Support de conférence

21 juin 2018

Contact : 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 :

I – Règlement Général sur la Protection des Données

II – Quatrième directive LCB FT

III – Projet de cinquième directive LCB FT

IV – DSP2

I – Règlement Général sur la Protection des Données

Règlement Général sur la Protection des Données

regulation partners

1. RGPD : Cadre juridique
2. Les acteurs clés
3. Les données à caractère personnel
4. Finalité d'un traitement de données à caractère personnel
5. Sécurité et notification d'une violation de données à caractère personnel
6. Les droits des personnes concernées
7. Responsabilité accrue des responsables de traitements et des sous-traitants
8. Sanctions et pouvoirs des autorités de contrôle
9. Registre des activités de traitements
10. Les études d'impact sur la vie privée

1. RGPD : Cadre juridique

Territorial	**Entreprise, responsable du traitement/sous-traitant dans l'UE**
	A destination de l'UE ou concernant données d'un citoyen européen
	Hors UE mais dans zone où droit de l'UE s'applique du fait du droit international public
Matériel	**Traitement de données personnelles**
	Données personnelles de personnes physiques
	Traitement automatisé en tout ou partie

- Le **RGPD s'applique à tous les traitements de données personnelles dès que** *(Article 3 - Champ d'application territorial du RGPD 2016/679)* **:**
  - le responsable de traitement ou le sous traitant est basé dans l'UE
  - le traitement d'une société basée dans l'UE est réalisé ou non dans l'UE
- **Le RGPD s'applique à toute société non établie dans l'UE dès lors que les traitements sont liés :**
  - à l'offre des biens ou des services dans l'Union
  - au suivi des comportements des personnes au sein de l'Union
- **Les compagnies hors de l'UE et traitant des données de citoyens européens doivent** *(Article 27 - Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union)* **:**
  - être en conformité
  - définir un représentant dans l'UE

Applicable mai 2018

2. Les acteurs clés

Personne concernée

Responsable du traitement :
- détermine seul ou conjointement les **finalités**
- dispose des **moyens** de traitement

<u>Sous-traitant :</u> effectue le traitement pour le compte du responsable du traitement

- Destinataire : personne habilitée à recevoir un traitement
- Peut devenir responsable d'un autre traitement

Tiers : personne non autorisée à recevoir le traitement

2. Les acteurs clés

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

2.2 - Sous-traitant : C'est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

2.3 – Destinataire : Il est 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.

2.4 – Tiers : Il est une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

Le tiers n'est donc pas autorisé à traiter les données à caractère personnel

2. Les acteurs clés

2.5 - Le délégué à la protection des données ? (DPD en français et DPO en anglais Data protection officer)

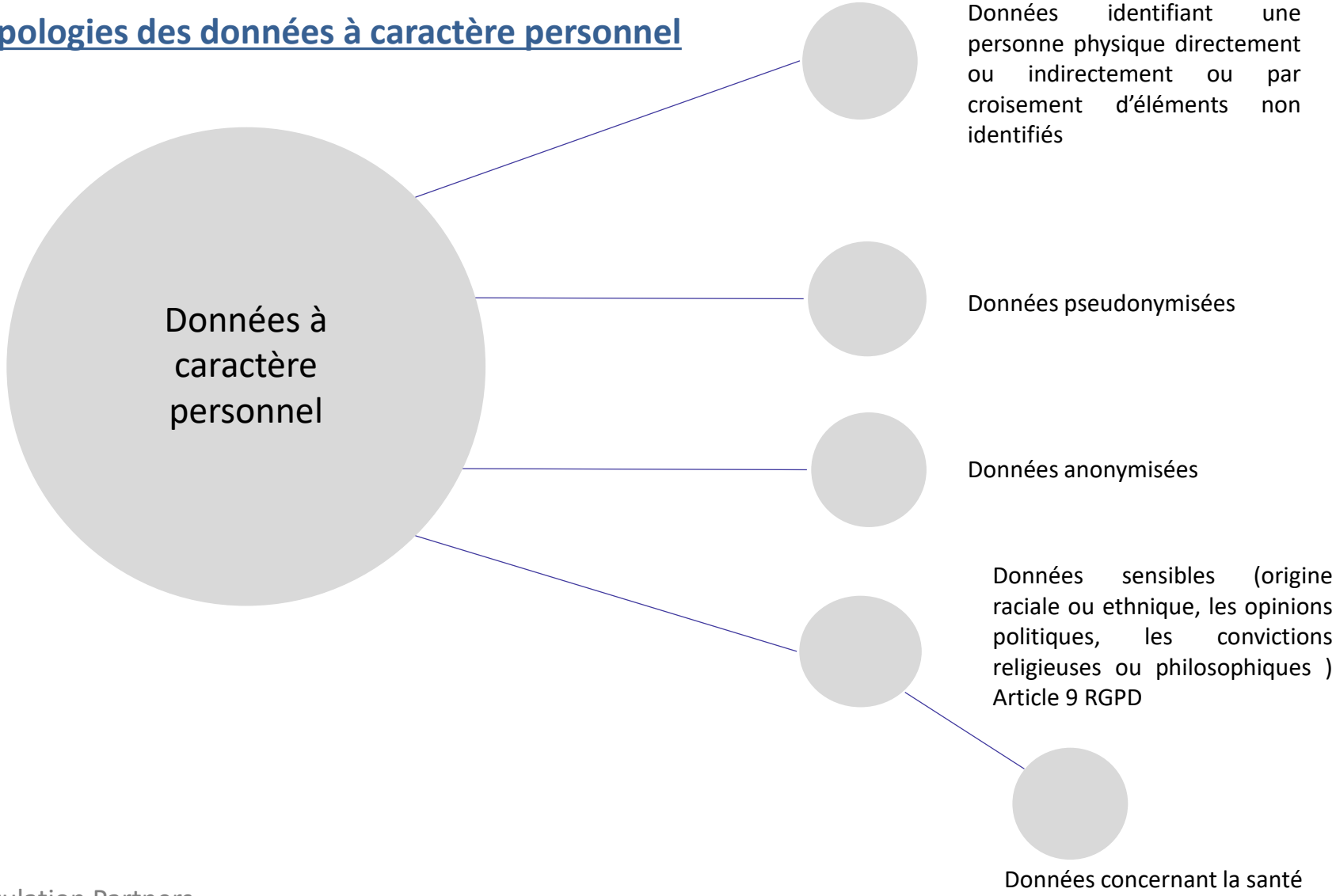
Le responsable du traitement et le sous-traitant désignent un délégué à la protection des données (DPD) à la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions.
Les missions du délégué à la protection des données sont au moins les suivantes :

- **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 en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données;
- **contrôler le respect du règlement**, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données 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;
- 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;
- 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.

Article 37 du RG

3. Les données à caractère personnel

Typologies des données à caractère personnel



4. Finalité d'un traitement de données à caractère personnel

Finalité explicite, déterminée, légitime

Article 6 de la Loi Informatique et Libertés

- Les données doivent être recueillies dans **un but précis**, pour une finalité déterminée, qui doit être **respectée tout au long de l'utilisation du fichier**

- **Aucune utilisation ultérieure** de ces données ne peut être faite pour un autre but que celui prévu initialement (**test de compatibilité** de la CNIL) ; **Exemple** : *Interdiction d'utiliser les données d'une base de recrutement à des fins marketing ;*

  Tout détournement de finalité : 5 ans de prison et 300 000 euros d'amende (Article 226-21 du Code Pénal)

- Tout nouvel usage des données, même s'il s'agit d'une simple extension doit faire l'objet de **formalités complémentaires** auprès de la CNIL et d'une nouvelle **information** des personnes concernées (article 32 de la Loi Informatique et Libertés), ces dernières devant être mises en mesure de s'**opposer à un tel usage** (article 38 de la Loi Informatique et Libertés) ;

  Défaut d'accomplissement des formalités : 5 ans de prison et 300 000 euros d'amende (Article 226-16 du Code pénal)

4. Finalité d'un traitement de données à caractère personnel

Finalité explicite, déterminée, légitime

Article 5 de RGPD

Les données à caractère personnel doivent être :

- traitées de manière **licite, loyale et transparente** au regard de la personne concernée (licéité, loyauté, transparence);

- collectées pour des **finalités déterminées lors de la collecte des données, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités

  - ⇨ le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales (limitation des finalités)

- **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées;

4. Finalité d'un traitement de données à caractère personnel

Finalité explicite, déterminée, légitime

Article 5 de RGPD

Les données à caractère personnel doivent être :

conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard:

- **Exactes et, si nécessaire, tenues à jour ;** toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)

- **conservées** sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées

- traitées de façon à **garantir une sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

