monétaire et financier…) ou par la CNIL. A défaut, le Règlement européen sur la protection des données personnelles (GDPR) prévoit que la durée de conservation des données personnelles doit être limitée à une période strictement nécessaire à la réalisation des objectifs pour lesquels les données ont été collectées.

Finalité du traitement	Durée de conservation	Fondement juridique
Communication externe		
Données nécessaires à la gestion d'un site internet (identité des visiteurs, données de connexion…)	1 an	DI-007 Article 3 du décret n° 2011-219 du 25 février 2011
Gestion d'un fichier client	Les données des clients sont conservées au maximum pendant le temps de la relation commerciale. Elles peuvent être conservées à des fins de prospection commerciale au maximum pendant 3 ans à compter de la fin de cette relation commerciale (par exemple, à compter d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou du dernier contact émanant du client).	NS-048
Constitution et gestion d'un fichier de prospects non client (ex : envoi de sollicitations tels que l'emailings, appels téléphoniques, télécopies, SMS, etc.)	Au maximum 3 ans à compter de leur collecte par le responsable de traitement ou à compter du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel) Attention : l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect	NS-048
Statistiques de mesures d'audience Les informations stockées dans le terminal des utilisateurs (ex : cookies) ou tout autre élément utilisé pour identifier les utilisateurs et permettant de les tracer	13 mois au maximum	NS-048

1

I.2. Les grands principes du RGPD

- Principe de sécurité et de confidentialité : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;

I.2. Les grands principes du RGPD

Exercice : Dispositif biométrique de pointage des heures de travail dans un commerce alimentaire

Finalité : …

Proportionnalité et pertinence : …

Durée de conservation limitée : …

Confidentialité : …

Sécurité : …

I.2. Les grands principes du RGPD

❑ Les droits des personnes (développé sur plusieurs diapos)

Les personnes concernées par des traitements de données personnelles disposent de droits leur permettant de garder la maîtrise des informations les concernant.

Le responsable de fichier doit expliquer aux personnes concernées la procédure (où, comment et à qui s'adresser ?) permettant de les exercer concrètement.

Le responsable du fichier dispose d'un délai d'un mois pour répondre aux demandes (exception à 2 mois).

I.3. RGPD et DROITS des personnes

RÉCAPITULATIF DES NOUVEAUX DROITS

Intitulé	Définition	Complexité
droit d'accès	demander la confirmation ou infirmation que ses données font l'objet d'un traitement, et en demander l'accès (dont types de traitement et finalités)	moyenne
droit de rectification	demander la rectification de ses données	moyenne
droit à l'effacement	demander l'effacement de ses données dans les meilleurs délais	faible
droit à la limitation du traitement	demander la limitation du traitement de ses données (ou le non-effacement)	moyenne
droit à la portabilité des données	recevoir sur demande ses données personnelles dans un format structuré, utilisé et lisible pour le transmettre éventuellement à un nouveau responsable de traitement	forte
droit d'opposition	s'opposer au traitement de ses données (dont profilage)	faible
droit au refus d'une décision sur traitement automatisé	refuser de faire l'objet d'une prise de décision fondée uniquement sur un traitement automatisé	moyenne
droit d'informations de collectes et traitements de données	être informé de la collecte, conservation, et exploitation de ses données pour une finalité précise	forte

I.3. RGPD et DROITS des personnes

Le droit à l'information

Pour être loyale et licite, la collecte de données personnelles doit s'accompagner d'une information claire et précise des personnes sur :

- l'identité du responsable du fichier ;
- la finalité du fichier ;
- le caractère obligatoire / facultatif des réponses et des conséquences d'un défaut de réponse ;
- les destinataires des données ;
- leurs droits (droit d'accès, de rectification, et d'opposition) ;
- les éventuels transferts de données vers des pays hors UE.

I.3. RGPD et DROITS des personnes

Le droit d'opposition

Les personnes doivent pouvoir s'opposer à la réutilisation par le responsable du fichier de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat. Une case à cocher, non cochée par défaut, doit leur permettre d'exprimer leur choix directement sur le formulaire ou le bon de commande à remplir. La simple mention de l'existence de ce droit dans les conditions générales n'est pas suffisante.

Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale (ex : fichiers des impôts).

