Les rendez-vous de la régulation financière et de la conformité - 10ème édition

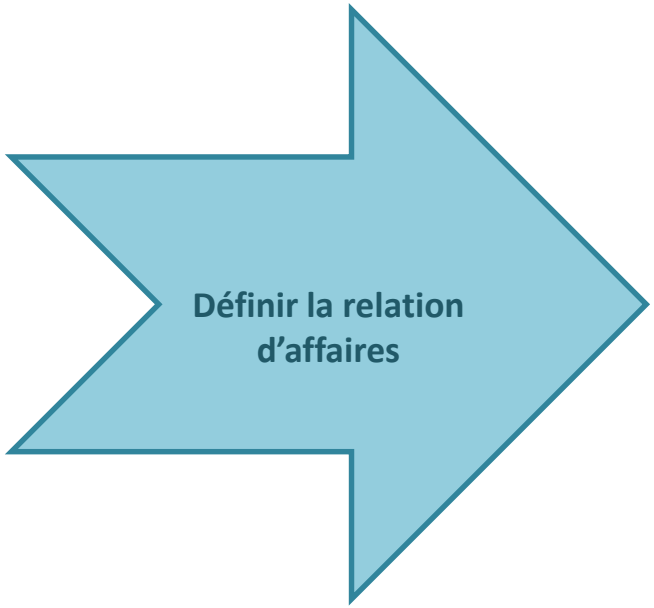
EIFR – European Institute of Financial Regulation

Marie-Agnès NICOLET
Regulation Partners
Présidente fondatrice
35, Boulevard Berthier 75017 Paris
marieagnes.nicolet@regulationpartners.com
+33.6.58.84.77.40 / +33.1.46.22.65.34

Sommaire

- Lutte anti-blanchiment : point sur la 4ème Directive
- Loi Sapin 2 : lutte contre la corruption
- Gouvernance : guide d'évaluation des administrateurs
- RGPD : les principales évolutions

Lutte anti-blanchiment : point sur la 4ème Directive



- **Identification / connaissance**

➢ *Identification des **bénéficiaires effectifs** (BE).*
⇒ *recherches vers Infogreffe (en application d'une nouveauté 4ème directive)*

➢ *L' élargissement aux **personnes politiquement exposées** (PPE) nationales (nouveauté de la 4ème directive)*

• Classification des risques LCB/FT

➢ *L'approche par les risques permet :*
- *de définir des diligences différenciées à l'entrée en relation*
- *d'adapter la périodicité de revue des relations d'affaires*
- *d'adapter la vigilance constante*

Elaboration d'une classification des risques LCB en 4 axes selon:

Client/ Le type de la relation d'affaires

Le type de produit

Le canal de distribution

Les conditions de réalisation de la transaction

Un 5ème axe à venir

Un axe pays/territoire d'origine/destination des fonds

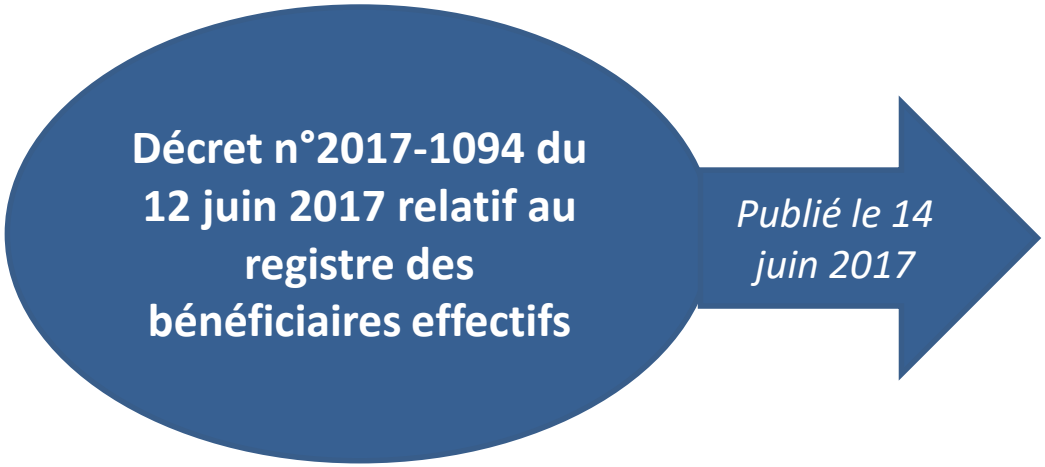
Identifier le risque global de la relation d'affaires

Le cumul des quatre axes détermine le niveau de sensibilité

Risque faible	Risque modéré	Risque élevé
Diligences simplifiées	Diligences standard	Diligences renforcées