- Finalité « ultérieure compatible » :
  - G29 estime que compatibilité s'apprécie en fonction :
    - du contexte dans lequel les données sont collectées
    - de l'impact du traitement ultérieur sur la personne concernée
    - des mesures de protection prises pour éviter l'impact indu sur les personnes concernées

5. Sécurité et notification des violations de données à caractère personnel

Principe : « Garantir une sécurité appropriée des données à caractère personnel y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide des mesures techniques ou organisationnelles appropriées » (article 5)

Procédure de notification à mettre en place

En cas de violation de données à caractère personnel :

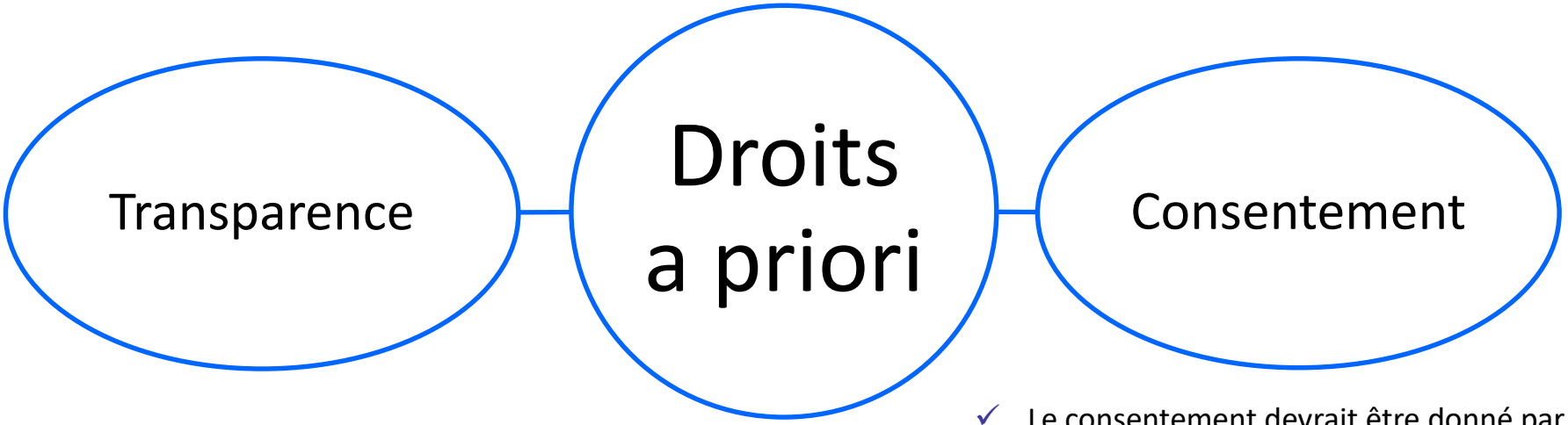
- le responsable du traitement en **notifie la violation** en question à l'autorité de contrôle compétente conformément à l'article 55,
- **dans les meilleurs délais et, si possible, 72 heures au plus tard** après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible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

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

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

- 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;
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés de la personne concernée n'est plus susceptible de se matérialiser;
- La communication exigerait des efforts disproportionnés : dans ce cas, il est procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

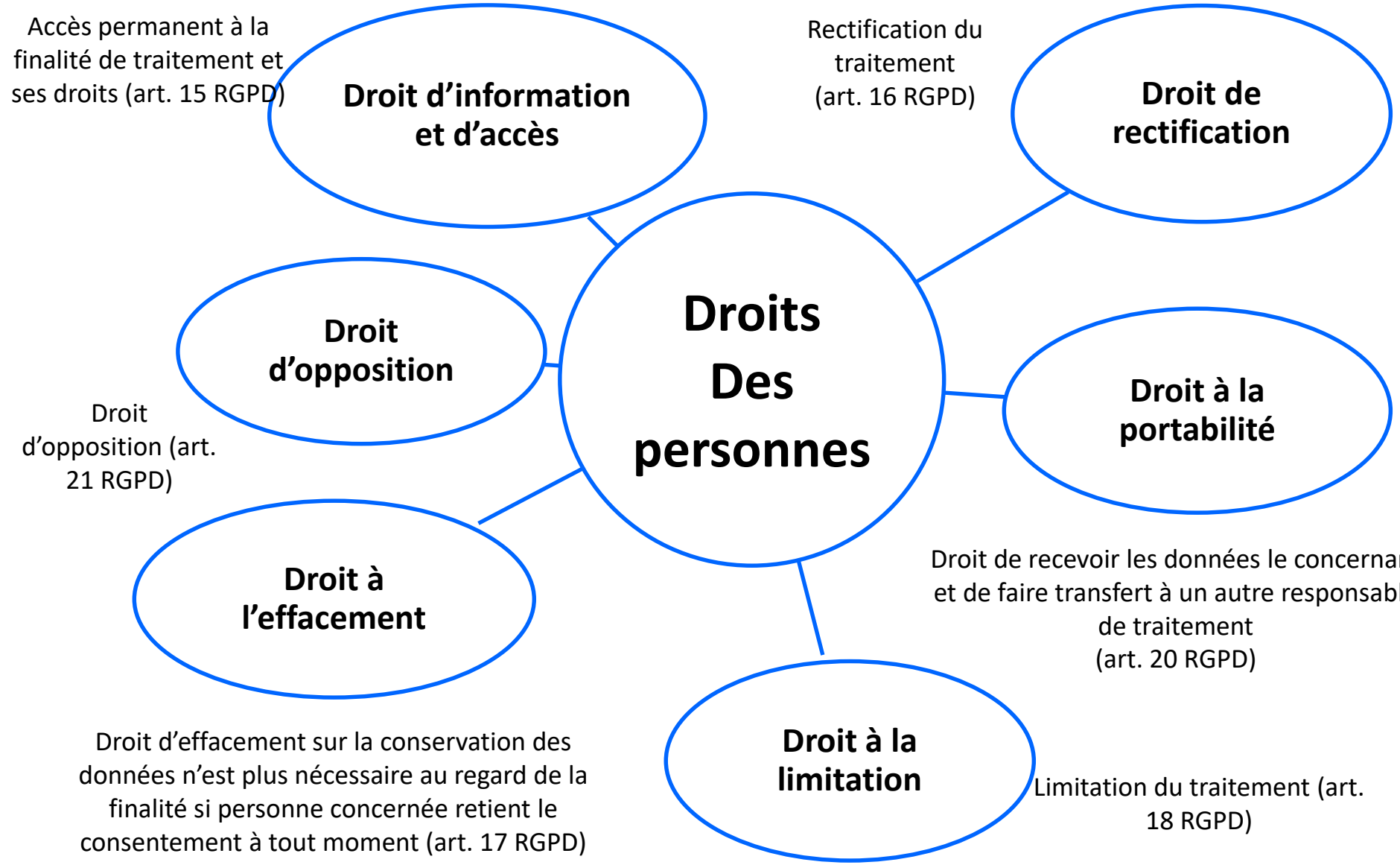
6. Les droits des personnes concernées



Le responsable du traitement prend des mesures appropriées pour fournir toute information à caractère personnel ainsi que pour procéder à toute communication au titre du **droit d'accès de la personne concernée, à rectification, d'opposition et à l'effacement de ses données à caractère personnel et de la violation de données à caractère personnel.**

- ✓ Le consentement devrait être donné par un **acte positif clair** par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant
- ✓ La personne concernée dispose d'un droit de retrait.
- ✓ Consentement spécifique nécessaire pour :
  - Collecte des données sensibles,
  - Profilage,
  - Transfert des données vers un pays n'assurant pas une protection adéquate, etc.

