Séminaire Protection des données à caractère personnel

Le Règlement Européen n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 dit « RGPD »

relatif à la protection des personnes physiques
à l'égard du traitement des données à caractère personnel
et à la libre circulation de ces données.

Animateur : Ryad BOUADI
Société : AGERIS Group SAS
Tél. : +33 (0)6 42 10 52 96
ryad.bouadi@ageris-group.com

Objectifs de cette présentation

1. Présenter les **exigences du RGPD** et **les impacts** pour l'organisme

2. Présenter les **bonnes pratiques** à appliquer **et le plan d'actions** pour se mettre en conformité avec le RGPD

Actualité :

- **25 mai 2018 ???**
- **Le 28 mai 2018 : La quadrature du net ???**
- **Le 20 juin 2018 : LIL 3 ???**
- **11 octobre 2018 : certification ???**

RGPD
Contexte général et enjeux du nouveau règlement

Descartes nous a appris: **Je pense, donc je suis.**

<u>Aujourd'hui, pour être, penser ne suffit plus, il faut</u> :

- communiquer,
- partager,
- aimer (ou "liker")
- socialiser.

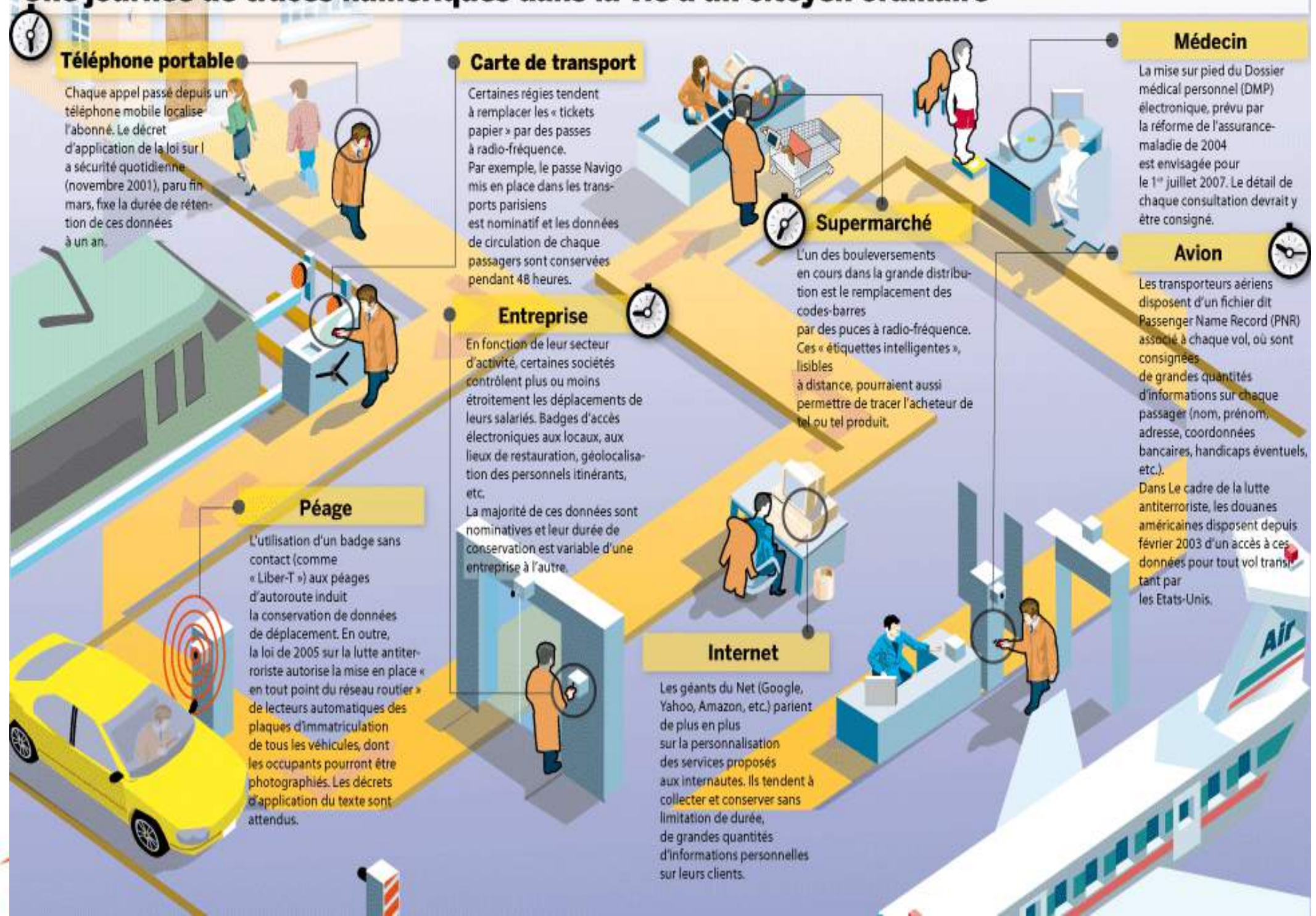

QUI VOUS
OBSERVE ?
L'ABSENCE DE VIE PRIVÉE SUR INTERNET


BIG BROTHER
IS WATCHING
YOU
THE INDEPENDENT
LIVERPOOL'S EUROPEAN
DREAM CRUSHED BY MILAN
Google
IS WATCHING
YOU
facebook
IS WATCHING
YOU

La législation concernant la protection des données personnelles et le rôle de la CNIL

Jacques Chirac : *"Est-ce que j'ai la tête de quelqu'un qui veut porter atteinte aux droits de l'homme ?*

Une journée de traces numériques dans la vie d'un citoyen ordinaire



Téléphone portable

Chaque appel passé depuis un téléphone mobile localise l'abonné. Le décret d'application de la loi sur l a sécurité quotidienne (novembre 2001), paru fin mars, fixe la durée de rétention de ces données à un an.

Carte de transport

Certaines régies tendent à remplacer les « tickets papier » par des passes à radio-fréquence. Par exemple, le passe Navigo mis en place dans les transports parisiens est nominatif et les données de circulation de chaque passagers sont conservées pendant 48 heures.

Médecin

La mise sur pied du Dossier médical personnel (DMP) électronique, prévu par la réforme de l'assurance-maladie de 2004 est envisagée pour le 1er juillet 2007. Le détail de chaque consultation devrait y être consigné.

Supermarché

L'un des bouleversements en cours dans la grande distribution est le remplacement des codes-barres par des puces à radio-fréquence. Ces « étiquettes intelligentes », lisibles à distance, pourraient aussi permettre de tracer l'acheteur de tel ou tel produit.

Avion

Les transporteurs aériens disposent d'un fichier dit Passenger Name Record (PNR) associé à chaque vol, où sont consignées de grandes quantités d'informations sur chaque passager (nom, prénom, adresse, coordonnées bancaires, handicaps éventuels, etc.).
Dans Le cadre de la lutte antiterroriste, les douanes américaines disposent depuis février 2003 d'un accès à ces données pour tout vol transitant par les Etats-Unis.

Entreprise

En fonction de leur secteur d'activité, certaines sociétés contrôlent plus ou moins étroitement les déplacements de leurs salariés. Badges d'accès électroniques aux locaux, aux lieux de restauration, géolocalisation des personnels itinérants, etc.
La majorité de ces données sont nominatives et leur durée de conservation est variable d'une entreprise à l'autre.

Péage

L'utilisation d'un badge sans contact (comme « Liber-T ») aux péages d'autoroute induit la conservation de données de déplacement. En outre, la loi de 2005 sur la lutte antiterroriste autorise la mise en place « en tout point du réseau routier » de lecteurs automatiques des plaques d'immatriculation de tous les véhicules, dont les occupants pourront être photographiés. Les décrets d'application du texte sont attendus.

Internet

Les géants du Net (Google, Yahoo, Amazon, etc.) parient de plus en plus sur la personnalisation des services proposés aux internautes. Ils tendent à collecter et conserver sans limitation de durée, de grandes quantités d'informations personnelles sur leurs clients.

1. Introduction et rappel historique

	1971	1ère Loi en Allemagne
	1973	1ère Loi en Suède
	1974	1ère Loi aux Etats-Unis d'Amérique (USA)
Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés et création de la CNIL	1978	
	1980	Lignes directrices de l'OCDE
	1981	Convention n° 108 du Conseil de l'Europe
	1990	Lignes directrices de l'ONU
	1994	Lignes directrices de l'OMC
	1995	Directive européenne n°95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel	2004	
Décret d'application n° 2005-1309 du 20 octobre 2005	2005	
Obligation de notification en cas de " violation de données à caractère personnel " - Ordonnance du 24 août 2011 à la charge des fournisseurs de services de communications électroniques	2011	
Loi organique n°2011-333 du 29 mars 2011 relative au Défenseur des droits et son Décret d'application n° 2011-2023 du 29 décembre 2011 relatif aux pouvoirs de contrôle et de sanction de la CNIL (modification du décret de 2005)	2011	
Le CIL est désormais reconnu par pôle emploi	2012	
	2016	Règlement du Parlement européen et du Conseil n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, (Règlement général sur la protection des données).

Le cadre réglementaire

Le cadre réglementaire évolue

LIL 1

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL)

LIL 2

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

RGPD

Le Règlement européen n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Délai de mise en conformité 25 mai 2018

LIL 3

Loi du 14/05/2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

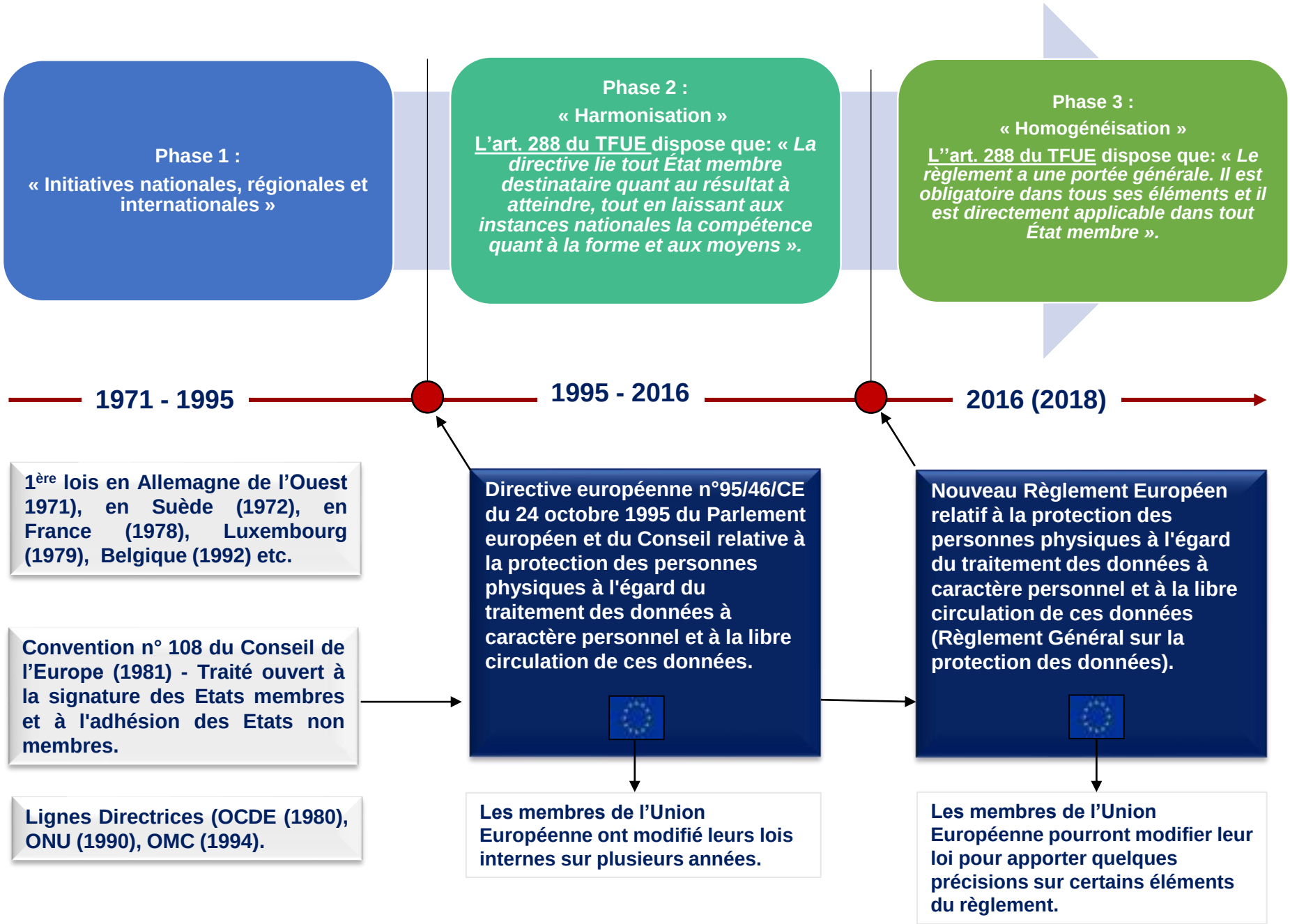
La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen. Elle permet la mise en œuvre concrète du Règlement général sur la protection des données (RGPD) et de la Directive « police-justice », applicable aux fichiers de la sphère pénale.

Le RGPD s'applique directement en droit français : il remplace sur de nombreux points (droits des personnes, bases légales des traitements, mesures de sécurité à mettre en œuvre, transferts, etc.) la loi nationale.

Sur d'autres points (les « marges de manœuvre nationales »), la loi Informatique et Libertés reste en vigueur et vient compléter le RGPD :

- il s'agit par exemple du traitement des données de santé ou des données d'infraction, de la fixation à 15 ans du seuil d'âge du consentement des mineurs aux services en ligne, des dispositions relatives à la mort numérique, etc.
- Enfin, la loi nationale reste pleinement applicable pour tous les fichiers « répressifs », qu'il s'agisse de la sphère pénale ou du domaine du renseignement et de la sûreté de l'Etat. De nombreuses dispositions spéciales sont prévues en ces matières.

Historique de la réglementation



Les enjeux du nouveau règlement

1. Prendre en compte les évolutions technologiques

Nos données deviennent un enjeu économique

2. Prendre en compte les nouveaux usages des technologies de l'information

Les mêmes droits pour tous les citoyens, les mêmes obligations pour tous les organismes

3. Renforcer les droits du citoyen
(quelque que soit sa résidence et sa nationalité)

Redonner aux citoyens le contrôle de leurs données

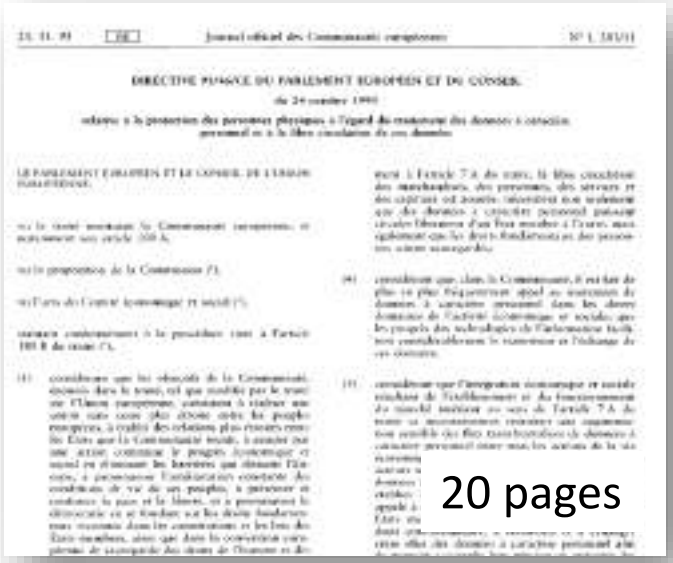
4. Responsabiliser les dirigeants et les sous-traitants
(présents ou non au sein de l'UE)

La protection des personnes physiques à l'égard du traitement des DCP est un droit fondamental.

L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

Le nouveau règlement

Directive 1995



DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL

20 pages

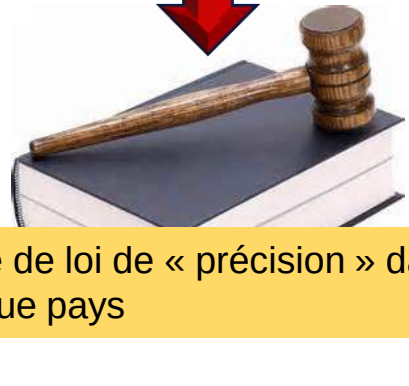
Texte de loi de « transposition et de précision» dans chaque pays

Règlement 2016

RÈGLEMENTS

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

88 pages



Texte de loi de « précision » dans chaque pays

Le moins qu'on puisse dire c'est que le texte du nouveau règlement européen va profondément changer la donne en matière de protection des données personnelles :

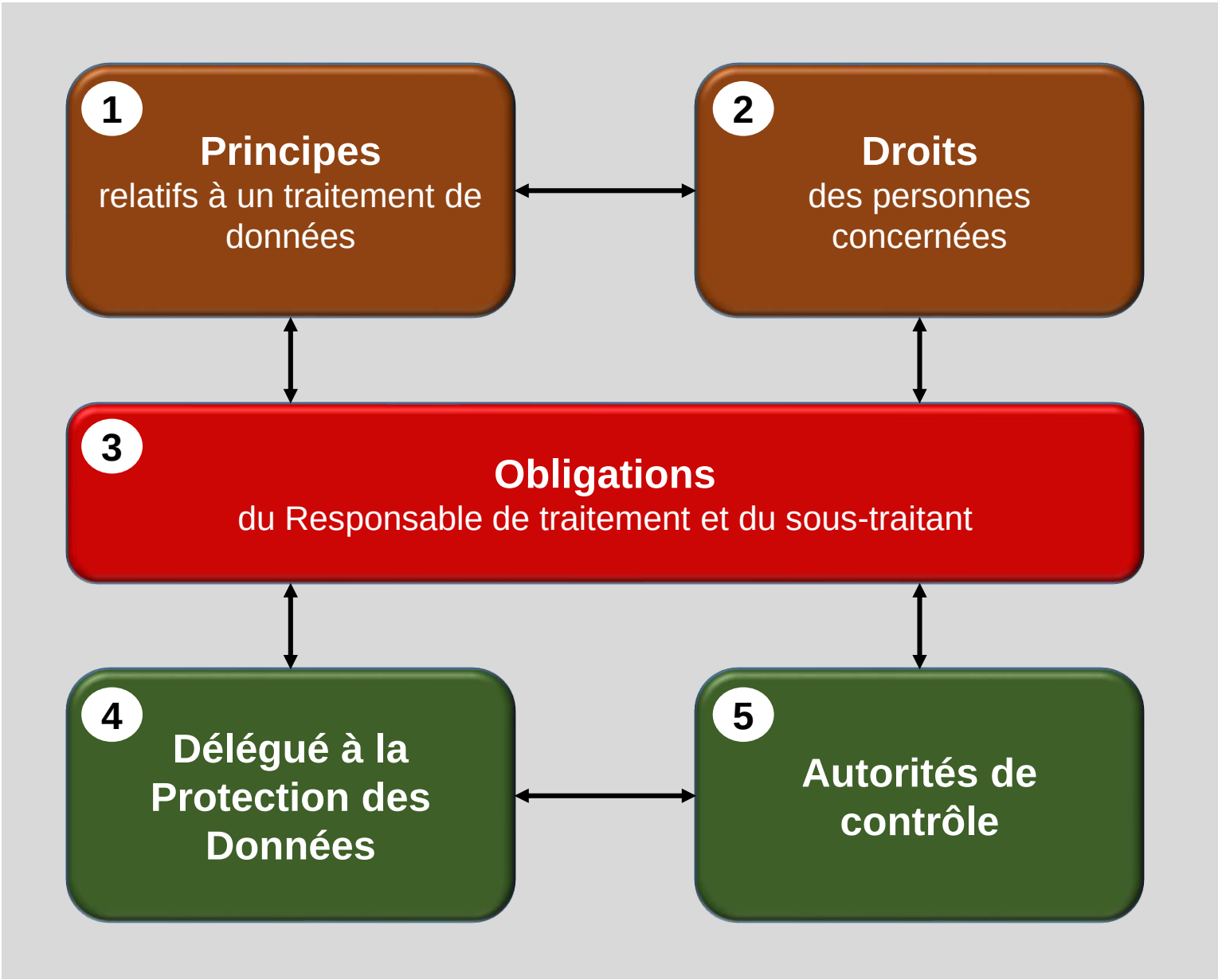
- 88 pages d'obligations à respecter
- 99 articles de loi
- 20 millions d'euros de sanctions en cas d'infraction pour les PME,
- 4% du CA global du groupe pour les grandes entreprises (soit entre 3 et 5 MILLIARDS d'euros de risques de sanctions pour des entreprises comme Google et Amazon…)
- de nombreux acteurs ont intérêt à déposer plainte (syndicats, représentants du personnel, salariés licenciés, associations de consommateurs, associations de défense de la vie privée, clients mécontents…)

Avec des montants aussi importants de sanctions – et autant d'intervenants qui ont intérêt à se lancer dans un contentieux, cette règlementation va devenir un contre-pouvoir majeur dont bon nombre d'organisation vont faire les frais.

Beaucoup d'acteurs vont découvrir à leurs dépens que le temps où la protection des données personnelles pouvait être facilement ignorée a touché à sa fin.

RGPD
Exigences, nouveautés et impacts pour l'organisme

RGPD – Les exigences relatives aux traitements de données à caractère personnel



Définitions

Donnée à caractère personnel (article 4 du RGPD) 	**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.
« Données sensibles » (article 9 du RGPD)	Données à caractère personnel qui révèle l'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 sensibles » (article 10 du RGPD)	Données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté.

06.42.10. ****

Mon adresse ip : *37.58.187.57*

→ **Résumé de la définition de DCP**: Toute donnée relative à une personne physique, qui peut être identifiée par quelqu'un, quel que soit le moyen utilisé.

- ✓ Données directement identifiantes : nom et prénom, photo, e-mail nominatif, …
- ✓ Données indirectement identifiantes : NIR, empreinte digitale, …
- ✓ Les recoupements d'informations anonymes : le fils aîné du notaire habitant au 11 bd Raspail à Paris, …

• **Enjeu →** application de la loi Informatique et Libertés

• ATTENTION : Existence de **méthodes d'anonymisation, au stade de la collecte ou de l'exploitation →** casse le lien entre l'information et la personne

Traitement de données à caractère personnel	**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

Cycle de vie de la donnée

Fichier de données à caractère personnel	Tout **ensemble structuré de données** à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique


CV

Définitions (article 4 du RGPD)

Responsable de traitement

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités, les conditions et les moyens du traitement** de données à caractère personnel

Généralement admis

La personne morale

En pratique et en général, la personne morale incarnée par son représentant légal, sur lequel pèse la responsabilité du respect des obligations.

Exemples :

-Secteur privé : la société DULAIT représentée par son président

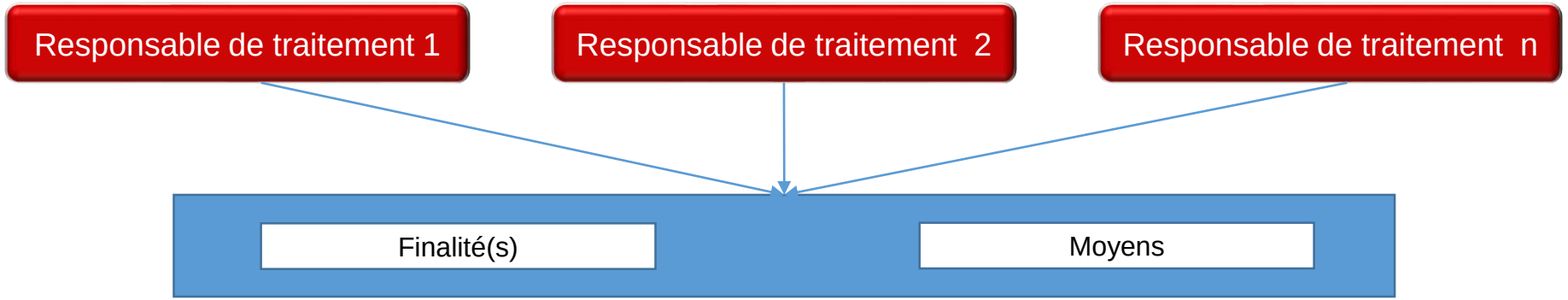
-Secteur public : la collectivité territoriale représentée par son maire ou président

Les services en charge de la mise en oeuvre des traitements

Directeurs / chefs de services

Responsables conjoints

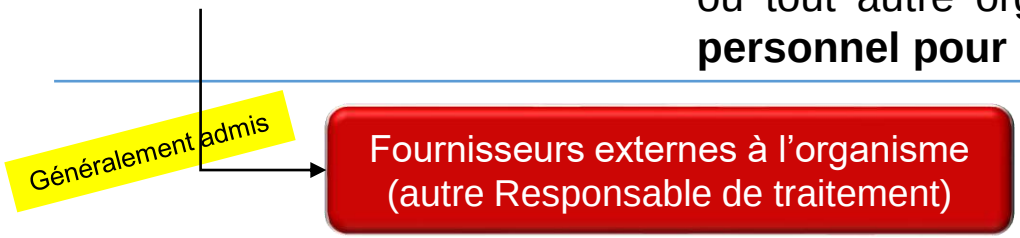
Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement



Définitions (article 4 du RGPD)

Sous-traitant

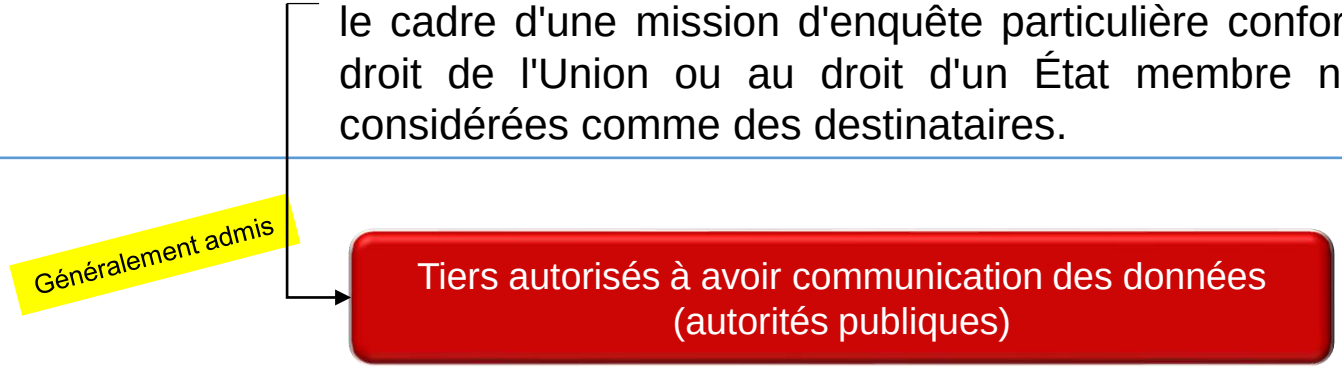
La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui **traite des données à caractère personnel pour le compte du responsable du traitement**



Destinataire

La 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.

Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires.



Les acteurs impliqués dans les traitements

Les acteurs

3 Les sous- traitants

« La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »

Celui qui agit sur instruction documentée..

2 Le responsable du traitement

« La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens du traitement de données à caractère personnel; lorsque les finalités, les conditions et les moyens du traitement sont déterminés par le droit de l'Union ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou par la législation d'un État membre ».

4 Les destinataires

« la 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.

Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ».

1 La personne concernée par le traitement

« 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 ».

! Client, salarié, salarié de fournisseur ou de partenaire, visiteur, ….
Quelque soit sa nationalité et son lieu de résidence

5 Les tiers autorisés à avoir communication des données

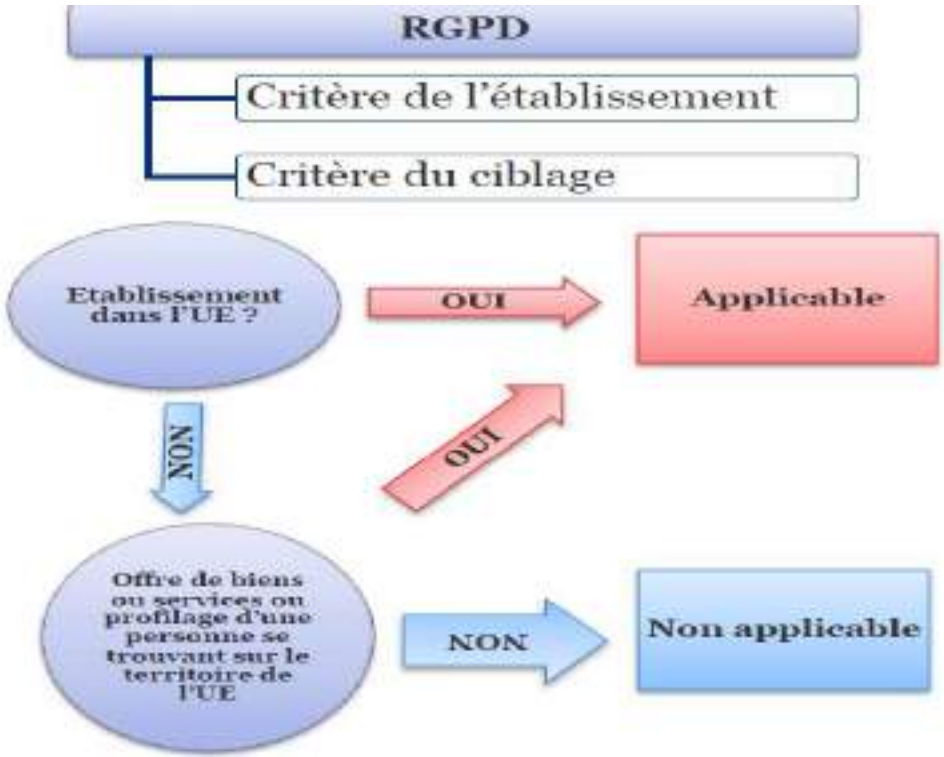
! Autorités judiciaires, impôts / trésorerie, Organismes sociaux, …..