Prise en compte des orientations EBA/ESMA/ EIOPA

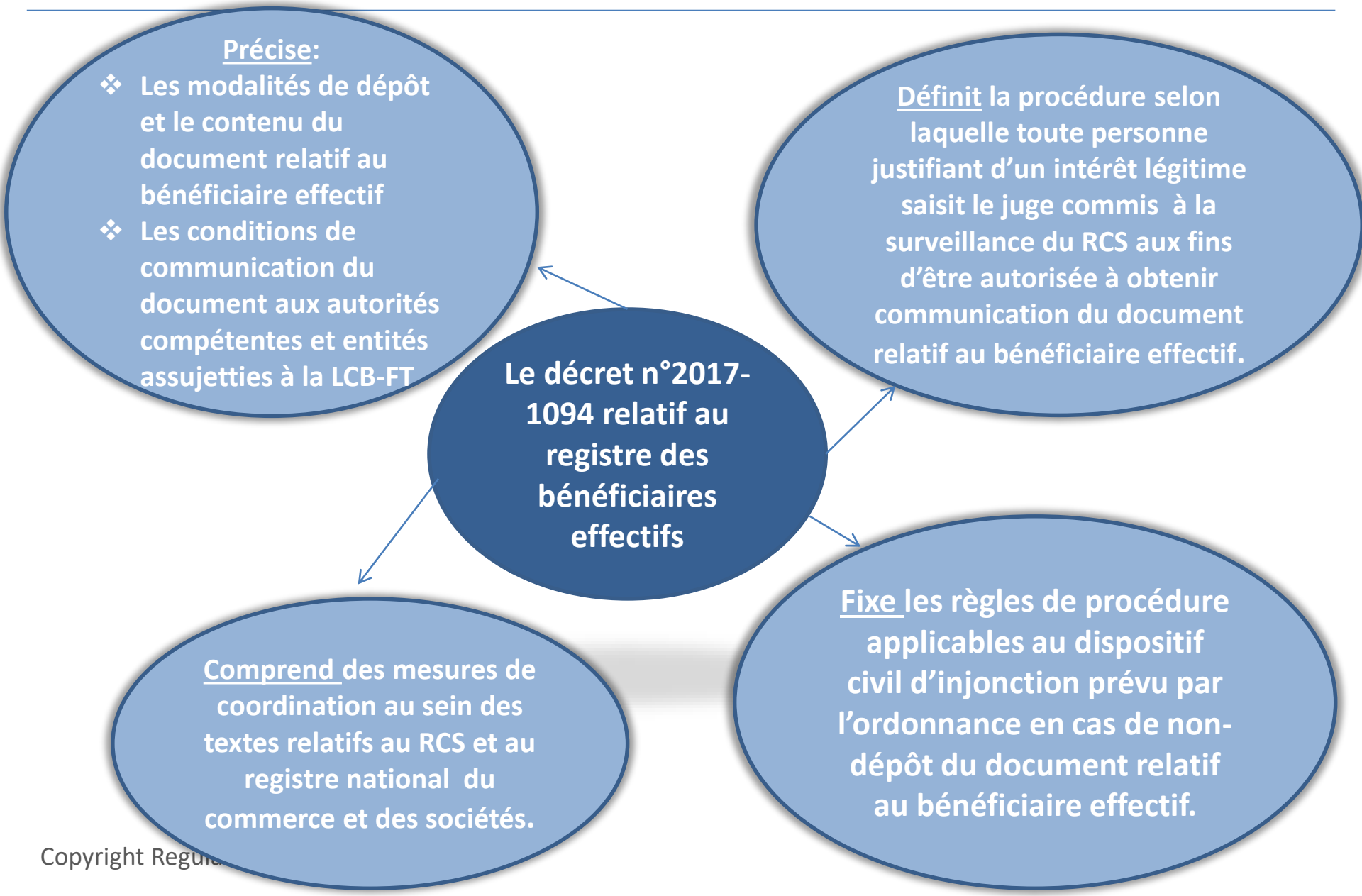
• Registre des bénéficiaires effectifs



- Entrée en vigueur le **1er août 2017**
- Personnes immatriculées au RCS avant le 1er août 2017 disposent d'un délai **jusqu'au 1er avril 2018 pour se conformer aux dispositions**

- Ce décret est relatif à l'**ordonnance n°2016-1635** renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme, transposant **l'article 30 de la directive 2015/849/UE** qui crée le registre des bénéficiaires effectifs des personnes morales.

• Registre des bénéficiaires effectifs



Où et quand déposer le document? : R. 561-55 CMF

Le document relatif au bénéficiaire effectif est **déposé au greffe du tribunal de commerce pour être annexé au RCS**:

- Lors de la **demande d'immatriculation à ce registre**
- OU au plus tard dans **un délai de 15 jours** à compter de la **délivrance du récépissé de dépôt de dossier de création d'entreprise**

Un nouveau document est déposé **dans les 30 jours suivant tout fait ou acte rendant nécessaire la rectification ou le complément des informations qui y sont mentionnées.**

Sommaire

- Lutte anti-blanchiment : point sur la 4ème Directive
- Loi Sapin 2 : lutte contre la corruption
- Gouvernance : guide d'évaluation des administrateurs
- RGPD : les principales évolutions

Loi Sapin 2 : lutte contre la corruption

La **Loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique,** dite Loi Sapin 2, a été publiée au Journal officiel de la République française le 10 décembre 2016.

Création d'une agence française anticorruption

PROTECTION DES LANCEURS D'ALERTE

LUTTE CONTRE LES MANQUEMENTS A LA PROBITE

Loi Sapin II: Agence française anticorruption

Création d'une agence française anticorruption

Art. 1 - Service à **compétence nationale**, ayant pour mission **d'aider les autorités compétentes** et les personnes qui y sont confrontées à prévenir et à détecter les faits:

- de corruption,
- de trafic d'influence,
- de concussion,
- de prise illégale d'intérêt,
- de détournement de fonds publics et de favoritisme.

Agents habilités à faire **des contrôles** sur place et à **se faire communiquer**, le cas échéant à prendre des copies**, de tout document professionnel**, quel qu'en soit le support, et **de toute information utile.**

Organisation

Art 2 -Agence dirigée par un **magistrat hors hiérarchie** de **l'ordre judiciaire** nommé par décret du Président de la République pour 6 ans, non renouvelable.
Il ne peut être mis fin à ses fonctions :

- que sur sa demande ou
- en cas d'empêchement ou
- en cas de manquement grave

Commission des sanctions

En cas de manquement constaté, et après avoir mis la personne concernée en mesure de présenter ses observations, le **magistrat qui dirige l'agence peut adresser un avertissement aux représentants de la société**.
Il peut **saisir la commission des sanctions** afin que soit enjoint à la société et à ses représentants **d'adapter les procédures de conformité internes destinées à la prévention et à la détection des faits de corruption ou de trafic d'influence**

Loi Sapin II: Agence française anticorruption

Missions de l'agence française anticorruption – Art.3

Participe à la **coordination administrative, centralise** et **diffuse les informations** permettant d'aider à prévenir et à détecter *les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme.*

Elabore des recommandations destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter *les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme*

Contrôle, de sa propre initiative, la qualité et l'efficacité des procédures mises en œuvre au sein des administrations de l'Etat, des collectivités territoriales, de leurs établissements publics et sociétés d'économie mixte, et des associations et fondations reconnues d'utilité publique pour prévenir et détecter *les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme.*

Avise le procureur de la République compétent en application de l'article 43 du code de procédure pénale des faits dont elle a eu connaissance dans l'exercice de ses missions et qui sont susceptibles de constituer un crime ou un délit…

Adresser un avertissement aux représentants de la société, saisir la commission des sanctions afin que soit enjoint à la société et à ses représentants d'adapter les procédures de conformité internes destinées à la prévention et à la détection des *faits de corruption ou de trafic d'influence.;*

Loi Sapin II : protection des lanceurs d'alerte

Définition du lanceur d'alerte
Art 6.

- Personne physique **qui révèle ou signale,** de manière désintéressée et de bonne foi, **un crime ou un délit, une violation grave** et **manifeste** :
  - ⇒ d'un engagement international régulièrement ratifié ou approuvé par la France,
  - ⇒ d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement,
  - ⇒ de la loi ou du règlement, ou **une menace ou un préjudice graves pour l'intérêt général**,

  dont elle a eu personnellement connaissance.