6. Les droits des personnes concernées



7. Responsabilité accrue des responsables de traitements et des sous-traitants

7.1 - Responsabilité du responsable du traitement

Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

7.2 - Responsables conjoints du traitement

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

Synthèse de la responsabilité

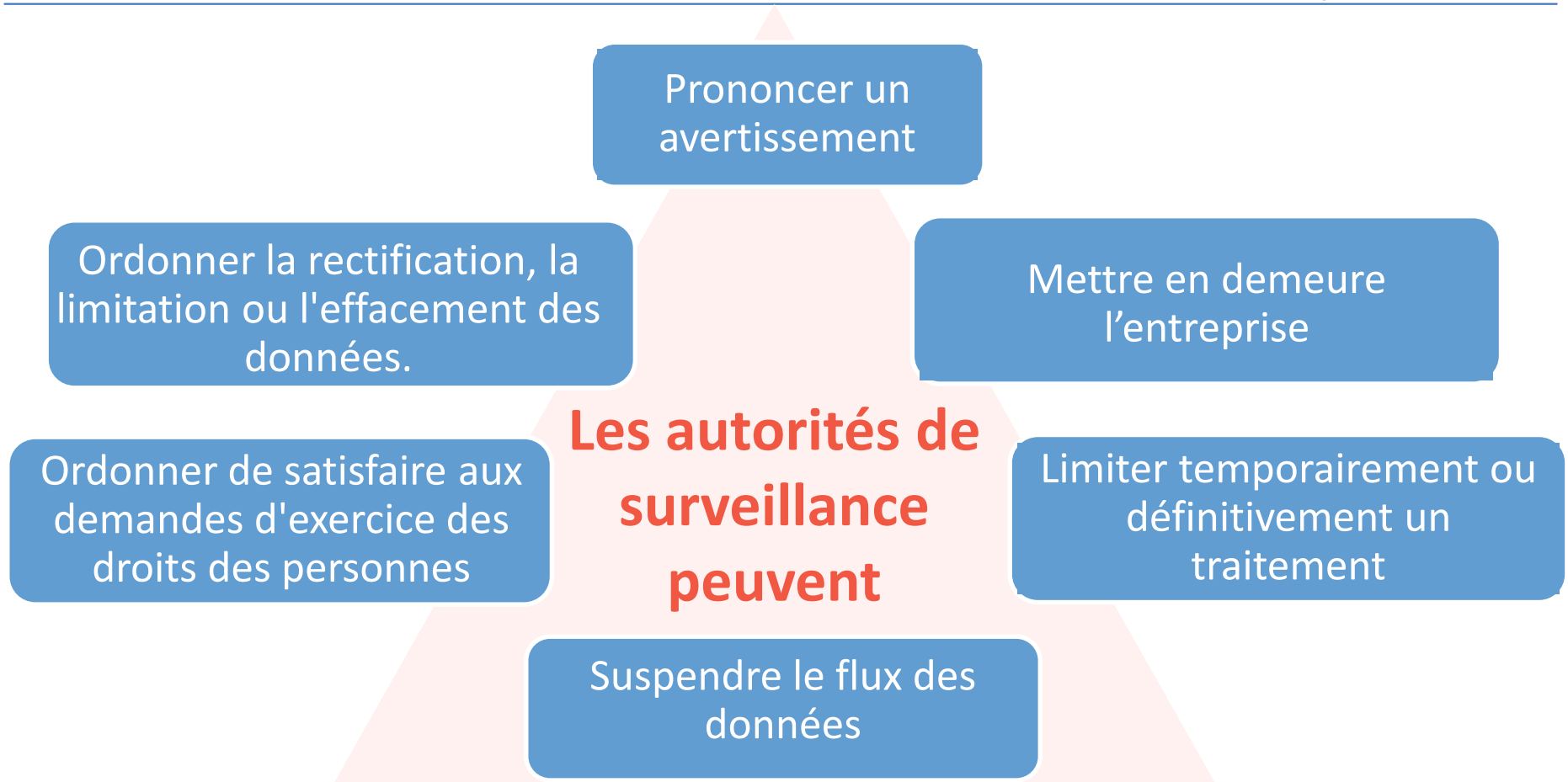
Entre un responsable et un sous-traitant [art. 24, 28 et 29 du RGPD] :

- En conformité avec le RGPD au regard du service fourni et ce quel que soit la localisation
- La responsabilité est partagée
- Le sous-traitant peut être contrôlé et sanctionné au même titre que le responsable de traitement

Entre les responsables (déterminent ensemble les finalités de traitements) [art.24 et 26 du RGPD] :

- Responsabilité partagée déterminée par un contrat

8. Sanctions



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 RGPD

9. 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;

10. Etude d'impact sur la vie privée (EIVP) ou Privacy Impact Assessment (PIA)

Quelles données ?

- **Données sensibles** (ci-après)
- Traitements pouvant présenter un **risque pour la liberté des personnes** :
  - **profilage**,
  - traitement à grande échelle de données,
  - **vidéosurveillance**…

⇨ Mettre en place une politique d'évaluation des risques pour les projets
-encadrer clairement quand un PIA est nécessaire.

⇨ S'assurer de la clarté de la documentation
-description du processus, évaluation de la proportionnalité du traitement, évaluation du risque au regard du droit et de la liberté des personnes, etc.

II – Quatrième directive LCB FT

Ordonnance transposant la 4ème directive européenne

4ème directive européenne 2015/849 de lutte contre le blanchiment adoptée le 20 mai 2015.

Transposition en droit français par **l'Ordonnance n°2016-1635 du 1er décembre 2016** renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme

Publication le 2 décembre 2016 au Journal officiel de la République française

décret n°2018-284 18 avril 2018

Définition précise des bénéficiaire effectif
Précision des mesures de vigilances

Obligation de vigilance avant d'entrer en relation d'affaires : Art. L561-5 CMF

Reformulation de l'article L.561-5 du code monétaire et financier créé par l'ordonnance du 30 janvier 2009 **modifié par l'ordonnance n°2016-1635 du 1er décembre 2016**

I. **Avant d'entrer en relation d'affaires ou d'assister leur client dans la préparation ou la réalisation d'une transaction**, les **personnes assujetties** :

- **1° Identifient** leur **client** et, le cas échéant, le **bénéficiaire effectif**
- **2° Vérifient ces éléments d'identification** sur présentation de **tout document écrit à caractère probant.**

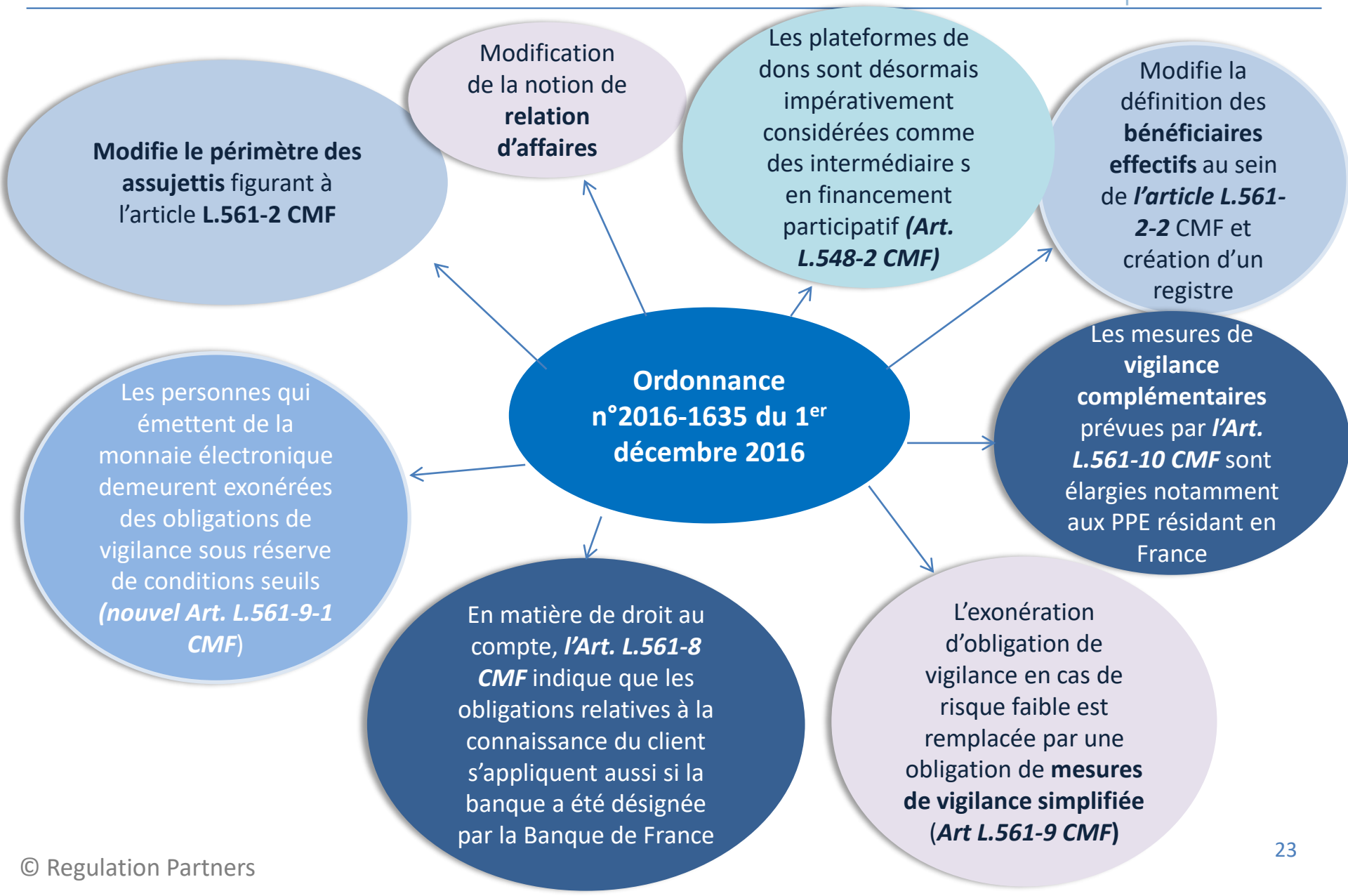
II. Elles identifient et vérifient dans les mêmes conditions **l'identité de leurs clients occasionnels et, le cas échéant, de leurs** bénéficiaires effectifs:

- lorsqu'elles soupçonnent qu'une opération pourrait participer au blanchiment des capitaux ou au financement du terrorisme ou
- lorsque les **opérations sont d'une certaine nature ou dépassent un certain montant.**

III. Lorsque le client souscrit ou adhère à un **contrat d'assurance-vie ou de capitalisation**, les personnes concernées identifient et vérifient également l'identité des bénéficiaires de ces contrats et le cas échéant des bénéficiaires effectifs de ces bénéficiaires (*nouveauté de l'article*)

IV. **Par dérogation au I**, lorsque le risque de blanchiment des capitaux ou de financement du terrorisme paraît faible et que c'est **nécessaire pour ne pas interrompre l'exercice normal de l'activité**, les obligations mentionnées au 2° dudit I peuvent être satisfaites **durant l'établissement de la relation d'affaires**.

Grandes modifications apportées par l'ordonnance



Niveau 1 : Risque faible
Diligences simplifiées

Article 30 du décret 2018-284

Vigilances *simplifiées* et non plus allégées

1 Les entités recueillent les informations justifiant que le client ou le produit présente un faible risque de blanchiment de capitaux ou de financement du terrorisme ou remplit les conditions prévues aux articles R. 561-15 et R. 561-16. Elles mettent en place un dispositif général de surveillance et d'analyse des opérations adapté aux principales caractéristiques de leur clientèle et de leurs produits et leur permettant de détecter toute transaction inhabituelle ou suspecte

2 Elles Peuvent différer la vérification de l'identité de leur client et du bénéficiaire effectif

3 Elles Peuvent simplifier les autres mesures de vigilance en adaptant au risque faible identifié le moment de réalisation de ces mesures et leur fréquence de mise en œuvre, l'étendue des moyens mis en œuvre, la quantité d'information collectées et la qualité des sources d'informations utilisées

4 Elles Sont en mesure de justifier auprès de l'autorité de contrôle que l'étendue des mesures de vigilance qu'elles mettent en œuvre est adaptée aux risques qu'elles ont évalués.

Niveau 2 : risque standard

Lorsque le client est une personne physique, par le recueil de ses nom et prénoms, ainsi que ses dates et lieux de naissance

Lorsque le client est une personne morale : recueil de sa forme juridique, de sa dénomination, de son numéro d'immatriculation, ainsi que de l'adresse de son siège social.

Lorsque le client intervient dans le cadre d'une fiducie ou d'un dispositif juridique comparable de droit étranger : recueil des nom et prénoms, ainsi que des date et lieu de naissance, des constituants, des fiduciaires, des bénéficiaires et, le cas échéant, du tiers ou recueil du nom de leurs équivalents pour tout autre dispositif juridique comparable relevant d'un droit étranger.

Dans le cas où les bénéficiaires sont désignés par des caractéristiques ou une catégorie particulières, les entités recueillent les informations permettant de les identifier au moment du versement des prestations ou au moment où ils exercent leurs droits acquis

Lorsque le client est un placement collectif qui n'est pas une société, par le recueil de sa dénomination, de sa forme juridique, de son numéro d'agrément, de son numéro international d'identification des valeurs mobilières, ainsi que de la dénomination, de l'adresse et du numéro d'agrément de la société de gestion qui le gère.

Les entités identifient également les personnes agissant pour le compte du client selon les modalités prévues au présent article et vérifient leurs pouvoirs.

Modification du Décret 2018-284 du 18 AVRIL 2018

Les modalités d'identification

Lorsque le client est une personne physique présentation de **l'original d'un document officiel en cours de validité comportant sa photographie** et soit par la prise d'une copie de ce document, soit par la collecte des mentions suivantes : les nom, prénoms, date et lieu de naissance de la personne, ainsi que la nature, les date et lieu de délivrance du document et les nom et qualité de l'autorité ou de la personne qui a délivré le document et, le cas échéant, l'a authentifié

Lorsque le client est une personne morale : **communication de l'original ou de la copie de tout acte ou extrait de registre officiel datant de moins de trois moi**s ou extrait du Journal officiel, constatant la dénomination, la forme juridique, l'adresse du siège social et l'identité des associés et dirigeants sociaux mentionnés aux 1° et 2° de l'article R. 123-54 du code de commerce, des représentants légaux ou de leurs équivalents en droit étranger

Lorsque le client est une personne physique, la vérification de l'identité peut également être obtenue **en recourant à un moyen d'identification électronique** délivré dans le cadre d'un schéma français d'identification électronique notifié à la Commission européenne

ou en recourant à un moyen d'identification électronique présumé fiable au sens de l'article L. 102 du code des postes et des communications électroniques;

Mesures de vigilance complémentaires : Article L.561-10 et R.561-20 CMF Art 37 décret 2018-284

Diligences complémentaires à mettre en œuvre (*Art. R.561-20 CMF*)(art 37 décret 2018-284)

1° Le client ou son représentant légal n'est **pas physiquement présent** aux fins de l'identification au moment de l'établissement de la relation d'affaires

Au moins l'une des mesures de vigilance complémentaires suivantes (ou deux en cas d'ouverture d'un compte):

- ❑ Obtenir **une pièce justificative supplémentaire** permettant de confirmer l'identité (R.561-20) Obtenir une copie d'un document ainsi que d'un document justificatif supplémentaire permettant de confirmer l'identité du client (art 37 2018-284)

- ❑ Mettre en œuvre des mesures de vérification et de **certification de la copie du document officiel** ou de l'extrait de registre officiel .Mettre en œuvre des mesures de vérification et de certification de la copie d'un document officiel ou d'un extrait de registre officiel
  par un tiers indépendant de la personne à identifier (art 37 2018-284)

- ❑ **Exiger que le premier paiement** des opérations soit effectué en provenance ou à destination d'un compte ouvert au nom du client auprès **d'un organisme financier de l'UE ou pays équivalent** E
- ❑ Obtenir **directement une confirmation** de l'identité du client de la part d'un organisme financier

- ❑ Recourir à un moyen d'identification électronique délivré dans le cadre d'un schéma français d'identification électronique notifié à la Commission européenne ou d'un schéma notifié par un autre Etat membre de l'Union européenne dans les mêmes conditions, dont le niveau de garantie correspond au niveau de garantie substantiel (art 37 2018-284)
- ❑ Recueillir une signature électronique avancée ou qualifiée ou un cachet électronique avancé ou qualifié valide reposant sur un certificat qualifié comportant l'identité du signataire ou du créateur de cachet et délivré par un prestataire de service de confiance qualifié inscrit sur une liste de confiance nationale en application de l'article 22 du règlement (UE) n° 910/2014

Mesures de vigilance complémentaires : Article L.561-10 et R.561-20 CMF Art 38 décret 2018-284

Diligences complémentaires à mettre en œuvre (*Art. R.561-20 CMF*)(art 38 décret 2018-284)

2° le client, ou le bénéficiaire effectif, est une personne mentionnée au 2° de l'article L. 561-10 ou le devient au cours de la relation d'affaires (PPE)

Lorsque le client, ou son bénéficiaire effectif, est une personne mentionnée au 2° de l'article L. 561-10 ou le devient au cours de la relation d'affaires (PPE), les personnes mentionnées à l'article L. 561-2, en sus des mesures prévues aux articles L. 561-5 à L. 561-6, appliquent les mesures de vigilance complémentaires suivantes :

- ❑ Elles s'assurent que la décision de nouer ou maintenir une relation d'affaires avec cette personne ne peut être prise que par un membre de l'organe exécutif ou toute personne habilitée à cet effet par l'organe exécutif ;
- ❑ Elles recherchent, pour l'appréciation des risques de blanchiment de capitaux et de financement du terrorisme, l'origine du patrimoine et des fonds impliqués dans la relation d'affaires ou la transaction ;
- ❑ Elles renforcent les mesures de vigilance prévues à l'article R. 561-12-1.