Champ d'application territorial

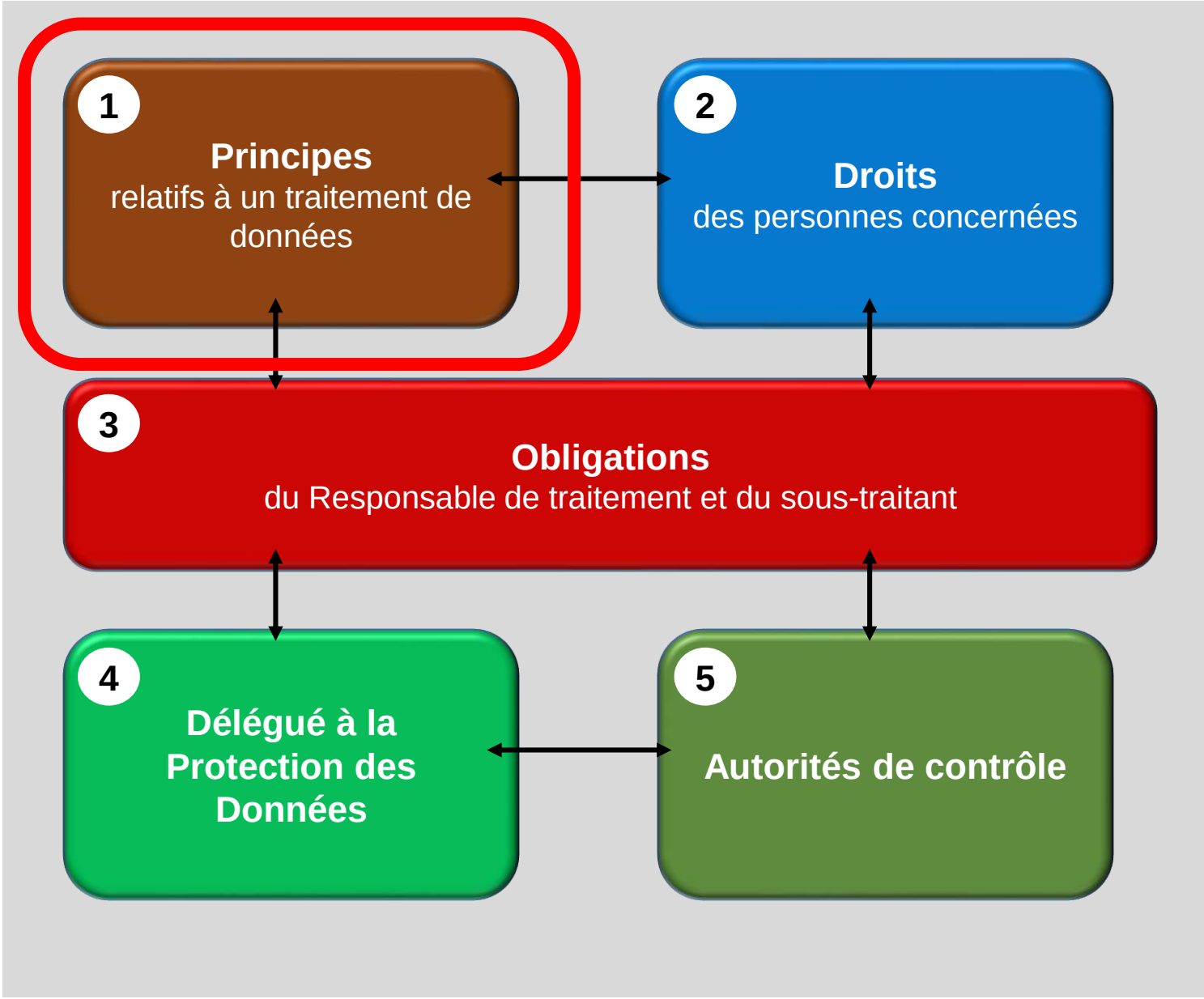
Le RGPD s'applique :

• aux traitements effectués dans le cadre des activités de RT ou de ST établis sur le territoire de l'UE (critère de l'établissement)

• mais aussi aux traitements effectués pour le compte de RT ou ST non établis sur le territoire de l'UE dès lors qu'ils visent des personnes se trouvant sur le territoire de l'UE dans le cadre des activités suivantes (critère du ciblage) :
- offre à ceux-ci de biens ou de services ou
- suivi de leur comportement au sein de l'UE



RGPD – Les exigences relatives aux traitements de données à caractère personnel



Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Principe 1 Licéité, loyauté, transparence	Les données doivent être traitées de manière **licite, loyale et transparente**
Principe 2 Limitation des finalités	Les données doivent être traitées pour des **finalités déterminées, explicites et légitimes**
Principe 3 Minimisation des données	Les données doivent être **adéquates, pertinentes et limitées**
Principe 4 Exactitude	Les données doivent être **exactes et, si nécessaire, tenues à jour**
Principe 5 Limitation de la conservation	Les données doivent être **conservées pendant une durée n'excédant pas celle nécessaire**
Principe 6 Intégrité et confidentialité	 Les données doivent être traitées de façon à **garantir une sécurité appropriée** des données

ACCOUNTABILITY: Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté.

- L'accountability est un processus de mise en conformité d'une entreprise à la réglementation Informatique et libertés.

- Grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes, le responsable du traitement peut s'acquitter de son obligation de rendre des comptes.

Accountability : la mise en œuvre

Principe.

L'obligation d'accountability implique pour le responsable du traitement :

→*de prendre des mesures efficaces et appropriées afin de se conformer au règlement européen ;*

d'apporter la preuve*, sur demande de l'autorité de contrôle, que les mesures appropriées ont été prises.*

Mise en pratique. Certaines mesures sont décrites dans le règlement général sur la protection des données à savoir notamment :

- l'adoption de règles internes ;
- l'obligation de conserver une trace documentaire de tout traitement effectué sous la responsabilité du responsable du traitement ou du sous-traitant ;
- l'adoption de l'approche « Privacy by design » ;

Article 5 du RGPD

Principes relatifs au traitement des DCP

- Les DCP doivent être traitées de manière licite, loyale et transparente
- Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes
- Les DCP doivent être adéquates, pertinentes et limitées
- Les DCP doivent être exactes et, si nécessaire, tenues à jour
- Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire
- Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Principe 1

Licéité, loyauté, transparence

Les données doivent être traitées de manière **licite, loyale et transparente**

« Fondement » ou (base) juridique du traitement

Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

*a) **la personne concernée a consenti au traitement** de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;*

*b) **le traitement est nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;*

*c) **le traitement est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis;*

*d) **le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne** concernée ou d'une autre personne physique;*

*e) le traitement est nécessaire à **l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique** dont est investi le responsable du traitement;*

*f) **le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement** ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.*

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Un traitement de données à caractère personnel ne peut être mis en place que s'il repose sur :

- le **consentement de la personne concernée**,
  ou
- **l'exécution stricte d'un contrat** auquel la personne concernée est partie,
  ou
- le **respect d'une obligation légale** ou réglementaire,
  ou
- la sauvegarde des intérêts vitaux d'une personne physique,
  ou
- **l'exécution d'une mission d'intérêt public**,
  ou
- **l'intérêt légitime poursuivi par le responsable de traitement** ou par un tiers, sauf s'il est contraire aux intérêts ou aux droits fondamentaux de la personne concernée.

Exemples :


Transmission des données clients à des partenaires ;
Collecte de données de santé ;

Gestion des données clients ;
Facturation d'un bien / service ;

Conservation des bulletins de paie ;
Déclaration obligatoire d'emploi des travailleurs handicapés (DOETH) ;


Gestion des urgences ;


Gestion des risques (naturels, sanitaires, nucléaires…) pour la prévention et la protection des citoyens ;


Détection des fraudes ;
Transmission des données au sein d'un groupe d'entreprises…

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Principe 1

Licéité, loyauté, transparence

Les données doivent être traitées de manière **licite, loyale et transparente**

Traitement portant sur des catégories particulières de données à caractère personnel

1.Le traitement des données à caractère personnel qui révèle l'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 **sont interdits**.

2.Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie:

a) la personne concernée a donné son consentement explicite

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle

g) le traitement est nécessaire pour des motifs d'intérêt public important

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques

Principe 1	Les données doivent être traitées de manière **licite, loyale et transparente**
Licéité, loyauté, transparence	

Conditions applicables au consentement (article 7)

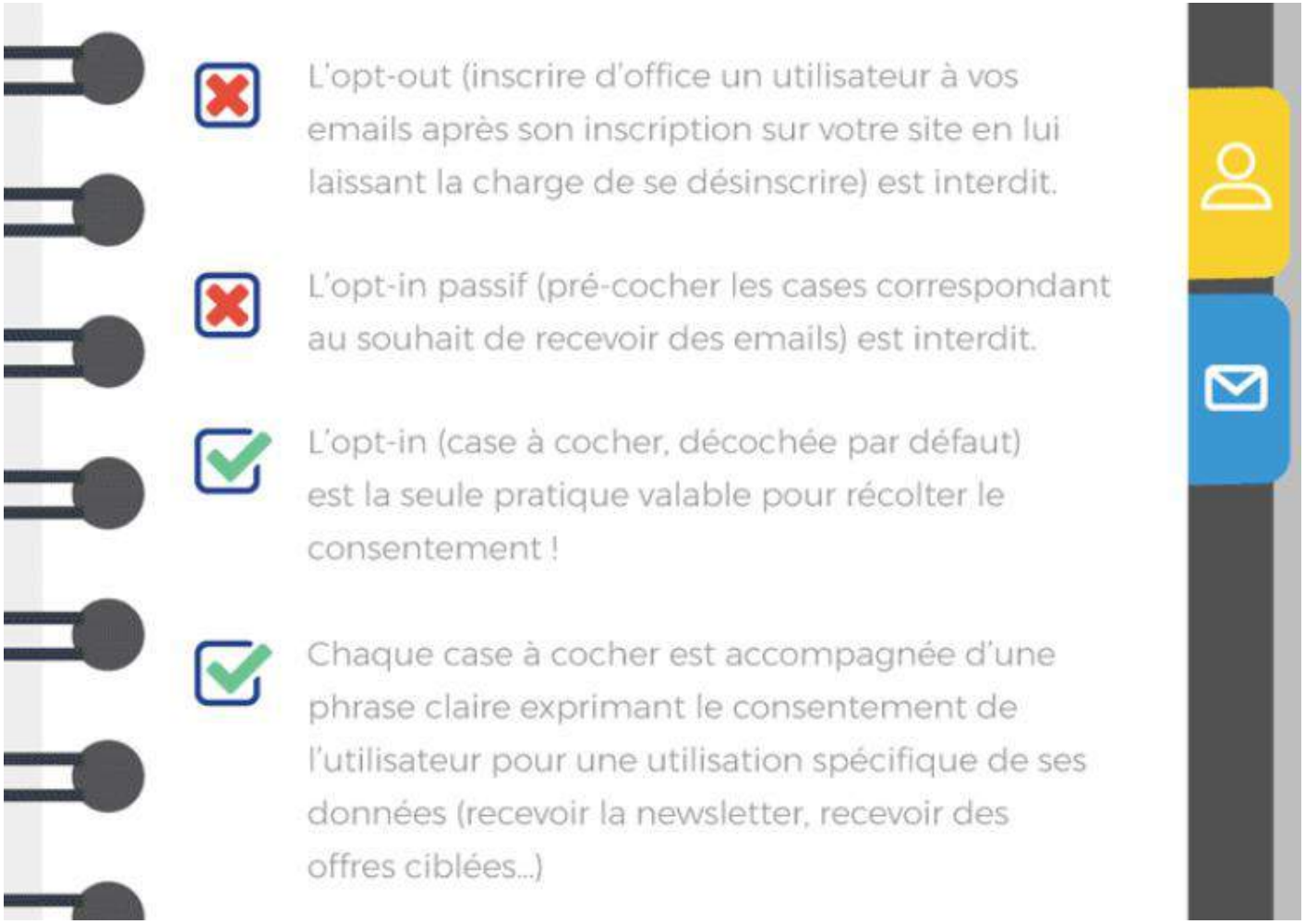
1.Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de **démontrer que la personne concernée a donné son consentement** au traitement de données à caractère personnel la concernant.

2.Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

3.La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

4.Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Le consentement: un acte positif éclairé, spécifique et univoque



Un consentement spécifique :

Un consentement libre :

Quelques exceptions au consentement :

Le traitement est nécessaire **à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Exemples : traitement de son adresse pour que des produits achetés en ligne puissent être livrés ; traitement des informations bancaires pour que les salariés puissent être payés.

Le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

Les données sont utilisées pour faire de **la prospection commerciale** par mail à un client ou ancien client pour lui proposer des **services / produits analogues** à ceux qu'il a déjà commandés.

Attention ces exceptions sont strictement encadrées !

Applications mobiles : mises en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire

19 juillet 2018

La Présidente de la CNIL met en demeure les sociétés FIDZUP et TEEMO de recueillir le consentement des personnes au traitement de leurs données à des fins de ciblage publicitaire par le biais d'une technologie (SDK) installée dans des applications mobiles.

La CNIL a contrôlé les traitements de données mis en œuvre par les sociétés FIDZUP et TEEMO qui ont recours à des technologies permettant de collecter des données personnelles *via* les smartphones, et de réaliser des campagnes publicitaires sur les mobiles.

Ces sociétés ont recours à des outils techniques dénommés « SDK ». Ces outils sont intégrés dans le code d'applications mobiles de leurs partenaires. Ils leur permettent de collecter les données des utilisateurs des

Le RGPD, La CNIL et… Alexandre Benalla

Etude réalisée à partir de messages postés sur Twitter : la CNIL est saisie du dossier

09 août 2018

La CNIL est actuellement saisie d'un nombre important de plaintes concernant les conditions dans lesquelles EU DisinfoLab a effectué une étude sur certains messages publiés sur le réseau Twitter relatifs à l'affaire BENALLA.

La collecte et le traitement de données à caractère personnel sont soumis au RGPD (Règlement Général sur la Protection des Données), qui protège tout particulièrement les données relatives aux opinions politiques des personnes. L'ONG à l'origine de l'étude étant située en Belgique, la CNIL instruira les plaintes dont elle a été saisie dans le cadre de la coopération européenne instaurée par le RGPD.

Les mots clés associés à cet article

#Plainte

Une étude belge a analysé les tweets consacrés à l'affaire Benalla, notamment en classant les émetteurs des messages en fonction de leur appartenance politique supposée. Inondée de plaintes, la CNIL ouvre un dossier.

En résumé, selon l'étude :

- En moins de trois semaines, 4,5 millions de tweets en français ont été échangés par 247.701 auteurs différents, ce qui en fait un phénomène tout à fait exceptionnel ;
- Près de la moitié des contenus (47%) ont été générés par 1 % des acteurs (ceci exclut les médias) ;
- Parmi ces comptes hyperactifs, certains le sont encore plus que d'autres : moins de 500 acteurs ont publié près de 800.000 tweets ;
- Les 1 % les plus actifs présentent des caractéristiques troublantes : activité hors norme sur certains sujets très politiques et sensibles, activité concentrée à certains moments spécifiques (élections, crise), mass following dans le but d'augmenter la visibilité des tweets, pratique fréquente du pseudonyme ; information géographique du compte souvent manquante ; 27 % d'entre eux ont des liens avec des médias officiels russes suspectés de désinformation et près de 10% d'entre eux ont été identifiés dans le passé comme relayant sciemment des campagnes de désinformation.
- Au moins trois comptes utilisent un système de tweets automatisés ou semi-automatisés.

C’est la suite de l’étude qui a créé la polémique. En effet, les chercheurs ont tenté de classer les auteurs de tweets en quatre catégories :

- Les souverainistes, LR et proches des mouvements contre le mariage pour tous ;
- La communauté du rassemblement national, des souverainistes et quelques personnes des mouvements contre le mariage pour tous ;
- La communauté constituée par la France insoumise avec des porosités de lien avec les autres communautés qui occasionne quelques faux positifs ;
- La communauté constituée des médias et des porosités avec les autres communautés, et LREM.

L’étude se penche alors sur le comportement spécifique de chacune de ces catégories. Par exemple, la catégorie 3 serait une des plus actives mais aussi une des moins susceptibles de désinformer, tandis que les catégories 1 et 2 seraient plus à risque sur le plan de la fiabilité de l’information et utiliseraient des comptes automatisés.

Dans un premier temps, les auteurs de l’étude ont rendu accessibles les données brutes sur lesquelles ils ont travaillé. L’idée était de permettre à quiconque de vérifier la méthodologie et la fiabilité des enseignements tirés.
On a donc des fichiers Excel qui circulent contenant une liste de pseudonymes, le nombre total de tweets, et des informations permettant de positionner le compte sur l’échiquier politique

➢ **<u>Le consentement des personnes :</u>**

Les titulaires des comptes analysés par l'étude, n'ont pas consenti au traitement qu'engendre l'étude.

Et alors ? Le consentement n'est qu'une hypothèse de légitimité parmi d'autres. Condamner au motif que *« En l'espèce, les abonnés de Twitter n'ont jamais été sollicités par EUDisinfoLab pour donner leur consentement à l'enquête »* est donc un raccourci erroné s'il y a une autre base de licéité, tel par exemple l'intérêt légitime poursuivi par le responsable du traitement.

➢ **Le traitement de données relatives aux opinions politiques :**

L'étude contient un volet dans lequel les auteurs des comptes sont positionnés sur l'échiquier politique. Pour ce traitement-là, des règles spécifiques s'appliquent.

Une des règles spécifiques veut que la poursuite d'un intérêt légitime, qui peut justifier de façon générale un traitement, n'est plus une hypothèse de licéité pour les données « sensibles ».

Or, en déduire qu'il faut un consentement est un raccourci erroné !

Même en présence de données sensibles, il y a d'autres hypothèses de licéité, notamment :

- Le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée (contrairement à Cambridge Analytica avec laquelle il n'y a pas de parallèle à faire, les traitements ont porté sur des données mises en ligne par les auteurs des tweets sans restriction de diffusion) ;
- Le traitement est nécessaire pour des motifs d'intérêt public important (**la liberté d'expression et d'information, *a fortiori* au sujet d'un débat d'intérêt général, doit être prise en compte**) ;
- Le traitement est nécessaire à des fins de recherche scientifique ou historique ou à des fins statistiques.

L'article 85 du RGPD dispose: *« Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire. »*

→C'est donc aux Etats qu'il appartient d'établir un équilibre entre des valeurs tout aussi respectables l'une que l'autre.

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Article 5 du RGPD

Principes relatifs au traitement des DCP

- **Les DCP doivent être traitées de manière licite, loyale et transparente**
- **Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes**
- **Les DCP doivent être adéquates, pertinentes et limitées**
- **Les DCP doivent être exactes et, si nécessaire, tenues à jour**
- **Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire**
- **Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données**

Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

La limitation des finalités

Concernant la finalité, la loi impose en réalité deux obligations :

- D'une part, réaliser une collecte pour des finalités déterminées, explicites et légitimes, ce qui contraint le responsable du traitement à **établir de manière précise la finalité** pour laquelle un traitement va être réalisé.

On peut comprendre également cette règle *a contrario*, celle-ci sanctionnant alors des finalités vagues, ou inexistantes, inscrites lors des formalités préalables (telle que « collecte pour exploitation », « collecte pour conservation », « récupération de données pour tout usage », etc.).

- D'autre part, la loi impose également de ne pas détourner le traitement des finalités initiales.

Une exception est toutefois prévue pour les traitements réalisés à des fins statistiques, historiques ou scientifiques à condition qu'un tel traitement soit réalisé dans le respect des autres dispositions légales et qu'il ne soit pas utilisé pour prendre des décisions à l'égard des personnes concernées (art. 6, 2°).

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

La finalité

La pratique enseigne que le danger pour les libertés provient plus de l'objectif poursuivi par le détenteur des données que de leur nature ou contenu, aussi le contrôle du respect de la finalité est essentiel

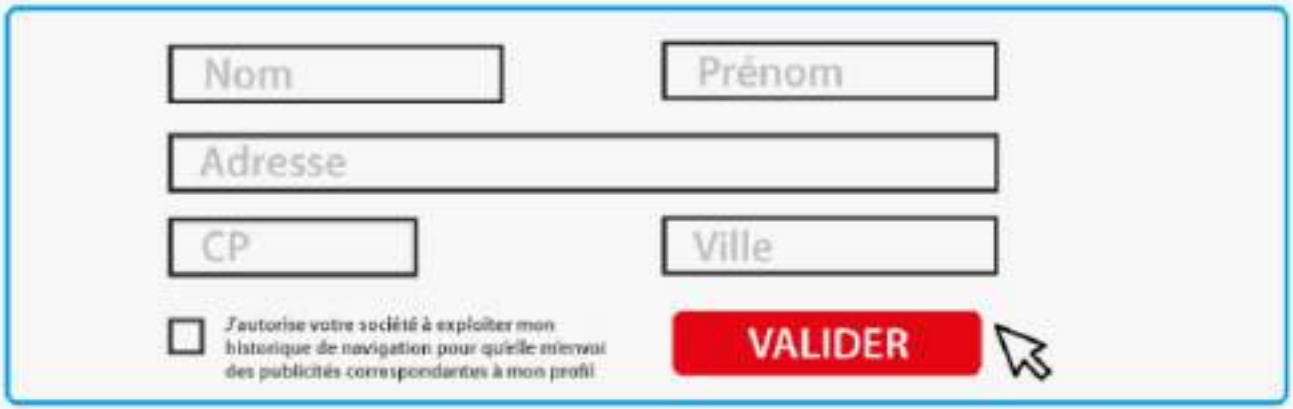
La finalité déclarée revêt donc une importance capitale puisque c'est elle qui déterminera pendant toute la vie du traitement, l'existence ou non d'un détournement de finalité. Il est donc nécessaire dès le départ de prévoir l'ensemble des besoins susceptibles de naître, et de réexaminer le traitement régulièrement pour s'assurer qu'il est bien conforme aux finalités initiales.

Tout détournement de finalité est passible de sanctions pénales

Exemples

La mise en place d'un dispositif de localisation GPS ne peut avoir pour objectif le contrôle des déplacements de salariés

Le fichier du personnel et l'adresse électronique des employés ne peuvent être utilisés à des fins de propagande politique



Chaque finalité de traitement devra être **explicite**

☐ J'autorise la société X à effectuer des actions de profilage dans le but de recevoir des offres adaptées à mes centres d'intérêts.

La case pré-cochée sera formellement **interdite**

~~☑ Oui, je souhaite recevoir...~~

Mise en demeure de cinq sociétés d'assurance pour détournement de finalité des données des assurés

18 octobre 2018

La Présidente de la CNIL met en demeure des sociétés des groupes HUMANIS et MALAKOFF-MÉDÉRIC de cesser d'utiliser pour de la prospection commerciale des données personnelles collectées exclusivement afin de payer les allocations retraite.

Les groupes Humanis et Malakoff-Médéric interviennent dans tous les domaines de la protection sociale, pour les entreprises et les particuliers, soit plus de 16 millions de personnes.

Parmi leurs activités, ces groupes et les sociétés qui les composent sont chargés de mettre en œuvre les régimes de retraite complémentaire en réalisant des opérations de gestion. À ce titre, ils ont accès à des données personnelles mises à disposition par les fédérations AGIRC-ARRCO aux fins de recouvrer les cotisations et payer les allocations retraite.

Au titre du programme annuel des contrôles défini par la CNIL au en 2017, des contrôles ont été réalisés dans les locaux de ces groupes en février et mars 2018.

À cette occasion, la CNIL a constaté que les sociétés des groupes Humanis et Malakoff-Médéric utilisent les données personnelles qu'elles détiennent dans le cadre de leur mission d'intérêt général de mise en œuvre des régimes de retraite complémentaire afin de faire de la prospection commerciale pour des produits et services de

OPH de Rennes : sanction pécuniaire pour une utilisation du fichier des locataires incompatible avec la finalité initiale

31 juillet 2018

La formation restreinte de la CNIL a prononcé une sanction de 30 000 euros à l'encontre de l'OPH de Rennes Métropole ARCHIPEL HABITAT pour avoir utilisé le fichier de ses locataires à d'autres fins que celle de gestion de l'habitat social.

En octobre 2017, la CNIL a reçu une plainte concernant l'utilisation du fichier des locataires de logements sociaux par la Présidente de l'OPH, également Maire de Rennes, pour leur adresser un courrier spécifique critiquant l'annonce du gouvernement de diminuer le montant des aides personnalisées au logement (APL). Ce courrier mentionnait par ailleurs des initiatives nationales tendant à mobiliser les locataires autour de cette problématique.

La formation restreinte de la CNIL a rappelé que, en vertu de la loi Informatique et libertés les données personnelles doivent être collectées pour des finalités « *déterminées, explicites et légitimes* ». Par ailleurs, la loi

L'OPH a justifié sa démarche, au regard de ces principes, en indiquant que ce courrier avait pour seule finalité d'informer les locataires sur les nouvelles dispositions réglementaires relatives au montant des APL. L'OPH considérait ainsi agir dans le cadre de ses missions de gestion locative et de mise en œuvre des politiques publiques concernant l'habitat social. L'OPH indiquait également pouvoir traiter des données à des fins de communication externe.

La formation restreinte a cependant considéré qu'au regard des termes utilisés dans le courrier *(« cette mesure est injuste. […] cette orientation […] aurait des répercussions terribles sur la qualité de votre cadre de vie »)* et de la teneur générale du message, *qui a d'ailleurs été envoyé à l'ensemble des locataires qu'ils bénéficient ou non des APL,* il ne s'agissait pas d'un simple courrier d'information. La formation restreinte a également considéré que ce courrier ne pouvait se rattacher à la « mise en œuvre » d'une politique publique concernant l'habitat à caractère social dès lors que son objet n'était pas de traiter les données personnelles des locataires afin d'appliquer concrètement une politique publique mais bien de critiquer une annonce gouvernementale concernant la baisse à venir des APL.

Sans mettre en cause la possibilité pour l'OPH de s'exprimer sur une réforme en cours, la formation restreinte a par conséquent estimé que l'utilisation des données personnelles issues du fichier des locataires de l'OPH pour adresser ce courrier était incompatible avec la finalité initiale de la collecte de ces données, à savoir la gestion des demandes de logement social ou du parc immobilier. La formation restreinte a prononcé, pour ce manquement à l'article 6.2° de la loi Informatique et Libertés, une sanction de 30 000 euros

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Article 5 du RGPD

Principes relatifs au traitement des DCP

- **Les DCP doivent être traitées de manière licite, loyale et transparente**
- **Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes**
- **Les DCP doivent être adéquates, pertinentes et limitées**
- **Les DCP doivent être exactes et, si nécessaire, tenues à jour**
- **Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire**
- **Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données**

Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

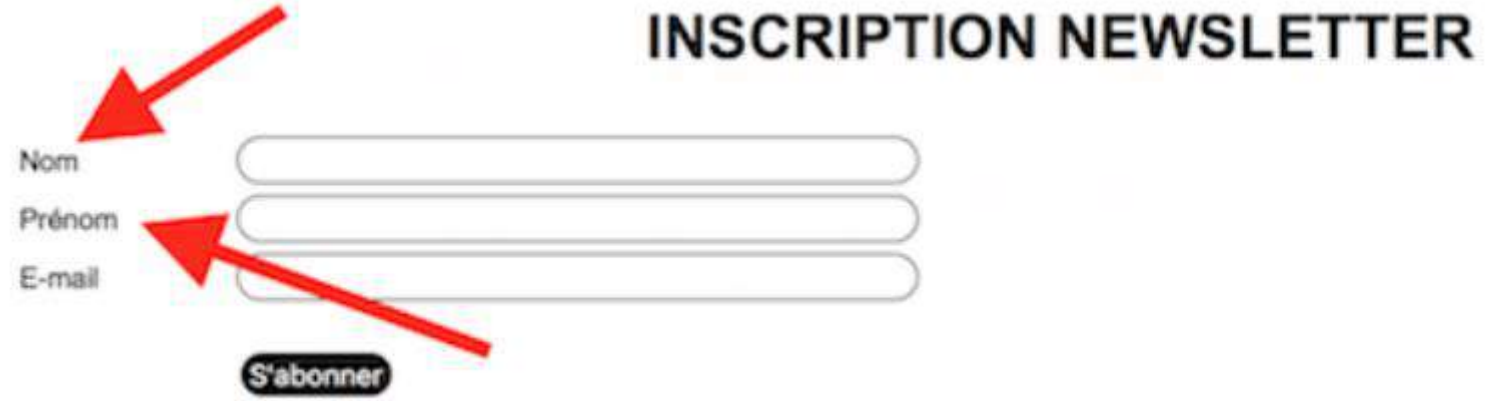
VÉRIFIER LA PERTINENCE DES DONNÉES
Seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées : c'est le principe de minimisation de la collecte.

Le responsable de traitement ne doit donc pas collecter plus de données que ce dont il a vraiment besoin.
Il doit également faire attention au caractère sensible de certaines données.

Ce principe a un **impact pratique majeur** quant aux données collectées.

Prenons un exemple concret afin d'illustrer notre propos :
la mise en place d'une newsletter. Le règlement impose, dans un tel cas, de ne collecter que les données qui sont strictement nécessaires à cette newsletter.

→Quelles sont donc les données susceptibles de pouvoir être collectées à cet égard ?



ni le prénom, ni le nom, ni l'adresse, ni le fait que la personne soit un homme, ou une femme, ni les coordonnées physiques de la personne… Aucune de ces données ne serait en effet strictement nécessaire pour l'envoi de la newsletter (sauf justification particulière – évidemment si vous envoyez une lettre papier – auquel cas vous justifiez alors du besoin de collecter ces informations dans vos finalités).

<u>Deux process devront donc être mis en oeuvre à ce titre :</u>

- purger l'ensemble des données qui ne sont pas strictement nécessaires au sein des applications existantes
- s'assurer de limiter les données collectées à l'avenir.

Attention donc à bien veiller à mettre ces principes en place pour les différents traitements tels que :

- Site Internet
- Paie
- Plan de continuité
- Liste de partenaires
- Contrôle d'accès aux locaux
- Cantine
- Monétique
- Vidéo surveillance
- Géolocalisation de véhicules
- Postes de travail
- Facturation
- Embauche (CV…)
- Outils de prospection commerciale
- Traçabilité des actions informatiques, Logs de serveurs
- Gestion d'accès des sauvegardes
- Centrale téléphonique

Chaque traitement doit être analysé et l'on doit définir une liste de données qui sont nécessaires par rapport aux besoins relatifs à ce traitement – le reste devant être purgé.