- **Sont exclus** les faits, informations ou documents, **couverts par :**
  - ⇒ Le secret de la défense nationale,
  - ⇒ Le secret médical ou
  - ⇒ Le secret des relations entre un avocat et son client.

Loi Sapin II : protection des lanceurs d'alerte

Procédures de signalement Art.8

- **Obligatoires** pour les entreprises d'au moins 50 salariés
- Ces procédures garantissent une **stricte confidentialité de l'identité des auteurs du signalement**, des personnes visées par celui-ci et des informations recueillies par l'ensemble des destinataires du signalement.

L'alerte est portée à la connaissance :

⇒ du supérieur hiérarchique, direct ou indirect,
⇒ de l'employeur ou
⇒ d'un référent désigné par celui-ci.

En l'absence de diligences de la personne destinataire de l'alerte à vérifier, dans un délai raisonnable, la recevabilité du signalement, **celui-ci est adressé :**

⇒ à l'autorité judiciaire,
⇒ à l'autorité administrative ou
⇒ aux ordres professionnels.

Toute personne peut adresser son signalement au Défenseur des droits afin d'être orientée vers l'organisme approprié de recueil de l'alerte.

En cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles, le signalement peut être porté directement à la connaissance de ces organismes.

En dernier ressort, à défaut de traitement par l'un de **ces organismes dans un délai de trois mois**, le signalement peut être rendu public.

Loi Sapin II : protection des lanceurs d'alerte

L'AMF et l'ACPR mettent en place des procédures permettant à leurs personnels de recevoir des signalements d'alerte – Art. 16

L'AMF et l'ACPR mettent en place des **procédures permettant que leur soit signalé tout manquement aux obligations** définies par les règlements européens et par le CMF ou le RGAMF et dont la surveillance est assurée par l'une ou l'autre de ces autorités.

- **Le règlement général de l'Autorité des marchés financiers**, pour ce qui concerne l'AMF, et
- **un arrêté du ministre chargé de l'économie**, pour ce qui concerne l'ACPR,

->fixent les modalités d'application du présent chapitre.

Les personnes physiques ayant signalé de bonne foi à l'AMF et à l'ACPR des faits susceptibles de caractériser l'un ou plusieurs des manquements susvisés **ne peuvent faire l'objet, pour ce motif,** *d'un licenciement, d'une sanction, d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération ou d'évolution professionnelle, ou de toute autre mesure défavorable.*

Loi Sapin II : lutte contre les manquements à la probité

Autres mesures de lutte contre la corruption et divers manquements à la probité

Obligation de prendre les mesures destinées à prévenir et à détecter la commission, en France ou à l'étranger, de faits de corruption ou de trafic d'influence, pour :

- sociétés employant au moins 500 salariés, ou appartenant à un groupe de sociétés dont la société mère a son siège social en France et dont l'effectif comprend au moins 500 salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est > à 100 millions d'euros

- établissements publics à caractère industriel et commercial employant au moins 500 salariés, ou appartenant à un groupe public dont l'effectif comprend au moins cinq cents salariés, et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros

Loi Sapin II : lutte contre les manquements à la probité

Autres mesures de lutte contre la corruption et divers manquements à la probité

Mesures et procédures à mettre en place par ces entreprises, avant le 1er juin 2017 ,pouvant être contrôlées par l'Agence française anti-corruption, notamment :

- **code de conduite** définissant et illustrant les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence, intégré au règlement intérieur.
- **dispositif d'alerte interne** permettant de recueillir des signalements émanant d'employés et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société.
- **cartographie des risques** prenant la forme d'une documentation régulièrement actualisée et destinée à identifier, analyser et hiérarchiser les risques d'exposition de la société à des sollicitations externes aux fins de corruption, en fonction notamment des secteurs d'activités et des zones géographiques dans lesquels la société exerce son activité
- **procédures d'évaluation** de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques
- **procédures de contrôles comptables**, internes ou externes, destinées à s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence.
- **dispositif de formation** destiné aux cadres et aux personnels les plus exposés aux risques de corruption et de trafic d'influence
- **régime disciplinaire** permettant de sanctionner les salariés de la société en cas de violation du code de conduite de la société
- **dispositif de contrôle** et **d'évaluation interne** des mesures mises en œuvre

Sommaire

- Lutte anti-blanchiment : point sur la 4ème Directive
- Loi Sapin 2 : lutte contre la corruption
- Gouvernance : guide d'évaluation des administrateurs
- RGPD : les principales évolutions

Gouvernance :
guide d'évaluation des administrateurs

regulation partners

- Champ d'application de l'évaluation par la BCE de l'honorabilité et de la compétence
- Les principes
- Les cinq critères d'évaluation

• Champ d'application de l'évaluation par la BCE de l'honorabilité et de la compétence

Évaluation de l'honorabilité et de la compétence des membres de l'organe de direction

À la fois

- Dans leur fonction exécutive
- Dans leur fonction de surveillance

De tous les établissements soumis à la surveillance directe de la BCE (établissements importants)

Qu'il s'agisse

- Établissements de crédit
- Compagnies financières holding (mixtes)

➔ **Établissements moins importants**: Dans le cas de demande d'agrément ou de participations qualifiées

➢ **Autorités nationales compétentes** (ANC) = responsables des **nominations ordinaires** dans les établissements moins importants (*hors du contexte de demande d'agrément ou de participations qualifiées*)

• Principes

1) Responsabilité première des établissements de crédit de:

sélectionner et nommer à leur organe de direction des personnes qui **satisfont aux exigences d'honorabilité et de compétence *(« aptitude »)***

s'assurer qu'elles peuvent compter sur une **coopération entièrement transparente des personnes concernées**.

fournir aux autorités compétentes **toutes les informations nécessaires** pour évaluer l'honorabilité et la compétence, quel que soit le cas (*nouvelle nomination, faits nouveaux, changement de fonction, etc.*) **dans les meilleurs délais et de manière précise.**

faire preuve de la **diligence requise** et **procéder à l'évaluation** des membres de l'organe de direction non seulement avant leur nomination mais aussi de manière continue *(par exemple en cas d'une modification importante des responsabilités d'un membre de l'organe de direction).*

• Les cinq critères d'évaluation de l'honorabilité et de la compétence des membres de l'organe de direction

regulation partners

1. Expérience

- Expérience pratique et théorique
- Expériences spécifiques à la fonction et exigences minimales
- Approche d'évaluation (par rapport à des seuils/ complémentaire)

2. Réputation

- Absence de proportionnalité
- Procédures judiciaires (en cours)

3. Conflits d'intérêts et indépendance d'esprit

- Divulgation, atténuation, gestion et prévention des conflits d'intérêts
- Évaluation des conflits d'intérêts