I.3. RGPD et DROITS des personnes

Les droits d'accès et de rectification

Toute personne peut :
- accéder à l'ensemble des informations la concernant,
- connaître l'origine des informations le concernant,
- accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant (par exemple, les éléments qui auraient servi pour ne pas vous accorder une promotion ou le score attribué par une banque et qui a conduit au rejet de votre demande de crédit),
- en obtenir la copie (des frais n'excédant pas le coût de la reproduction peuvent être demandés)
- exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

I.3. RGPD et DROITS des personnes

Les droits d'accès et de rectification

Par écrit : courrier postal, accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.

Sur place : avec présentation d'une pièce d'identité. Il est possible de se faire accompagner par la personne de son choix. La consultation doit durer suffisamment longtemps pour prendre note commodément et complètement. Il est possible de demander une copie des données.

1 mois pour répondre à compter de la date de réception de la demande.

I.3. RGPD et DROITS des personnes

Les limites au droit d'accès

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

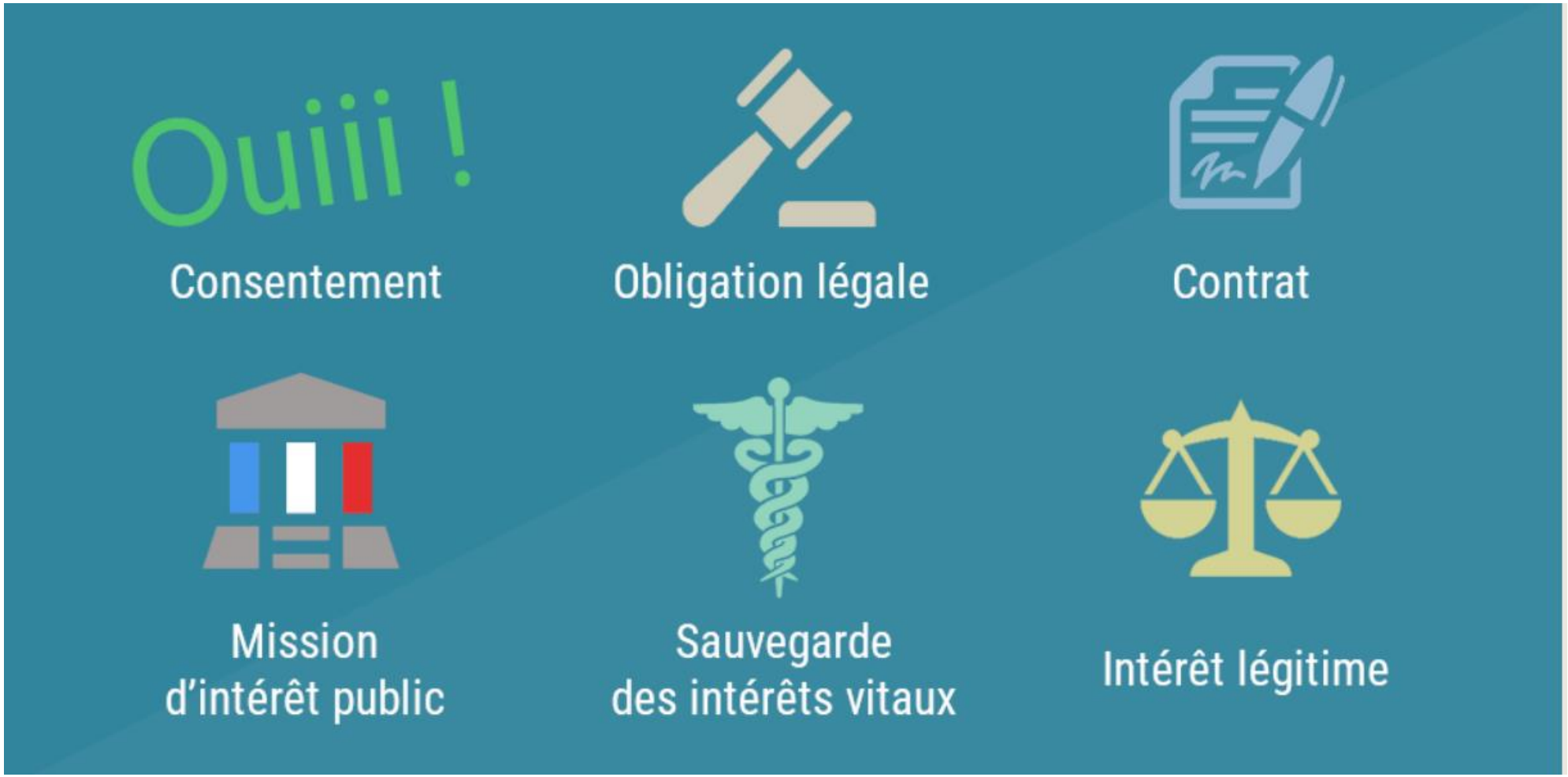
. . . . . .