Mesures de vigilance complémentaires : Article L.561-10 et R.561-20 CMF Art 36 décret 2018-284

Diligences complémentaires à mettre en œuvre (*Art. R.561-19 CMF*)(art 36 décret 2018-284)

3° Le produit ou l'opération présente, **par sa nature**, un risque particulier de blanchiment de capitaux ou de financement du terrorisme, **notamment lorsqu'ils favorisent l'anonymat**

Le produit ou l'opération présente, par sa nature, un risque particulier de blanchiment de capitaux ou de financement du terrorisme, notamment lorsqu'ils favorisent l'anonymat, 3° de l'article L.561-10.

- Article R.561-19 « Les produits et opérations mentionnés au 3° de l'article L. 561-10 sont les bons, titres et contrats au porteur ainsi que les opérations portant sur ces produits.
- Lors du remboursement d'un bon, titre ou contrat mentionné au premier alinéa, l'organisme identifie et vérifie l'identité de son porteur, et le cas échéant du bénéficiaire effectif de ce dernier, selon les modalités prévues respectivement aux articles R. 561-5, R. 561-5-1 et R. 561-7. En outre, lorsque le porteur est différent du souscripteur, ou lorsque le souscripteur est inconnu, l'organisme recueille auprès du porteur des informations sur les modalités d'entrée en possession du bon, titre ou contrat ainsi que, le cas échéant, des justificatifs permettant de corroborer ces informations. »

Mesures de vigilance complémentaires : Article L.561-10 CMF et R.561-20

Situations concernées (*Art. L. 561-10 CMF*)	Diligences complémentaires à mettre en œuvre (*Art. R.561-20 CMF*)
4° L'opération est une **opération pour compte propre** ou **pour compte de tiers** effectuée avec des personnes physiques ou morales, *y compris leurs filiales ou établissements*, domiciliées, enregistrées ou établies dans un Etat ou un territoire figurant sur les listes publiées par: • le GAFI ou • la Commission européenne en application de l'article 9 de la directive (UE) 2015/849 du 20 mai 2015.	❑ 1° Evaluer le niveau de risque que l'opération présente ; ❑ 2° Appliquer, lorsque l'opération présente un **niveau élevé de risque** chacune des mesures suivantes : a) La décision de nouer ou de maintenir la relation d'affaires ne peut être prise que par un membre de l'organe exécutif ou toute personne habilitée à cet effet par l'organe exécutif si le client est domicilié, enregistré ou établi dans un Etat ou territoire mentionné au VI de l'article L. 561-15 ; b) Elles recueillent des éléments d'informations complémentaires relatifs à la connaissance de leur client ainsi qu'à l'objet et à la nature de la relation d'affaires ; c) Elles renforcent la fréquence de mise à jour des éléments nécessaires à la connaissance de leur client et, le cas échéant, du bénéficiaire effectif de la relation d'affaires ; d) Pour les personnes mentionnées aux 1° à 6° de l'article L. 561-2, les modalités de suivi des opérations doivent être définies par le responsable mentionné au 1° du I de l'article R. 561-38. Ce dernier s'assure de leur mise en œuvre.

Identification de la personne politiquement exposée

LIGNES DIRECTRICES RELATIVES AUX PPE 20/04/2018 Article R. 561-18

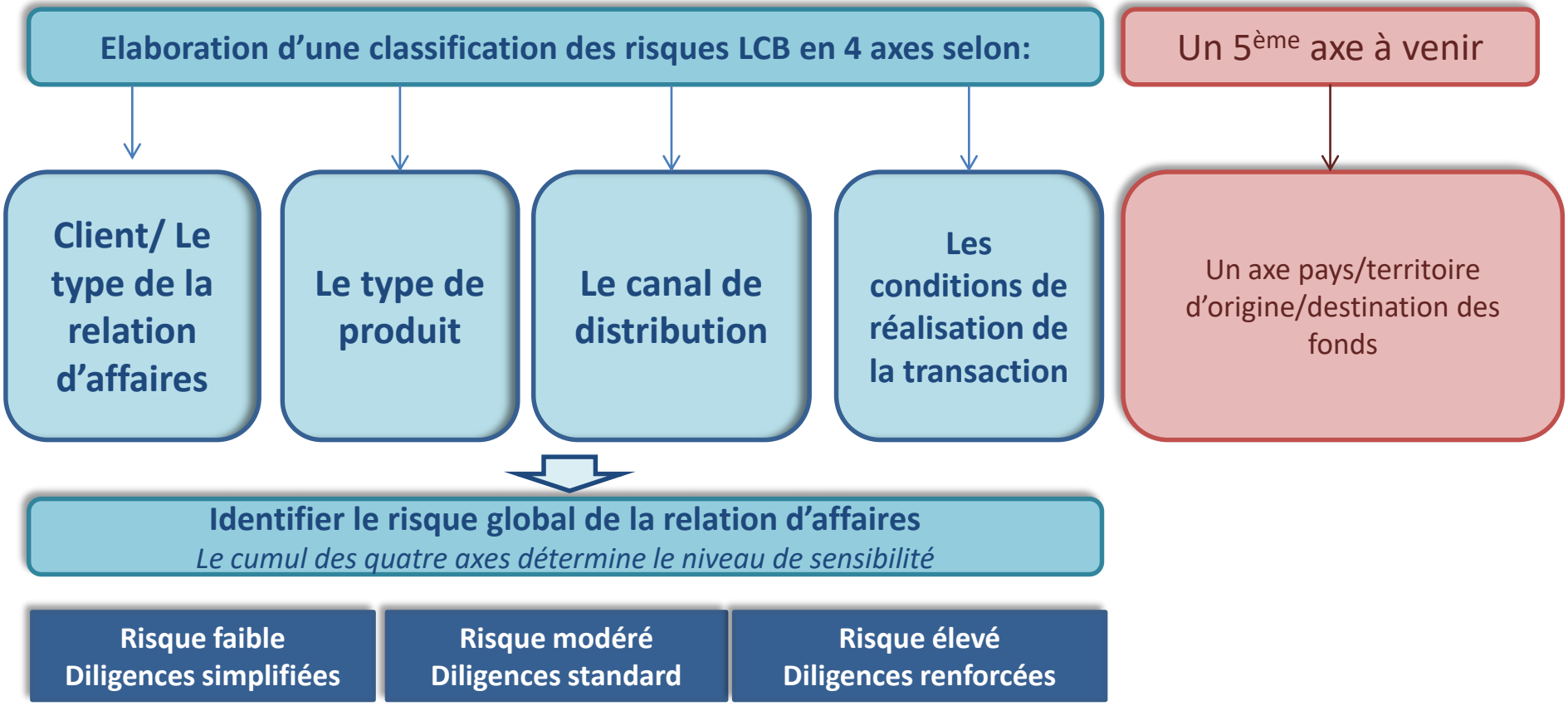
article L. 561-10 2° du Code monétaire et financier Les personnes mentionnées à l'article L. 561-2 appliquent des mesures de vigilance complémentaires à l'égard de leur client, en sus des mesures prévues aux articles L. 561-5 et L. 561-5-1 Le client, le cas échéant son bénéficiaire effectif, le bénéficiaire d'un contrat d'assurance-vie ou de capitalisation, le cas échéant son bénéficiaire effectif, est une personne qui est exposée à des risques particuliers en raison des fonctions politiques, juridictionnelles ou administratives qu'elle exerce ou a exercées pour le compte d'un Etat ou de celles qu'exercent ou ont exercées des membres directs de sa famille ou des personnes connues pour lui être étroitement associées ou le devient en cours de relation d'affaires	
Article R. 561-18 I du Code monétaire et financier8 Art. R. 561-18. – I. – Pour l'application du 2° de l'article L. 561-10, une personne exposée à des risques particuliers en raison de ses fonctions est une personne qui exerce ou a cessé d'exercer depuis moins d'un an l'une des fonctions suivantes :	1° Chef d'Etat, chef de gouvernement, membre d'un gouvernement national ou de la Commission européenne ; 2° Membre d'une assemblée parlementaire nationale ou du Parlement européen, membre de l'organe dirigeant d'un parti ou groupement politique ou d'un parti ou groupement politique étranger ; 3° Membre d'une cour suprême, d'une cour constitutionnelle9 ou d'une autre haute juridiction dont les décisions ne sont pas, sauf circonstances exceptionnelles, susceptibles de recours10 ; 5° Dirigeant ou membre de l'organe de direction d'une banque centrale ; 6°Ambassadeur ou chargé d'affaires ; 7° Officier Général ou officier supérieur assurant le commandement d'une armée ; 8° Membre d'un organe d'administration, de direction ou de surveillance d'une entreprise publique ; 9° directeur , directeur adjoint membres du conseil d'une organisation internationale crée par un traité ou une personne qui occupe une position équivalente en son sein
Article R. 561-18 II du Code monétaire et financier II. - Sont considérées comme des personnes connues pour être des membres directs de la famille :	1° Le conjoint ou le concubin notoire ; 2° Le partenaire lié par un pacte civil de solidarité ou par un contrat de partenariat enregistré en vertu d'une loi étrangère ; 3° Les enfants, ainsi que leur conjoint, leur partenaire lié par un pacte civil de solidarité ou par un contrat de partenariat enregistré en vertu d'une loi étrangère ; 4° Les ascendants au premier degré.