4.Disponibilité

- Exigences quantitatives et qualitative
- Évaluation quantitative de la disponibilité
- Évaluation qualitative de la disponibilité
- Informations à fournir par l'entité soumise à la surveillance prudentielle

5. Aptitude collective

- Auto-évaluation et contrôle continu de la gouvernance
- Motivation au moment de la nomination

• Expérience

Expérience pratique et théorique	• disposer des **connaissances**, des **compétences** et de l'**expérience** nécessaires à l'exercice de leurs attributions • « *expérience* » couvre à la fois : ⇒ L'expérience **pratique** et **professionnelle** acquise dans le cadre de fonctions antérieures ⇒ L'expérience **théorique** (connaissances et compétences) résultant de l'enseignement

Expériences spécifiques à la fonction et exigences minimales	• Plus les caractéristiques de la fonction donnée et de l'établissement sont complexes, plus le niveau d'expérience requis est élevé. • **Tous les membres de l'organe de direction** doivent disposer, au minimum, d'une **expérience théorique de base** dans le **domaine bancaire**, qui leur permette de comprendre *les activités et les principaux risques* de l'établissement. • L'expérience requise (en termes de niveau et de nature) d'un membre de l'organe de direction **dans sa fonction exécutive** peut différer de celle nécessaire à un membre de l'organe de direction **dans sa fonction de surveillance**, en particulier lorsque ces fonctions sont exercées par des organes distincts.	**Expérience théorique de base** *(pouvant être acquise dans le cadre d'une formation spécifique pour certaines fonctions):* • les marchés financiers, • le cadre réglementaire et les exigences juridiques, • la planification stratégique et la compréhension de la stratégie commerciale ou du plan d'activité (*business plan*) d'un établissement de crédit et de sa mise en œuvre, • la gestion des risques (identification, évaluation, suivi, contrôle et atténuation des principaux types de risques d'un établissement de crédit), y compris l'expérience liée directement aux responsabilités du membre, • la comptabilité et l'audit, • l'évaluation de l'efficacité des dispositifs d'un établissement de crédit, garantissant des mécanismes de gouvernance, de surveillance et de contrôle efficaces, • l'interprétation des informations financières d'un établissement de crédit, l'identification des problèmes majeurs sur la base de ces informations et la mise en place des mesures et contrôles appropriés

• Une **expérience supplémentaire** peut **être jugée nécessaire** sur la base de facteurs pertinents, tels que la fonction sollicitée, la nature, la taille et la complexité de l'entité.

• Expérience

Afin d'apprécier l'**expérience théorique** d'un membre **dans le domaine bancaire**, il est tenu compte en particulier du **niveau et du type d'études réalisées,** qui devraient avoir un **lien avec le secteur bancaire et financier** ou tout autre domaine pertinent (*principalement la banque et la finance, l'économie, le droit, l'administration, la réglementation financière, l'information et la technologie, l'analyse financière et les méthodes quantitatives*).

L'**expérience pratique** est évaluée sur **la base des fonctions exercées antérieurement**, en tenant compte de la *durée du contrat, de la taille de l'entité, des responsabilités, du nombre de subordonnés, de la nature des activités effectuées, de la réelle pertinence de l'expérience acquise*, etc.

Sans préjudice des formulaires nationaux, l'entité soumise à la surveillance prudentielle doit soumettre, au minimum, **un curriculum vitæ détaillé de la personne nommée.** Les programmes de formation déjà suivis ou à suivre par la personne nommée sont aussi pris en considération.

L'évaluation de l'honorabilité et de la compétence est **toujours traitée au cas par cas**. Cependant, en vue d'améliorer l'efficacité de l'évaluation et d'en réduire la durée, **une approche en deux phases est mise en œuvre**.

- Au cours de la phase 1, l'expérience de la personne nommée est appréciée **par rapport à des seuils à partir desquels l'expérience est supposée suffisante**. Même lorsque ces seuils ne sont pas atteints, la personne nommée peut encore être considérée comme apte.
- Dans pareils cas, il est toutefois nécessaire de procéder à une **évaluation complémentaire** (phase 2).

• Expérience

Phase 1: Evaluation par rapport à des seuils

L'expérience est évaluée par rapport à des **présomptions générales d'expérience** suffisante en fonction **de seuils.**

Lorsque les seuils sont atteints, la personne nommée est généralement **présumée disposer d'une expérience suffisante**, sauf indication contraire.

Ces seuils sont sans préjudice du **droit national** et **ne permettent pas de conclure automatiquement** que les personnes nommées qui ne les atteignent pas ne font pas preuve d'honorabilité et de compétence.

« *L'expérience pertinente* » peut être plus large pour le président ou un directeur non exécutif que pour un directeur exécutif. Quoi qu'il en soit**, il n'est pas nécessaire que l'ensemble des membres de l'organe de direction, dans sa fonction de surveillance, disposent d'une expérience pratique dans les domaines liés au secteur bancaire ou financier.**

• Expérience

Phase 1: Evaluation par rapport à des seuils

Présomption d'une expérience suffisante pour l'organe de direction dans sa **fonction exécutive**		Présomption d'une expérience suffisante pour l'organe de direction dans sa **fonction de surveillance**	
Directeur général	**Directeur**	**Président**	**Administrateur non exécutif**
Fonction exécutive : dix ans d'expérience pratique récente dans les domaines liés au secteur bancaire et financier. Cela doit inclure une part significative de postes de direction de très haut niveau.	**Fonction exécutive : cinq ans d'expérience** pratique récente dans les domaines liés au secteur bancaire et financier à des postes de direction de très haut niveau.	**Président du board: dix ans d'expérience pratique récente pertinente**. Cela comprend: - une part significative de postes de direction de très haut niveau et - une expérience théorique approfondie dans le secteur bancaire ou dans un domaine similaire pertinent.	**Administrateur non exécutif: trois ans d'expérience pratique récente à des postes de direction de haut niveau ***(*y compris une expérience théorique dans le secteur bancaire*). L'expérience pratique acquise dans le **secteur public ou universitaire** peut également être pertinente selon la fonction occupée.
Expérience pratique récente : qui ne remonte pas à plus de 12 ans **Poste de direction de très haut niveau**: c'est-à-dire au moins une expérience dans un organe de direction dans sa fonction exécutive ou à un niveau en-dessous.		• S'agissant de l'évaluation de la pertinence, il convient de tenir compte du **degré de similitude,** en termes de **taille et de complexité**, des établissements dans lesquels l'expérience antérieure a été acquise. *Un ou deux niveaux en dessous de l'organe de direction dans sa fonction exécutive.	