Le principe de proportionnalité et de pertinence des données

Seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis

Exemples

Exemples de données non pertinentes ou excessives au regard de l'objectif

- 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
- *La mise sous vidéosurveillance permanente d'un poste de travail ne pourrait intervenir qu'en cas de risque particulier et dûment avéré pour la sécurité du salarié concerné ».*
- *La mise en place d'une base d'empreintes digitales, pour contrôler l'accès à des locaux, ne peut se justifier que face à un fort impératif de sécurité et en l'absence de solutions alternatives moins intrusives ».*

Conformément au Code du travail, la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter de restrictions aux droits et libertés des personnes qui ne seraient pas proportionnées au but recherché et justifiées par l'intérêt légitime de l'entreprise (article 1121 du Code du travail)

Application du principe de minimisation des données:

FOCUS 1 : UTILISATION DE COOKIES

LES RECOMMANDATIONS DE LA CNIL

Information

Etape 1

Informer sur les cookies utilisés via une bandeau dédié et une Charte Cookies

Etape 2

Avoir une page « En savoir plus » où l'utilisateur peut paramétrer les cookies

Consentement

Cookies de fonctionnement et/ou non intrusifs

Pas de consentement nécessaire

Cookies « optionnels »
(marketing, monitoring, profiling)

Consentement nécessaire

FOCUS 2: LA PROSPECTION COMMERCIALE

Par téléphone

Pas de consentement

Information préalable et droit d'opposition

Article 38 de la loi I&L
Articles L.34 et R.10 du CPCE

Par automate d'appel

Consentement préalable

Exceptions

Prospection de nature caritative

Conditions

- préciser l'identité de l'annonceur,
- proposer un moyen simple de s'opposer

Article L.34-5 du CPCE
Article.L.121-20-5 du Code de la consommation

Par SMS

Consentement préalable

Exception

Prospection non commerciale (caritative, etc.)
Déjà client + produits et services analogues

Conditions

- préciser l'identité de l'annonceur,
- proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations

FOCUS 2 : LA PROSPECTION COMMERCIALE PAR COURRIER ÉLECTRONIQUE

PAS DE CONSENTEMENT PRÉALABLE

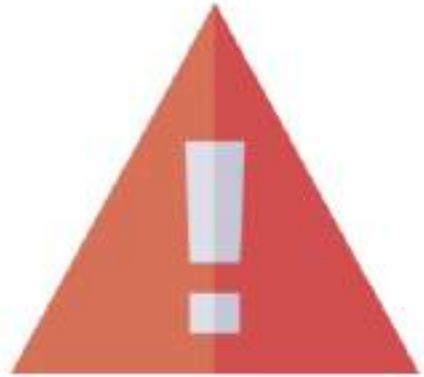
Prospection B2B

Publicité envoyée sur une adresse électronique professionnelle générique (contact@societe.com)

Sollicitation en rapport avec sa profession

Prospection B2C

Publicité concerne des produits ou services analogues à ceux déjà acquis par le consommateur auprès du même organisme



Obligations impératives

Informer que l'adresse électronique sera utilisée à des fins de prospection

Possibilité de s'opposer à cette utilisation de manière simple et gratuite

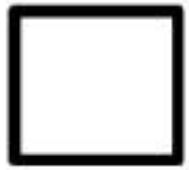
RECUEILLIR LE CONSENTEMENT DES CLIENTS

Art 4 du RGPD : « 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 »

Un consentement par finalité

Collecte opt-out / opt-in passif (case pré-cochée)

Interdite par RGPD



Collecte opt-in (case décochée)

Refus par défaut, préconisé par le RGPD

Règle en matière de prospection commerciale

Retrait du consentement

Le client concernée peut de retirer son consentement à tout moment

FOCUS 3 : L'ENCADREMENT DU PROFILAGE

Traitement automatisé de données personnelles

visant à évaluer, analyser ou prédire les caractéristiques des utilisateurs

Droit de ne pas faire l'objet d'une décision

Fondée exclusivement sur le traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative

Exceptions

(alternatives)

- Consentement explicite
- Nécessaire à l'exécution du contrat
- Autorisé par la législation

FOCUS 3 : L'ENCADREMENT DU PROFILAGE

Réaliser une PIA

Informer
les utilisateurs de l'existence d'un profilage

- Droit d'exprimer son point de vue
- Droit de contester la décision
- Droit d'obtenir une intervention humaine

Mettre en place une procédure d'opposition au profilage

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Article 5 du RGPD

Principes relatifs au traitement des DCP

- **Les DCP doivent être traitées de manière licite, loyale et transparente**
- **Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes**
- **Les DCP doivent être adéquates, pertinentes et limitées**
- **Les DCP doivent être exactes et, si nécessaire, tenues à jour**
- **Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire**
- **Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données**

Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Article 5 du RGPD

Principes relatifs au traitement des DCP

- **Les DCP doivent être traitées de manière licite, loyale et transparente**
- **Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes**
- **Les DCP doivent être adéquates, pertinentes et limitées**
- **Les DCP doivent être exactes et, si nécessaire, tenues à jour**
- **Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire**
- **Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données**

Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Le principe de conservation limitée des données

Les données à caractère personnels doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Exemples

Par exemple (source CNIL) :

Gestion du personnel : *Les données ne sont* ***pas conservées*** *par les services gestionnaires* ***au-delà de la période d'emploi*** *de la personne concernée, sans préjudice de dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression de ces données. Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heures de délégation ne sont pas conservées au-delà de la période de sujétion de l'employé concerné. Au-delà, ces données peuvent être archivées sur un support informatique distinct et à accès très limité, conformément aux règles applicables en matière d'archives publiques et d'archives privées.*

Contrôle d'accès physique aux locaux : *Les éléments d'identification des salariés ou des agents publics ne doivent pas être conservées au delà de* ***5 ans après le départ*** *du salarié ou de l'agent de l'entreprise ou de l'administration.* ***Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois****. Toutefois, les informations relatives aux salariés ou aux agents publics peuvent être conservées pendant 5 ans lorsque le traitement a pour finalité le contrôle du temps de travail. La conservation des données relatives aux motifs d'absence est limitée à une durée de 5 ans sauf dispositions législatives contraires.*

Gestion de la restauration ainsi que la mise en place d'un système de paiement associé : *En cas de paiement direct ou de pré-paiement des repas, les données monétiques ne peuvent être conservées plus de 3 mois. En cas de paiement par retenue sur le salaire, la durée de conservation est de 5 ans.*

Source : – CNIL http://www.cnil.fr

Voir guide sur les durées de conservation de la CNIL…

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Article 5 du RGPD

Principes relatifs au traitement des DCP

- **Les DCP doivent être traitées de manière licite, loyale et transparente**
- **Les DCP doivent être traitées pour des finalités déterminées, explicites et légitimes**
- **Les DCP doivent être adéquates, pertinentes et limitées**
- **Les DCP doivent être exactes et, si nécessaire, tenues à jour**
- **Les DCP doivent être conservées pendant une durée n'excédant pas celle nécessaire**
- **Les DCP doivent être traitées de façon à garantir une sécurité appropriée des données**

Le responsable du traitement est responsable du respect des principes évoqués et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

La sécurité et la confidentialité des données

Règlement européen du 27 Avril 2016

Article 32

« *1. **Compte tenu de l'État des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie**, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adaptée au risque, y compris entre autres, selon les besoins:*

a) ***la pseudonymisation et le chiffrement** des données à caractère personnel;*

b) *des moyens permettant de **garantir la confidentialité, l'intégrité, la disponibilité et la résilience** constantes des systèmes et des services de traitement;*

c) *des moyens permettant de rétablir la **disponibilité des données à caractère personnel et l'accès** à celles-ci dans **des délais appropriés en cas d'incident physique ou technique;***

d) *une procédure visant à **tester, à analyser et à évaluer régulièrement l'efficacité** des mesures techniques et organisationnelles pour assurer la sécurité du traitement.*

*2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier **des risques** que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.*

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément attestant du respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, ˆ moins d'y être obligée par le droit de l'Union ou le droit d'un État membre ».

La sécurité et la confidentialité des données

Règlement européen du 27 Avril 2016

Article 33: Notification à l'autorité de contrôle d'une violation de données à caractère personnel

« 1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

3. La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, sipossible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données

e) à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article ».

La sécurité et la confidentialité des données

Règlement européen du 27 Avril 2016

Article 34: Communication à la personne concernée d'une violation de données à caractère personnel

« 1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

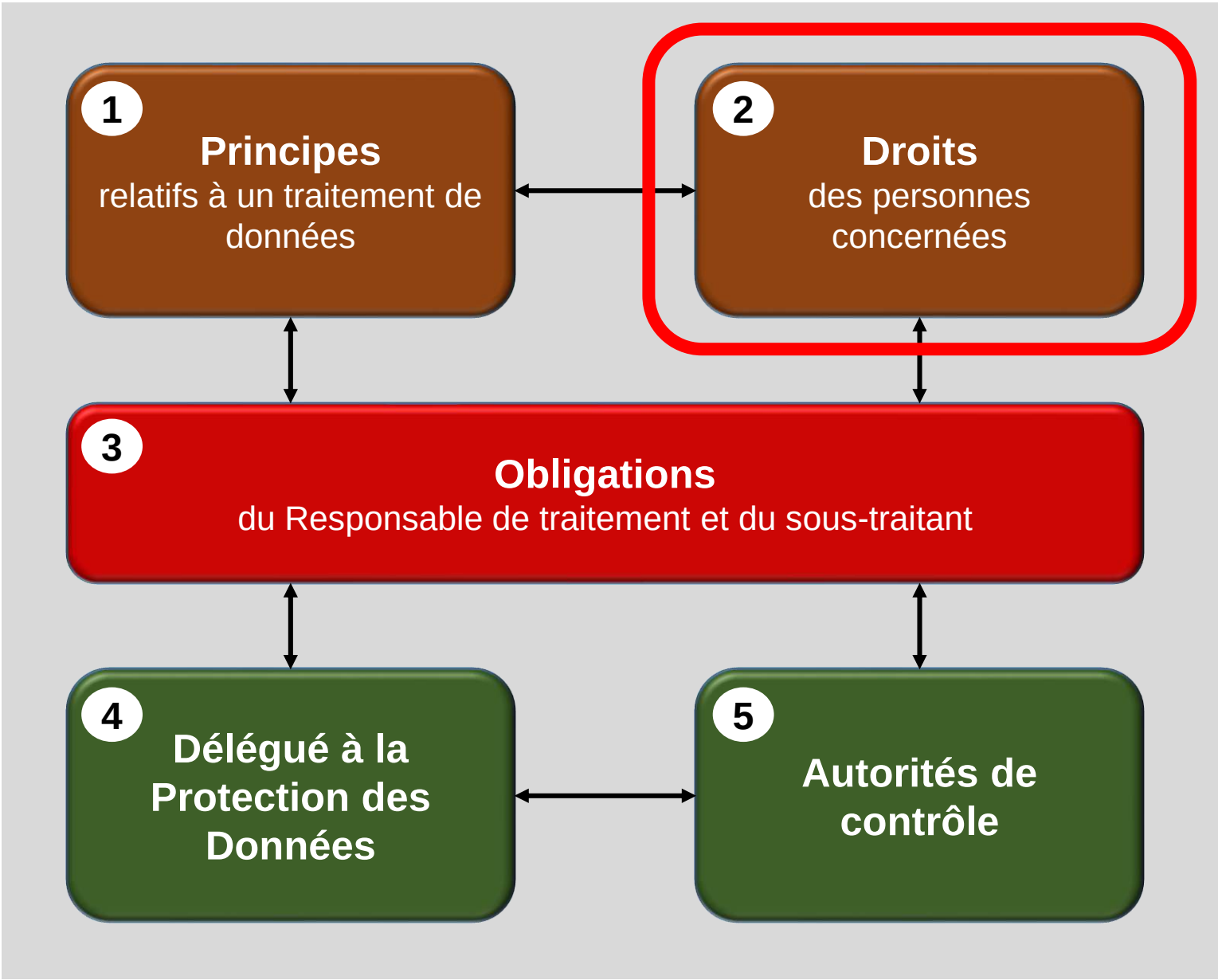
2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et recommandations prévues à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

- *a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces dernières ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;*
- *b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;*
- *c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.*

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie ».

RGPD – Les exigences relatives aux traitements de données à caractère personnel



Droit d'information

Article 12

Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

Le responsable du traitement prend des mesures appropriées pour fournir à la personne concernée toute information en ce qui concerne le traitement d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Les informations sont fournies **par écrit ou par d'autres moyens** y compris, lorsque c'est approprié, par **voie électronique**.

Lorsque la personne concernée en fait la demande, les informations peuvent être fournies **oralement**, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée**, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande**. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes

Aucun paiement n'est exigé pour fournir les informations.

Lorsque les demandes d'une personne concernée sont manifestement **infondées ou excessives**, notamment en raison de leur caractère répétitif, le responsable du traitement peut:

a) **exiger le paiement** de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées;

ou

a) **refuser de donner suite** à ces demandes.

Droit d'information

Article 13

Informations à fournir lorsque des données à caractère personnel sont **collectées auprès de la personne** concernée

Les informations à fournir (selon le type de traitement) :

1. l'identité et les coordonnées du RT
2. les coordonnées du délégué à la protection des données;
3. les finalités du traitement ainsi que la base juridique du traitement;
4. Les intérêts légitimes poursuivis par le RT ou par un tiers;
5. Les destinataires ou les catégories de destinataires des données
6. Le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation
7. la durée de conservation des données
8. l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;
9. l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement
10. le droit d'introduire une réclamation auprès d'une autorité de contrôle;
11. des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat
12. l'existence d'une prise de décision automatisée, y compris un profilage

Droit d'information

Article 14

Informations à fournir lorsque les données à caractère personnel **n'ont pas été collectées** auprès de la personne concernée

En plus des informations évoquées au paragraphe précédent, le responsable du traitement doit **préciser la source d'où proviennent les données** à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

Le responsable du traitement fournit les informations :

a) dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées;

b) si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne; ou

c) s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente.

Droits des personnes concernées (article 12 à 22 du RGPD)

Droit d'accès Article 15	La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel
Droit de rectification Article 16	La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes.
Droit d'effacement (droit « à l'oubli ») Article 17	La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais.
Droit d'opposition Article 21	La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant, y compris un profilage.
Droit à la portabilité Article 20 	Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle

Les délais de traitements des demandes passent à 1 mois maximum (Prolongement de 2 mois possible)

Droits des personnes concernées (article 12 à 22 du RGPD)

Droit à la limitation du traitement

Article 20

La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique:

a) l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel;
b) le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;
c) le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;
d) la personne concernée s'est opposée au traitement en vertu de l'article 21, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement

Article 19

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande.

Décision individuelle automatisée, y compris le profilage

Article 22

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.


Accès
Rectification
Effacement
Limitation
Oui
Non
Opposition
a
b
Portabilité
CNIL
Réclamation
Actions

Gestion des demandes : Exemple de procédure de traitement d'une demande

1. Procédure à appliquer

Actions à réaliser		Description de l'action	Responsable de l'action	Document(s) associé(s) à l'action
1	Vérifier la légitimité de la demande	A réception de la demande par écrit et après vérification de l'identité du demandeur, le Service Juridique la légitimité de la demande. Il peut formuler par écrit au demandeur des précisions sur la demande. Toute demande non recevable doit être juridiquement argumentée et les motifs du refus de traiter la demande doivent être transmis par écrit au demandeur	Le Service Juridique	
2	Informer les Directeurs concernés par la demande	Le Service Juridique informe par courriel les responsables de service concernés par la demande et leur précisant : • La nature des actions à mener pour traiter la demande • Le délai de réponse attendu	Le Service Juridique	Courrier du demandeur
3	Traiter la demande	Les responsables des services concernés se chargent de traiter la demande et de préparer les documents, traces, preuves de la bonne exécution de la demande Ils doivent sans délai informé le Service Juridique pour toutes difficultés rencontrées dans l'application de la demande en les justifiant.	Les responsables concernés par la demande	
4	Constituer le de dossier de réponse	Le Service Juridique se charge de recueillir tous les documents, traces et preuves auprès des responsables de service et prépare le dossier de réponse.	Le Service Juridique	Documents, traces et preuves de réalisation de la demande
5	Transmettre les résultats de la demande au demandeur	**Après vérification de la qualité et complétude du dossier de réponse, le Service Juridique** transmet le dossier de réponse au demandeur par courrier postal en recommandé avec accusé de réception.	Le Service Juridique	Courrier de réponse
6	Mise à jour du registre des demandes	**Le Service Juridique met à jour le registre des demandes afin de conserver les traces de suivi**	Le Service Juridique	Registre des demandes
Fin du cas particulier (attente du courrier : procédure générale)				

Gestion des demandes : Exemple de registre de suivi des demandes

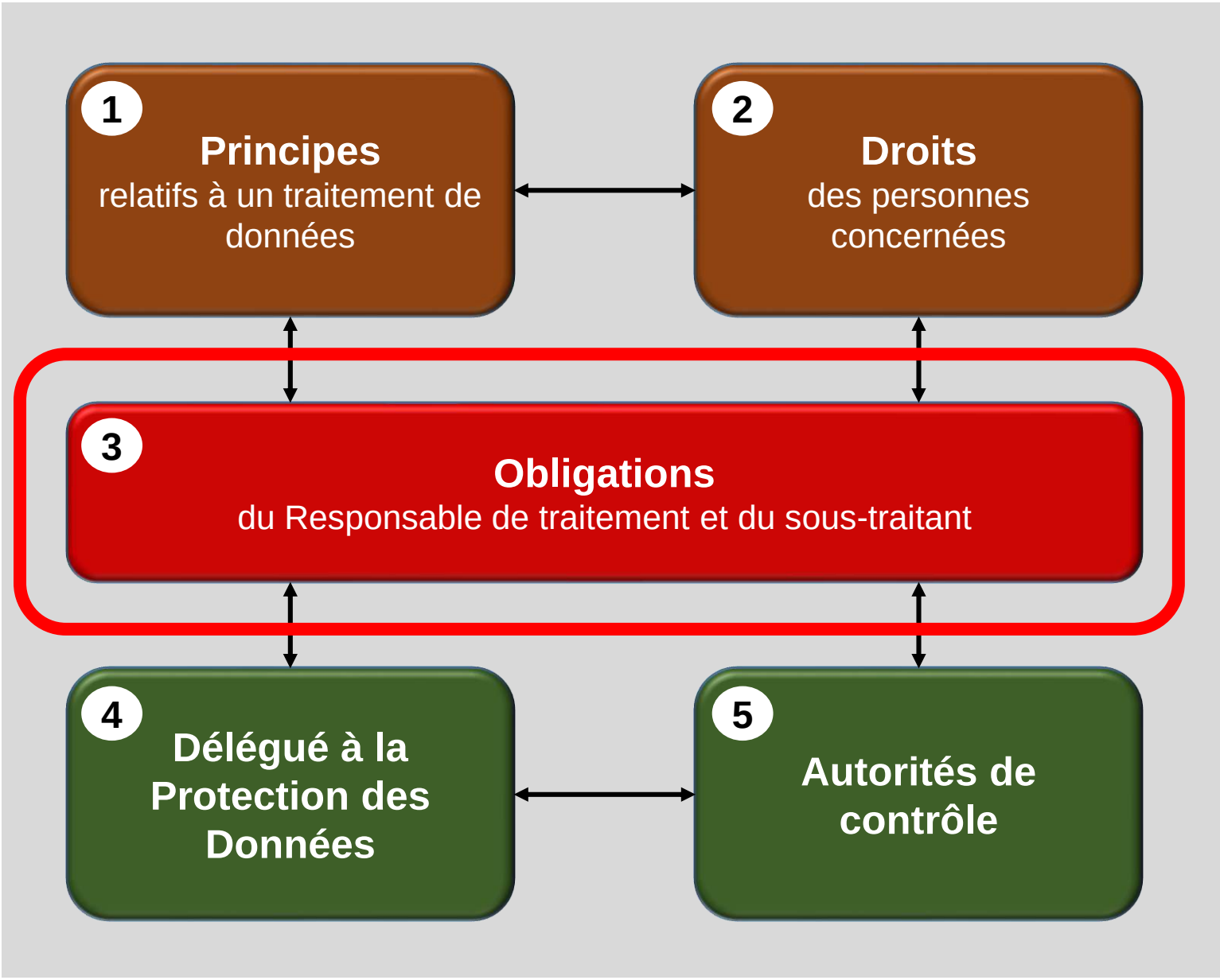
Registre des réclamations

Description de la réclamation					Gestion de la réclamation			
Type de réclamation	Description synthétique de la réclamation	Origine de la réclamation	Date de réception de la réclamation	Services et traitements concernés par la réclamation	Délai de traitement de la réclamation	Services impliqués dans le traitement de la réclamation	Alerte du RT	Statut de la réclamation

Recours pour les personnes concernées (article 12 à 22 du RGPD)

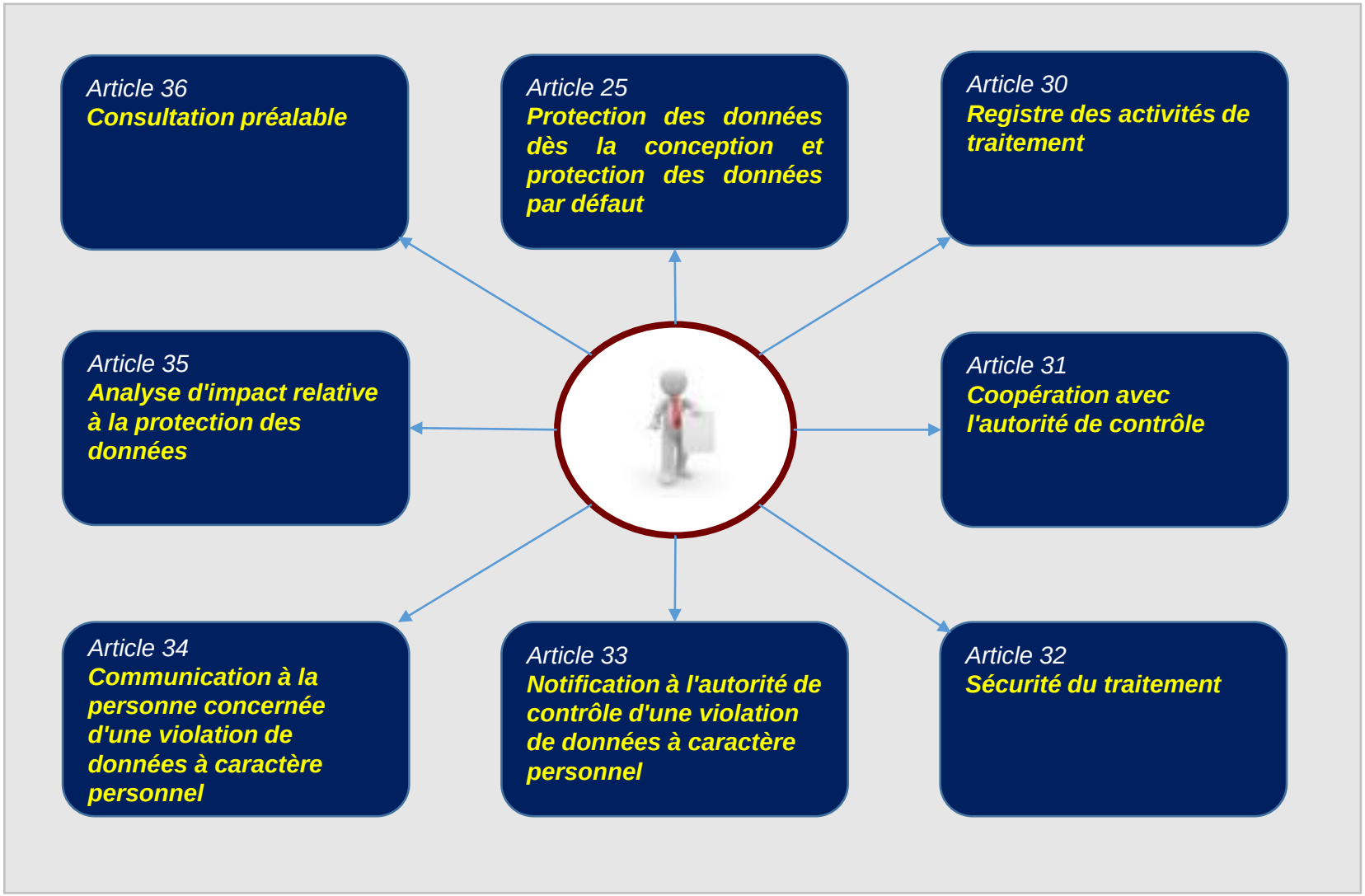
Droit d'introduire une réclamation auprès de la CNIL Article 77	Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.
Droit à un recours juridictionnel contre la CNIL Article 78 	Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.
Droit à un recours juridictionnel contre un RT et un sous-traitant Article 79 	Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement.
Représentation des personnes concernées Article 80 	La personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits visés aux articles 77, 78 et 79 et exerce en son nom le droit d'obtenir réparation visé à l'article 82 lorsque le droit d'un État membre le prévoit.

RGPD – Les exigences relatives aux traitements de données à caractère personnel



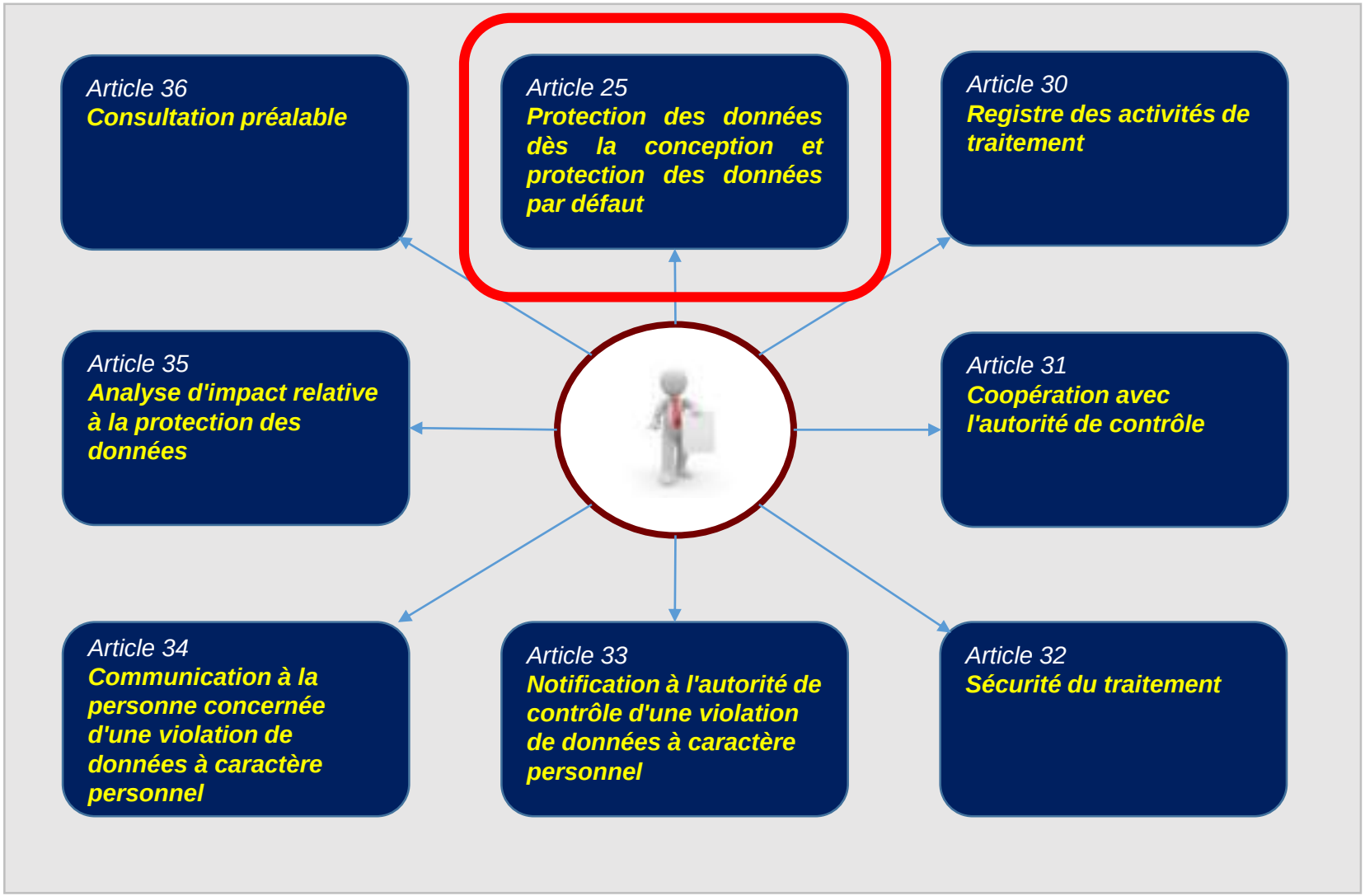
Responsabilités du responsable des traitements

«responsable du traitement», la 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



Responsabilités du responsable des traitements

«responsable du traitement», la 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



Protection des données dès la conception et protection des données par défaut

Articles 25

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le **responsable du traitement met en œuvre tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées**, telles que la pseudonymisation, qui sont destinées à mettre en oeuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, **par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées**. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

L'approche « Privacy By Design » consiste pour une entreprise à développer des produits et des services en prenant en compte, dès leur conception et tout au long de leur cycle de vie, les aspects liés à la protection de la vie privée et des données à caractère personnel.

Cela implique de prendre en compte, dès la conception de projets informatiques destinés à traiter des données personnelles, les exigences en matière de protection de la vie privée et les intégrer aux systèmes informatiques, infrastructures des réseaux et pratiques de l'entreprise.