I.4. Bases de traitements

La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de collecter ou d'utiliser des données personnelles.
On peut également parler de « fondement juridique » ou de « base juridique » du traitement.
Six bases légales sont prévues par le RGPD :

- le consentement ;
- le contrat ;
- l'obligation légale ;
- la sauvegarde des intérêts vitaux ;
- l'intérêt public ;
- les intérêts légitimes.

I.4. Bases de traitements



I.4. Bases de traitements

La base contractuelle

Le contrat est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale suppose que le traitement soit objectivement nécessaire à l'exécution d'un contrat entre l'organisme traitant les données et les personnes concernées.

I.4. Bases de traitements

Le consentement

Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée (préalablement à la collecte).
Dans un formulaire en ligne (une case à cocher non cochée par défaut).

- en cas de collecte de données sensibles
- de réutilisation des données à d'autres fins
- d'utilisation de cookies pour certaines finalités
- d'utilisation des données à des fins de prospection commerciale par voie électronique

I.4. Bases de traitements

L'obligation légale

L'obligation légale est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale se justifie lorsque la mise en œuvre d'un traitement est imposée à un organisme par des textes européens ou nationaux.

I.4. Bases de traitements

L'intérêt public

La mission d'intérêt public est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale se justifie en particulier pour les traitements mis en œuvre par les autorités publiques aux fins d'exécuter leurs missions.

Ex. services des impôts

I.4. Bases de traitements

L'intérêt légitime

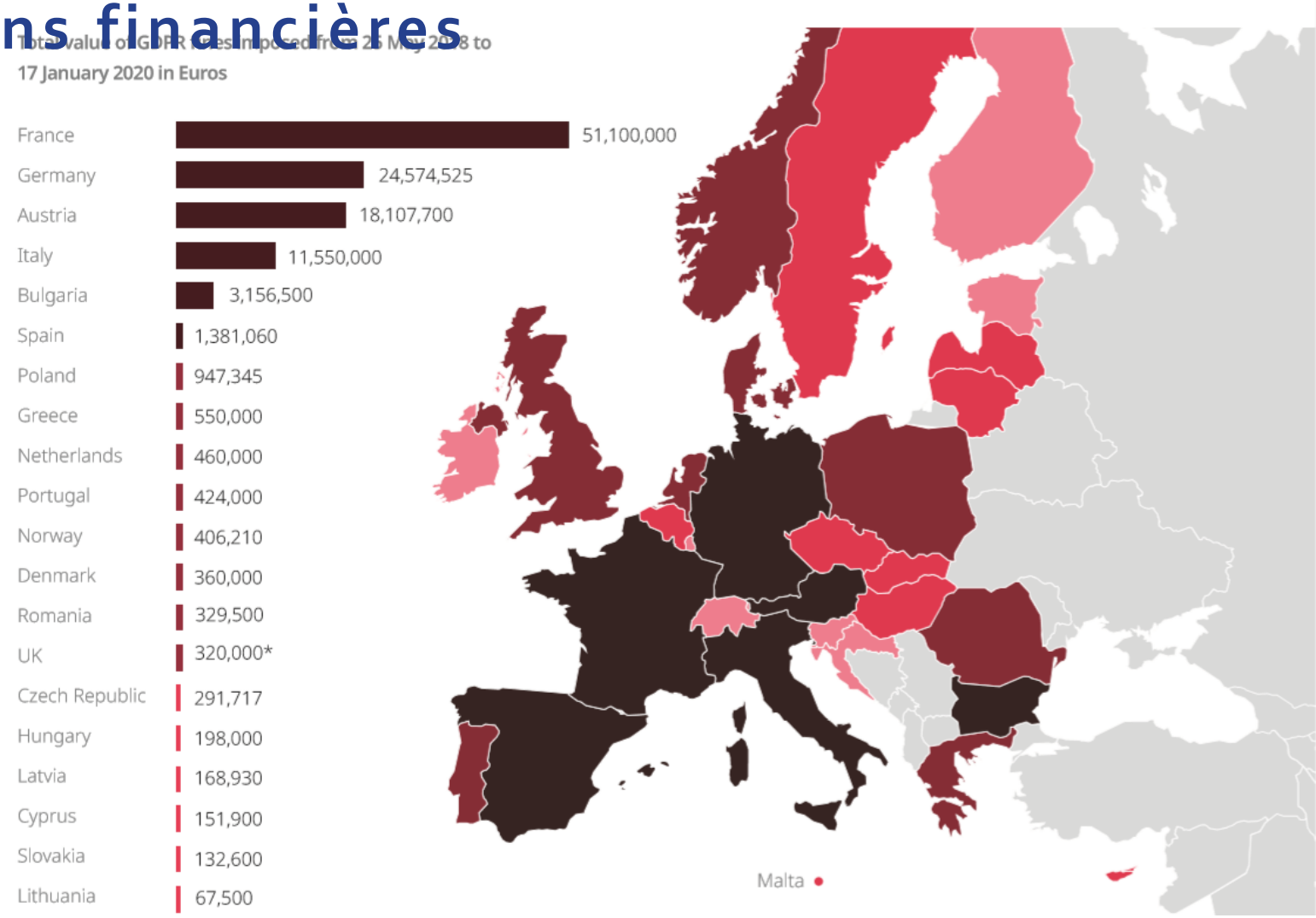
L'intérêt légitime est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale suppose que les intérêts (commerciaux, de sécurité des biens, etc.) poursuivis par l'organisme traitant les données ne créent pas de déséquilibre au détriment des droits et intérêts des personnes dont les données sont traitées.