• Expérience

Phase 2: Evaluation complémentaire

Si les seuils permettant de présumer d'une expérience suffisante **ne sont pas atteints**

la personne nommée *peut encore être considérée comme apte* **si l'entité** soumise à la surveillance prudentielle **est en mesure de le justifier de manière adéquate**.

une évaluation complémentaire de l'expérience de la personne nommée

Évaluation complémentaire en tenant compte :

- de la nécessité **de disposer d'une diversité suffisante** et
- d'un **large éventail d'expériences au sein de l'organe de direction**

➔ Et, le cas échéant, des **exigences nationales** de nommer des représentants du personnel dans l'organe de direction.

• Expérience

Phase 2: Evaluation complémentaire

Les justifications peuvent être :

- *un programme de formation* en cas de manque partiel d'expérience dans un domaine précis,
- *l'aptitude collective générale* des membres de l'organe de direction déjà présents,
- *la nomination pour une fonction particulière limitée dans le temps* (dans le cas d'un établissement en liquidation par exemple) ou
- *lorsque la personne nommée dispose d'une expérience théorique ou pratique spécifique* dont a besoin l'établissement.

À titre d'exemple, un membre de l'organe de direction dans sa fonction de surveillance qui n'atteint pas les seuils mentionnés ci-dessus pour la position peut encore être considéré comme apte si :

a) *le membre a une expérience dans le domaine informatique qui répond aux besoins spécifiques de l'établissement,*
b) *le membre et l'établissement s'engagent à ce que la formation requise soit suivie afin de pallier au manque de connaissances de base dans le domaine bancaire et*
c) *le membre satisfait à toutes les autres exigences d'honorabilité et de compétence.*

• Conflits d'intérêts et indépendance d'esprit

Divulgation, atténuation, gestion et prévention des conflits d'intérêts

Principe: Les membres des organes de direction doivent être en mesure de prendre des **décisions judicieuses, objectives et en toute indépendance** (*c'est-à-dire d'agir en faisant preuve d'indépendance d'esprit*)
L'indépendance d'esprit peut être compromise par des **conflits d'intérêts**.

- L'entité soumise à la surveillance prudentielle doit disposer de **politiques de gouvernance assurant l'identification, la divulgation, l'atténuation, la gestion et la prévention des conflits d'intérêts**, que ces derniers soient *réels, potentiels* (c'est-à-dire raisonnablement prévisibles) *ou perçus* (c'est-à-dire dans l'esprit du public).
- **Il y a conflit d'intérêts lorsque la poursuite des intérêts du membre affecte défavorablement les intérêts de l'entité soumise à la surveillance prudentielle.**

- Une personne nommée qui est dans une situation de conflit d'intérêts **n'est pas nécessairement considérée comme inapte.**
- Cela sera uniquement le cas si le conflit d'intérêts présente un risque important et s'il n'est pas possible de prévenir, d'atténuer de manière adéquate ou de gérer le conflit d'intérêts en vertu des règles écrites de l'entité soumise à la surveillance prudentielle.

• Conflits d'intérêts et indépendance d'esprit

Situations dans lesquelles il est considéré qu'un conflit d'intérêts important existe

Type de conflit	Période	Degré et type de relation et, le cas échéant, seuil
Personnel	*Actuelle*	La personne nommée • a un **lien personnel étroit** avec un membre de l'organe de direction, le titulaire d'un poste clé ou un actionnaire qualifié dans l'entité soumise à la surveillance prudentielle ou dans la société mère/ses filiales ; • est impliquée dans des **procédures judiciaires** engagées contre l'entité soumise à la surveillance prudentielle ou contre la société mère/ses filiales ; • mène des **activités significatives**, de façon privée ou par l'intermédiaire d'une société, avec l'entité soumise à la surveillance prudentielle ou avec la société mère/ses filiales.
Professionnel	*Actuelle ou au cours des deux dernières années*	La personne nommée ou une personne proche : - **occupe dans le même temps** un **poste** de cadre ou de cadre supérieur dans l'entité soumise à la surveillance prudentielle, **chez l'un de ses concurrents** ou **dans la société mère/ses filiales ;** - entretient une **relation commerciale** significative avec l'entité soumise à la surveillance prudentielle, un de ses concurrents ou la société mère/ses filiales. L'importance de l'intérêt commercial dépendra de **la valeur (financière)** qu'il représente pour l'activité de la personne nommée ou de la personne proche d'elle.

• Conflits d'intérêts et indépendance d'esprit

regulation partners

Situations dans lesquelles il est considéré qu'un conflit d'intérêts important existe

Type de conflit	Période	Degré et type de relation et, le cas échéant, seuil
Financier	*Actuelle*	La personne nommée ou une personne proche détient un **intérêt financier important** ou une **obligation financière importante** • dans/envers l'entité soumise à la surveillance prudentielle ; • dans/envers la société mère ou ses filiales ; • chez/envers l'un des clients de l'entité soumise à la surveillance prudentielle ; • chez/envers l'un des concurrents de l'entité soumise à la surveillance prudentielle. Les participations, les investissements autres que les participations et les prêts sont des exemples d'intérêt financier/d'obligations financières. L'importance dépend de la valeur (financière) que l'intérêt ou l'obligation représente par rapport aux ressources financières de la personne nommée. Sont considérés en principe sans importance : l'ensemble des prêts personnels garantis (tels que les hypothèques privées) accordés à un taux non préférentiel (c'est-à-dire aux conditions normales de marché de la banque concernée) qui sont performants ; tous les autres prêts performants à taux non préférentiel de moins de 200 000 euros, garantis ou non ; les participations actuelles ≤ 1 % ou les autres investissements d'une valeur équivalente.

