RGPD :
zones de risque et litiges potentiels

Marie Soulez

Avocat à la cour

Lexing Alain Bensoussan Avocat

Directeur du département Propriété intellectuelle contentieux

Introduction

- Le RGPD encadre les nouveaux modes d'utilisation des données par les entreprises sans freiner leur développement économique

- Il répond à l'aspiration générale d'augmentation du niveau de protection des données

- Ce nouvel encadrement s'accompagne nécessairement de nouvelles contraintes et de nouvelles règles à respecter, et d'un renforcement des sanctions

→ Nécessité de se mettre en conformité dès à présent pour anticiper son entrée en vigueur au 25 mai 2018

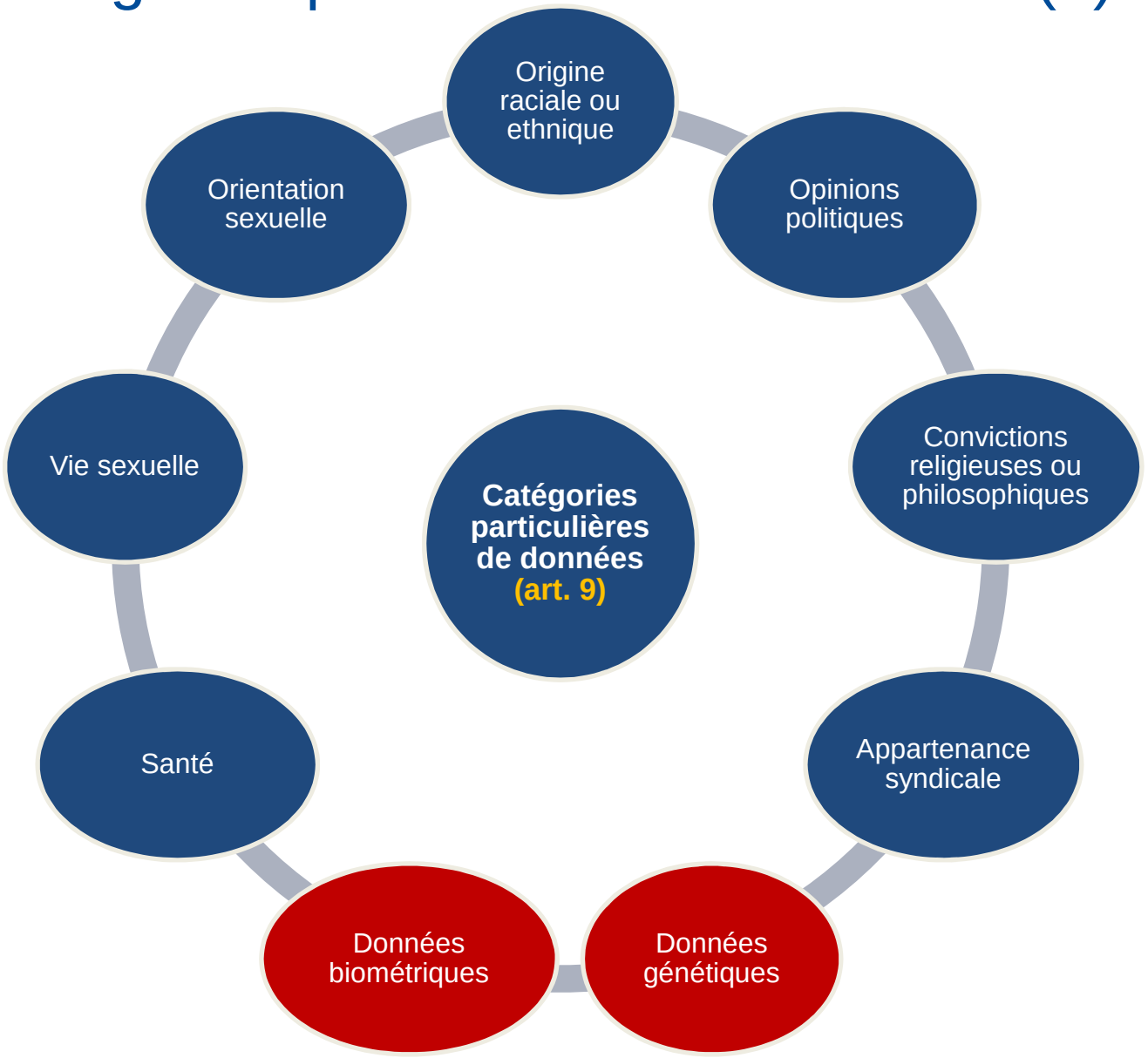
Plan

1. Identification des zones de risque
2. Le droit au recours
3. Les sanctions
4. Anticiper les risques
5. La procédure devant la Cnil

1. Identification des zones de risque

1. Catégories particulières de données
2. Transfert de données hors UE
3. Respect des droits des personnes

1.1 Catégories particulières de données (1)



1.1 Catégories particulières de données (2)

- Consentement explicite de la personne concernée
- Exécution des obligations et de l'exercice des droits propres au responsable de traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale
- Sauvegarde des intérêts vitaux de la personne concernée
- Fondation, association ou tout autre organisme à but non lucratif
- Données rendues publiques par la personne concernée
- Constatation, exercice ou défense d'un droit en justice
- Motifs d'intérêt public important
- Médecine préventive ou médecine du travail, appréciation de la capacité de travail du travailleur, diagnostics médicaux, prise en charge sanitaire ou sociale, gestion des systèmes et des services de soins de santé ou de protection sociale
- Motifs d'intérêt public dans le domaine de la santé publique
- Archives dans l'intérêt public