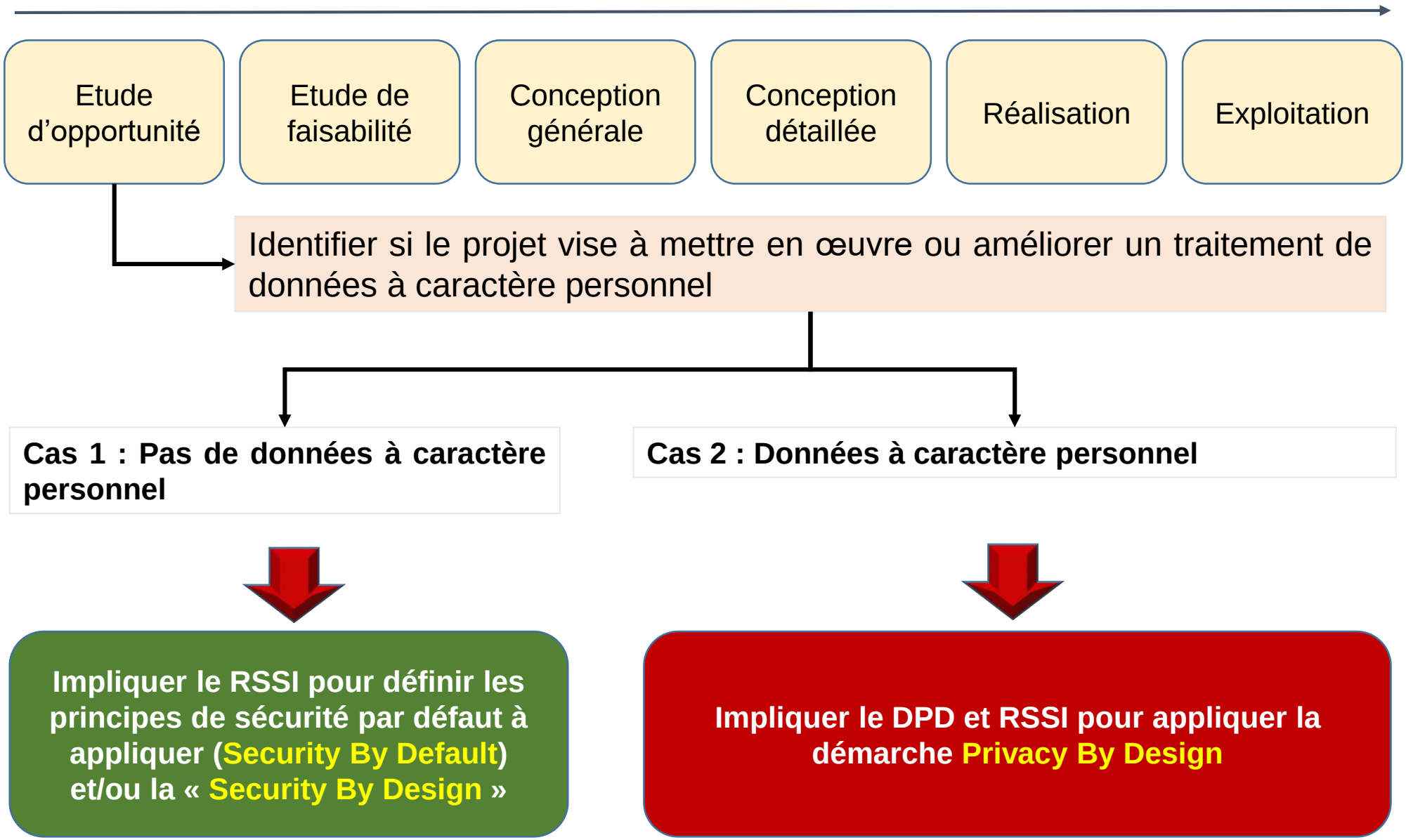
Avant le RGPD

Message de géolocalisation par défaut pendant l'utilisation d'une application

Après le RGPD

La géolocalisation devra être activée dans les paramètres. Par défaut, elle sera inactive.

Intégration des étapes du Privacy By Design dans la démarche projet



Intégration des étapes du Privacy By Design dans la démarche projet

Etude d'opportunité | Etude de faisabilité | Conception générale | Conception détaillée | Réalisation | Exploitation

Identifier si le traitement de données présente des risques élevés pour les droits et les libertés des personnes concernées

Renseigner une fiche de déclaration d'un traitement

Cas 1 : Pas de risques élevés pour les personnes concernées

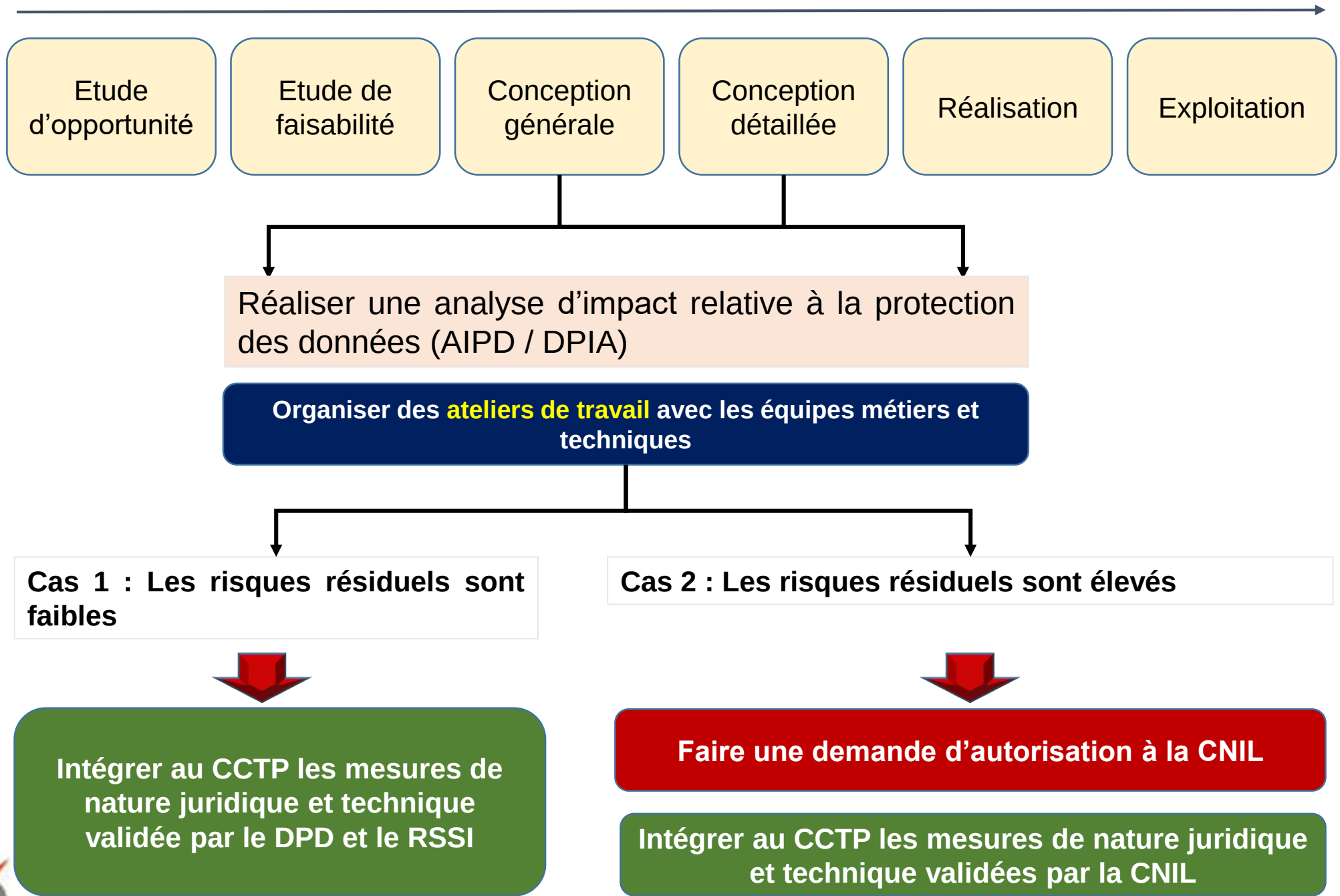
Appliquer des principes de « Privacy By Defaut »

- **Respect des droits des personnes**
- **Purge de données**
- **Limitation des données**
- **Qualité des données**
- **Sécurité de base des données**

Cas 2 : Traitement susceptible de présenter des risques élevés pour les personnes concernées

Faire une Analyse d'impact relative à la protection des données DPIA / AIPD

Intégration des étapes du Privacy By Design dans la démarche projet



Intégration des étapes du Privacy By Design dans la démarche projet

Etude d'opportunité | Etude de faisabilité | Conception générale | Conception détaillée | Réalisation | Exploitation

S'assurer que les mesures de nature juridique et technique sont mises en œuvre dans les solutions retenues

Cas 1 : le projet est réalisé en interne (pas d'hébergeur externe, pas de sous-traitance, …)

RSSI : Réaliser des tests de sécurité (basé sur le guide PASSI de l'ANSSI)
DPD : Valider la mise en œuvre des mesures de nature juridique (audit de conformité)

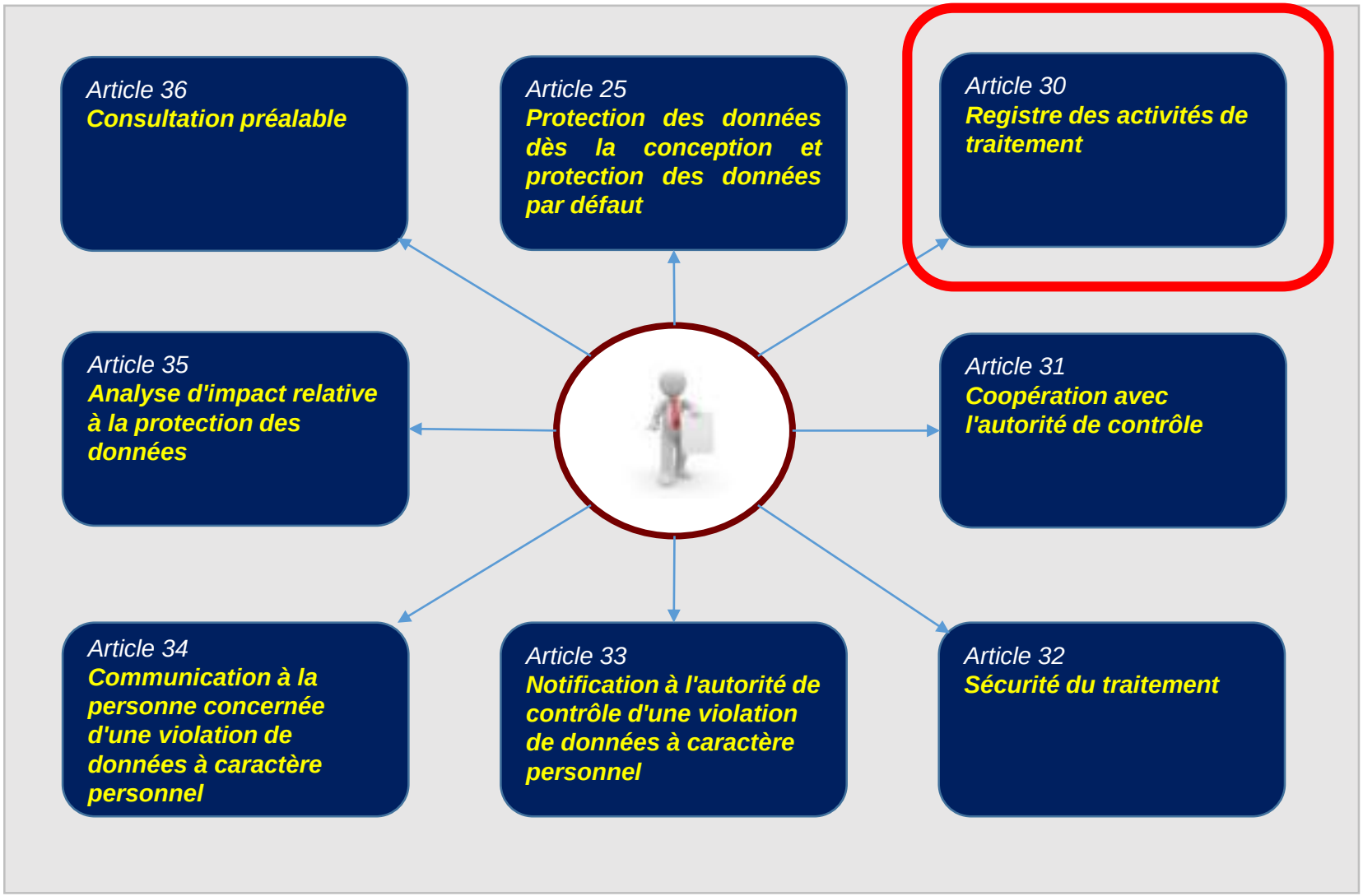
Cas 2 : Le projet prévoit des sous-traitants

Prévoir les Clauses Contractuelles au contrat (prise en compte des articles 28,29 et 30 du RGPD)

RSSI : Réaliser des tests de sécurité (basé sur le guide PASSI de l'ANSSI)
DPD : Valider la mise en œuvre des mesures de nature juridique (audit de conformité)

Responsabilités du responsable des traitements

«responsable du traitement», la 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



Les formalités préalables à la mise en œuvre d'un traitement

Les différents régimes de formalités préalables selon la loi « Informatique & Libertés »

Applicable jusqu'au 25 mai 2018

5 Procédures

1 — Dispense

art° 24 II de la LIL

Pour les catégories les plus courantes de traitements de DCP et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée

2 — Déclarations simplifiées

Cadres de référence qui définissent les finalités, les données pouvant être collectées et les modalités de mise en œuvre du traitement afin de simplifier les formalités à accomplir

Déclaration de conformité

Normes Simplifiées

art°24 de la LIL

Pour les fichiers ou traitements de DCP les plus courants qui ne portent pas atteinte à la vie privée ou aux libertés

Autorisation Unique

art°25 II de la LIL

Pour les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires

Secteur public et secteur privé

3 — Déclaration normale

art° 22 et 23 de la LIL

Traitement des DCP ne soulevant pas de difficultés particulières (et/ou portant sur des données courantes)

Acte Règlementaire Unique (RU)

art° 26 IV de la LIL

Secteur public et secteur privé chargé d'une mission de service public

4 — Demande d'autorisation

art° 25 de la LIL

Traitement des DCP sensibles ou perçues comme sensible. Traitements pouvant présenter des risques pour la vie privée. Réponse sous 2 mois (renouvelable), au delà rejetée.

Méthodologie de référence

art° 54 IV de la LIL

Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

5 — Demande d'avis

Traitement des DCP sensibles ou perçues comme sensible. Traitements pouvant présenter des risques pour la vie privée.

Demande d'avis facultative Art. 11 d) de la LIL

Réponse de la CNIL aux demandes d'avis des pouvoirs publics et des juridictions

Demande d'avis obligatoires art. 26 et 27 de la LIL

Autorisé par arrêté du(es) ministre(s) compétent(s), pris après avis motivé et publié de la CNIL

Les formalités préalables à la mise en œuvre d'un traitement

Les différents régimes de formalités préalables selon la loi « Informatique & Libertés »

Maintenu après le 25 mai 2018

5 Procédures

1 — Dispense

art° 24 II de la LIL

Pour les catégories les plus courantes de traitements de DCP et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée

2 — Déclarations simplifiées

Cadres de référence qui définissent les finalités, les données pouvant être collectées et les modalités de mise en œuvre du traitement afin de simplifier les formalités à accomplir

Déclaration de conformité

Normes Simplifiées

art° 24 de la LIL

Pour les fichiers ou traitements de DCP les plus courants qui ne portent pas atteinte à la vie privée ou aux libertés

Secteur public et secteur privé

Autorisation Unique

Secteur de la santé
Recherche en santé

Pour les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires

Acte Règlementaire Unique (RU)

art° 26 IV

Secteur public et secteur privé chargé d'une mission de service public

Méthodologie de référence

Santé et secteur public

art° 54 IV de la LIL

Pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé.

3 — Déclaration normale

art° 22 et 23 de la LIL

Traitement des DCP ne soulevant pas de difficultés particulières (et/ou portant sur des données courantes)

4 — Demande d'autorisation

art° 25 de la LIL

Traitement des DCP sensibles ou perçues comme sensible. Traitements pouvant présenter des risques pour la vie privée. Réponse sous 2 mois (renouvelable), au delà rejetée.

5 — Demande d'avis

Traitement des DCP sensibles ou perçues comme sensible. Traitements pouvant présenter des risques pour la vie privée.

Demande d'avis facultative Art. 11 d) de

Activités régaliennes de l'état

Réponse de la CNIL aux demandes d'avis des pouvoirs publics et des juridictions

Demande d'avis obli…

Autorisé par arrêté du(es) ministre(s) compétent(s), pris après avis motivé et publié de la CNIL

Seuls deux régimes de formalités à réaliser auprès de la CNIL demeurent, pour des hypothèses très ciblées :

1. Le régime de l'autorisation pour :

- Les traitements présentant une **finalité d'intérêt public**.

Ex : la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.
La CNIL exigera la production d'une analyse d'impact pour instruire les demandes d'autorisation présentant une finalité d'intérêt public.

- Les traitements automatisés dont la finalité est ou devient **la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention**.

2. Le régime de la demande d'avis sur un projet d'acte réglementaire autorisant un traitement de données de santé.

Les traitements de données de santé comportant le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques (NIR) doivent être prévus par un décret cadre, pris après avis motivé et publié de la CNIL, à l'exception de ceux d'entre eux qui entrent dans le champ de l'autorisation (traitement fondé sur l'intérêt public ou concernant une recherche).

Registre des traitements

Article 30

Chaque responsable du traitement et, le cas échéant, le représentant du 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, le cas échéant, du responsable conjoint du traitement, 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, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

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.

Pour les responsables de traitement	Pour les sous-traitants
• Nom et coordonnées du responsable du traitement, de son représentant et du DPO ; • Finalités du traitement ; • Catégories de personnes et de données à caractère personnel ; • Catégories de destinataires ; • Transfert vers pays tiers ; • Délais de conservation ou les moyens de déterminer ce délai de conservation ; et • Description des mesures de sécurité si possible	• Nom et coordonnées du responsable du traitement et du/des sous-traitant, de leur représentant et du DPO ; • Catégories de traitements pour chaque responsable de traitement ; • Les transferts vers des pays tiers ; et • La description générale des mesures de sécurité si possible.

	Information à faire figurer	RT	ST	Informations à faire figurer par le sous-traitant (société Y) dans sa fiche de registre
QUI ?	Nom et coordonnées du RT (+ son représentant et DPO le cas échéant)Nom et coordonnées du sous-traitant (+ son représentant et DPO le cas échéant)	✖	✖	Société X – DPO : Madame Marie MARTIN
	Nom et coordonnées du sous-traitant		✖	Société Y
Pourquoi ?	Finalités du traitement	✖		Gestion de la clientèle (gestion des commandes et des les livraisons ; suivi de facturation ; Marketing et publicité personnalisés)
	Catégories de traitement		✖	• ST : hébergement des données, effacement à la demande du RT • RT : enregistrement, stockage, envoi de mails, SMS, courriers
Quoi ?	Personnes concernées et catégories de données concernées	✖		• clients de la société X • nom, prénom, titre, sexe, adresse, numéro de téléphone, adresse mail…)
Où ?	Destinataires	✖		Société X (équipe commerciale, DAF)
	Transfert vers un pays tiers ou organisation internationale	✖	✖	Aucun transfert – données hébergées en France
Jusqu'à quand ?	Délais de conservation et d'effacement des données	✖		Durée du contrat avec le Client + 2 ans
Comment ?	Description de mesures de sécurité techniques et organisationnelles	✖	✖	RT : Identification et mot de passe pour accéder à l'application… ST : cloisonnement des architectures réseau, sondes anti-intrusion…

A noter :

- **Une entreprise pourra voir une double-casquette.**
  Exemple : un hébergeur sera à la fois responsable de traitement (pour les traitements relatifs à la gestion de son personnel) et sous-traitant (pour les clients pour le compte desquels il assure l'hébergement).

- **La liste des traitements qui font chacun l'objet d'une fiche distincte doit être établie par finalité principale (et non par outil ou applicatif utilisé).**
  Exemple : La société X a mis en place plusieurs dispositifs de sécurité : caméra de vidéosurveillance, badges d'entrée pour les salariés. Ces 2 outils collectent des données personnelles. Une fiche pour le traitement « Surveillance des biens et locaux » sera créée dans le registre des activités de la société ayant pour finalités : assurer la sécurité des biens et des personnes, prévenir les risques. Mais les badges d'entrée remis aux salariés servent également à surveiller les horaires d'arrivée des salariés, ce qui correspond à un autre traitement et fera donc l'objet d'une autre fiche.

Exemple de fiche permettant de recenser les traitements

Fiche de traitement

Nom du Traitement		Date de renseignement de la fiche de déclaration du traitement	
Service en charge de la mise en œuvre du traitement		Site(s) conconcerné(s) par le traitement	
Responsable du service en charge de la mise en œuvre du traitement		Nombre de personnel impliqué dans la réalisation des opérations de traitement	

1. Finalité(s) du traitement		**Fondement juridique du traitement**	**Référence du fondement juridique**
Finalité Principale			
Sous-Finalité			
Sous-Finalité			
Sous-Finalité			
Sous-Finalité			
Sous-Finalité			

2. Catégorie(s) de personnes concernées par le traitement			
Personnes concernées par le traitement			
Volumétrie (approximative) du nombre de personnes concernées			

3. Description des données collectées dans le cadre du traitement			
Type de données collectées	Lister dans le détail les **données traitées**	Lister les **destinataires** externes ou internes à qui les données peuvent être transmises	**Durée de conservation** des données nécessaire au regard de la finalité du traitement
Etat-civil, identité, données d'identification, images (nom, prénom, adresse, photographie, date et lieu de naissance, etc.)			
Vie personnelle (habitudes de vie, situation familiale, etc.)			
Vie professionnelle (CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)			
Informations d'ordre économique et financier (revenus, situation financière, coordonnées bancaires, etc.)			
Données de connexion (adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)			
Données de localisation (déplacements, données GPS, GSM, …)			
Internet (cookies, traceurs, données de navigation, mesures d'audience, …)			
Données à caractère hautement personnel (difficultés sociales, mouvement financiers / bancaires, …)			
Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques ou appartenance syndicale, données génétiques et biométriques, données concernant la santé, la vie sexuelle ou l'orientation sexuelle)			
Données relatives aux condamnations pénales ou aux infractions			
Numéro d'identification national unique (NIR ou numéro de sécurité sociale)			
Autres données à préciser			

Exemple de fiche permettant de recenser les traitements

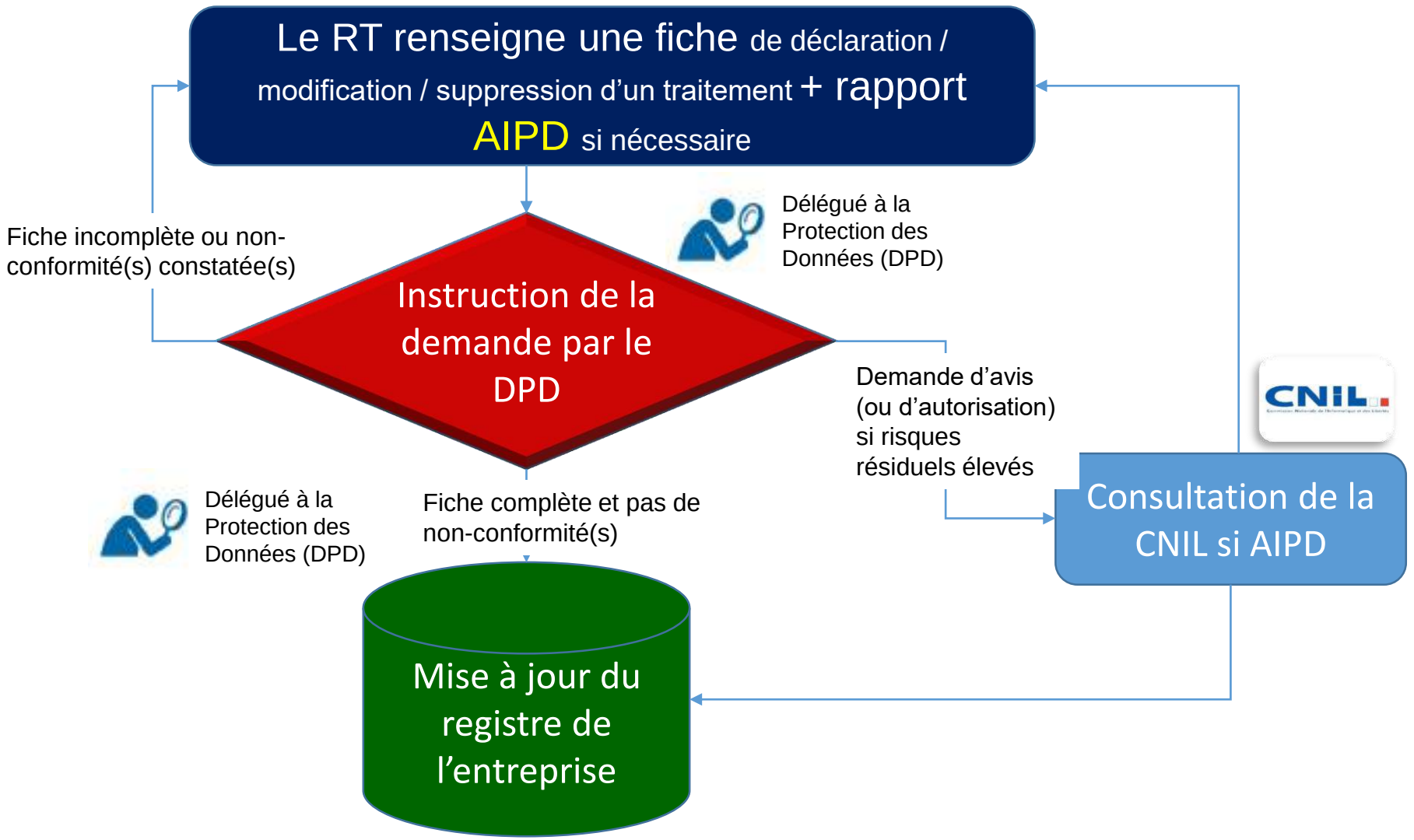
4. Sous-traitants impliqués dans la réalisation du traitement			
Nom du sous-traitant	Opération(s) sous-traitée(s)	Référence du contrat signé	Durée du contrat

5. Transfert de données hors UE			
Des données personnelles sont-elles transmises hors de l'Union européenne ?		Si oui, vers quel(s) pays	

6. Liste des moyens utilisés pour la mise en œuvre du traitement			
Moyens **informatiques** permettant la **collecte** des données		**Autres moyens** permettant la **collecte** des données	
Moyens **informatiques** permettant la **conservation ou le stockage** des données		**Autres moyens** permettant la **concervation ou le stockage** des données	
Moyens **informatiques** permettant **l'utilisation** des données		**Autres moyens** permettant **l'utilisation** des données	
Moyens **informatiques** permettant le **transfert** des données		**Autres moyens** permettant le **transfert** des données	
Moyens **informatiques** permettant la **destruction** des données		**Autres moyens** permettant la **destruction** des données	
Moyens **informatiques** permettant l'archivage des données		**Autres moyens** permettant l'archivage des données	

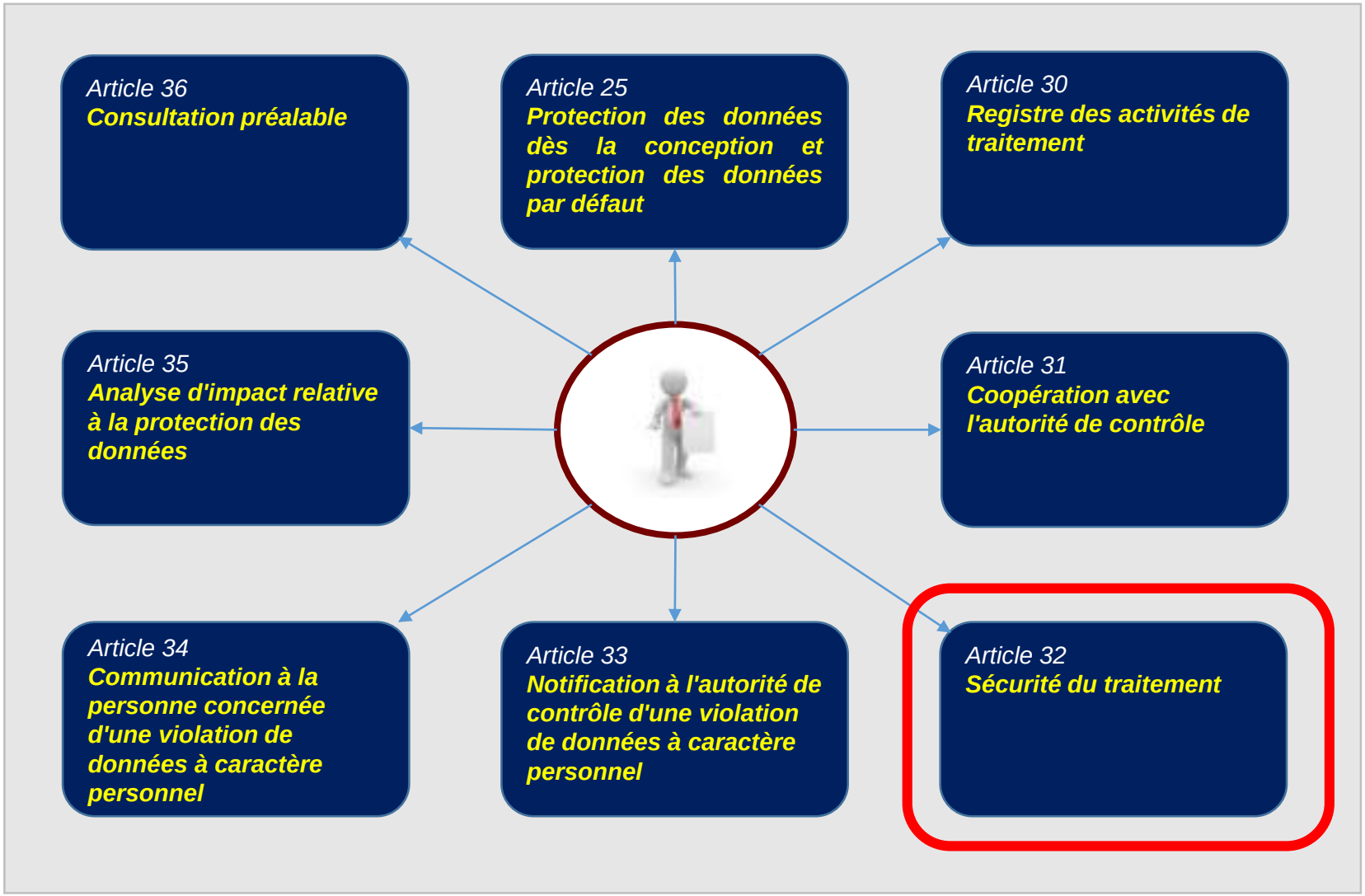
7. Description des mesures techniques et organisationnelles de sécurité			
Catégorie de mesure de sécurité	Description des mesures de sécurité	Catégorie de mesure de sécurité	Description des mesures de sécurité
Contrôle de l'accès aux installations : Empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement		**Contrôle des supports de données** : Empêcher que des supports de données puissent être lus, copiés, modifiés ou supprimés de façon non autorisée	
Contrôle de la conservation : Empêcher l'introduction non autorisée de données à caractère personnel dans le fichier, ainsi que l'inspection, la modification ou l'effacement non autorisé de données à caractère personnel enregistrées		**Contrôle des utilisateurs** : Empêcher que les systèmes de traitement automatisé puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données	
Contrôle de l'accès aux données : Garantir que les personnes autorisées à utiliser un système de traitement automatisé ne puissent accéder qu'aux données à caractère personnel sur lesquelles porte leur autorisation		**Contrôle de la transmission :** Garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données	
Contrôle de l'introduction : Garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé, et à quel moment et par quelle personne elles y ont été introduites		**Contrôle du transport** : Empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou supprimées de façon non autorisée	
Restauration : Garantir que les systèmes installés puissent être rétablis en cas d'interruption et rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique		**Intégrité** : Garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système	
Sensibilisation / formation du personnel : S'assurer que le personnel a suffisament été sensibilisé et responsabilisé sur les obligations qui lui incombe en matière de sécurité des données et de transparence sur les traitements réalisés		**Gestion des violations de données** : Garantir que les incidents de sécurité sur les données sont détectés et traités pour réduire les risques sur les droits et les libertés des personnes concernées	
Test et audit : procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement		**Protection des documents (papiers)** : Garantir que les documents papiers sont suffisament protégés contre le vol, la destruction ou la perte	

La démarche de mise à jour du registre des traitements :



Responsabilités du responsable des traitements

«responsable du traitement», la 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



Sécurité du traitement

Article 32

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre **les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; d)une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Sanction de 75 000 euros pour une atteinte à la sécurité des données de demandeurs de logements

28 juin 2018

La formation restreinte de la CNIL a prononcé une sanction de 75 000 euros à l'encontre de l'Association pour le Développement des Foyers (ADEF) pour avoir insuffisamment protégé les données des utilisateurs de son site internet.