I.4. Bases de traitements

Sauvegarde des intérêts vitaux

Il s'agit d'une base juridique dont l'utilisation est limitée étant donné qu'il faut démontrer d'une part qu'il y a un intérêt vital en jeu et d'autre part qu'un traitement de données est nécessaire pour sauvegarder cet intérêt.
En ce qui concerne l' "intérêt vital", le considérant 46 du RGPD précise qu'il s'agit d'un "intérêt essentiel à la vie" de la personne concernée ou d'une autre personne physique. L'application est donc limitée à des situations qui menacent la vie. L'application la plus évidente est la situation où une personne est victime d'un accident et, étant gravement blessée, elle est admise dans un hôpital alors qu'elle est inconsciente et qu'elle n'est pas en état de donner son consentement pour le traitement de ses données en vue de son traitement. Le traitement en vue d'un traitement médical planifié préalablement ne relève pas du champ d'application de cette base juridique.

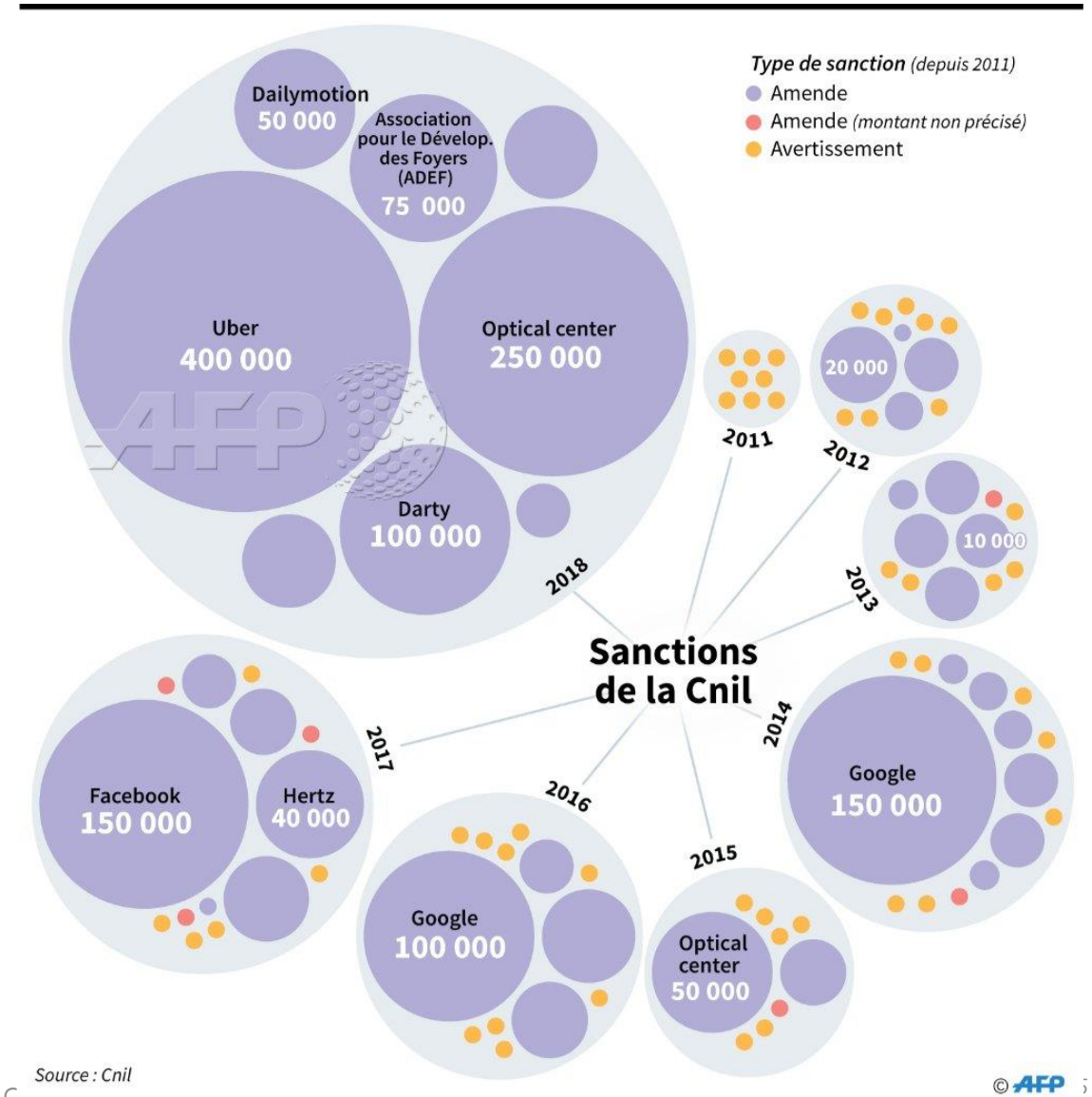
II.1. Sanctions financières



Sanctions de la CNIL

Amendes

Google	50 000 000€ (en contestation)
Uber	400 000€
Bouygues Telecom	250 000€
Optical Center	250 000€



II.2 Sanctions pénales

Art. 226-16

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 3° du III de l'article 20 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

II.2 Sanctions pénales

Art. 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Art. 226-18-1

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

II.2 Sanctions pénales

Art. 226-20

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

II.2 Sanctions pénales

Art. 226-21

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Art. 226-18-1

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

III. Violation de données

Violation de données

Tous les organismes qui traitent des données personnelles doivent mettre en place des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu'une violation cause des dommages ou des préjudices aux organismes comme aux personnes concernées.