1.1 Catégories particulières de données (3)

- Nouveauté du RGPD : en raison de la qualité des données et en particulier lorsqu'il s'agit de catégories particulières de données, des obligations particulières peuvent s'imposer

- Exemples :
  - une analyse d'impact
  - l'avis de la Cnil

1.2 Transferts de données hors UE ou vers des organisations internationales (1)

- Principe (art. 44 à 48) :

Transferts assortis d'une décision relative au caractère adéquat du niveau de protection	Transferts moyennant des garanties appropriées
Transfert libre (Ø d'autorisation particulière)	Transfert libre (Ø d'autorisation particulière) **seulement si des garanties appropriées sont mises en œuvre** : - Instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics - Règles d'entreprises contraignantes (BCR) - Clauses types de protection des données - Code de conduite ou mécanisme de certification approuvé - Clauses contractuelles types (subordonnées à l'autorisation préalable d'une autorité de contrôle)

Obligation générale d'information renforcée des personnes concernées

1.2 Transferts de données hors UE ou vers des organisations internationales (2)

Dérogations (art. 49) :

- Consentement de la personne concernée
- Transfert nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée
- Transfert nécessaire à la conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et une autre personne physique ou morale
- Transfert nécessaire pour des motifs importants d'intérêt public
- Transfert nécessaire à la constatation, l'exercice ou la défense de droits en justice
- Transfert nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes quand la personne concernée est dans l'incapacité de donner son consentement
- Transfert a lieu au départ d'un registre destiné à fournir des informations au public et est ouvert à la consultation du public

1.2 Transferts de données hors UE ou vers des organisations internationales (3)

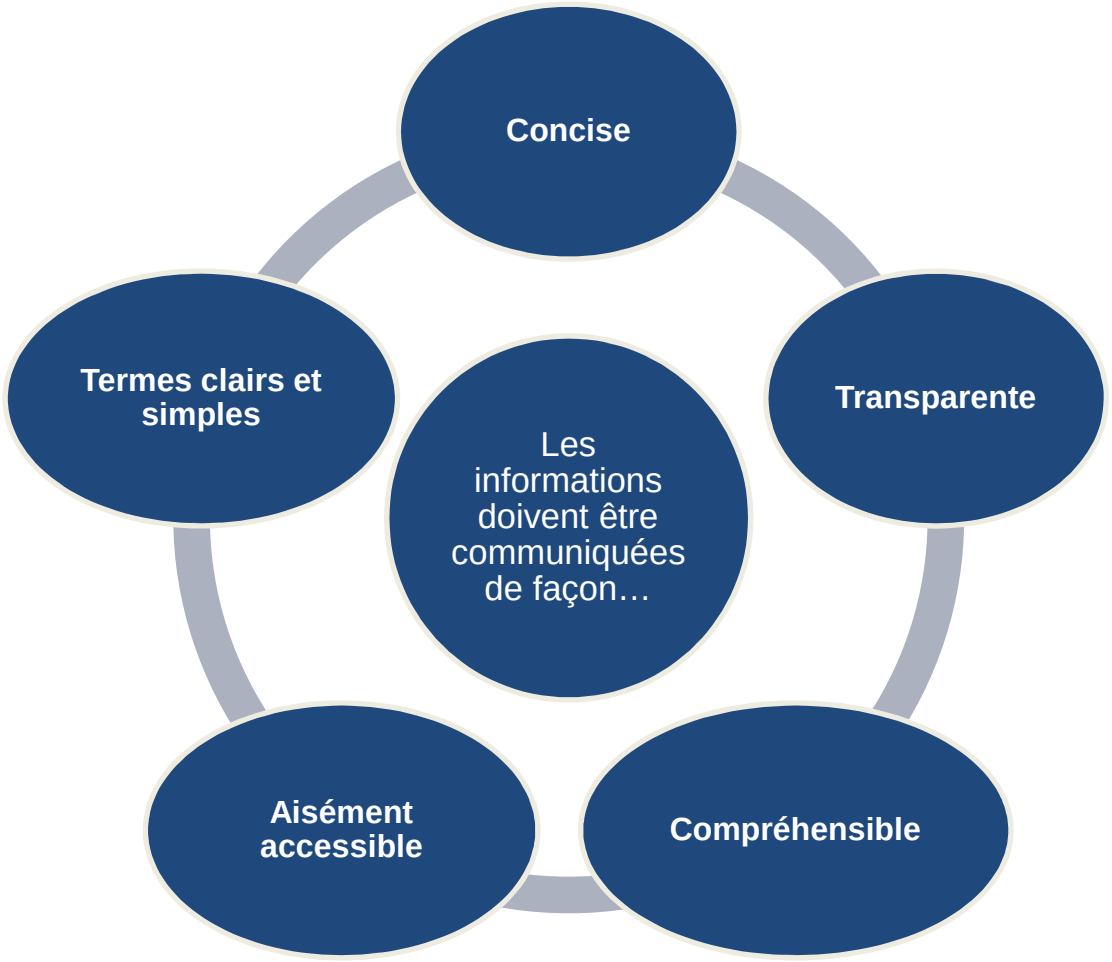
Zoom sur le *Privacy Shield* (accord de transfert des données personnelles vers les Etats-Unis) :