• Conflits d'intérêts et indépendance d'esprit

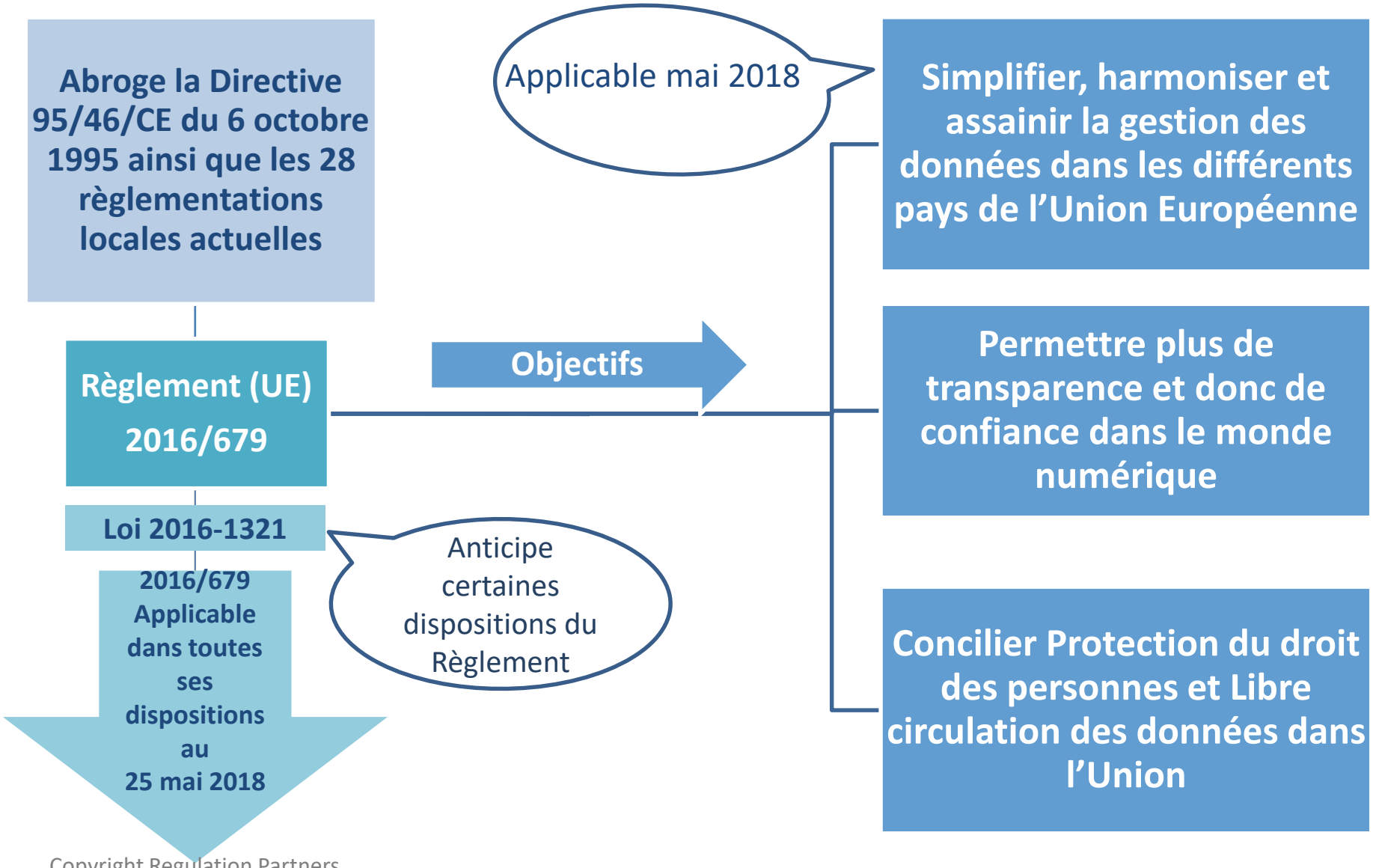
Situations dans lesquelles il est considéré qu'un conflit d'intérêts important existe

Type de conflit	Période	Degré et type de relation et, le cas échéant, seuil
Politique	Actuelle ou au cours des deux dernières années	La personne nommée ou une personne proche occupe un poste lui octroyant une **forte influence politique**. La « forte influence » est possible à tous les niveaux : élu local (maire, par exemple) ; élu régional ou national (ministre, par exemple) ; fonctionnaire (emploi gouvernemental, par exemple) ; représentant de l'État. L'importance du conflit d'intérêts dépend de la présence ou non de pouvoirs ou d'obligations spécifiques inhérents à une fonction politique susceptibles d'empêcher la personne nommée d'agir dans l'intérêt de l'entité soumise à la surveillance prudentielle.

Sommaire

- Lutte anti-blanchiment : point sur la 4ème Directive
- Loi Sapin 2 : lutte contre la corruption
- Gouvernance : guide d'évaluation des administrateurs
- RGPD : les principales évolutions

RGPD : les principales évolutions



RGPD : les principales évolutions

Logique de responsabilisation et de transparence

- Changement de culture interne nécessitant de mobiliser toutes les compétences (*DSI, prestataires, services juridiques, directions métier*)
- Les grands principes de la loi Informatique et Libertés demeurent et sont même renforcés (*information, consentement*)

Logique d'accountability

- Prise en compte de la protection des données **dès la conception** d'un service ou d'un produit et par défaut => « *privacy by design* »

- La mise en place d'une organisation, de mesures et d'outils internes garantissant une **protection optimale des personnes dont les données sont traitées**.

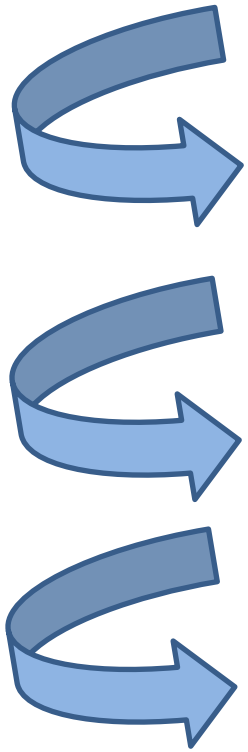
RGPD : les principales évolutions

Les organismes devront :

- désigner un pilote pour assurer la gouvernance des données personnelles de leur structure (le délégué à la protection des données sera obligatoire dans certains cas)
- réaliser l'inventaire des traitements de données personnelles mis en œuvre
- maintenir une documentation assurant la traçabilité des mesures
- identifier les risques associés aux opérations de traitement et prendre les mesures nécessaires à leur prévention
- évaluer leurs pratiques et mettre en place des procédures (notification des violations de données, gestion des demandes des personnes concernées, des réclamations, etc.)

RGPD : les principales évolutions

D'un point de vue opérationnel, la conformité au règlement européen repose sur différents outils:



- le registre des activités de traitements et la documentation interne
- l'analyse d'impact relative à la protection des données (DPIA ou Privacy Impact Assessment) pour les traitements à risque
- la notification de violations de données personnelles

La mise en œuvre de ces outils implique, **au préalable**, la désignation d'un pilote interne : **le délégué à la protection des données,** véritable « chef d'orchestre » de la protection des données personnelles au sein de l'organisme.