Identification de la personne politiquement exposée

LIGNES DIRECTRICES RELATIVES AUX PPE 20/04/2018	
Article R. 561-18 III du Code monétaire et financier III. - Sont considérées comme des personnes étroitement associées aux personnes mentionnées au I :	1° Les personnes physiques qui, conjointement avec la personne mentionnée au I, sont bénéficiaires effectifs d'une personne morale, d'un placement collectif, d'une fiducie ou d'un dispositif juridique comparable de droit étranger ; 2° Les personnes physiques qui sont les seuls bénéficiaires effectifs d'une personne morale, d'un placement collectif, d'une fiducie ou d'un dispositif juridique comparable de droit étranger connu pour avoir été établi au profit de la personne mentionnée au I ;3° Toute personne physique connue comme entretenant des liens d'affaires étroits avec cette personne

Appliquer la classification des risques à chaque relation d'affaires selon leur niveau de risque

- *L'approche par les risques permet :*
  - *De définir le périmètre d'application et*
  - *De construire le dispositif de maitrise des risques de blanchiment de capitaux et de financement du terrorisme.*
- *Cette classification des risques est mise à jour régulièrement.*



Création du registre les bénéficiaires effectifs

- Les entités assujetties, ont l'obligation d'**obtenir et de conserver des informations adéquates, exactes et actualisées sur leurs bénéficiaires effectifs, à savoir** :

  - Les nom, nom d'usage, pseudonyme, prénoms, date et lieu de naissance, nationalité, adresse personnelle de la ou des personnes physiques ;
  - Les modalités du contrôle exercé sur la société ou l'entité juridique mentionnée au 1°, déterminées conformément aux articles R. 561-1, R. 561-2 ou R. 561-3 ;
  - La date à laquelle la ou les personnes physiques sont devenues le ou les bénéficiaire(s) effectif(s) de la société ou de l'entité juridique mentionnée au 1°.

Sanction ACRP du 22 mars 2018 à l'encontre de l'Etablissement de crédit B 1/3

Blâme et 8 millions EUR

Sur le dispositif de suivi automatisé des relations d'affaires	Commentaires opérationnels
Selon **le grief 1,** l'outil de suivi automatisé mis en place par l'établissement de crédit B pour détecter les opérations atypiques est incomplet et insuffisamment efficace : - Il ne comporte aucun critère, scénario ou seuil en lien avec un crédit à la consommation, alors que ce produit est largement distribué par l'établissement de crédit , et que les risque de Financement du Terrorisme (FT) auxquels cette activité l'expose ont été mentionnés dans plusieurs publications (Rapport annuel de Tracfin 2013, plan d'action du ministre des finances et des comptes publics pour lutter contre FT et l'instruction groupe relative à la LCB-FT) ; - Les scénarios paramétrés dans l'outil et relatifs aux retraits d'espèces ne mentionnent pas la détection du FT ; - Le scénario relatif à des retraits d'espèces par des particuliers avait un seuil de déclenchement d'une alerte de 50 000 € par mois, ce qui est inadapté au risque de FT ; - L'outil de suivi automatisé n'était pas en mesure de cumuler les retraits d'espèces effectués par un même client sur un mois glissant ni de cumuler ceux réalisés sur plusieurs comptes.	**L'outil de suivi automatisé** mis en place par un établissement de crédit pour détecter les opérations atypiques, doit être pertinent et efficace. Il devrait comporter un critère, scénario ou seuil, en lien avec la prise en compte du risque de FT notamment dans le cas **de retraits d'espèces faisant suite à l'octroi d'un crédit à la consommation.**

Sanction ACRP du 22 mars 2018 à l'encontre de l'Etablissement de crédit B 2/3

Blâme et 8 millions EUR

Sur le respect des obligations de vigilance et de déclaration	Commentaires opérationnels
Selon le grief 2, l'établissement de crédit B a manqué à ses obligations de vigilance constante, d'examen renforcé et par suite de déclaration des opérations suspectes à Tracfin. Il est reproché à l'établissement de crédit de ne pas avoir procédé à un examen renforcé, alors que : - L'accumulation, dans ce dossier, d'opérations de retraits d'espèces atypiques au regard des revenus et du fonctionnement du compte de la cliente, en raison de leur montant en valeur absolue et en proportion du prêt consenti ; - Les motifs avancés au sujet des retraits, de manière parfois contradictoire, leur caractère prétendument urgent ; - Les déplafonnements de retrait par carte sollicités et le comportement en agence de la cliente ; - Le déplacement de la cliente dans une autre agence; Rendent un tel examen nécessaire dans ce dossier.	De multiples retraits d'espèces atypiques d'un client faisant suite à l'octroi d'un crédit à la consommation nécessite un niveau de vigilance et de réactivité, voire d'un examen renforcé de la part de l'établissement de crédit.

Sanction ACRP du 22 mars 2018 à l'encontre de l'Etablissement de crédit B 3/3

Blâme et 8 millions EUR

Sur le dispositif d'information et de formation du personnel	Commentaires opérationnels
Selon **le sous-grief 3.1,** la partie consacrée à la LCB-FT du site intranet de l'établissement de crédit B n'est pas régulièrement actualisée. A la date du contrôle, le site intranet ne mentionnait pas : - Les rapports annuels et les rapports sur les tendances et analyses de risques de Tracfin; - Les derniers principes d'application sectoriels et lignes directrices publiées par l'ACPR en matière de LCB-FT, notamment les lignes directrices de 2015 et les lignes directrices sur le gel des avoirs ; - Le décret n° 2016-1523 du 10 novembre 2016, relatif à la LFT, qui renforce les règles de vigilance à l'égard du crédit à la consommation. De plus, l'information du personnel des agences de l'établissement de crédit B en matière de LCB-FT n'était pas actualisé dans des délais suffisamment rapides.	**Le site intranet** d'un l'établissement de crédit doit être régulièrement actualisé, en y faisant figurer l'ensemble des derniers rapports, décrets et lignes directrices en matière de LCB-FT. **Le dispositif d'information du personnel** des agences d'un l'établissement de crédit doit également faire l'objet d'une actualisation régulière.
Selon **le sous-grief 3.2,** la formation générale du personnel des agences en matière de LCB-FT reposait sur une formation à distance sous forme d' »e-learning », proposé par le centre de formation de la profession bancaire et mise à jour en 2015. Ainsi, l'ancienneté de la formation générale du personnel n'apparait pas de nature à garantir un niveau suffisant de sensibilisation à la LCB-FT.	Un établissement de crédit doit s'assurer de la mise à jour régulière de son dispositif de **formation du personnel**.

III – Le projet de la cinquième directive LCB FT

Introduction

Le projet de la cinquième Directive européenne contre le blanchiment d'argent et le financement du terrorisme a été élaboré pour modifier la quatrième directive européenne 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et pour modifier les directives 2009/138/EC et 2013/36/UE .

Des modifications ont été apportées à plusieurs articles de la directive 2015/849

Champ d'application

Concernant les entités assujetties à la Directive européenne 2015/849, quelques modifications

- Les fournisseurs engagés dans des services d'échange entre des monnaies virtuelles et des monnaies fiduciaires
- Les personnes négociant ou agissant comme intermédiaires dans le commerce des œuvres d'art, y compris lorsque cela est effectué par des galeries d'art et des maisons d'enchères, dont le montant de la transaction (ou une série de transactions liées) est de 10 000 euros ou plus.
- Les personnes qui stockent, négocient ou agissent en tant qu'intermédiaires dans le commerce d'œuvres d'art, lorsque cela est effectué par les ports libres et dont la valeur de la transaction (ou une série de transactions liées) est de 10 000 euros ou plus.
- Agents immobiliers, y compris lorsqu'ils agissent en tant qu'intermédiaires dans la location de biens immeubles, mais uniquement pour les opérations dont les montants de loyer mensuel s'élevent à 10 000 euros ou plus.
- Toute autre personne qui s'engage à fournir directement ou indirectement (ou par d'autres personnes auxquelles cette autre personne est liée), une aide matérielle, assistance ou des conseils sur les questions fiscales comme activité principale ou activité professionnelle
- « Custodian wallet providers »

Objet et définition

De nouveaux concepts ont été introduits : (Article 3)

=> « Monnaie virtuelle » : signifie une représentation digitale d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, elle n'est pas nécessairement attachée à une monnaie et n'ayant pas un statut juridique de monnaie ou d'argent, mais elle est acceptée comme un moyen d'échange. Cette monnaie peut être transférée, stockée et échangée électroniquement.