- CJUE, 6 octobre 2015, *Schrems* : annulation de la décision d'adéquation du *Safe Harbor*
- 12 juillet 2016 : adoption du *Privacy Shield* et décision d'adéquation de la Commission européenne
- 4 grandes garanties pour les activités des services de renseignements américains :
  - Traitement fondé sur des règles claires, précises et accessibles
  - L'Etat doit démontrer la nécessité et la proportionnalité de ses activités de renseignement
  - Un système de supervision et de contrôle indépendant effectif et impartial
  - Un droit pour les individus de faire valoir ses droits devant un organe indépendant

Risque non négligeable de remise en cause du *Privacy Shield* qui fait face à de nombreuses critiques : Data Rights Ireland a d'ailleurs intenté une action devant les tribunaux européens afin de faire annuler la décision d'adéquation du *Privacy Shield*

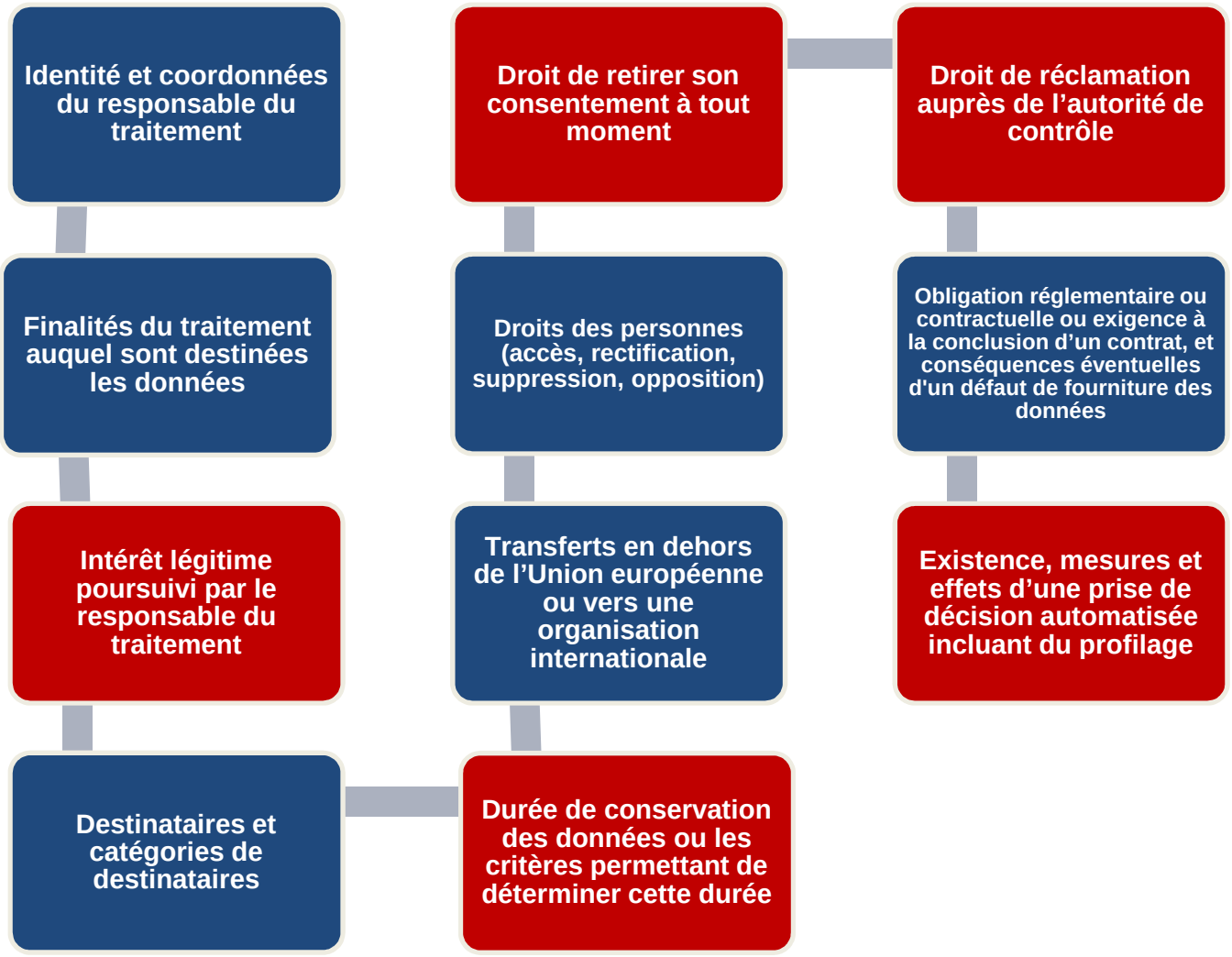
1.3 Respect des droits des personnes (1)

Le droit à la compréhension (art. 12)



1.3 Respect des droits des personnes (2)

Droit à l'information renforcé (art. 13)



1.3 Respect des droits des personnes (3)

Droit à l'oubli et à l'effacement (art. 17)

Obligation d'effacer les données d'une personne dans les cas suivants

- Les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées
- La personne concernée retire le consentement sur lequel est fondé le traitement et aucun fondement légal n'existe
- La personne concernée s'oppose au traitement et il n'existe aucun motif légitime supérieur pour le responsable de traitement
- Les données ont fait l'objet d'un traitement illicite
- Il existe une obligation légale d'effacer les données à laquelle est soumis le responsable du traitement
- Les données ont été collectées dans le cadre de l'offre de services de la société de l'information pour des enfants âgés de moins de 16 ans