RGPD : Le délégué à la protection des données

Mission

Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Désignation

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.
Elle est obligatoire pour :

- *Les autorités ou les organismes publics,*
- *Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,*
- *Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles »*

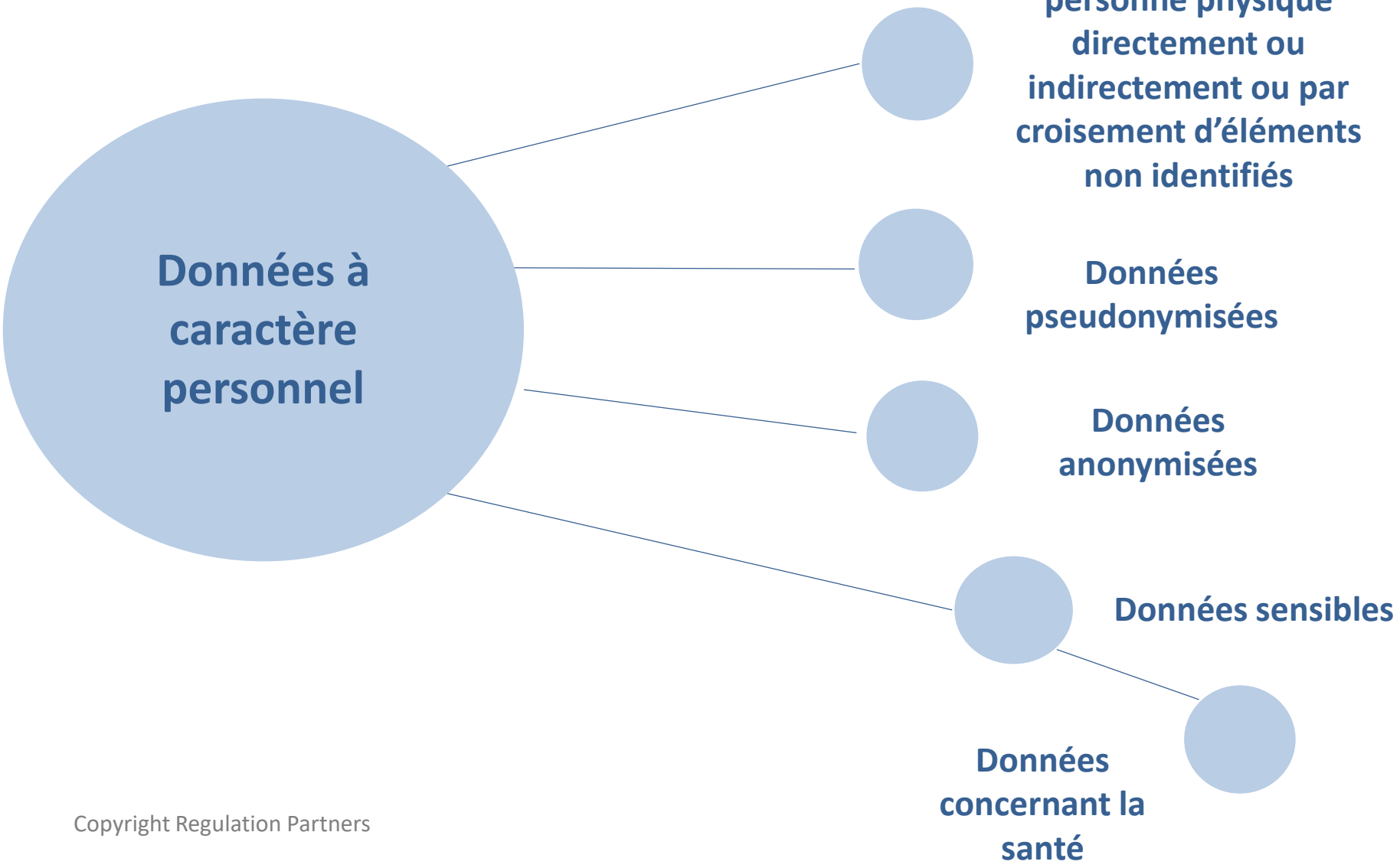
Compétence

Pour garantir l'effectivité de ses missions, le délégué :
- doit disposer de qualités professionnelles et de connaissances spécifiques,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

La mise en place de la fonction de délégué nécessite d'être anticipée.

RGPD: Les données à caractère personnel

Typologies des données à caractère personnel



RGPD: Les données à caractère personnel

- **Nature des données**

Données identifiantes

Article 2 de la loi informatique et Libertés

Article 4, 1° RGPD

Une donnée à caractère personnel est une information qui permet **d'identifier** une personne ou de la **reconnaitre** :

- **Données directement identifiantes** : nom, prénom, sexe, photo
- **Données indirectement identifiantes** : date de naissance, adresse postale, adresse électronique, adresse IP d'un ordinateur, numéro de téléphone, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, empreinte digitale, ADN, numéro de sécurité sociale…
- **Données ni directement ni indirectement identifiantes seules mais indentifiantes par rapprochement** : pathologie, âge, poids, centre de soins…

RGPD: Les données à caractère personnel

- **Nature des données**

Données sensibles

Article 8 de la Loi Informatique et Libertés

Certaine données sont jugées sensibles et ne peuvent être recueillies et utilisée qu'avec le consentement explicite de la personne concernée.

Exemples : données sur l'origine raciale ou ethnique, les opinions politiques, philosophiques, religieuses, l'appartenance syndicale, la **santé** ou la vie sexuelle.

Données de santé

- La notion de donnée de santé recouvre un sens très large et est susceptible de couvrir tous types de données dès lors que ces données se rattachent à « **l'état de complet bien-être physique, mental et social** » de la personne concernée (Préambule de la constitution de l'OMS du 19-22 juin 1946) ;

- Elles sont définies comme étant des données à caractère personnel « *liées à la santé physique ou mentale d'une personne, y compris la fourniture de services de soins de santé, qui révèlent des informations sur son état de santé* » (article 4, 12° RGPD) ;

- Elles ne concernent pas nécessairement une maladie ou une infirmité en particulier et peuvent viser un bon état de santé.

RGPD: Les données à caractère personnel

Données pseudonymisées
Article 4, 5° RGPD

Un dispositif de pseudonymisation est utilisé comme une mesure de sécurité et pour renforcer le niveau de protection de la vie privée de la personne **à un « instant t »** (appauvrissement de l'identification par la neutralisation des données indirectement identifiantes) ;

Concrètement, il s'agit d'une séparation **de base de données** :

-> conservation de l'identifiant dans une base de données ;
-> conservation des autres éléments dans une seconde base de données ;

Les données pseudonymisées permettent, en débit du procédé de « pseudonymisation » de remonter indirectement vers la personne concernée ;

Les données pseudonymisées sont donc des données à **caractère personnel indirectement identifiantes.**

RGPD: Les données à caractère personnel

A faire

Faire un inventaire précis des traitements

=> Réaliser une cartographie de tous les traitements effectuées en reprenant tous les éléments du traitement considéré

Recenser les informations du traitement par catégorie

- → Identification de responsable de traitement
- → Finalité de traitement
- → Personnes concernées par le traitement

Registre des activités de traitements

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 :

- 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;
- les finalités du traitement;
- une description des catégories de personnes concernées et des catégories de données à caractère personnel;
- 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;
- 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, §1, al. 2, les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, §1.