L'association ADEF a pour mission la mise à disposition de logements dans des résidences et foyers notamment pour des étudiants, des familles monoparentales et des travailleurs migrants.

En juin 2017, la CNIL a été informée de l'existence d'un incident de sécurité qui conduisait à rendre librement accessibles les données personnelles des demandeurs de logement ayant effectué une démarche d'inscription sur le site internet de l'association.

ALLIANCE FRANCAISE PARIS ÎLE DE FRANCE : sanction de 30.000€ pour une atteinte à la sécurité des données des utilisateurs

27 septembre 2018

La formation restreinte de la CNIL a prononcé une sanction de 30.000 euros à l'encontre de l'association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE pour avoir insuffisamment sécurisé les données des personnes suivant les cours de français qu'elle dispense.

En novembre 2017, la CNIL a été informée de l'existence d'un incident de sécurité sur le site internet de l'association **ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE** qui conduisait à rendre librement accessibles les données des personnes suivant des cours de français.

Un contrôle en ligne effectué en décembre 2017 a permis de constater qu'en modifiant un numéro d'identifiant contenu dans une URL correspondant à l'espace utilisateur, il était possible de télécharger des documents contenant des données personnelles, tels que des factures, des certificats d'inscription ou des récapitulatifs des cours suivis.

DAILYMOTION : sanction de 50.000€ pour une atteinte à la sécurité des données des utilisateurs

02 août 2018

La formation restreinte de la CNIL a prononcé une sanction de 50.000 euros à l'encontre de la société DAILYMOTION pour avoir insuffisamment sécurisé les données des utilisateurs inscrits sur sa plateforme d'hébergement de contenus vidéo.

En décembre 2016, un article de presse faisait état d'une importante fuite de données relative à la plateforme DAILYMOTION.

Au cours d'un contrôle réalisé au sein des locaux de la société, celle-ci a indiqué que la violation de données résultait d'une attaque menée en plusieurs étapes et que celle-ci avait concerné 82,5 millions d'adresses emails ainsi que 18,3 millions de mots de passe chiffrés.

Les informations transmises par la société ont fait apparaître que les attaquants sont parvenus à accéder aux identifiants d'un compte administrateur de la base de données de la société, stockés en clair sur la plateforme collaborative de développement « Github ». Les attaquants ont ensuite exploité une vulnérabilité trouvée dans le code de la plateforme DailyMotion sur « GitHub ». Cette vulnérabilité leur a permis d'utiliser le compte administrateur pour accéder à distance à la base de données de la société et extraire les données personnelles des utilisateurs.

OPTICAL CENTER : sanction de 250.000€ pour une atteinte à la sécurité des données des clients du site internet www.optical-center.fr

07 juin 2018

La formation restreinte de la CNIL a prononcé une sanction de 250.000 euros à l'encontre de la société OPTICAL CENTER pour avoir insuffisamment sécurisé les données de ses clients effectuant une commande en ligne à partir de son site internet.

En juillet 2017, la CNIL a été informée d'une « *fuite de données conséquentes* » concernant la société OPTICAL CENTER.

Un contrôle en ligne a permis aux équipes de la CNIL de constater qu'il était possible, en renseignant plusieurs URL dans la barre d'adresse d'un navigateur, d'accéder à des centaines de factures de clients de la société. Ces factures contenaient des données telles que les nom, prénom, adresse postale ainsi que des données de santé (correction ophtalmologique) ou encore, dans certains cas, le numéro de sécurité sociale des personnes concernées.

Alertée le même jour par la CNIL, la société s'est rapprochée de son prestataire pour qu'il prenne les mesures nécessaires afin de mettre fin à cet incident de sécurité.

Principes relatives aux traitements de données à caractère personnel (article 5 à 11 du RGPD)

Confidentialité	Ex. : Vols/divulgations de DCP et/ou matériel, erreurs d'habilitation/intrusions donnant accès à des données, diffusion d'informations confidentielles en interne ou en externe	Portée
Niveaux	**Exemples**	**Nbr de PC**
Critique	• Vol/perte de matériel donnant accès à des informations très sensibles **(niveau 3/4)** quelle que soit la protection • Erreurs d'habilitation sur une application donnant accès à des informations très sensibles **(niveau 3/4)** • Divulgation externe d'informations très sensibles **(niveau 3/4)**	
Important	• Vol/perte de matériel donnant accès à des informations sensibles **(niveau 2**) facilement accessibles (absence de chiffrement…) • Erreurs d'habilitation sur une application donnant accès à des informations sensibles **(niveau 2)** • Divulgation externe d'informations sensibles **(niveau 2)**	
Mineur	• Vol/perte de matériel • Erreurs d'habilitation sur une application donnant accès à des informations peu sensibles **(niveau 1)** • Divulgation externe d'informations peu sensibles **(niveau 1)**	

Intégrité	Ex : Dégradation de la qualité des données/corruption des bases quelle que soit la cause (erreur humaine, problème informatique…), infection virale ciblée non détectée ou quasi-généralisée, d'effacement du site internet, installation de logiciels non autorisés	Portée
Niveaux	**Exemples**	**Nbr de PC**
Critique	• Perte d'intégrité dans une application ou des données très sensibles **(niveau 3/4)** • Reconstruction des données impossible ou partielle entraînant une interruption du processus métier ou des risques juridiques • Code malicieux non intercepté par l'antivirus ayant infecté un poste contenant des informations très sensibles **(niveau 3/4)**	
Important	• Perte d'intégrité dans une application ou des données sensibles (niveau 2) • Reconstruction des données possible mais nécessitant une interruption du processus métier ou un effort supérieur à n j/h • Code malicieux non intercepté par l'antivirus ayant infecté un poste contenant des informations sensibles **(niveau 2)**	
Mineur	• Perte d'intégrité dans une application ou des données standard (niveau 1) • Reconstruction des données possible mais nécessitant une interruption du processus métier ou un effort inférieur à n j/h • Code malicieux non intercepté par l'antivirus ayant infecté un poste contenant des informations peu sensibles **(niveau 1)**	

Disponibilité	Ex. : Indisponibilité d'une salle machine, d'un site utilisateur ou d'applications/services quelle que soit la cause	Portée
Niveaux	**Exemples**	**Nbr de PC**
Critique	• Indisponibilité totale ou partielle des applications très sensibles **(niveau 3/4)** ou d'applications en phase critique de fonctionnement	
Important	• Indisponibilité totale ou partielle des applications sensibles **(niveau 2)** ou d'applications en phase critique de fonctionnement	
Mineur	• Indisponibilité totale ou partielle d'applications peu sensibles **(niveau 1)**	

Guide de la sécurité des données personnelles

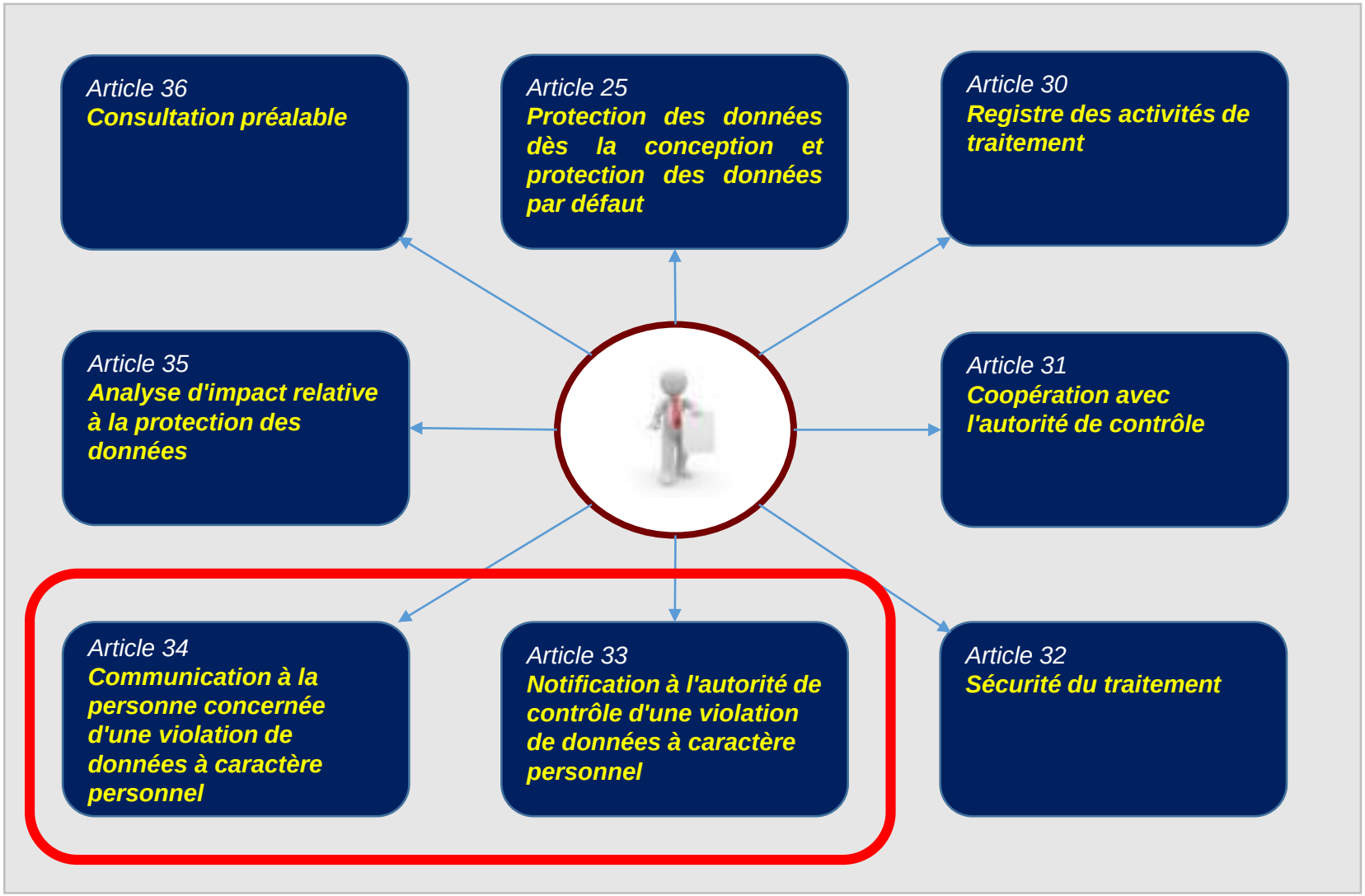
Guide la CNIL : Guide de la sécurité des données personnelles		
1	**Sensibiliser les utilisateurs**	Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée
2	**Authentifier les utilisateurs**	Reconnaître ses utilisateurs pour pouvoir ensuite leur donner les accès nécessaires.
3	**Gérer les habilitations**	Limiter les accès aux seules données dont un utilisateur a besoin
4	**Tracer les accès et gérer les incidents**	Journaliser les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).
5	**Sécuriser les postes de travail**	Prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment via Internet.
6	**Sécuriser l'informatique mobile**	Anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile.
7	**Protéger le réseau informatique interne**	Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place
8	**Sécuriser les serveurs**	Renforcer les mesures de sécurité appliquées aux serveurs
9	**Sécuriser les sites web**	S'assurer que les bonnes pratiques minimales sont appliquées aux sites web

Guide de la sécurité des données personnelles

Guide la CNIL : Guide de la sécurité des données personnelles		
10	**Sauvegarder et prévoir la continuité d'activité**	Effectuer des sauvegardes régulières pour limiter l'impact d'une disparition non désirée de données
11	**Archiver de manière sécurisée**	Archiver les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux
12	**Encadrer la maintenance et la destruction des données**	Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels
13	**Gérer la sous-traitance**	Encadrer la sécurité des données avec les sous-traitants
14	**Sécuriser les échanges avec d'autres organismes**	Renforcer la sécurité de toute transmission de données à caractère personnel
15	**Protéger les locaux**	Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.
16	**Encadrer les développements informatiques**	Intégrer sécurité et protection de la vie privée au plus tôt dans les projets
17	**Chiffrer, garantir l'intégrité ou signer**	Assurer l'intégrité, la confidentialité et l'authenticité d'une information

Responsabilités du responsable des traitements

«responsable du traitement», la 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



Notification à l'autorité de contrôle d'une violation de données à caractère personnel

Article 33

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

« *Une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction,* ***la perte, l'altération, la divulgation ou la consultation non autorisées*** *de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou* ***l'accès non autorisé*** *de telles données ».*

Communication à la personne concernée d'une violation de données à caractère personnel

Article 34

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La communication à la personne concernée n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe précédent est remplie.

Communication à la personne concernée d'une violation de données à caractère personnel

Article 34

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La notification visée au paragraphe 1 doit, à tout le moins:

a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;

c) décrire les conséquences probables de la violation de données à caractère personnel;

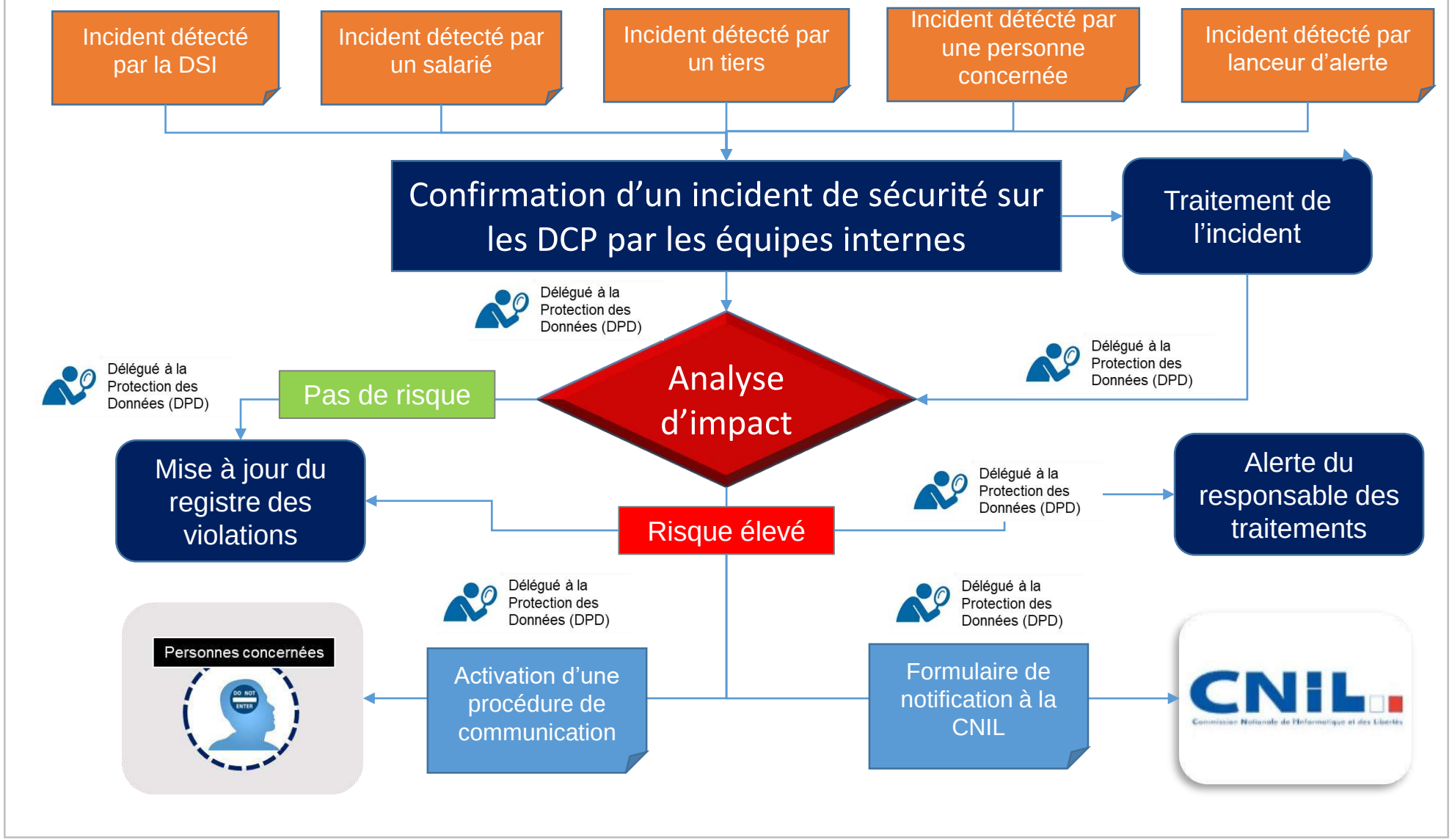
d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier.

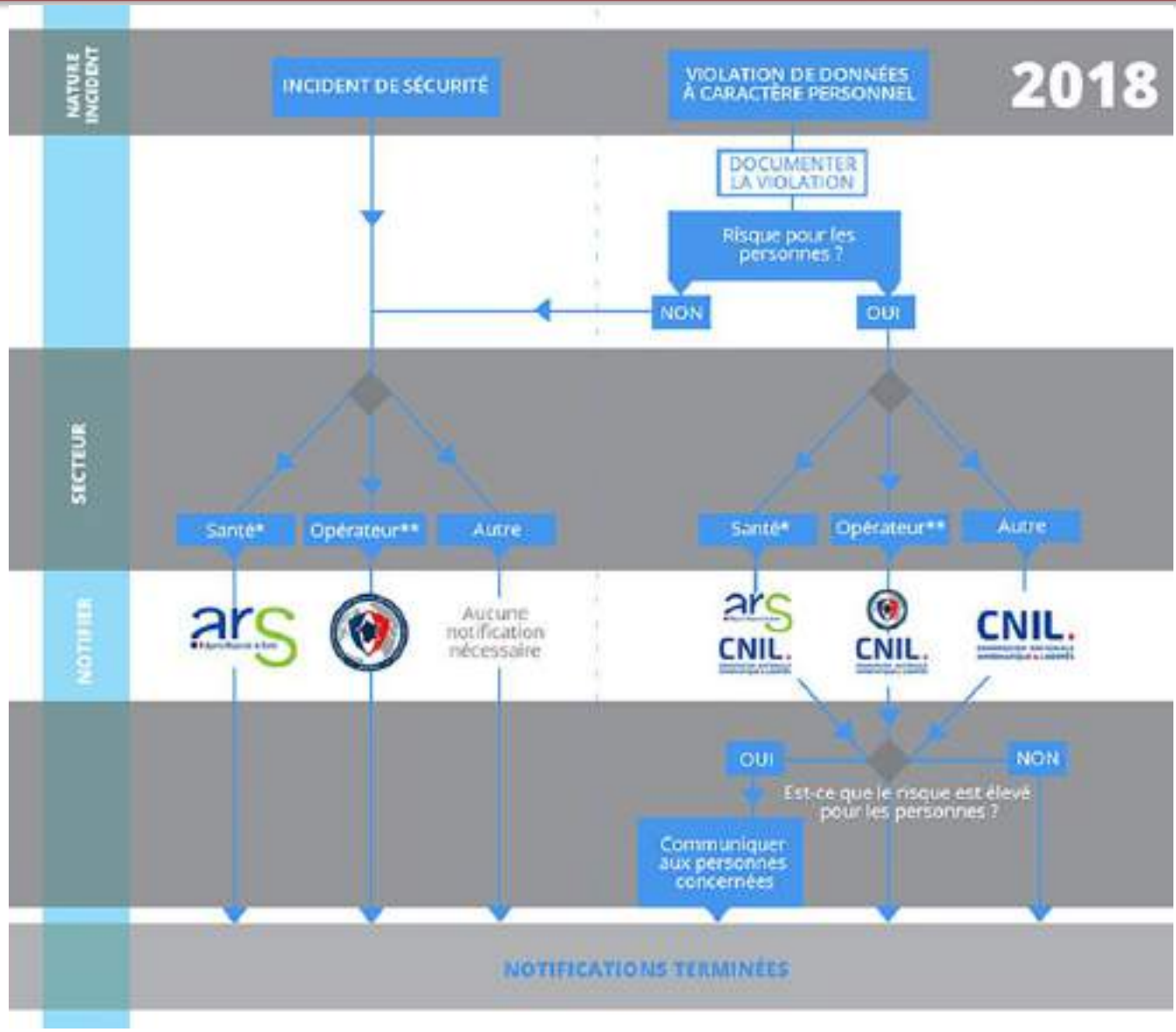
Démarche de traitement d'une violation de DCP

La démarche de traitement d'une violation de DCP:



La chaine d'alerte en France

La chaine d'alerte vers les autorités compétentes



Source CNIL

- *Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie*

*** Opérateur d'importance vitale (OIV), opérateur de service essentiel (OSE) ou opérateur de service numérique (OSN) mettant à disposition des places de marché et les moteurs de recherche en ligne et des services d'informatique en nuage, service de confiance (SDC), ou opérateurs Télécom*

Exemple de procédure

	PROCÉDURE RELATIVE AU TRAITEMENT D'UNE VIOLATION DE DONNEES		
Protection de la Vie Privée	Rédacteur	Vérificateur	Approbateur
	Service Juridique	Comité de Direction	Directeur Général
Objectif de la procédure	Cette procédure vise à décrire les actions à mener dans le cas où une violation de données à caractère personnel serait identifiée		
Prérequis	Disposer des moyens et procédures permettant de gérer les incidents de sécurité		
Qui déclenche la procédure ?	Le Service Juridique		
Procédures mères	Sans objet	**Procédures filles**	Alerte du RT

Historique de modification de la procédure	Date
Version 1a : Création de la procédure	

Historique de contrôle de la procédure	Date du contrôle

1. Procédure

1.1. Rappel du contexte

Dans le cadre de la mise en conformité des traitements et afin de répondre aux exigences imposées par le RGPD (Art. 33 et 34), la présente procédure a pour objectif de décrire les modalités de gestion d'une violation[1] de données à caractère personnel.

Cette procédure s'applique dans les 4 cas suivants :

1. Un incident de sécurité touchant des données à caractère personnel a été **identifié par les équipes techniques** de la Direction Informatique dans le cadre du traitement des incidents de sécurité.
2. Une violation de données à caractère personnel a été **identifiée par les personnes concernées** et a fait l'objet fait l'objet d'une réclamation auprès du service juridique ou de l'autorité de contrôle (CNIL).
3. Un incident de sécurité touchant des données à caractère personnel a été **identifié par un salarié** et fait l'objet d'un signalement au travers du processus d'alerte interne (mentionnée dans la charte utilisateur).
4. Un incident de sécurité a été **identifié par un partenaire sous-traitant** et a fait l'objet d'un signalement au travers de la procédure d'alerte associée au contrat liant le sous-traitant avec le ..... (article 28 du RGPD).

1.2. Procédure à appliquer

Actions à réaliser		Description de l'action	Responsable de l'action	Document(s) associé(s) à l'action
1	Qualification de la violation de données	La qualification en tant que violation de données d'un incident de sécurité incombe au Service Juridique sur la base des informations à sa disposition. En cas de doute sur la qualification, le service Juridique pourra se rapprocher du responsable du service concerné ou du Directeur Informatique. **La qualification d'un incident en violation de données à caractère personnel ne peut excéder les 2 heures après identification de l'incident de sécurité.**	Service Juridique	Informations transmises par le responsable ayant signalé l'incident
2	Analyse d'impact de la violation sur les droits et les libertés des personnes concernées	Le(s) responsable(s) de service concerné(s) réalise(nt) une analyse d'impact sur les droits et les libertés des personnes concernées selon les modalités définies dans la procédure « traitement d'une AIPD ». En cas de risques élevés pour les droits et les libertés des personnes concernées il convient d'activer les procédures de communication à la CNIL (point 4 ci-dessous) et aux personnes concernées (point 5 ci-dessous).	Responsables de Services concernés	Procédure relative à l'AIDP

Exemple de procédure

3	Rédaction du rapport de violation de données	Le(s) responsable(s) de service concerné(s) renseigne(nt) le formulaire de description de la violation mis à la disposition des entreprises par la CNIL. En cas de risque(s) élevé(s) pour les droits et les libertés des personnes concernées par la violation, la rédaction du rapport ne peut pas dépasser le délai de 48h00 après l'identification de l'incident.	Responsables de Services concernés	Modèle de déclaration d'une violation de la CNIL
4	Notification de la violation à la CNIL	La notification de la violation à la CNIL est obligatoire si le(s) risque(s) sur les droits et les libertés des personnes concernées par la violation sont élevé(s) (cf. point 2). Cette notification doit être réalisée dans un délai maximum de 72 heures après identification de l'incident de sécurité au travers des moyens mis en œuvre par la CNIL (téléservice – déclaration en ligne). Le Service Juridique est en charge de renseigner le téléservice avec l'appui des Directeurs de services concernés. Lorsque la notification à CNIL n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.	Service Juridique	CF. modèle de courrier en annexe
5	Notification de la violation aux personnes concernées	Conformément aux exigences du RGPD (art. 34), la notification de la violation aux personnes concernées est obligatoire si le(s) risque(s) sur leurs droits et les libertés est (sont) élevé(s) (cf. point 2). Cette communication doit être réalisée dans les meilleurs délais, dans la mesure du possible dans un délai ne dépassant pas les 72 heures après identification de l'incident. La communication aux personnes concernées décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel.	Service Juridique	CF. modèle de courrier en annexe
6	Mise à jour du registre des violations de données	Le registre central des violations de données tenu à jour par le Service Juridique est renseigné sur la base du rapport de la violation (point 3) et, le cas échant, des informations notifiées à la CNIL (point 4) et aux personnes concernées (point 5).	Service Juridique	Registre des violations
Fin de la procédure				

Direction

Affaire suivie par :

Tél.
Email

CNIL
3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Objet : Notification d'une violation de données à caractère personnel
PJ : Rapport de violation de données

(Lettre recommandée avec accusé de réception)

Madame la Présidente

Le [date], Le .....a constaté une violation de données à caractère personnel.

Le document annexé décrit les éléments suivants :

- la nature de la violation de données à caractère personnel y compris les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- Le nom et les coordonnées du service juridique, point contact auprès duquel des informations supplémentaires peuvent être obtenues;
- Les conséquences probables de la violation de données à caractère personnel;
- Les mesures prises ou que le .....propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Je reste à votre disposition pour toute information complémentaire à [adresse email/ numéro de téléphone].

Je vous prie de croire, Madame la Présidente, en l'assurance de ma considération distinguée.

Le Président du .....

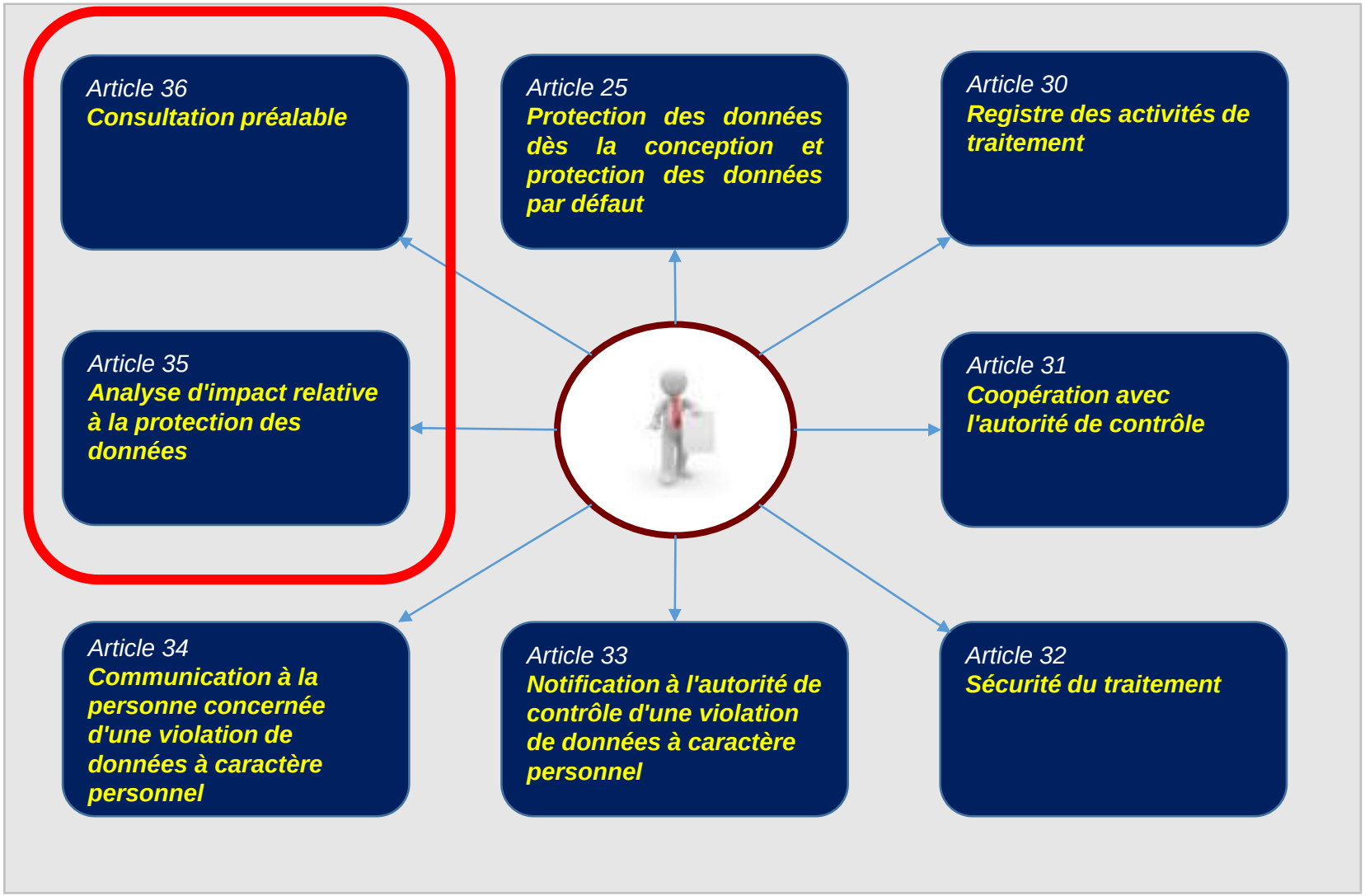
Exemple de registre de suivi des violations

Registre des violations

Description de la violation						Gestion de l'incident			
Nature de la violation	Description synthétique de la violation	Catégories de personnes concernées par la violation	Niveau de gravité de la violation pour les personnes concernées	Date de détection de la violation	Origine du signalement de la violation	Délai de traitement de la violation	Services impliqués dans le traitement de la violation	Notification de la violation à la CNIL	Communication de la violation aux personnes concernées

Responsabilités du responsable des traitements

«responsable du traitement», la 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



Analyse d'impact relative à la protection des données

Article 35

AIPD / DPIA

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est **susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques**, le responsable du traitement effectue, avant le traitement, **une analyse de l'impact des opérations de traitement envisagées** sur la protection des données à caractère personnel.

Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Consultation préalable

Article 36

Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un **risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.**

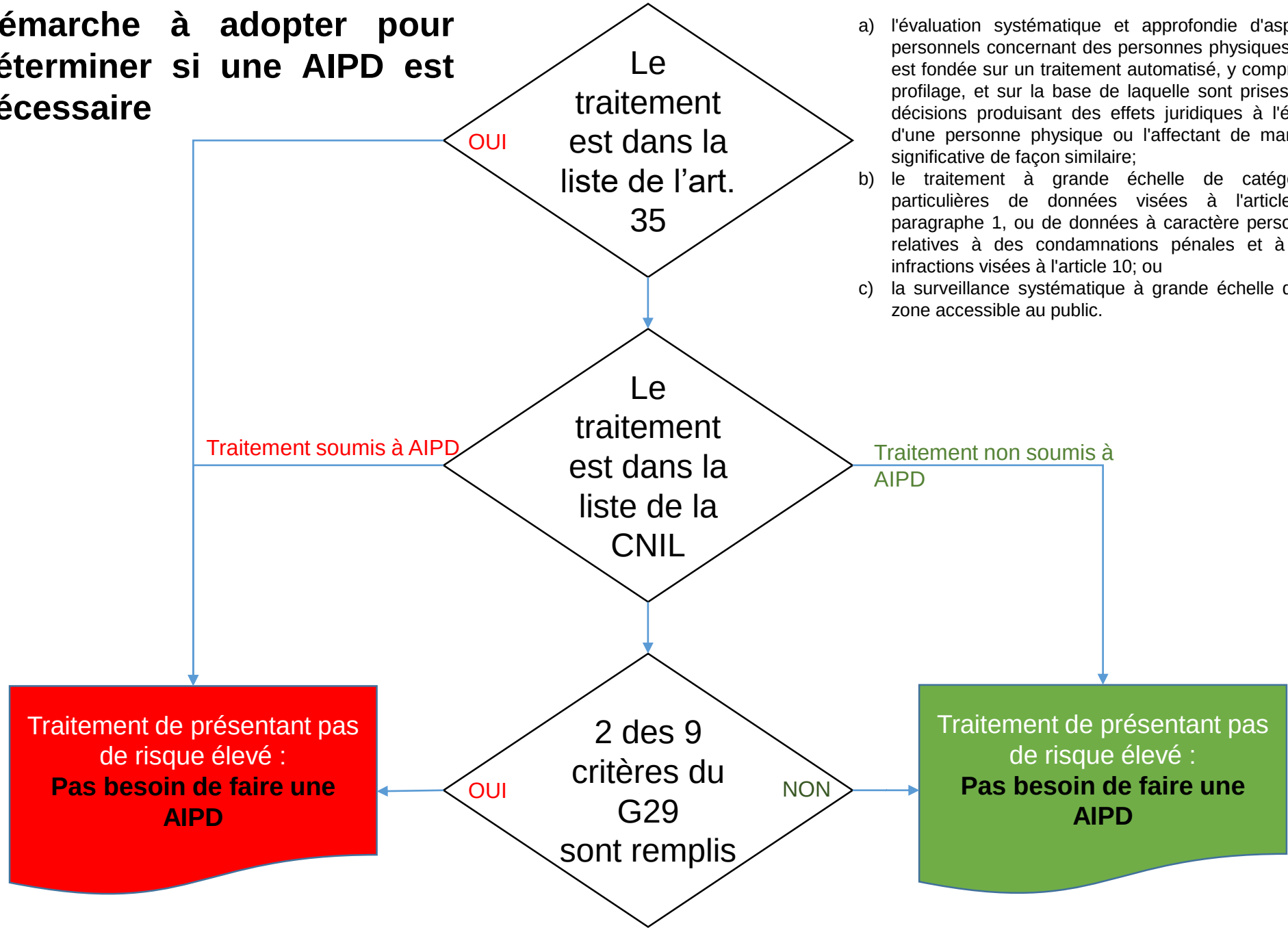
Lorsque l'autorité de contrôle est d'avis que le traitement envisagé, constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un **délai maximum de huit semaines** à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage des pouvoirs visés à l'article 58.

Ce délai peut être **prolongé de six semaines**, en fonction de la complexité du traitement envisagé.

L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation.

Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

Démarche à adopter pour déterminer si une AIPD est nécessaire



a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

Analyse d'impact relative à la protection des données (AIPD)

Les 9 critères du G29 pour déterminer si une AIPD est nécessaire :

1. **Évaluation ou notation, y compris les activités de profilage et de prédiction,** portant notamment sur des «*aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements*»

2. **Prise de décisions automatisée avec effet juridique ou effet similaire significatif**: traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant «*des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire*»

3. **Surveillance systématique**: traitement utilisé pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux ou par «la surveillance systématique […] d'une zone accessible au public»

4. **Données sensibles ou données à caractère hautement personnel**: il s'agit de catégories particulières de données à caractère personnel visées à l'article 9 (informations concernant les opinions politiques des personnes, par exemple) ainsi que des données à caractère personnel relatives aux condamnations pénales ou aux infractions visées à l'article 10.

5. **Données traitées à grande échelle**: le RGPD ne précise pas ce qu'il faut entendre par «grande échelle», même si le considérant 91 fournit quelques indications à ce sujet. Quoi qu'il en soit, pour déterminer si le traitement est effectué à grande échelle, le G29 recommande de prendre en compte, en particulier, les facteurs suivants:
   a. le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée;
   b. le volume de données et/ou l'éventail des différents éléments de données traitées;
   c. la durée ou la permanence de l'activité de traitement de données;
   d. l'étendue géographique de l'activité de traitement.

Les 9 critères du G29 pour déterminer si une AIPD est nécessaire :

6. **Croisement ou combinaison d'ensembles de données**, par exemple issus de deux opérations de traitement de données, ou plus, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée

7. Données concernant des personnes vulnérables : le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits.

8. **Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles**: utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc.

9. **Traitements en eux-mêmes qui *«empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat»***. Ces traitements incluent notamment les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat.

Le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD.

Néanmoins, dans certains cas, **le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD.**

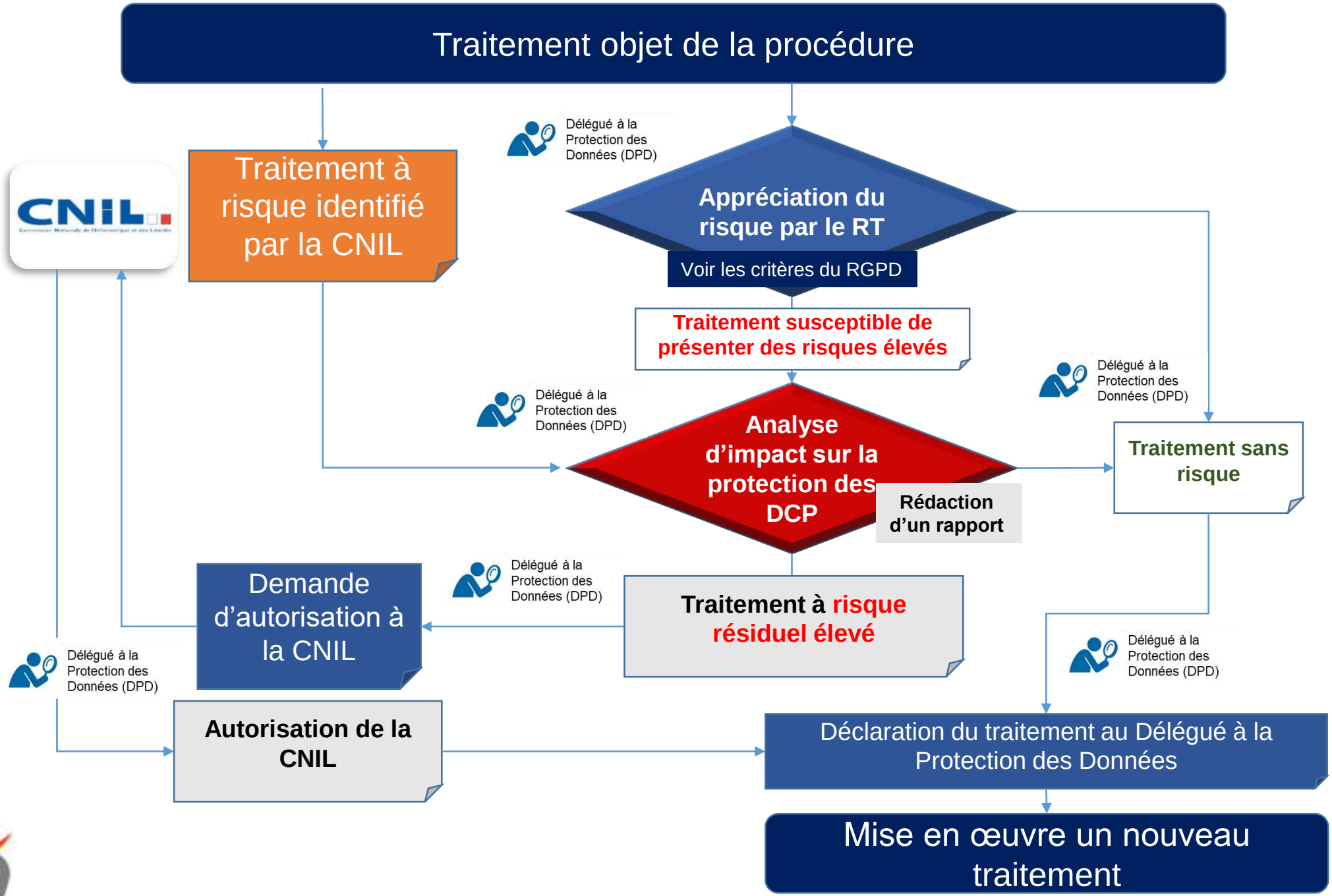
Quelques exemples de traitements :

Traitement	Critères du G29	Nécessite une AIPD
Traitement par un hôpital des données génétiques et des données de santé de ses patients (système d'information hospitalier).	• Données sensibles ou données à caractère hautement personnel. • Données concernant des personnes vulnérables. • Données traitées à grande échelle.	Oui
Utilisation d'un système de caméras pour surveiller les comportements routiers. Le responsable du traitement envisage d'utiliser un système d'analyse vidéo intelligente pour isoler les véhicules et reconnaître automatiquement les plaques d'immatriculation.	• Surveillance systématique. • Utilisation innovante ou application de solutions technologiques ou organisationnelles.	Oui
Surveillance systématique par une entreprise des activités de ses employés, y compris leur poste de travail, leur activité sur internet, etc.	• Surveillance systématique. • Données concernant des personnes vulnérables.	Oui
Collecte de données sur les réseaux sociaux publics dans le but de générer des profils.	• Évaluation ou notation. • Données traitées à grande échelle. • Croisement ou combinaison d'ensembles de données. • Données sensibles ou données à caractère hautement personnel.	Oui

Quelques exemples de traitements :

Traitement	Critères du G29	Nécessite une AIPD
Création par une institution d'une base de données spécialisée dans la notation de crédit ou «antifraude» au niveau national.	• Évaluation ou notation. • Prise de décisions automatisée avec effet juridique ou effet similaire significatif. • Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat. • Données sensibles ou données à caractère hautement personnel.	Oui
Stockage à des fins d'archivage de données à caractère personnel sensibles, pseudonymisées, concernant des personnes vulnérables participant à des projets de recherche ou à des essais cliniques.	• Données sensibles. • Données concernant des personnes vulnérables. • Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.	Oui
Traitement de «données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel»	• Données sensibles ou données à caractère hautement personnel. • Données concernant des personnes vulnérables.	Non
Utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés son numéro quotidien	• Données traitées à grande échelle.	Non

Nouvelle procédure à partir du 25 mai 2018



Démarche AIPD de la CNIL

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :

En résumé, pour mener un PIA, il convient de :

1. délimiter et décrire le **contexte** du(des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des **principes fondamentaux** : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les **risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. formaliser la **validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

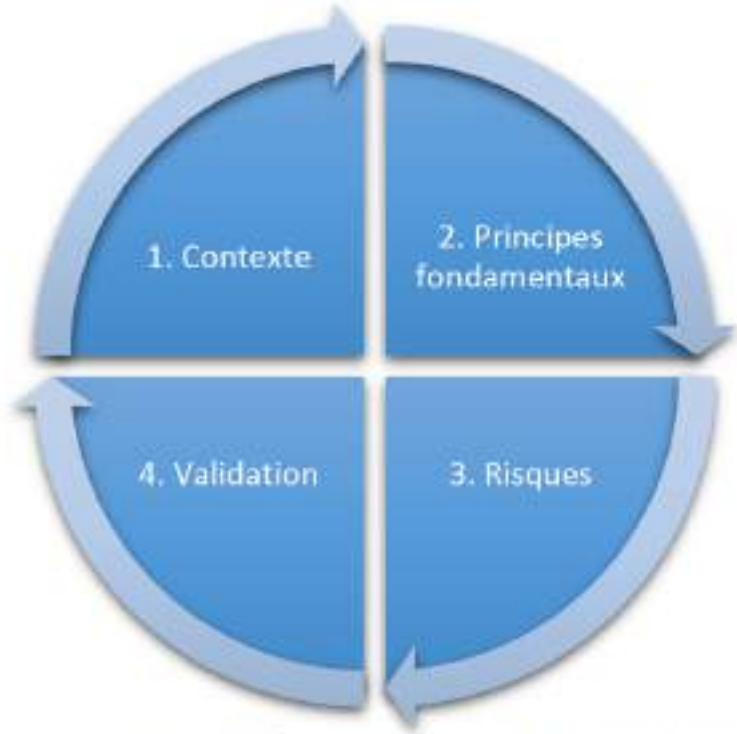


Figure 2 – Démarche générale pour mener un PIA

Présentation de l'outil PIA de la CNIL

Obligations des sous-traitants

Sous-traitant

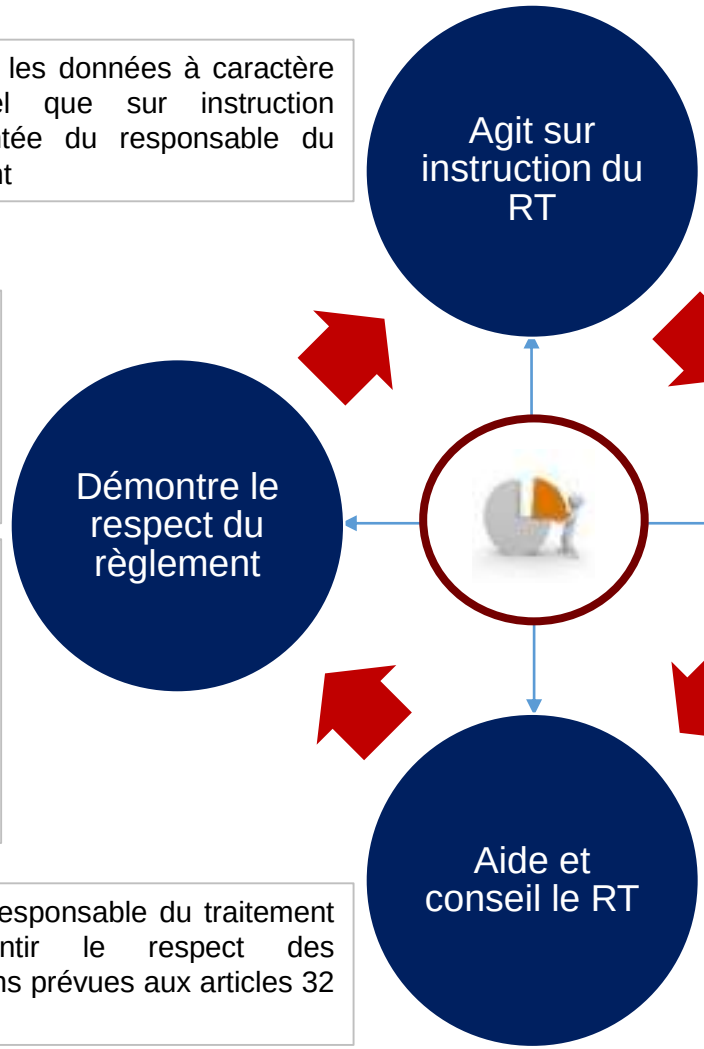
Articles 28

Lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel à des **sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées** de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée

Le sous-traitant **ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable**, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

Responsabilités du sous-traitant

3.Le traitement par un sous-traitant est régi par **un contrat ou un autre acte juridique.**
Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :



Ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement

Supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes

Veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité

Prend toutes les mesures requises en vertu de l'article 32 (sécurité du traitement)

Aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées

Aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36

L'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé pour démontrer l'existence des garanties suffisantes

Met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations et pour permettre la réalisation d'audits et contribuer à ces audits

Le registre des traitements

Les exigences du RGPD :

Article 30 **Registre des activités de traitement**

2.Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.

3.Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

4.Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande.

Clauses contractuelles proposées par la CNIL

[…], situé à […] et représenté par […]

(ci-après, « ***le responsable de traitement***»)

D'une part,

ET

[…], situé à […] et représenté par […] (ci-après, « ***le sous-traitant***»)

d'autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « ***le règlement européen sur la protection des données*** »).

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [……].

La nature des opérations réalisées sur les données est [……].

La ou les finalité(s) du traitement sont [……].

Les données à caractère personnel traitées sont [……].

Les catégories de personnes concernées sont [……].

Pour l'exécution du service objet du présent contrat, le **responsable de traitement** met à la disposition du sous-traitant les informations nécessaires suivantes [……].

Clauses contractuelles proposées par la CNIL

III. Durée du contrat

Le présent contrat entre en vigueur à compter du [.....] pour une durée de [.....].

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance.

2. traiter les données **conformément aux instructions documentées** du **responsable de traitement** figurant en annexe du présent contrat. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer **responsable de traitement** de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public

3. garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat

4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :

- s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
- reçoivent la **formation** nécessaire en matière de protection des données à caractère personnel

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut**

Clauses contractuelles proposées par la CNIL

6. **Sous-traitance**

Choisir l'une des deux options

***Option A** (autorisation générale)*

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « ***le sous-traitant ultérieur*** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le **responsable de traitement** de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le **responsable de traitement** dispose d'un délai minium de [...] à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le **responsable de traitement** n'a pas émis d'objection pendant le délai convenu.

***Option B** (autorisation spécifique)*

Le sous-traitant est autorisé à faire appel à l'entité [.....] (ci-après, le « ***sous-traitant ultérieur*** ») pour mener les activités de traitement suivantes : [.....]

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du **responsable de traitement**.

***Quelle que soit l'option** (autorisation générale ou spécifique)*

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du **responsable de traitement**. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en oeuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le **responsable de traitement** de l'exécution par l'autre sous-traitant de ses obligations.

Clauses contractuelles proposées par la CNIL

7. **Droit d'information des personnes concernées**

Choisir l'une des deux options

Option A

Il appartient au **responsable de traitement** de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Option B

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le **responsable de traitement** avant la collecte de données.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le **responsable de traitement** à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Choisir l'une des deux options

Option A

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à […] (*indiquer un contact au sein du responsable de traitement*).

Option B

Le sous-traitant doit répondre, au nom et pour le compte du **responsable de traitement** et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

Clauses contractuelles proposées par la CNIL

9. **Notification des violations de données à caractère personnel**

Le sous-traitant notifie au **responsable de traitement** toute violation de données à caractère personnel dans un délai maximum de [...] heures après en avoir pris connaissance et par le moyen suivant [.....]. Cette notification est accompagnée de toute documentation utile afin de permettre au **responsable de traitement**, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Option possible

Après accord du **responsable de traitement**, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du **responsable de traitement**, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du **responsable de traitement**, le sous-traitant communique, au nom et pour le compte du **responsable de traitement**, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Clauses contractuelles proposées par la CNIL

11. **Mesures de sécurité**

Le sous-traitant s'engage à mettre en oeuvre les mesures de sécurité suivantes :

[*Décrire les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres*

- *la pseudonymisation et le chiffrement des données à caractère personnel*
- *les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
- *les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;*
- *une procédure visant à tester, à 'analyser et à 'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement]*

Le sous-traitant s'engage à mettre en oeuvre les mesures de sécurité prévues par [*code de conduite, certification*].

[*Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en oeuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en oeuvre*]

12. **Sort des données**

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :

Au choix des parties :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

Clauses contractuelles proposées par la CNIL

14. **Registre des catégories d'activités de traitement**

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du **responsable de traitement** comprenant :

- le nom et les coordonnées du **responsable de traitement** pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;
- les catégories de traitements effectués pour le compte du **responsable de traitement**;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  - la pseudonymisation et le chiffrement des données à caractère personnel;
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
  - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. **Documentation**

Le sous-traitant met à la disposition du **responsable de traitement** la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le **responsable de traitement** ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Clauses contractuelles proposées par la CNIL

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le **responsable de traitement** s'engage à :

1. fournir au sous-traitant les données visées au II des présentes clauses

2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant

3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant

4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant

ANNEXE I : Instructions du **responsable de traitement** relatives au traitement des données

A compléter

Gestion des flux de données vers des pays tiers

Cas particulier : Les transferts de données à caractère personnel vers des pays tiers.

Besoin de transférer des données en dehors de l'UE

Article 45 **Transferts fondés sur une décision d'adéquation**

1.Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale **peut avoir lieu lorsque la Commission a constaté** par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question **assure un niveau de protection adéquat**.

Un tel transfert ne nécessite pas d'autorisation spécifique

Le Règlement européen précise en détail l'évaluation du caractère adéquat du niveau de protection, ce que ne fait pas la Loi Informatique et Libertés, à savoir:

- **Il doit s'agir d'un Etat de droit respectant les droits de l'Homme et les libertés fondamentales**
- **Il doit exister une autorité de contrôle indépendante dans ce pays,**
- **Des engagements internationaux doivent avoir été pris.**

Le règlement prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale

Article 46 **Transferts moyennant des garanties appropriées**

1.En l'absence de décision en vertu de l'article 45, paragraphe 3, **le responsable du traitement ou le sous-traitant ne peut transférer** des données à caractère personnel vers un pays tiers ou à une organisation internationale **que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives**

Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par:

Voir diapositive suivante

Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par:

Voir diapositive suivante

Article 49 **Dérogations pour des situations particulières**

1.En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

Le consentement de la PC,

L'exécution d'un contrat entre la PC et le RT,

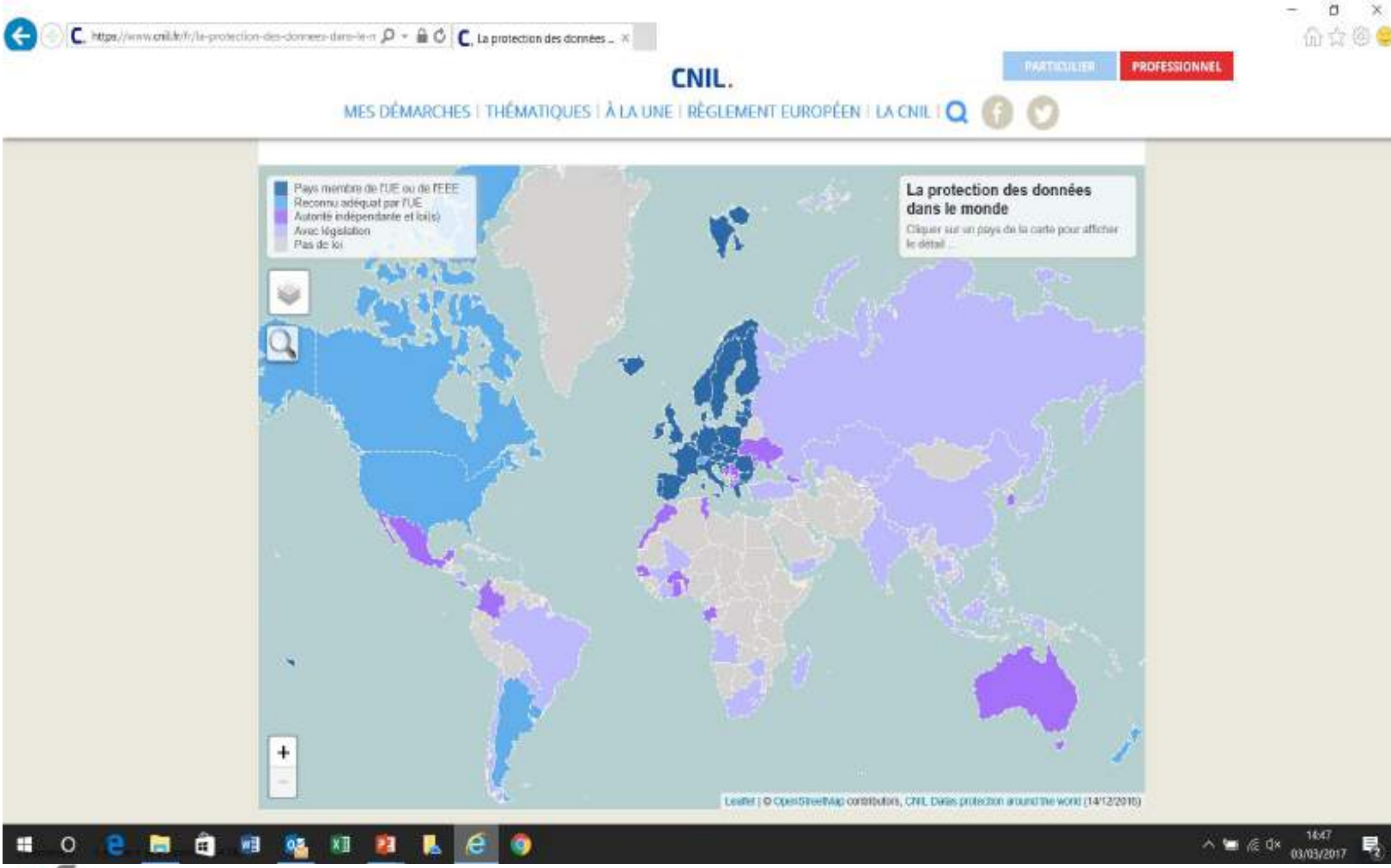
La conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la PC,

Des motifs importants d'intérêt public,

Nécessaire à la constatation, à l'exercice ou à la défense de droits en justice,

Nécessaire à la sauvegarde des intérêts vitaux de la PC ou d'autres personnes lorsque la PC se trouve dans l'incapacité physique ou juridique de donner son consentement.

Voir diapositive relative aux conditions complémentaires


CNIL.
PARTICULIER
PROFESSIONNEL
MES DÉMARCHES | THÉMATIQUES | À LA UNE | RÈGLEMENT EUROPÉEN | LA CNIL
Pays membre de l'UE ou de l'EEE
Reconnu adéquat par l'UE
Autorité indépendante et loi(s)
Avec législation
Pas de loi
La protection des données dans le monde
Cliquer sur un pays de la carte pour afficher le détail ...
Leaflet | © OpenStreetMap contributors, CNIL Data protection around the world (14/12/2016)
14:47
03/03/2017

RGPD : une boîte à outils renouvelée et diversifiée pour les transferts internationaux de données

Outils de transfert sans autorisation préalable de la CNIL

BCR
Approuvées
(art. 47 du RGPD)

Certification
Approuvée
(art. 42 et 46-2 (f) du RGPD)

Code de conduite
Approuvé
(art. 40 et 46-2 (e) du RGPD)

Décisions d'adéquation
(dont privacy shield)
(art.45 du RGPD)

Clauses
Contractuelles types
Adoptées par la Commission européenne
(art. 46-2(c) du RGPD)

Clauses
Contractuelles types
Adoptées par les autorités
(art. 46-2(d) du RGPD)

Instruments
juridiquement contraignants et exécutoires entre autorités organismes publics
(art. 46.2(a) du RGPD)

Dérogations
(art. 49 du RGPD)

Outils de transfert avec autorisation préalable de la CNIL

Clauses contractuelles ad hoc
(art. 46.3.a du RGPD)

Dispositions intégrées
dans les arrangements administratifs entre autorités/organismes publics
(art. 46.3.b du RGPD)

Légende

- Outil existant
- Référentiel mis à jour RGPD
- Nouvel outil

La Commission européenne tient une liste des pays assurant une protection adéquate et ceux n'assurant pas une protection adéquate (ex.)