1.3 Respect des droits des personnes (4)

Droit à l'oubli et à l'effacement (suite)

Exceptions quand le traitement est nécessaire

- À l'exercice de la liberté d'expression et d'information
- Au respect d'une obligation légale de traiter les données et à laquelle le responsable du traitement est soumis
- Pour des motifs d'intérêt public dans le domaine de la santé publique
- À des fins d'archivage dans l'intérêt public ou à des fins de recherche scientifique ou historique, ou à des fins statistique
- À la constatation, l'exercice ou la défense des droits en justice

1.3 Respect des droits des personnes (5)

Droit à la portabilité (art. 20)

La personne concernée a le droit de transmettre à un responsable de traitement les données à caractère personnel la concernant préalablement fournies à un autre responsable de traitement

Dans un format structuré qui est couramment utilisé et lisible par machine (« machine-readable »), sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle

Lorsque le traitement est fondé sur le consentement ou sur un contrat et que le traitement est réalisé par des moyens automatisés

L'exercice de ce droit ne fait pas obstacle à l'exercice du droit à l'oubli, à l'effacement des données et aux droits et libertés de tiers

2. Le droit au recours

1. Droit de recours des personnes devant une autorité
2. Responsabilité
3. Recours de la personne concernée
4. Action de groupe

2.1 Droit de recours des personnes devant une autorité

Droit à un recours effectif en cas de traitement de données de la personne concernée en violation du règlement	• Régime complet de responsabilité du responsable de traitement et du sous-traitant
Action extrajudiciaire (autorité de contrôle)	• Violation du règlement par un traitement de données concernant la personne
Action judiciaire	• Recours contre la décision d'une autorité de contrôle • Recours contre resp. ou sous-traitant : Lien de causalité entre un fait générateur et un dommage matériel ou moral

2.2 Responsabilité

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement peut obtenir réparation dans sa totalité auprès de responsable de traitement ou du sous-traitant.

Objectif : réparation effective et intégrale

Partage des responsabilités :

Le responsable de traitement qui participe au traitement est responsable du dommage causé par une violation du règlement

Le sous-traitant n'est responsable que s'il n'a pas respecté les obligations du règlement qui incombent spécifiquement aux sous-traitants ou s'il a agi en dehors des instructions du responsable de traitement

Exonération si l'un ou l'autre prouve que le fait qui a provoqué le dommage ne lui est pas imputable

Possibilité de réclamer auprès des autres responsables de traitement ou sous-traitants la part de la réparation correspondant à leur part de responsabilité dans le dommage

2.3 Recours de la personne concernée (1)

Réclamation auprès d'une autorité de contrôle (art. 77)

Quoi ?

- Le droit pour la personne concernée d'introduire une réclamation auprès d'une autorité de contrôle (sans préjudice de tout autre recours administratif ou juridictionnel)

Pourquoi ?

- En cas de traitement de données à caractère personnel de la personne concernée constituant une violation du règlement

Où ?

- Autorité de contrôle de l'Etat membre dans lequel se trouve la résidence habituelle de la personne concernée, son lieu de travail ou le lieu où la violation aurait été commise

2.3 Recours de la personne concernée (2)

Recours juridictionnel (art. 78)

Droit à un recours juridictionnel effectif en cas de traitement de données de la personne concernée en violation du règlement

Mécanisme d'action directe de la personne concernée à l'encontre du responsable de traitement ou du sous-traitant

Juridiction de l'Etat membre dans lequel le responsable de traitement ou le sous-traitant dispose d'un établissement ou dans lequel la personne concernée a sa résidence habituelle

2.4 Action de groupe

Art. 91 de la Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle (ajoute un l'article 43 ter à la Loi Informatique et libertés)

« II. – Lorsque plusieurs personnes physiques placées dans une situation similaire subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions de la présente loi par un responsable de traitement de données à caractère personnel ou un sous-traitant, **une action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente.**

III. – Cette action tend exclusivement à la cessation de ce manquement.

IV. – Peuvent seules exercer cette action :

1° Les associations régulièrement déclarées depuis cinq ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ;