RGPD : La réalisation d'une analyse d'impact avant la mise en place d'un traitement de données

Article 35 RGPD

« 1. 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. »

Prise en compte du respect de la vie privée **dès la conception du traitement = «** *Privacy by design and by default* **»**

RGPD : Les droits reconnus à la personne

Trois droits reconnus à la personne par la loi Informatique et Libertés:

- *Opposition au traitement sous réserve de motif légitime*
- *Droit d'accès/communication aux données*
- *Droit de rectification/suppression*

11 droits dans le RGPD dont notamment :

- Droit à l'effacement («droit à l'oubli»)
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit à une information complète en langage clair
- Droit d'opposition

Etc...

Conclusion : droits étendus et facilités pour la personne concernée

Réaffirmation des principes essentiels de la vie privée:

- **Restriction d'utilisation**
- **Minimisation des données**
- **Précision**
- **Limitation du stockage**
- **Intégrité**
- **Confidentialité**
- **Licéité / loyauté / transparence**

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

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 s'effectue en des termes clairs et simples et contient au moins les informations suivantes :

- communiquer le nom et les coordonnées du DPD ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues
- décrire les conséquences probables de la violation de données à caractère personnel;
- 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.

RGPD : les 6 étapes proposées par la CNIL

regulation partners

1. Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : **le délégué à la protection des données**. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2. Cartogra-phier

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par **recenser de façon précise vos traitements de données personnelles**. L'élaboration d'un registre des traitements vous permet de faire le point.

3. Prioriser

Sur la base de votre registre, **identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir**. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

RGPD : les 6 étapes proposées par la CNIL

regulation partners

4. Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, **une analyse d'impact sur la protection des données** (PIA).

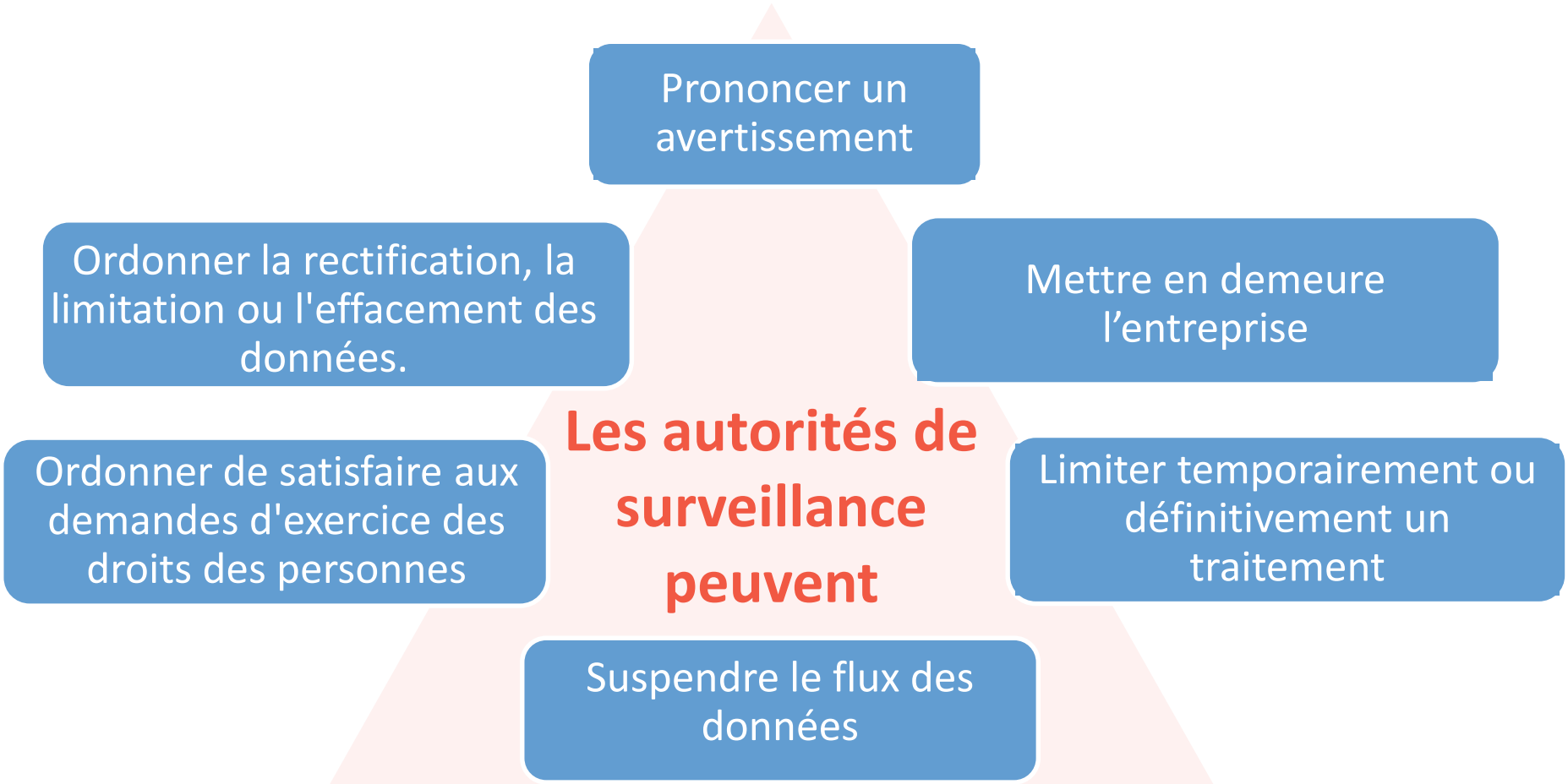
5. Organiser les processus

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (*ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).*

6. Documenter

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Pouvoirs des autorités de contrôle : adoption de mesures correctrices



Le non-respect d'une injonction émise par l'autorité de contrôle fait l'objet d'amendes administratives pouvant s'élever jusqu'à **20.000.000 €** ou, dans le cas d'une entreprise, jusqu'à **4 %** du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Art. 58 RG