=> « Custodian wallet providers » : désigne une entité qui fournit des services pour protéger les clés cryptographiques privées au nom de ses clients, ce qui permettra de détenir, stocker et transférer les monnaies virtuelles.

Obligations de vigilance à l'égard de la clientèle

- **Interdiction aux établissements de crédit et établissements financiers de tenir des comptes anonymes ou des livrets d'épargne anonymes. Les titulaires et les bénéficiaires de comptes anonymes ou de livrets d'épargne anonymes existants devraient être soumis aux mesures de vigilance à l'égard de la clientèle au plus tard six mois après l'entrée en vigueur de la cinquième directive. (Art 12)**

- **Concernant la monnaie électronique, certaines mesures de vigilance à l'égard de la clientèle ne seront pas appliquées aux entités assujetties, si l'instrument de paiement n'est pas rechargeable, ou est assorti d'une limite maximale mensuelle de 150 EUR (au lieu 250 EUR) pour les opérations de paiement utilisable uniquement dans cet État membre et si le montant maximal stocké sur un support électronique n'excède pas 150 EUR (au lieu de 250 EUR) (Art 12)**

- **Les États membres veillent à ce que les établissements de crédit et les établissements financiers agissant en tant qu'acquéreurs qui n'acceptent que les paiements effectués avec des cartes prépayées anonymes émises dans des pays tiers lorsque ces cartes répondent à des exigences précises. D'ailleurs, les États membres peuvent décider de ne pas accepter sur leur territoire des paiements effectués en utilisant des cartes prépayées anonymes.**

Obligations de vigilance à l'égard de la clientèle

- **Les États membres veillent à ce que la dérogation prévue au paragraphe 1 ne soit pas applicable en cas de remboursement en espèces ou de retrait d'espèces de la valeur monétaire de la monnaie électronique lorsque le montant remboursé est supérieur à 50 EUR, ou dans le cas des opérations de paiement à distance telles que définies au point (6) de l'article 4 de la directive (UE) 2015/2366 du Parlement européen et du Conseil, lorsque le montant payé est supérieur à 50 EUR par transaction.**

Les mesures de vigilance à l'égard de la clientèle comprennent:

- **Le projet met l'accent sur l'identification du client et la vérification de son identité en se basant sur des données ou informations obtenus d'une source fiable et indépendante, y compris, des moyens d'identification électronique, des services de confiance pertinents, ou tout autre processus d'identification sécurisé, distant ou électronique réglementé, reconnu, approuvé ou accepté par les autorités nationales compétentes.**
- **Outre, si le bénéficiaire effectif identifié est un dirigeant principal, les entités assujetties devraient prendre les mesures raisonnables nécessaires pour vérifier l'identité de la personne physique qui occupe ce poste et devraient disposer du registre des mesures prises ainsi que les difficultés rencontrées au cours du processus de vérification.**
- **Lorsque le client est une société ou une fiducie ou une autre entité juridique, les entités assujetties doivent collecter une preuve d'inscription ou un extrait du registre avant l'établissement de la relation d'affaires.**

Obligations de déclaration

- **Les États membres devraient mettre en place des mécanismes centralisé automatisés, tels que des registres centraux ou des systèmes centraux de recherche de données électroniques, permettant d'identifier, en temps utile, les personnes physiques ou morales détenant ou contrôlant des comptes de paiement, des comptes bancaires et des coffres-forts dans un établissement de crédit sur leur territoire. Les États membres notifient à la Commission les caractéristiques de ces mécanismes nationaux.**
- **Les États membres veillent à ce que les informations détenues dans les mécanismes centralisés visés au paragraphe 1 du présent article soient directement accessibles de manière immédiate et non filtrée aux CRF nationales. Les informations sont également accessibles aux autorités nationales compétentes pour remplir les obligations de la présente Directive. Les États membres veillent à ce que toute CRF soit en mesure de fournir en temps utile à d'autres CRF, conformément à l'article 53, des informations détenues dans les mécanismes centralisés introduits.**
- **D'ici le 26 juin 2020, la Commission présente au Parlement européen et au Conseil un rapport évaluant les conditions, les spécifications techniques et les procédures permettant d'assurer une interconnexion sûre et efficace des mécanismes automatisés centralisés.**

IV – DSP2

DSP2 : vers une sécurisation ou de nouveaux risques systémiques ?

Contexte

La révision de la Directive Services de Paiement (DSP2)

Le **24 juillet 2013**, la Commission européenne a publié un **paquet législatif** comprenant, entre autres, une **proposition de révision de la directive sur les services de paiement** (DSP2) afin de :

- **prendre en compte les évolutions technologiques,**
- **Prendre en compte les nouveaux usages apparus sur le marché des paiements depuis l'adoption de la DSP1 en 2007 (croissance continue du e-commerce, développement du m-commerce...),**
- **assurer un haut niveau de sécurisation des moyens de paiement,**
- **maintenir la confiance des usagers des établissements bancaires**
- **Favoriser la concurrence (apparition de nouveaux acteurs).**

PSIC et PSIP

Des prestataires de service d'information sur les comptes :

Le point 16 de l'article 4 de la directive DSP2 en donne la définition suivante :

« Service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement ».

Prestataire de service d'initiation de paiement

Le point 17 de l'article 4 de la directive DSP2 en donne la définition suivante :

« Service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement »

Comment assurer la sécurité nécessaire au bon fonctionnement des moyens de paiements puisque ces nouveaux entrants proposent des services qui nécessitent l'accès aux données bancaires de leurs clients ?

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

Obligations de l'utilisateur de services de paiement, liées aux instruments de paiement et aux données de sécurité personnalisées :

- L'utilisateur a un usage conforme aux conditions préalablement définies, et qui se doivent d'être non discriminatoires, objectives et proportionnées.
- Quand l'utilisateur a connaissance de la perte - vol - détournement - utilisation non autorisée de l'instrument de paiement, il en informe sans tarder le prestataire, afin de préserver la sécurité de ses données personnelles

Obligations du PSP, liées aux instruments de paiement :

- Le PSP s'assure que les données personnelles ne sont pas accessibles à d'autres parties que l'utilisateur du service de paiement
- Le PSP s'abstient d'envoyer tout instrument de paiement non sollicité par l'utilisateur, sauf remplacement
- Le PSP fournit à l'utilisateur de services de paiement la possibilité de procéder à la notification en cas de perte / vol / détournement / utilisation non autorisée de l'instrument
- Le PSP empêche toute utilisation de l'instrument après notification de perte / vol / détournement / utilisation non autorisée par l'utilisateur de service de paiement
- Le PSP supporte le risque lié à l'envoi, à l'utilisateur de service de paiement, d'instrument de paiement ou de toute données personnelle relative à celui-ci.

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

regulation partners

Article L.133-44-I Code monétaire et financier – Authentification forte

L'authentification forte s'applique lorsque le payeur :

- Accède à son compte de paiement en ligne
- Initie une opération de paiement électronique
- Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou toute autre utilisation frauduleuse

❖ Appliquer une authentification forte du client comportant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés.

❖ Exécute une action grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou toute autre utilisation frauduleuse.

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

L'authentification forte du payeur :

Une authentification reposant sur l'utilisation de **deux éléments** ou plus appartenant aux **catégories « connaissance », « possession » et « inhérence »** (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification

1. **Connaissance** : quelque chose que seul l'utilisateur connaît (*comme un mot de passe, un code d'identification personnel, ou un « code PIN », etc.*)

2. **Possession** : quelque chose que seul l'utilisateur possède (*comme un «token », un téléphone mobile, une carte à micro-processeur ou « carte à puce » etc.*)

3. **Inhérence** : quelque chose qui est liée à la personne elle-même de l'utilisateur (*une caractéristique biométrique telle que l'empreinte digitale ou la voix par exemple*)

Dernières évolutions réglementaires en France

Ordonnance n°2017-1252 du 9 août 2017
Transposition de la Directive 2015-2366

Rappel

La **directive n° 2015/2366** comporte des dispositions relatives à quatre grandes thématiques :

- la première aux conditions d'exercice des ***prestataires de services de paiement*** ;
- la seconde aux droits et obligations des ***utilisateurs et des prestataires de services de paiement*** ;
- la troisième aux exigences en matière ***d'information relatives aux services de paiement*** ; et
- la quatrième aux exigences de ***sécurité renforcées pour les paiements électroniques et la protection des données financières des consommateurs*.**

- **L'Ordonnance n°2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur** publiée au Journal officiel de la République française **le 10 août 2017**.
- La présente ordonnance modifie le code monétaire et financier et **s'accompagne d'un décret en Conseil d'Etat, d'un décret simple et de cinq arrêtés**.