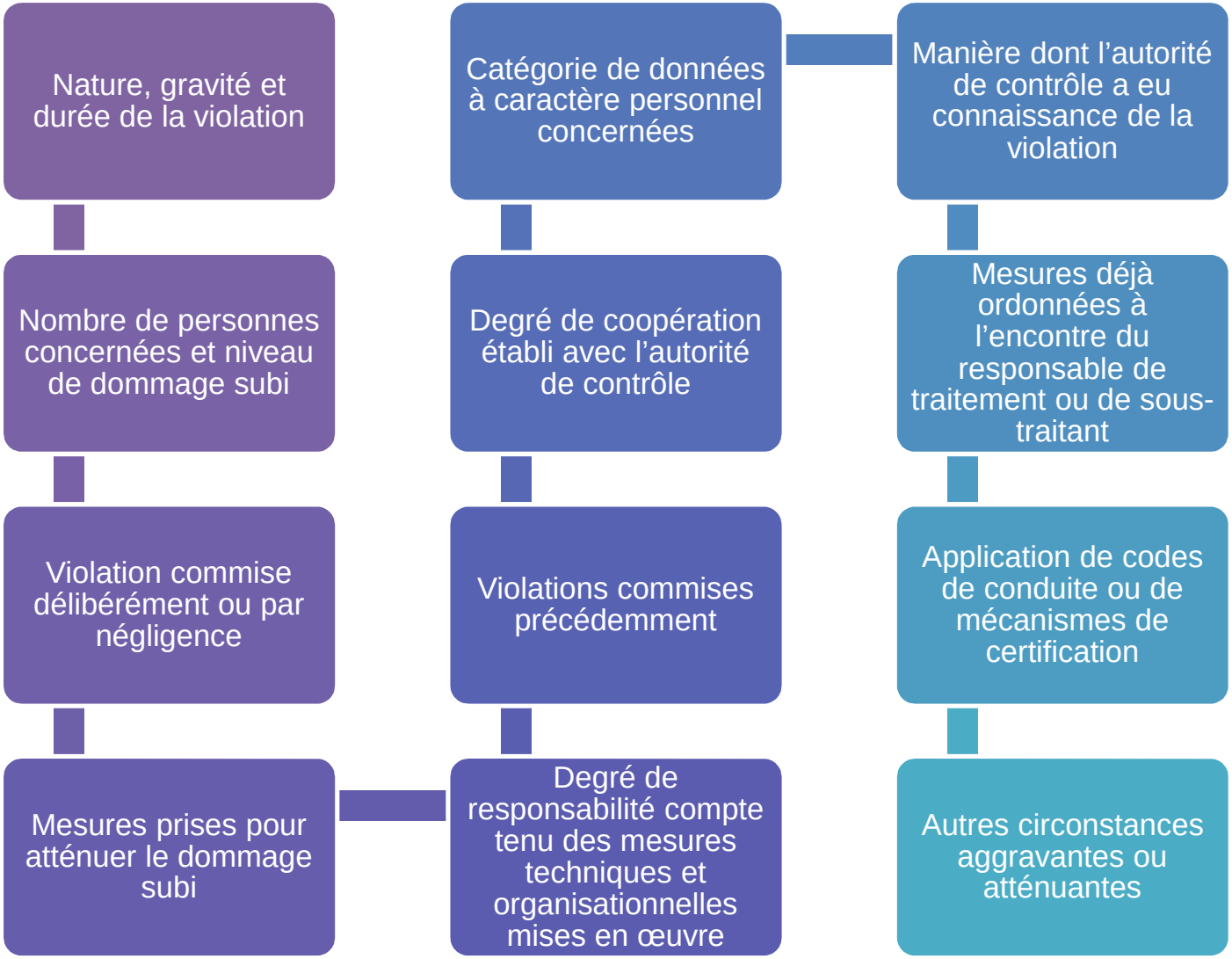
2° Les associations de défense des consommateurs représentatives au niveau national et agréées en application de l'article L. 811-1 du code de la consommation, lorsque le traitement de données à caractère personnel affecte des consommateurs ;

3° Les organisations syndicales de salariés ou de fonctionnaires représentatives au sens des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du code du travail ou du III de l'article 8 bis de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ou les syndicats représentatifs de magistrats de l'ordre judiciaire, lorsque le traitement affecte les intérêts des personnes que les statuts de ces organisations les chargent de défendre. »

3. Les sanctions

1. Eléments pris en compte
2. Causes et montant des sanctions

3.1 Eléments pris en compte



3.2 Causes et montants des sanctions

-Absence de protection des données dès la conception et protection des données par défaut

- Absence de représentant établi dans l'Union
- Absence de registre des activités de traitement
- Absence de coopération avec l'autorité de contrôle
- Absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation des données
- Absence d'analyse d'impact

10.000.000 €
ou
2 % du CA
annuel
mondial

- Non respect des principes de base d'un traitement (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.)
- Non-respect du droit des personnes
- Non-respect des règles relatives aux transferts de données à caractère personnel

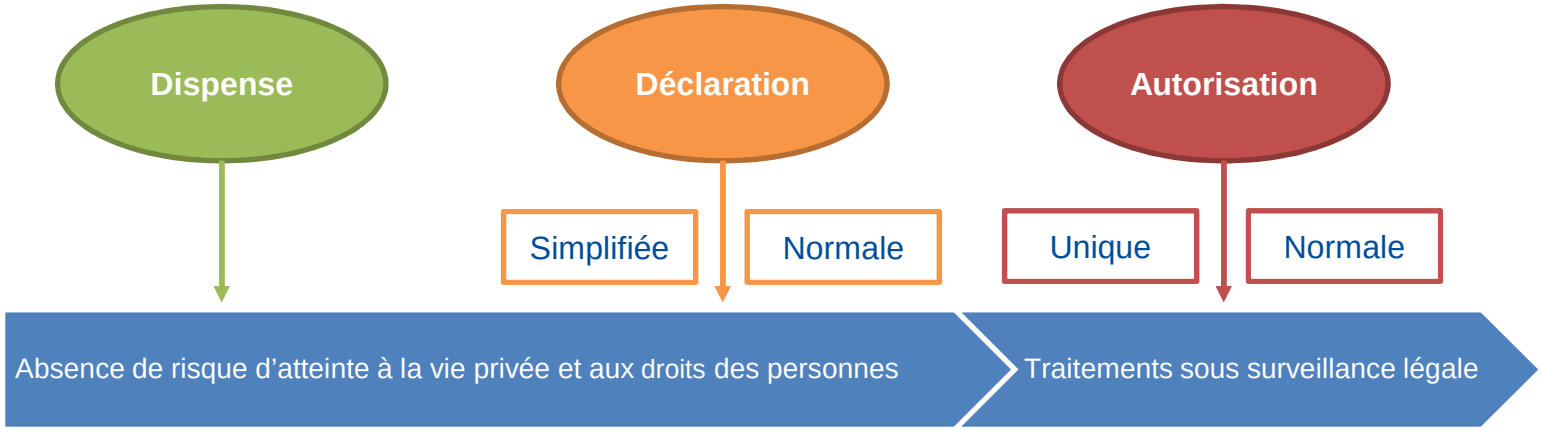
20.000.000 €
ou
4 % du CA
annuel
mondial