Exemples

Nom	zone	Niveau de protection	site	information
Algérie	Afrique	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Allemagne	Europe	Adéquat	http://www.datenschutz.de	Virtuelles Datenschutzbüro c/o Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein Independent Centre for Privacy Protection Schleswig-Holstein Holstenstraße 98 D-24103 Kiel Allemagne
Andorre	Europe	Adéquat	https://www.apda.ad/	Agència Andorrana de Protecció de Dades Edifici del Consell General Carrer Doctor Vilanova, 15-17 (planta-5) AD500 Andorra la Vella Principat d'Andorra
Angola	Afrique	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Antigua-et-Barbuda	Amérique du Nord	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Arabie saoudite	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Argentine	Amérique du Sud	Adéquat	http://www.jus.gob.ar/datos-personales.aspx	Dirección Nacional de Protección de Datos Personales (PDP) Sarmiento 1118 5º PISO C 1041 AAC Ciudad Autónoma de Buenos Aires Argentina
Arménie	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Australie	Océanie	Non Adéquat	http://www.privacy.gov.au	Office of the Australian Information Commissioner GPO Box 5218 - Sydney NSW 2001 AUSTRALIA
Autriche	Europe	Adéquat	https://www.dsb.gv.at/	Österreichischen Datenschutzkommission Hohenstaufengasse 2 1010 Wien Autriche
Azerbaïdjan	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Bahamas	Amérique du Nord	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Bahreïn	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Bangladesh	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Barbade	Amérique du Nord	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Belgique	Europe	Adéquat	http://www.privacycommission.be/fr	Commission de la protection de la vie privée Rue de la Presse, 35 1000 Bruxelles Belgique
Belize	Amérique du Nord	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Bénin	Afrique	Non Adéquat	www.cnilbenin.bj	Commission nationale de l'informatique et des libertés (CNIL) - BP 2028 Cotonou
Bermudes	Amérique du Sud	Non Adéquat		
Bhoutan	Asie	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.
Biélorussie	Europe	Non Adéquat	Pas de site web disponible.	Pas d'informations pour le moment.

Source : CNIL – http://www.cnil.fr ; 12/04/2016

Cas particulier : Les transferts de données à caractère personnel vers des pays tiers.

Cas 1 : Pas d'autorisation d'une autorité de contrôle	Cas 2 : Avec d'autorisation d'une autorité de contrôle
Les garanties appropriées visées au paragraphe 1 peuvent être fournies, **sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle**, par: a) un **instrument juridiquement contraignant** et exécutoire entre les autorités ou organismes publics; b) des **règles d'entreprise contraignantes** conformément à l'article 47 ; c) des **clauses types de protection des données adoptées par la Commission** en conformité avec la procédure d'examen; d) des **clauses types de protection des données adoptées par une autorité de contrôle** et approuvées par la Commission en conformité avec la procédure d'examen; e) un **code de conduite approuvé**, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou f) un **mécanisme de certification approuvé**, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.	**Sous réserve de l'autorisation de l'autorité de contrôle** compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par: a) des **clauses contractuelles** entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale; ou b) des **dispositions à intégrer dans des arrangements administratifs** entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

Chapitre 5 : L'encadrement des transferts de données hors de l'Union européenne

1. Les principes relatifs aux transferts de données en dehors de l'Union européenne

Transferts de DCP vers des pays tiers ou à des organisations internationales

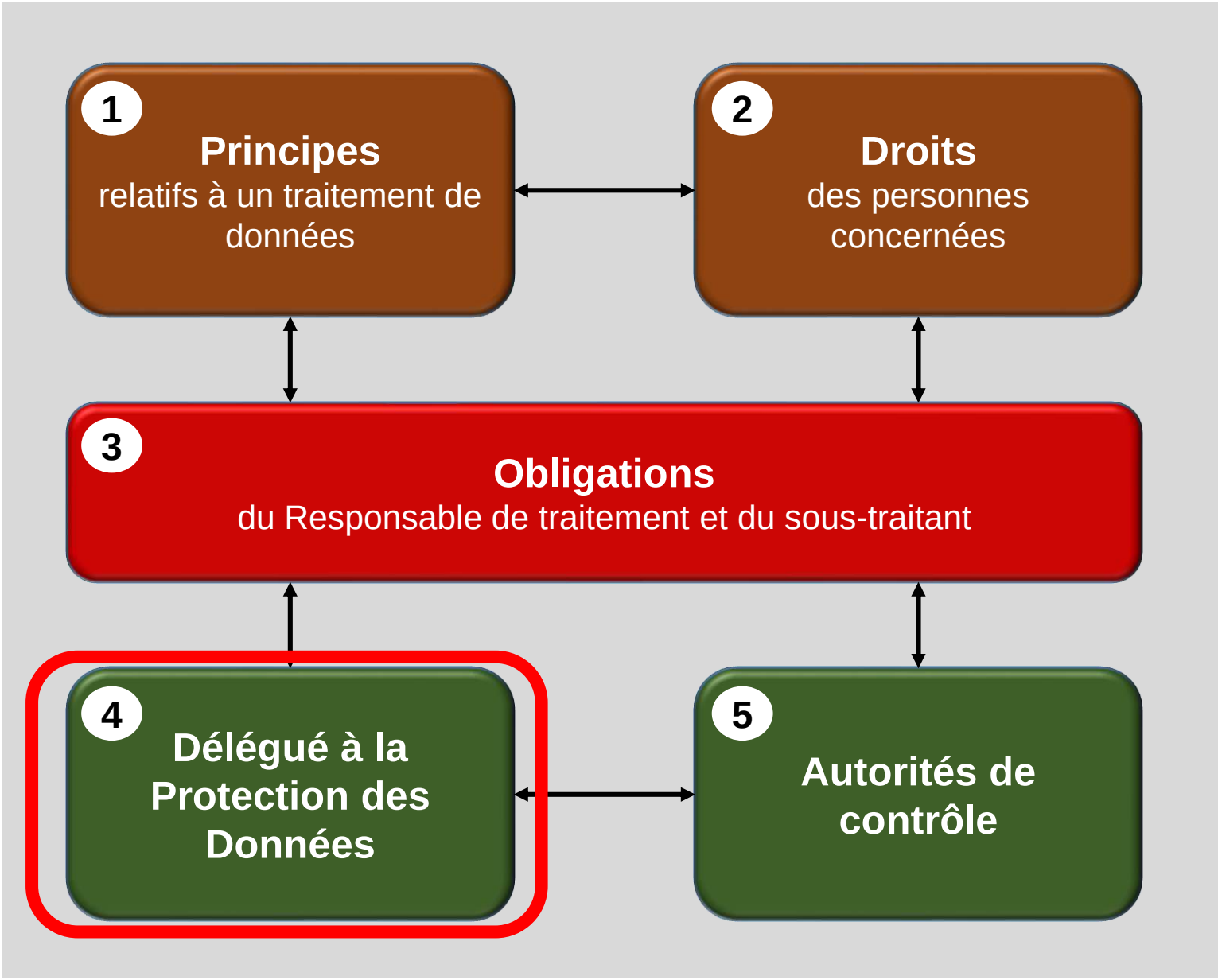
Article 49

Dérogations pour des situations particulières

En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

la PC a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriée	**le transfert est nécessaire à l'exécution d'un contrat entre la PC et le RT** ou à la mise en oeuvre de mesures précontractuelles prises à la demande de la PC	**le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat** conclu dans l'intérêt de la PC entre le RT et une autre personne physique ou morale	**le transfert est nécessaire pour des motifs importants d'intérêt public**	**le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice**	**le transfert est nécessaire à la sauvegarde des intérêts vitaux de la PC ou d'autres personnes, lorsque la PC trouve dans l'incapacité physique ou juridique de donner son consentement**	**le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un ÉM, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.**
						

RGPD – Les exigences relatives aux traitements de données à caractère personnel



Désignation du délégué à la protection des données

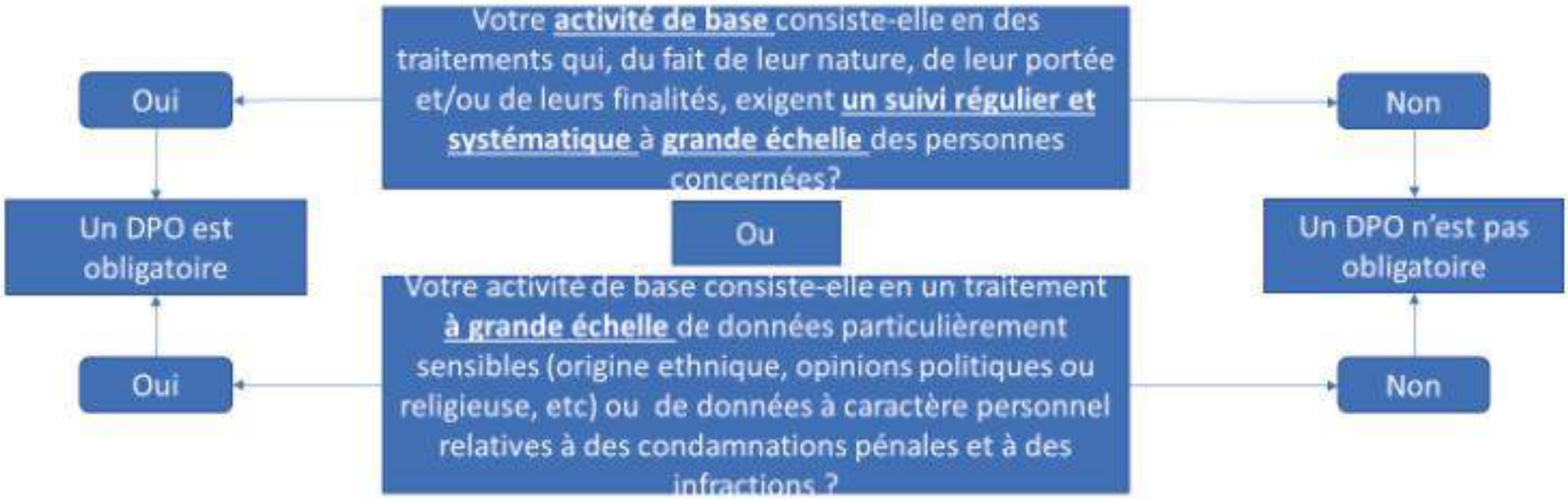
Article 37

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.



Désignation du délégué à la protection des données

Article 37

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses **connaissances spécialisées du droit et des pratiques en matière de protection des données**, et de sa capacité à accomplir les missions.

Désignation du délégué à la protection des données

Article 37

Le délégué à la protection des données peut être **un membre du personnel** du responsable du traitement ou du sous-traitant, ou **exercer ses missions sur la base d'un contrat de service**.

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

INTERNE

IL PEUT ÊTRE NOMMÉ EN INTERNE :

Poste sans conflits d'intérêts avec haut niveau de direction (ne peut être le DRH, DSSI ou directeur marketing)

Positionnement néanmoins efficace : rapport direct avec la direction

EXTERNE

CONTRAT DE SERVICE

Groupe de sociétés : 1 DPO possible et facilement joignable au sein du groupe.
ex : groupes internationaux : DPO du siège.

DPO mutualisé pour des associations et autre organisme représentant des catégories de RT ou de ST

Fonction du délégué à la protection des données

Article 38

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions.

Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Fonction du délégué à la protection des données

Article 38

Les **personnes concernées peuvent prendre contact avec le délégué** à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement.

Le délégué à la protection des données est **soumis au secret professionnel ou à une obligation de confidentialité** en ce qui concerne l'exercice de ses missions.

Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent **pas de conflit d'intérêts.**

Source CNIL) **A titre d'exemple**, les fonctions suivantes sont susceptibles de donner lieu à un **conflit d'intérêts** :

Secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle **si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement**.

Un conflit d'intérêt peut également exister par exemple si un délégué sur la base d'un contrat de service représente l'organisme devant les tribunaux.

Il travaille avec les différents services

Il est l'interlocuteur des autorités de contrôle en matière de protection des données personnelles et est le garant de l'application du RGPD au sein de l'entreprise.

Département Juridique | Département du Marketing | Département RH | Département DSI | Département Sécurité

Les qualités du DPO:

Le DPO doit être en mesure d'accomplir ses missions.

En plus des compétences, le DPO doit disposer des moyens techniques et humains nécessaires. L'entreprise doit donc, le cas échéant, établir un budget et une équipe. Elle devra également permettre au DPO de suivre des formations.
Le profil et la place du DPO dans l'organisation doit lui permettre de disposer de l'autorité nécessaire et de l'accès aux dirigeants.

Sur la base d'un état des lieux des traitements mis en oeuvre, l'entreprise pourrait formaliser les éléments suivants :
- Évaluation de la charge de travail ;
- Évaluation du budget
- Composition de l'équipe mis à la disposition du DPO et modalités de désignation ;
- Nombre d'heures de formations dont bénéficie le DPO ou son équipe ;
- Engagements de faire participer le DPO aux réunions des dirigeants ;
- Engagement de consulter le DPO sur toutes questions relatives à la protection des données
- Engagement d'informer le DPO de tout incident relatif à la protection des données à caractère personnel.

Il convient de veiller à ce que les mesures prises dans ces domaines ne viennent pas empiéter sur les missions du DPO. Il appartient également à l'entreprise de mettre en place la communication nécessaire pour asseoir l'autorité du DPO.

161

Missions du délégué à la protection des données

Article 39

Les missions du délégué à la protection des données sont au moins les suivantes:

a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent ;

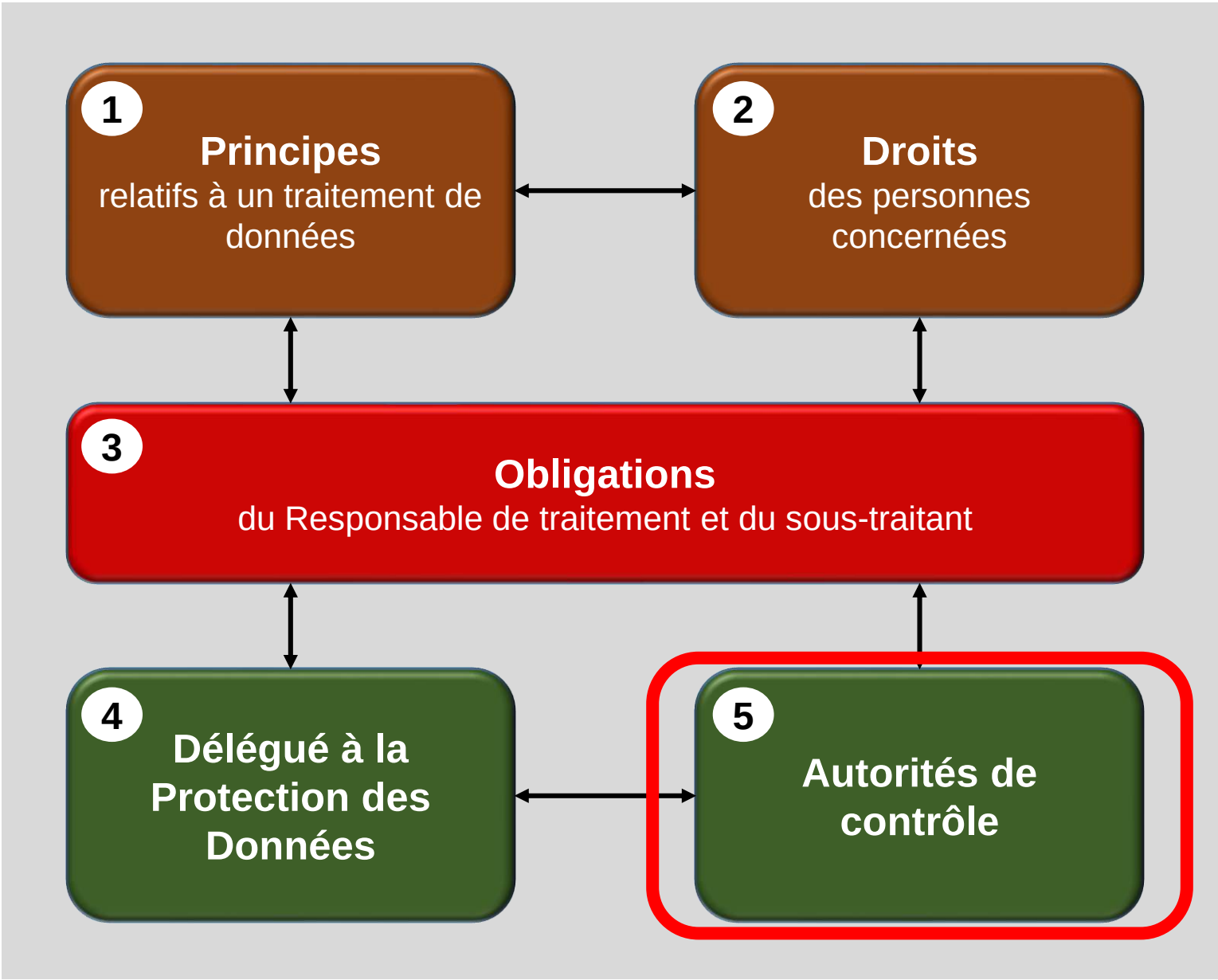
b) contrôler le respect du présent règlement et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35;

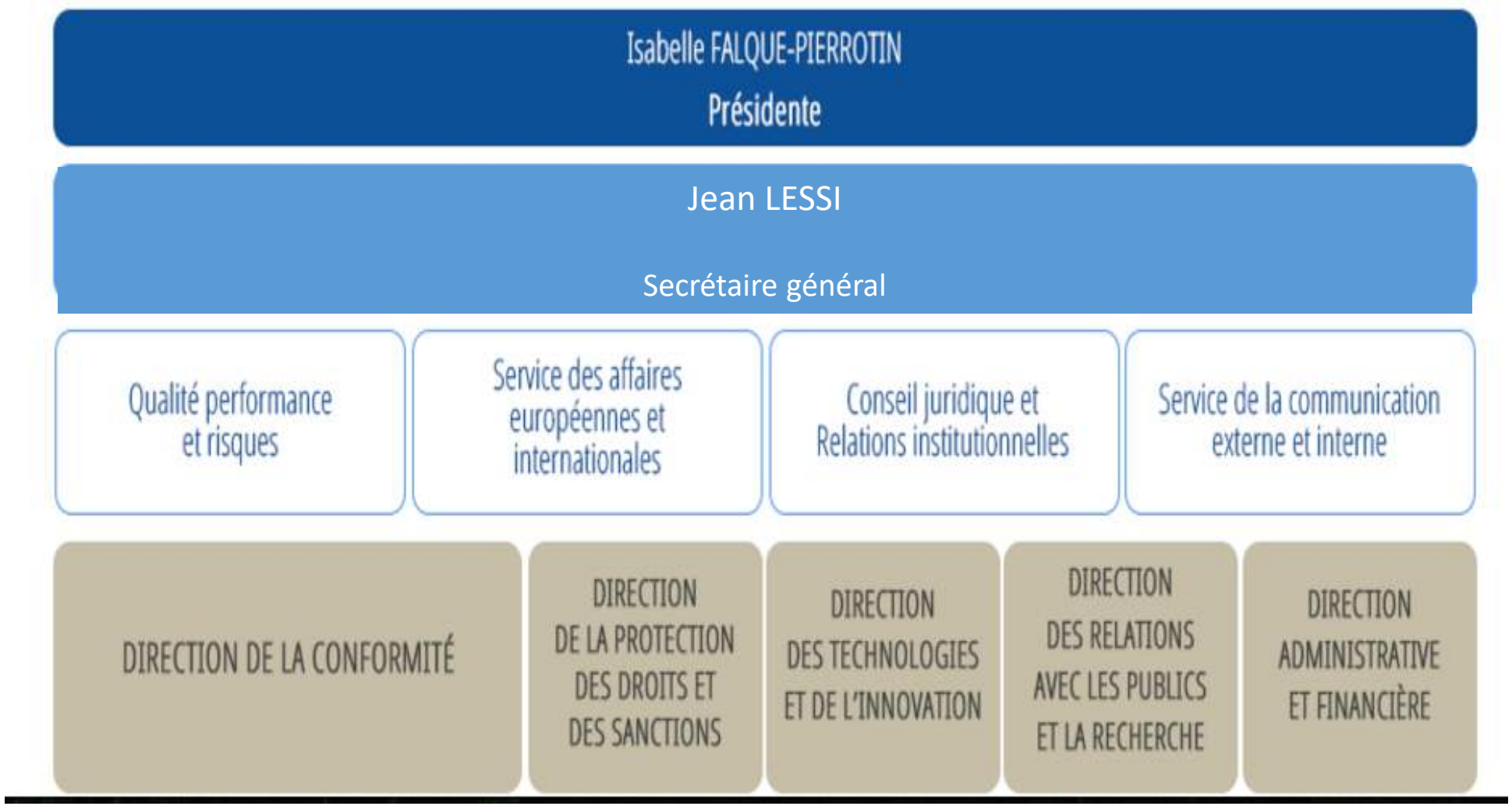
d) coopérer avec l'autorité de contrôle;

e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet.

RGPD – Les exigences relatives aux traitements de données à caractère personnel



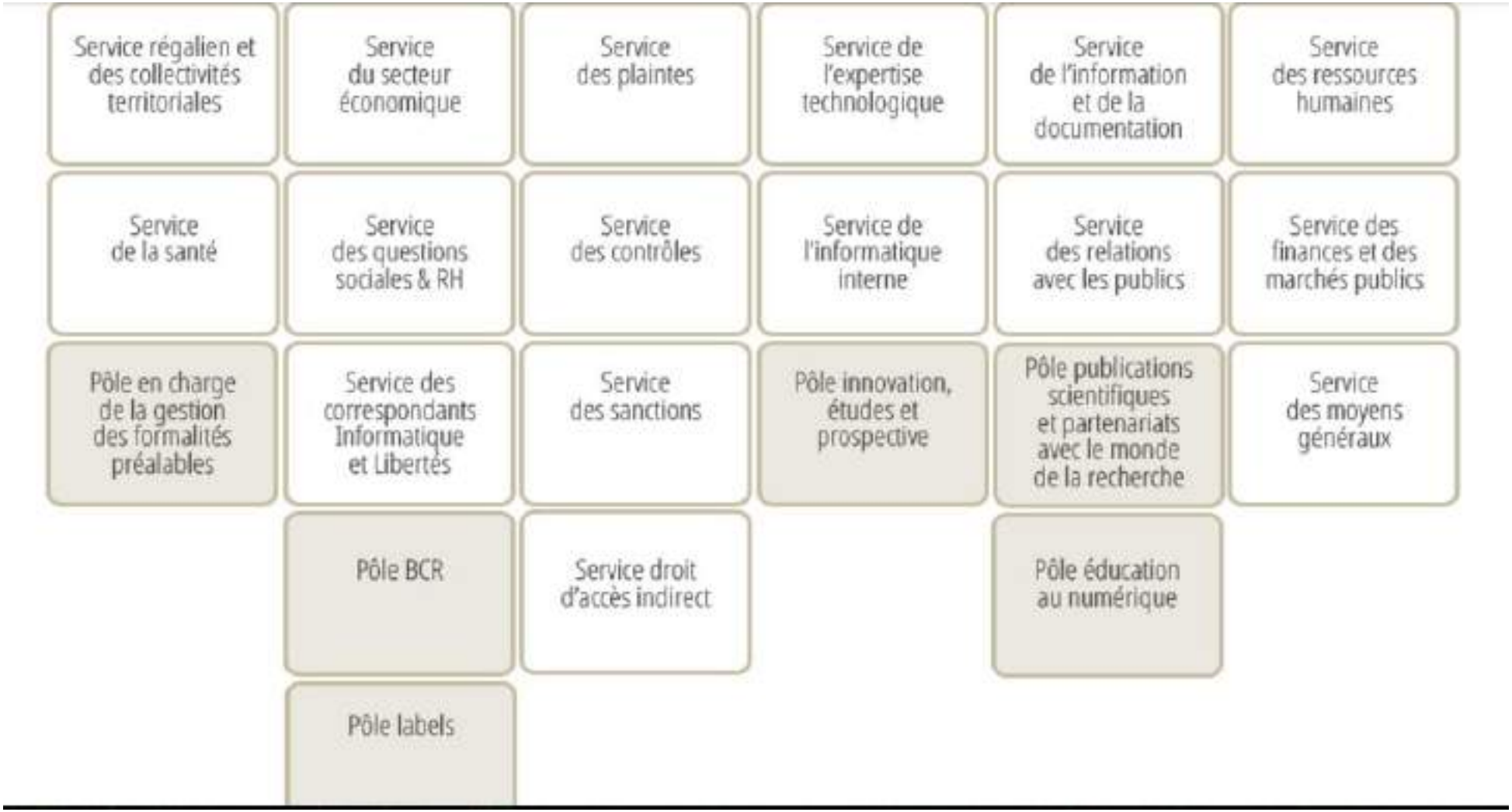
Présentation de la CNIL et de ses missions



Source : – CNIL http://www.cnil.fr

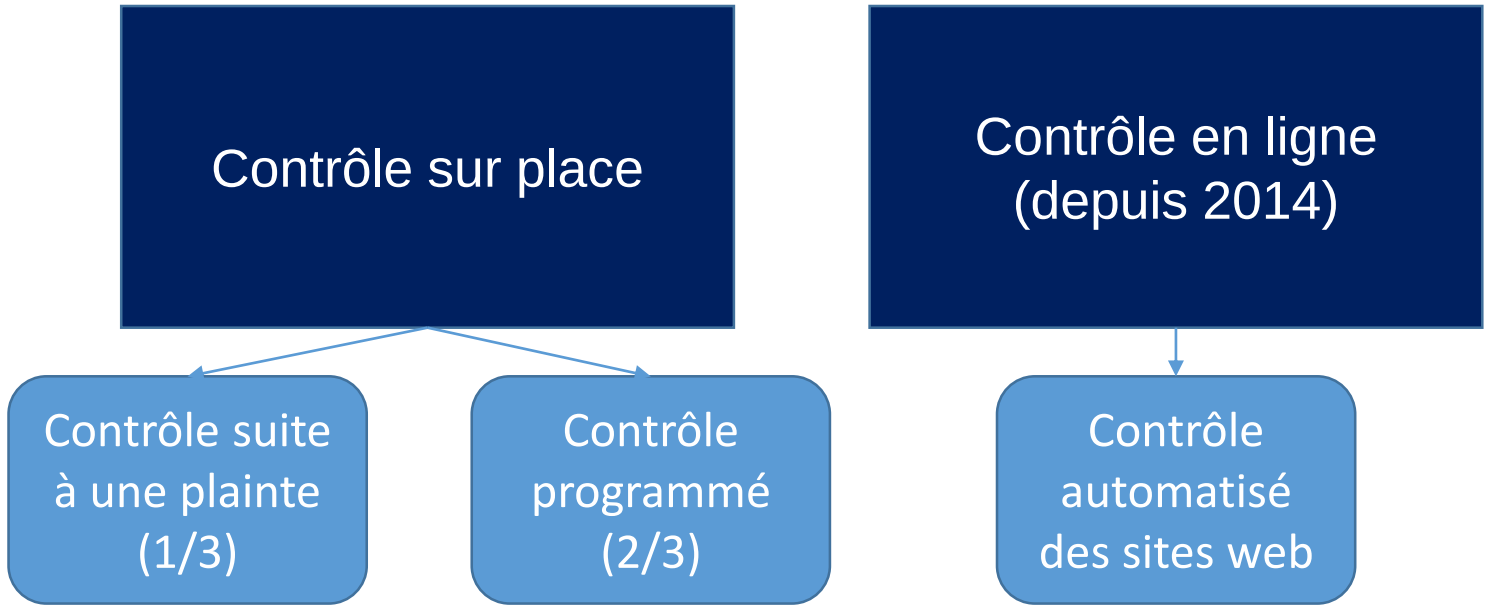
Présentation de la CNIL et de ses missions

2. La composition de la CNIL



Source : – CNIL http://www.cnil.fr

Les contrôles de la CNIL



Recommandations :

Prévoir une **procédure** d'accueil des agents de la CNIL

Réduire le risque de contrôle en traitant rapidement **les réclamations** des personnes concernées

Recommandations :

Prévoir une **procédure** d'accueil des agents de la CNIL

Mettre en place une démarche démontrant la bonne foi de l'organisme

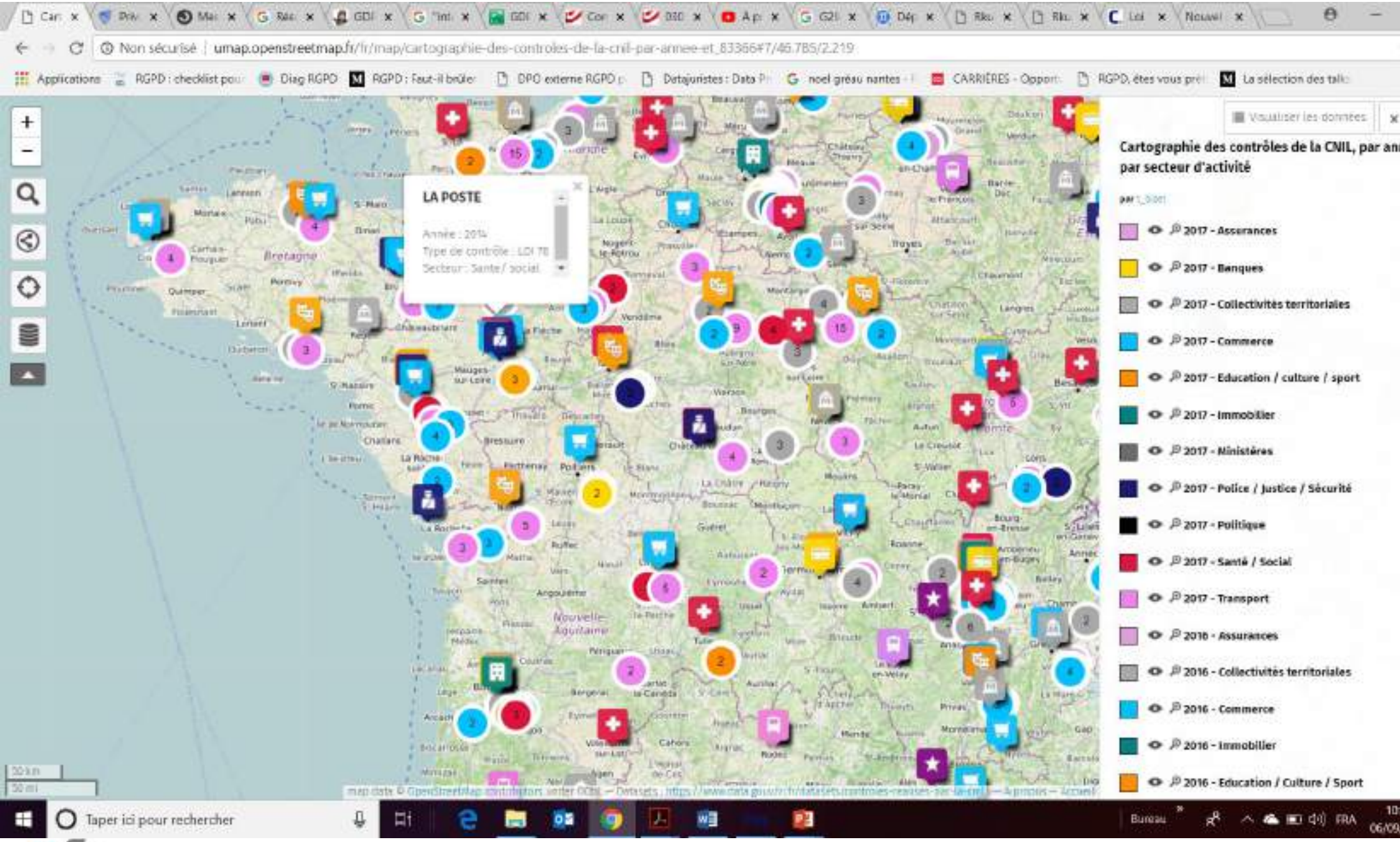
Mettre en conformité les traitements

Recommandations :

Mettre en conformité le(s) site(s) web :

- Absence de collecte excessive de données
- mentions légales
- sécurité des accès et des échanges
- homologation RGS (si concerné)

Recommandations générales : Sensibiliser tout le personnel, impliquer le management.


umap.openstreetmap.fr/fr/map/cartographie-des-controles-de-la-cnil-par-annee-et_83366#7/46.785/2.219
LA POSTE
Année : 2014
Type de contrôle : LDI 78
Secteur : Santé/ social
Cartographie des contrôles de la CNIL, par an
par secteur d'activité
2017 - Assurances
2017 - Banques
2017 - Collectivités territoriales
2017 - Commerce
2017 - Education / culture / sport
2017 - Immobilier
2017 - Ministères
2017 - Police / Justice / Sécurité
2017 - Politique
2017 - Santé / Social
2017 - Transport
2016 - Assurances
2016 - Collectivités territoriales
2016 - Commerce
2016 - Immobilier
2016 - Education / Culture / Sport
Taper ici pour rechercher


300
contrôles
seront effectués en 2018
1
les pièces justificatives
logement.
demandées par les agences
2
les données personnelles
emploi.
liées au recrutement
le contrôle du
stationnement.
par des prestataires privés
3

Rappel sur les sanctions pénales, administratives et civiles

Sanction pénale	Sanction administrative	Sanction civile
En droit pénal, une infraction ne sera sanctionnée que si trois éléments sont réunis: • **Un élément légal** (existence d'un texte sanctionnant un type d'action), • **Un élément matériel** (une tentative d'exécution ou un acte négatif), • **Un élément moral** (l'auteur a eu pleine conscience quant à l'acte commis).	Le Conseil d'Etat définit la sanction administrative comme une décision unilatérale par laquelle **une autorité administrative**, agissant dans le cadre de prérogatives de puissance publique, **inflige une peine sanctionnant une infraction aux lois et règlements**. Prévoyant la punition de celui qui ne se conforme pas aux ordres de l'administration, les sanctions administratives ont un effet dissuasif par la menace qu'elles comportent, qui contribue à favoriser l'exécution volontaire et ainsi à garantir l'effectivité des décisions de l'administration. Attention, **le Conseil constitutionnel a expressément exclu, dans sa décision du 28 juillet 1989, qu'une autorité administrative puisse infliger une peine privative de liberté.** **Les sanctions administratives sont quantifiés et définies dans le RGPD.** **Le RGPD permet aux états membres de compléter les sanctions administratives par des sanctions pénales et civiles**	La responsabilité civile se divise en 2: la responsabilité civile contractuelle et la responsabilité civile délictuelle ou extracontractuelle. **Pour l'engagement de la responsabilité civile délictuelle** sur le fondement de l'article 1382 du Code civil (qui va devenir l'article 1240 du Code civil avec la Réforme en droit des contrats), il faut: • Une faute, • Un dommage, • Un lien de causalité entre la faute et le dommage La réparation se fait par l'obtention de dommages et intérêts. **Pour l'engagement de la responsabilité civile contractuelle** sur le fondement de l'article 1147 du Code civil (art.1231-1 du Code civil avec la Réforme en droit des contrats), il faut: • L'inexécution d'une obligation découlant du contrat, • Un dommage découlant de l'inexécution de cette obligation contractuelle, • Un lien de causalité.