Articles 33 et 34 du RGPD

- prévenir toute violation de données
- réagir de manière appropriée en cas de violation, c'est-à-dire mettre fin à la violation et minimiser ses effets.

III. Violation de données

Un incident

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

Exemples :
suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ;
perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société ;
introduction malveillante dans une base de données scolaires et modification des résultats obtenus par les élèves.

III. Violation de données

L'article 4.12) du RGPD

Une violation de données à caractère personnel comme
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.

III. Violation de données

Procédures

La mise en place de mesures visant à détecter immédiatement une violation, à l'endiguer rapidement, à analyser les risques engendrés par l'incident et à déterminer s'il convient de notifier l'autorité de contrôle, voire les personnes concernées.

III. Violation de données

Procédures

Pour les personnes concernées, la violation engendre :	aucun risque	un risque	un risque élevé
Documentation interne, dans le « registre des violations »	X	X	X
Notification à la CNIL, dans un délai maximal de 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

III. Violation de données

Registre des violation

Le registre des violations devrait notamment contenir les éléments suivants :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

III. Violation de données

Information des personnes concernées

La notification aux personnes concernées doit a minima contenir et exposer, en des termes clairs et précis, les éléments suivants :

- la nature de la violation ;
- les conséquences probables de la violation ;
- les coordonnées de la personne à contacter (DPO ou autre) ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation.

FIN