4. Anticiper les risques

1. Anticiper la disparition des formalités déclaratives
2. Effectuer une analyse d’impact

1.1 Anticiper la disparition des formalités

Aujourd'hui :



Avec le RGPD : principe général de disparition des formalités déclaratives

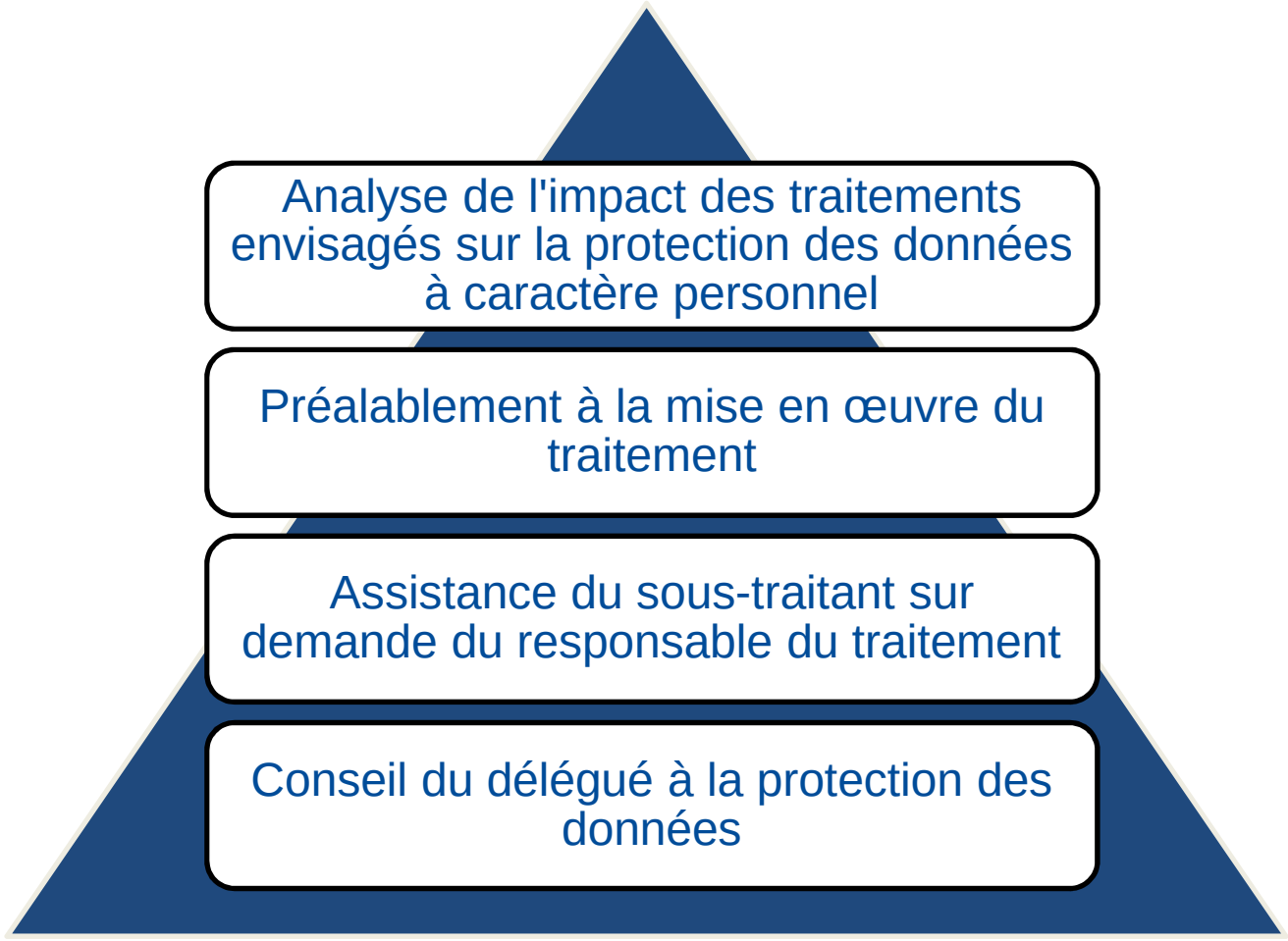
Mais en contrepartie, le responsable de traitement doit être en conformité avec les dispositions du règlement et être en mesure de démontrer cette conformité (Art. 5)

Le responsable reste par ailleurs tenu de **consulter l'autorité de contrôle** avant le traitement de données lorsqu'une analyse d'impact indique que le traitement présenterait un risque élevé si le responsable de traitement ne prenait pas de mesure pour atténuer le risque (Art. 36).