Mesures susceptibles d'être prises par l'autorité de contrôle

- Avertir un responsable du traitement ou un sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du présent règlement
- Rappeler à l'ordre un responsable du traitement ou un sous-traitant lorsque les opérations de traitement ont entraîné une violation des dispositions du présent règlement

- Ordonner au responsable du traitement ou au sous-traitant de **satisfaire aux demandes** présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement
- Ordonner au responsable du traitement ou au sous-traitant de **mettre les opérations de traitement en conformité** avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé
- Ordonner la **rectification ou l'effacement de données** à caractère personnel ou **la limitation du traitement** et la **notification de ces mesures aux destinataires** auxquels les données à caractère personnel ont été divulguées
- Ordonner la **suspension des flux de données** adressés à un **destinataire situé dans un pays tiers** ou à une organisation internationale.
- Retirer une **certification** ou **ordonner à l'organisme de certification de retirer une certification** délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites

- Imposer une **limitation temporaire ou définitive, y compris une interdiction, du traitement**
- Imposer une **amende administrative** en application de l'article 83, en complément ou à la place des mesures visées au présent paragraphe, en fonction des caractéristiques propres à chaque cas

Les amendes administratives

Éléments à prendre en compte pour l'amende administrative

Règlement européen

Pour fixer le montant de l'amende, l'autorité doit tenir compte, dans chaque cas, de pas moins de 11 éléments visés dans la disposition tels que: (facteurs atténuants ou aggravants)

- La nature, la gravité et la durée de la violation
- Le fait que la violation a été commise délibérément ou par négligence
- Toute mesure prise par le RT ou sous-traitant pour atténuer le dommage subi par les personnes concernées
- Le degré de responsabilité du RT ou du sous-traitant compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre
- Toute violation pertinente commise précédemment par le RT ou sous-traitant
- Le degré de coopération établi avec l'autorité de contrôle afin de remédier à la violation
- Les catégories de DCP concernées par la violation
- La manière dont l'autorité de contrôle a eu connaissance de la violation (notification par le RT ou sous-traitant)
- Le respect des mesures de l'article 58 § 2 par le RT ou sous-traitant
- L'application de Codes de conduite approuvés par l'autorité de contrôle
- Toute autre circonstance aggravante ou atténuante (pertes évitées etc.)

Les amendes administratives

Règlement européen

1. **Amendes administratives pouvant s'élever jusqu'à 10 000 000 euros ou dans le cas d'une entreprise jusqu'à 2% du CA annuel mondial :**
   - relatives au consentement des enfants en lien avec des services de la société de l'information (art. 8);
   - en matière de traitement ne nécessitant pas d'identification (art. 11);
   - en matière de protection des données dès la conception et de protection des données par défaut (art. 25);
   - des règles propres aux responsables conjoints du traitement (art. 26);
   - en matière de représentants des responsables qui ne sont pas établis dans l'Union (art. 27);
   - s'imposant dans la relation entre le responsable et le sous-traitant (art. 28);
   - en matière de traitement effectué sous l'autorité du responsable du traitement et du sous-traitant (art. 29);
   - relatives à la tenue du registre de toutes les catégories d'activités de traitement (art. 30);
   - concernant la coopération avec l'autorité de contrôle (art. 31) ;
   - relatives à la sécurité des traitements (art. 32) ;
   - relatives à la notification des violations de données à l'autorité de contrôle (art. 33) ;
   - relatives à la communication des violations de données aux personnes concernées (art. 34) ;
   - concernant l'analyse d'impact relative à la protection des données (art. 35) et la consultation préalable de l'autorité de contrôle (art. 36) ;
   - concernant la désignation du délégué à la protection des données (art. 37), ses fonctions (art. 38), ses missions (art. 39) ;
   - en matière de certification (art. 42) et de procédure de certification (art. 43);
   - des obligations de l'organisme de certification au sens des articles 42 et 43 (b) ;
   - des obligations de l'organisme chargé de surveiller le respect du code de conduite au sens de l'article 41, § 4 (c).

Les amendes administratives

Règlement européen

2. Amendes administratives pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4% du CA annuel mondial total :

- **les principes de base des traitements, en ce compris les conditions du consentement au sens des articles 5 (Principes relatifs au traitement des données à caractère personnel), 6 (licéité du traitement), 7 (conditions applicables au consentement) et 9 (Traitement des catégories particulières de données à caractère personnel) ;**
- **des droits des personnes concernées au sens des articles 12 à 22 du Règlement ;**
- **des règles relatives aux transferts de données à un destinataire d'un pays tiers ou d'une organisation (art. 44 à 49) ;**
- **toutes les obligations mises en place par le droit national conformément au chapitre IX: le chapitre IX laisse aux États membres une certaine marge d'appréciation en matière notamment de traitements des données à caractère personnel et liberté d'expression et d'information (cfr. art 85) ; traitements d'un numéro d'identification national (art 87) etc.;**
- **le non-respect d'une injonction de limitation temporaire ou définitive de traitement ou de suspension du flux de données, prononcée par une autorité de contrôle en vertu des articles 58, § 2 ou lorsque le responsable ne permet pas l'accès en violation de l'article 58, § 1er.**

Les amendes administratives

Règlement européen

2. Amendes administratives pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4% du CA annuel mondial total :

- **les principes de base des traitements, en ce compris les conditions du consentement au sens des articles 5 (Principes relatifs au traitement des données à caractère personnel), 6 (licéité du traitement), 7 (conditions applicables au consentement) et 9 (Traitement des catégories particulières de données à caractère personnel) ;**
- **des droits des personnes concernées au sens des articles 12 à 22 du Règlement ;**
- **des règles relatives aux transferts de données à un destinataire d'un pays tiers ou d'une organisation (art. 44 à 49) ;**
- **toutes les obligations mises en place par le droit national conformément au chapitre IX: le chapitre IX laisse aux États membres une certaine marge d'appréciation en matière notamment de traitements des données à caractère personnel et liberté d'expression et d'information (cfr. art 85) ; traitements d'un numéro d'identification national (art 87) etc.;**
- **le non-respect d'une injonction de limitation temporaire ou définitive de traitement ou de suspension du flux de données, prononcée par une autorité de contrôle en vertu des articles 58, § 2 ou lorsque le responsable ne permet pas l'accès en violation de l'article 58, § 1er.**

Synthèse des principales nouveautés portées par le RGPD & Plan d'actions de mise en conformité.

La démarche de mise en conformité

Doit être adaptée au niveau de maturité de l'organisme : **une approche progressive par palier** doit être mise en œuvre.

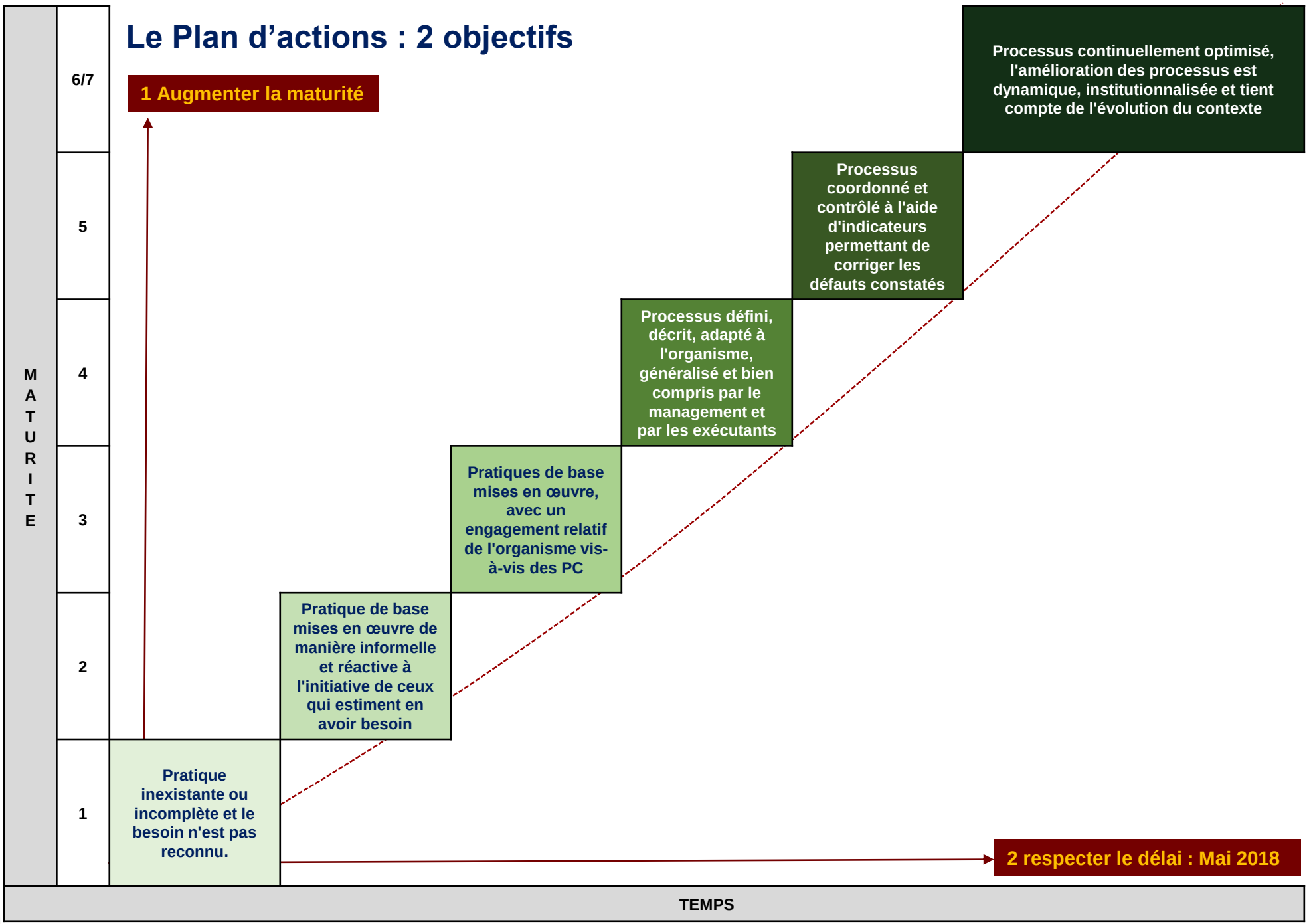
Doit impliquer la **Direction Générale :** la responsabilité juridique du responsable des traitements (RT) peut être engagée.

Doit aborder des aspects de nature **juridique** et de **sécurité des données :** des acteurs compétents doivent être désignés pour traiter ces sujets.

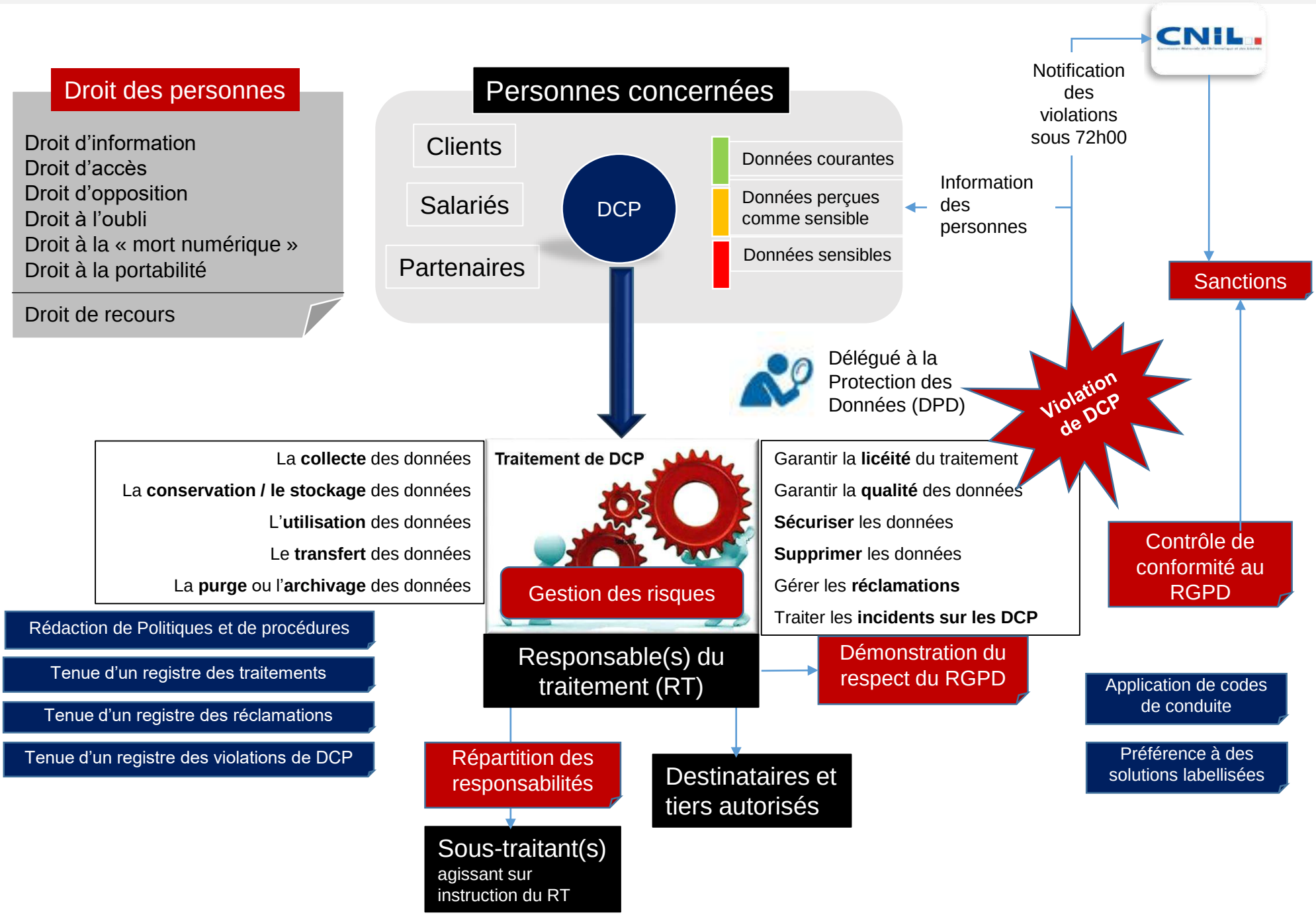
Nécessite de **formaliser des documents** (politiques, procédures, …) : un arbitrage doit être prévu sur certaines directives.

Nécessite de **sensibiliser et responsabiliser** tous les personnels traitant des données à caractère personnel : la culture « protection des DCP » doit être intégrée dans tous les services concernés.

Le Plan d'actions : 2 objectifs



Les concepts généraux relatifs à la protection des données à caractère personnel



Le Plan d'actions : Les mesures juridiques / Le Respect des droits de la PC

Les nouvelles mentions d'informations à fournir lorsque les DCP sont collectées auprès de la PC – ex. AGERIS GROUP concernant la collecte de DCP pour l'inscription à l'une de ses formations dispensée à des clients français et luxembourgeois

- **Le responsable du traitement est le Président de la société AGERIS, Monsieur Thierry RAMARD, 16 rue de Pont à Mousson – 57000 Metz.**
- **Les coordonnées du délégué à la protection des données sont les suivantes: dpo@ageris-group.com**
- **Les données collectées ont pour finalité d'effectuer des opérations relatives à la gestion des clients concernant les contrats, les commandes et les factures.**
- **Les destinataires des données collectées sont les services administratif et commercial d'AGERIS GROUP.**
- **Aucun transfert de DCP hors UE n'est envisagé.**
  - **Les données ne sont pas conservées au-delà de la durée strictement nécessaire à la gestion de la relation commerciale.**
  - **Conformément au Règlement n°2016/679, vous bénéficiez d'un droit d'accès, de rectification ou d'effacement, ainsi que d'un droit à la portabilité de vos données ou d'une limitation du traitement vous concernant. Vous pouvez également pour des motifs légitimes, vous opposer au traitement de vos données.**
  - **Vous pouvez à tout moment retirer votre consentement, et cela sans porter atteinte à la licéité du traitement fondé sur le consentement avant le retrait de celui-ci.**
  - **Vous avez le droit d'introduire une réclamation auprès d'une autorité de contrôle.**
  - **La personne concernée est tenue de fournir les données à caractère personnel la concernant dans la mesure où celles-ci conditionnent la conclusion du contrat.**
  - **Les DCP collectées ne font pas l'objet d'une prise de décision automatisée, y compris un profilage.**

Synthèse des nouvelles exigences portées par le RGPD

Acteurs	Nouveautés portées par le RGPD
Personnes concernées	**1. Nouveaux droits** : portabilité, limitation du traitement, opposition au profilage, ….. **2. Nouveaux recours** : représentation, recours contre la CNIL, …..
Responsable de traitement	1. Obligation de tenir à jour un **registre des traitements** (à fournir à la CNIL sur demande) 2. Obligation de prendre mettre en place une démarche de **protection par défaut** des données et **lors de la conception** des traitements 3. Obligation de **renforcer l'information** des personnes (nouvelles mentions légales) 4. Obligation de **sécuriser les données** et de **traiter les violations** de DCP (communication aux personnes, notification à la CNIL) 5. Obligation de **formaliser les instructions** à destination **des sous-traitants** (clauses contractuelles, révision des contrats) 6. Obligation de mettre en place une **démarche de gestion des risques** (AIPD) 7. Obligation de **démontrer l'application du RGPD** (charge de la preuve) en contre partie de la simplification des démarches CNIL 8. Obligation de désigner un **Délégué à la Protection des Données** (DPD) pour certains organismes (profil juridique et technique, pas en position de conflit d'intérêt, …)
Sous-traitant	**1. Responsabilité juridique** en cas de non-conformité **2. Obligation de s'engager** contractuellement (clauses contractuelles)
Autorités de contrôle	1. Application de **sanctions administratives** (jusqu'à 20 M€ ou 4% du CA) 2. Création d'un **comité européen à la protection des données (CEPD)** **3. Renforcement de la coopération** entre les autorités (autorité chef de file, …) 4. Propose une **révision du RGPD tous les 4 ans** à la commission européenne

Le plan d'actions

Chantiers	Actions à prévoir
Mettre en place une **organisation / gouvernance** adaptée	1. Désigner un **Délégué à la Protection des Données (DPD)** (ou à minima un chef de projet en charge du suivi du plan d'actions) 2. Faire un **état des lieux général** sur la conformité au RPGP (audit flash) **3. Sensibiliser la Direction Générale** sur les impacts du RGPD et son rôle **4. Sensibiliser les directeurs / chefs de service** sur leurs responsabilités 5. Mettre en place des **référents dans les directions** et un **comité de validation et de décision** (à intégrer au CODIR)
Faire la **liste des traitements**	1. Faire le **recensement** de tous les traitements (ateliers de travail avec les chefs de services) 2. Créer un **registre des traitements** et les **fiches de collecte** d'informations 3. Identifier **les non-conformités** et définir un **plan d'actions** correctifs par service concerné
Mettre à jour les **mentions légales**	1. Définir les **mentions légales types** **2. Recenser tous les formulaires** de collecte 3. Organiser avec les services concernés **la mise à jour des formulaires** de collecte
Sensibiliser tous les personnels	**1. Définir et faire valider un plan de sensibilisation annuel** **2. Organiser des actions de sensibilisation pour les nouveaux arrivants** **3. Organiser des actions de sensibilisation pour les personnels en poste** **4. Créer un espace intranet « RGPD » permettant la diffusion d'informations et la communications à l'ensemble du personnel**

Le plan d'actions

Thème	Actions à prévoir
Formaliser les **directives internes et les procédures**	1. Formaliser une **politique interne** de protection des données à destination des personnels cadres et non cadres 2. Formaliser une **politique externe** (public) à destination des clients / tiers 3. Mettre à jour la **charte des utilisateurs** (inclure des directives relatives à la protection des données et aux respects du RGPD) et prévoir des **actions de sensibilisation** 4. Mettre à jour la **PSSI** (intégrer les directives de la CNIL en matière de sécurité des données) 5. Rédiger les **procédures internes** (gestion des réclamations, gestion des violations de DCP, alerte du RT, gestion des contrôles de la CNIL, …..) et préparer les **registres associés** (registre des réclamations, des violations, ..)
Mettre en place une démarche de **gestion des risques**	**1. Identifier les traitements** soumis à obligation d'AIPD **2. Créer les référentiels** permettant de mener les AIPD (outillage d'analyse) 3. Organiser un **projet pilote** sur un traitement sensible (en impliquant le service concerné et les mettre d'œuvre) 4. Renforcer les **procédures et les moyens** de traitements **des incidents** de sécurité (gestion des violations)
Revoir les clauses contractuelles avec les sous-traitants	**1. Recenser les sous-traitants concernés par le RGDP** **2. Rédiger les clauses contractuelles types (modèle de la CNIL)** **3. Organiser la mise à jour des contrats actifs (courrier, réunion de travail, ..)** **4. Prévoir les clauses dans les nouveaux marchés**

Le plan d'actions

Thème	Actions à prévoir
Engager une démarche de protection par défaut et lors de la conception	1. Auditer l'application des principes « Privacy By Defaut » dans les applications les plus sensibles et définir un plan d'actions correctifs 2. Intégrer la protection des données et le respect du RGPD dans les démarches projets (formation des chefs de projets, outillage, définition des livrables à chaque étape d'un projet, …)
Faire **une veille** sur les nouvelles directives de la CNIL	**1. Surveiller la diffusion** par la CNIL **des modifications apportées à la loi** « Informatique et Libertés » (ordonnances) et analyser les impacts pour l'organisme **2. Surveiller la diffusion** par la CNIL **des codes de conduite** à appliquer **3. Adhérer à l'AFCDP** (Association Française des Correspondants à La Protection des Données).
Rédiger un bilan de toutes les actions de conformité réalisé en cours d'année	1. Organiser la **gestion des documents** et des éléments de traçabilité 2. Rédiger un **bilan annuel des actions réalisées** à remettre au responsable des traitements
Anticiper les besoins en ressources et en moyens	1. Définir les **besoins techniques** pour **renforcer la protection** des données (voir l'article 32 du RGPD) 2. Définir les **besoins humains** pour assurer le **maintien en condition opérationnelle** des mesures techniques et organisationnelles mises en oeuvre

Exemple de liste de documents à conserver dans les services

Registre des traitements :

- **Fiches de déclaration** des traitements au DPO signées par le Relai DPO et le Responsable de service
- **Fiches** de signalement **d'une modification ou une suppression** d'un traitement signées par le Relai DPO et le Responsable de service
- Traces démontrant le **fondement juridique** d'un traitement (preuve de consentement, référence aux textes légaux, ….)
- Trace démontrant le respect des **durées de conservation** des données
- Trace des **échanges avec le DPO** sur des questions relatives aux traitements

Registre des réclamations :

- Traces de **toutes les demandes** (courriers, mail)
- Traces démontrant la **vérification de l'identité du demandeur**
- Traces démontrant **l'accusé de réception** des demandes
- Copie du **dossier de réponse** aux demandes des personnes concernées
- Traces **des échanges avec les demandeurs** (si des échanges ont été nécessaires)
- Traces justifiant le **refus de répondre** à la demande

Exemple de liste de documents à conserver dans les services

Registre des violations de DCP :

- Traces relatives à la **date de détection** d'un incident de sécurité sur les données (signalés par un salarié, un partenaire ou les personnes concernées)
- **Rapport d'analyse de la violation** (contenant les éléments imposés par le RGPD article 33)
- Traces justifiant la décision de notification ou non à l'autorité de contrôle
- Traces justifiant la décision de communication ou non aux personnes concernées
- Copie des **échanges avec l'autorité de contrôle** (courrier de notification, réponse de l'autorité, courrier d'échange avec l'autorité de contrôle, ..)
- Copie des **courriers de communication aux personnes concernées**

Gestion des sous-traitants :

- Liste des **sous-traitants concernés** par le RGPD
- **Justificatifs** ayant permis **d'écarter des sous-traitants** de la liste
- Traces démontrant que la banque à **engager une démarche** de modification des contrats signés avant le 25 mai 2018 (courriers à destination des sous-traitants, CR de réunions avec des sous-traitants, copies de mails échangés, ...)
- Traces démontrant que les clauses « RGPD » sont **intégrées dans les nouvelles consultations** du marché
- Copie des **clauses contractuelles signées** avec les sous-traitants

Exemple de liste de documents à conserver dans les services

Contrôle de conformité au RGPD :

- Traces des **contrôles réalisés** par le DPO ou la CNIL
- Traces de **l'implication des personnels** dans la réalisation des contrôles (ex. fiches d'observation lors d'un contrôle, fiche de suivi du contrôle, PV de fin de contrôle, ...)
- Traces justifiant **l'impossibilité d'appliquer les recommandations** du DPO ou de la CNIL
- Traces justifiant la mise en place des **mesures correctives**

Privacy by Design, Privacy By Default et PIA :

- Traces démontrant la **participation du relai DPO dans la démarche projet** (CR de réunions projets, échanges de mail avec l'équipe projet, ..)
- Liste des **traitements soumis à une obligation de PIA**
- **Rapports des PAI réalisés** sur les traitements susceptibles de présenter des risques élevés pour les personnes concernées
- **Traces des échanges avec l'autorité de contrôle** dans le cas où le traitement présente des risques résiduels élevés
- **Traces des décisions de consultation ou non des personnes concernées** pour obtenir leurs avis sur le PIA

Exemple de liste de documents à conserver dans les services

Gouvernance, politique et procédures :

- Traces démontrant **l'implication du Relai DPO** dans la définition et la mise en application des procédures
- Traces de **remontée (alerte) vers le DPO** d'une non-conformité à la politique interne identifiée dans les services ou par le Relai DPO
- Traces démontrant l'implication **du Relai DPO** dans les réunions **d'échange avec le DPO**
- Traces démontrant l'implication du **Relai DPO dans les réunions de services**

Sensibilisation des personnels

- Liste des **actions de sensibilisation** réalisées au sein de la Direction
- Liste **des personnels ayant suivi une sensibilisation** au RGPD et à son application interne (feuille de présence, ...)
- Justificatifs **d'absence de personnel** aux sessions de sensibilisation
- Copie des **supports de sensibilisation**
- Justificatifs **d'actions de sensibilisation suivie en dehors des locaux** de la banque

Synthèse du plan d'actions

11 chantiers ; 37 actions à engager

↓

Une mobilisation de tous les personnels est nécessaire et une implication forte de la Direction Générale indispensable

↓

La conduite du projet de mise en conformité implique un engagement variable selon le niveau de maturité et la taille de l'organisation (jusqu'à 24 mois)

Merci pour votre attention