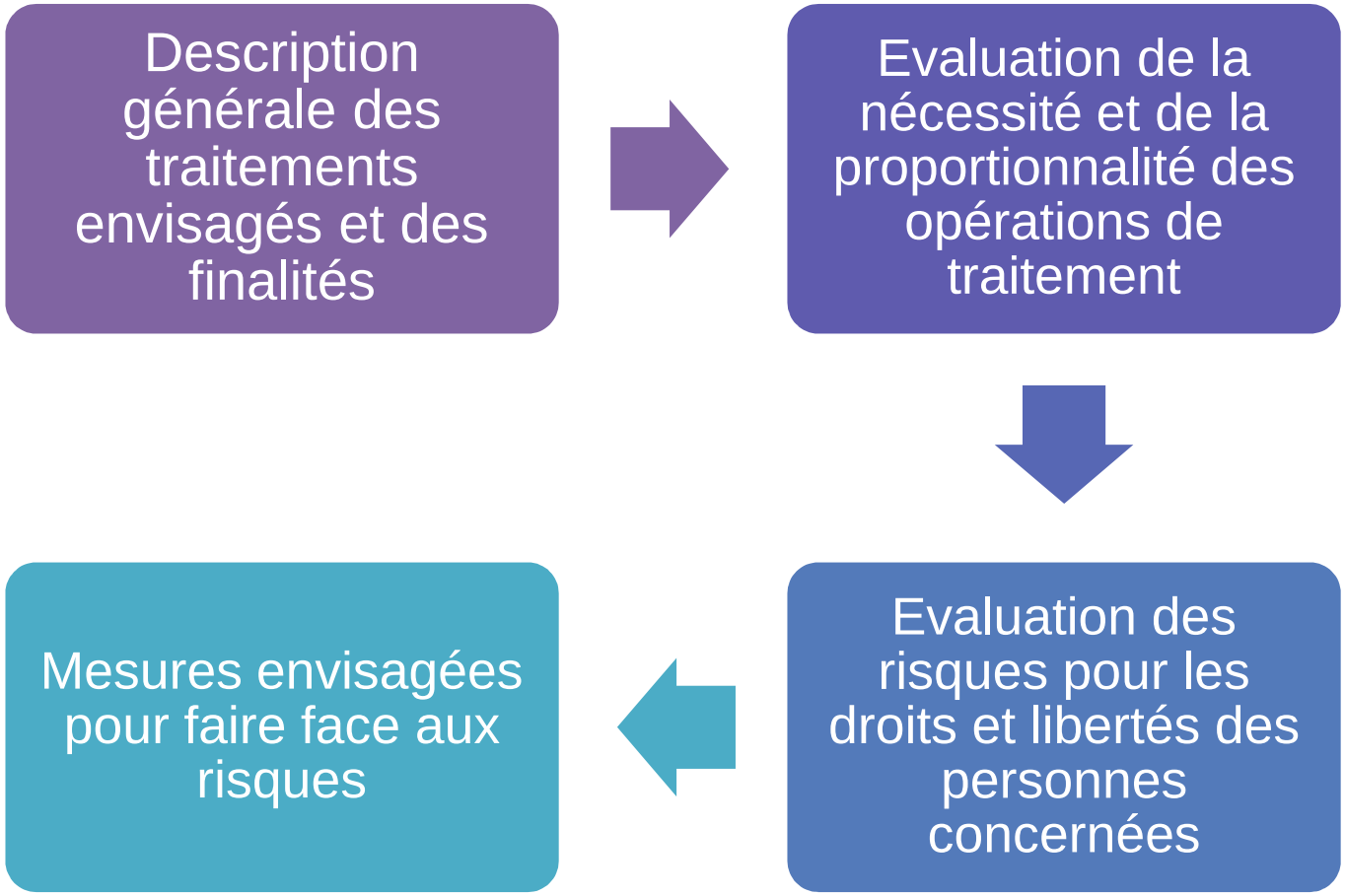
4.2 Analyse d’impact (1)

Traitements concernés		
Traitements présentant des risques particuliers du fait de leur nature, de leur portée, ou de leurs finalités	Traitements présentant des risques particuliers : - surveillance systématique à grande échelle d’une zone accessible au public - traitement à grande échelle d’informations sensibles - évaluation d’aspects personnels fondée sur un traitement automatique et permettant de prendre des décisions à l’égard d’une personne	Traitements considérés par l’autorité de contrôle comme étant susceptibles de présenter des risques spécifiques pour les droits et libertés des personnes concernées (liste publique)

4.2 Analyse d’impact (2)



4.2 Analyse d'impact (3)



Consultation préalable de l'autorité de protection des données si le résultat de l'analyse indique que le traitement présente un risque élevé

5. Procédure devant la Cnil

1. Aspects procéduraux
2. Publicité

- A la suite d'un contrôle (sur place ou en ligne), lorsque les manquements relevés sont sérieux, le dossier est transmis à la formation contentieuse de la Cnil, qui peut prononcer des sanctions administratives correctrices ou pécuniaires

- La Cnil peut sur le fondement de l'article 40 du Code de procédure pénale dénoncer au procureur de la République les infractions à la loi Informatique et libertés, prévues aux articles 226-16 à 226-24 du Code pénal

5.1 Aspects procéduraux (1)

Les droits de la défense

Un arrêt du Conseil d'état (CE, 19-2-2008 n° 311974) reconnaît à la formation restreinte de la Cnil la qualité de tribunal, au sens de l'article 6 de la Convention européenne des droits de l'homme.

En conséquence, les organismes ou personnes mis en cause peuvent :

- **être assistés d'un avocat**
- **accéder à leur dossier**
- **être entendus lors de la séance de la formation restreinte**

5.1 Aspects procéduraux (2)

Les moyens de défense

Par exemple, lorsqu'un manquement à l'obligation d'assurer la sécurité des données est reproché par la Cnil, les moyens de défense sont les suivants :

- **L'obligation de sécurité des données à la charge du responsable du traitement est une obligation de moyens et non de résultat. Le responsable du traitement doit donc mettre en œuvre tous les moyens pour préserver la sécurité des données, sans toutefois en garantir le résultat. En particulier, il doit :**
  - **mettre en œuvre des actions correctives et démontrer qu'il ne s'agit pas d'un problème structurel ;**
  - **mettre en œuvre des mesures préventives ;**
  - **mettre en œuvre des mesures de sensibilisation.**

- **Le responsable du traitement a collaboré avec la Cnil lors du contrôle qu'elle a effectué, notamment au regard :**
  - **des explications apportées par le responsable du traitement ;**
  - **de sa bonne foi ;**
  - **de sa coopération tout au long de la procédure ;**
  - **de sa volonté de s'inscrire dans le strict respect de la réglementation Informatique et Libertés.**

- **Le responsable du traitement a pris des engagements avant le rapport de la Cnil**

5.1 Aspects procéduraux (3)

Les voies de recours

Article 46 de la loi Informatique et libertés : « Les décisions prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'Etat ».

→Ce recours doit être formé dans un délai de 2 mois à compter de la notification ou de la publication de la décision attaquée (art. R. 31-1 4° du Code de la justice administrative)

→Néanmoins, la décision attaquée est exécutoire dès sa notification, et le recours formé devant le Conseil d'Etat n'a pas d'effet suspensif

→En cas d'urgence, il existe toutefois les référés, notamment le référé-suspension et le référé-liberté

→L'effet escompté d'un recours est l'annulation de la décision, sa réformation (modification) ou son remplacement

5.2 La publicité

Article 46 de la loi Informatique et libertés

Depuis la loi du 19 mars 2011 relative au défenseur des droits, la formation restreinte peut rendre publiques les sanctions qu'elle prononce

Avec la loi pour une République numérique du 7 octobre 2016, la formation restreinte peut, en outre, ordonner que les personnes sanctionnées informent individuellement de cette sanction, à leur frais, chacune des personnes concernées

MERCI

Questions - Réponses

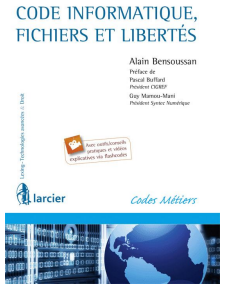
Qui sommes-nous ?

Le cabinet est distingué Law Firm of the Year pour l'année 2017 dans la catégorie Technologies de l'Information pour la France par la revue américaine Best Lawyers. Cette distinction fait suite à la désignation d'Alain Bensoussan comme Lawyer of the Year de 2011 à 2015 dans les catégories Nouvelles Technologies et Droit des Technologies.

Le cabinet a reçu le Trophée d'Or 2017 du magazine Décideurs (groupe Leaders League) dans la catégorie Nouvelles technologies: informatique, internet / données personnelles et télécommunications.

Le cabinet a obtenu, pour la 5e année consécutive, le Trophée d'Or du Palmarès des cabinets d'avocats 2017 dans la catégorie Technologie de l'information – Médias & Télécommunications, organisé par Le Monde du Droit en partenariat avec l'Association Française des Juristes d'Entreprise (AFJE), ainsi que, pour la première fois, le Trophée d'Or dans la catégorie Propriété intellectuelle. Il a également été élu Cabinet de niche de l'année.

Après avoir obtenu les labels Cnil « Lexing® formation informatique et libertés » pour son catalogue de formations informatique et libertés et « Lexing® audit informatique et libertés » pour sa procédure d'audit, le cabinet a obtenu le label « Gouvernance »



Lexing — Le premier réseau international d'avocats dédié au droit des technologies avancées

Réseau Lexing

LEXING NETWORK

Réseau international d'avocats en droit du numérique et des technologies avancées

Prévision 2017

Informations

Immeuble Cap Etoile
58, boulevard Gouvion Saint Cyr
75017 Paris
Tél. : +33 (0)1 82 73 05 05
Fax : +33 (0)1 82 73 05 06
paris@lexing.law
www.alain-bensoussan.com

Alain Bensoussan Avocats
@AB_Avocats
Lexing Alain Bensoussan Avocats

Alain Bensoussan Avocats

Mob. : +33 (0)7 85 53 57 52
Marie-soulez@lexing.law
Alain Bensoussan
@A_Bensoussan

Marie Soulez

Crédits photos

3d a background the future©valya_Fotolia.jpg
Cloud@morganimation Fotolia
Digital mind@alphaspirit - Fotolia
Disruptive technology innovation revolution word tag Energy@kentoh Fotolia
Futuristic network energy data grid@kentoh Fotolia
Flow chart or business processes reengineering©adrian_ilie825_Fotolia
Information word on computer pc keyboard key@fotoscool Fotolia