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des conditions d'exercice des établissements de paiement:

- Les **dispositions du CMF** relatives aux **conditions d'octroi de leur agrément sont complétées.**
- La **protection des fonds des utilisateurs** de services de paiement **reste obligatoire** pour l'ensemble de ces établissements par le biais d'un **cantonnement des fonds collectés** pour l'exécution d'opérations de paiement.
- Pour les **établissements dont la moyenne mensuelle de la valeur totale des opérations de paiement ne dépasse pas 3 millions d'euros**, **un agrément simplifié est ouvert**.
- Les **exigences prudentielles plus favorables** qui préexistaient sont **maintenues,** et les **informations requises dans le cadre du dossier de demande d'agrément sont allégées.**
- En matière de supervision des activités transfrontalières, la directive organise une **procédure de coopération entre les autorités compétentes** et **renforce les pouvoirs de l'Etat membre d'accueil**.
- Il est désormais permis à l'ACPR de **prendre des mesures conservatoires** en cas **d'urgence à l'égard des établissements agréés dans un autre Etat membre de l'Union européenne** et **exerçant leur activité en France,** lorsqu'une **action immédiate est nécessaire** pour **contrer une menace grave pour les intérêts collectifs des utilisateurs de services de paiement.**

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des droits et obligations des utilisateurs et des prestataires de services de paiement :

- La présente ordonnance introduit des dispositions nouvelles destinées **à renforcer les droits des utilisateurs** :

- **Réduction de leur responsabilité de 150 euros à 50 euros en cas de paiements non autorisés,** c'est-à-dire de paiements consécutifs à un vol, une perte ou un détournement de l'instrument de paiement.

- **Les utilisateurs doivent également être informés sans délai des incidents opérationnels et de sécurité majeurs** - c'est-à-dire des incidents affectant le fonctionnement de l'établissement ou la sécurité de l'opération de paiement - lorsque l'incident est susceptible d'avoir des répercussions sur leurs intérêts financiers.

- **Enfin, les utilisateurs de services de paiement doivent être informés des procédures de réclamation existantes, ainsi que des procédures de règlement extrajudiciaire en cas de litige.**

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des exigences en matière d'information relatives aux services de paiement :

- Les **prestataires de services de paiement** fournissant les services d'information sur les comptes ou les services d'initiation de paiement sont ainsi **tenus de fournir l'ensemble des informations requises relativement aux opérations de paiement.**

Les exigences de sécurité pour les paiements électroniques et la protection des données financières des consommateurs sont renforcées:

- **L'authentification forte du client**, consistant à vérifier l'identité du payeur lors de l'opération de paiement, par exemple **en renseignant un code additionnel**, **devient obligatoire** en application de cette directive suivant des conditions précisées par l'Autorité bancaire européenne.

- **La Banque de France et l'ACPR** sont par ailleurs **informées sans délai respectivement des incidents opérationnels majeurs et des incidents de sécurité majeurs.**

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Relatif aux relations entre les prestataires de services de paiement et leurs clients en matière **d'obligations d'information des utilisateurs de services de paiement** et précisant les principales stipulations devant figurer dans **les conventions de compte de dépôt et les contrats-cadres de services de paiement**

- Publié au Journal officiel de la République française le 2 septembre 2017.
- L'arrêté entre en vigueur le 13 janvier 2018 .

- Précise les informations à fournir/ mettre à disposition par le PSP immédiatement après avoir initié un ordre de paiement au payeur ou, le cas échéant au bénéficiaire

- Précise les informations que le PSP doit fournir ou mettre à la disposition pour la fourniture des services de paiement, avant que l'utilisateur de services de paiement ne soit lié par un contrat relatif à une opération de paiement isolée ou à la fourniture d'un service de paiement ne relevant pas d'une convention de compte de dépôt ou d'un contrat-cadre de services de paiement

- **Précise les informations contenues dans les conventions de compte de dépôt et les contrats cadres concernant les opérations de paiement** :

  - Sur le prestataire de services de paiement
  - Sur l'utilisation d'un service de paiement
  - Sur les frais, les taux d'intérêt et les taux de change
  - Sur la communication entre l'utilisateur et le prestataire de services de paiement
  - Sur les mesures de protection et les mesures correctives
  - Sur la modification et la résiliation du contrat
  - Sur les comptes joints
  - Sur les recours

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Le contrat de dépôt ou le contrat-cadre comporte les <u>informations suivantes</u> lorsqu'il s'agit d'opérations de paiement réalisées par des PSP

Des informations relatives aux comptes joints

notamment, les modalités de fonctionnement et de clôture d'un compte de paiement joint

Sur les recours : le droit applicable au contrat et la juridiction compétente, les voies de réclamation et recours extrajudiciaires

Sur la modification et la résiliation du contrat

Des informations sur les frais, les taux d'intérêt et les taux de change

Des informations relatives au PSP:

- le nom, l'adresse du siège social, toutes les adresses à prendre en compte pour la communication avec le PSP (*y compris l'adresse de courrier électronique*), etc.
- Les coordonnées des autorités de contrôle compétentes et les informations permettant à l'utilisateur de s'assurer de l'habilitation du PSP, (*y compris les informations permettant de consulter la liste des PSP*);

Sur la communication entre l'utilisateur et le PSP:

- Les moyens de communication,
- Les modalités et la fréquence selon lesquelles les informations sont fournies ou mises à disposition,
- La/les langues dans lesquelles le contrat est conclu,
- La mention du droit de l'utilisateur de services de paiement de recevoir les termes contractuels du contrat,
- Les finalités des traitements de données mis en œuvre par le PSP, les destinataires des informations, le droit de s'opposer à un traitement des données à des fins de prospection commerciale ainsi que les modalités d'exercice du droit d'accès aux informations concernant le client

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

regulation partners

Le contrat de dépôt ou le contrat-cadre comporte les informations suivantes lorsqu'il s'agit d'opérations de paiement réalisées par des PSP

Sur l'utilisation d'un service de paiement

- Une description des principales caractéristiques du service de paiement à fournir
- Les informations précises ou l'identifiant unique que l'utilisateur de services de paiement doit fournir aux fins de l'initiation ou de l'exécution correcte de son ordre de paiement;
- La forme et la procédure pour donner le consentement à l'initiation ou à l'exécution d'une opération de paiement et pour retirer ce consentement,
- Dans le cas d'instruments de paiement liés à une carte cobadgés, les droits de l'utilisateur de services de paiement
- Une information sur le moment de réception de l'ordre de paiement et l'éventuel délai limite établi par le PSP
- Les obligations de confidentialité à la charge du prestataire de services de paiement,
- Le sort du compte de paiement au décès du ou de l'un des titulaires du compte de paiement
- Les modalités de procuration, la portée d'une procuration et les conditions et conséquences de sa révocation;
- La possibilité, si elle existe, de convenir de limites de dépenses pour l'utilisation de l'instrument de paiement
- Le délai d'exécution maximal au cours duquel le service de paiement doit être fourni;

Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014

Nouvel article 249-1

« **Art. 249-1**. – En ce qui concerne les incidents majeurs au sens de l'**article L. 521-10 du code monétaire et financier**, les dirigeants effectifs informent sans retard injustifié l'ACPR de tout incident opérationnel et la Banque de France de tout **incident de sécurité**.»

Incident de sécurité

Définition

« Un événement ou une série d'événements imprévus résultant de processus internes inadaptés ou défaillants ou d'évènements extérieurs affectant la disponibilité, l'intégrité, la confidentialité et la continuité des systèmes d'information et de communication et/ou les informations utilisées pour la fourniture de services de paiement. Ceci inclut les incidents provenant de cyber-attaque ou de la non pertinence des mesures de sécurité physique. »

REPORTING DES INCIDENTS

Orientations de l'EBA du 19/12/2017 sur la notification des incidents majeurs en vertu de la directive UE 2015/2366 (DSP2)

Incidents majeurs

- Evaluation des impacts des incidents sur une base continue tout au long de l'incident, pour identifer tout changement de statut éventuel, ascendant (de non majeur à majeur) ou déscendant (de majeur à non majeur).
- Notification des incidents majeurs à l' autorité compétente dans l'état membre d'origine.
- Notification initiale envoyée dans les 4 heures suivant la détection de l'incident opérationnel ou de sécurité majeur.
- Notification finale lorsque l'analyse des causes a été réalisée et lorsque des chiffres réels sont disponibles pour remplacer les estimations.
- Modèle de notification pour les PSP (Annexe orientation EBA 2017/10)

Classification en tant qu'incident majeur

- Les prestataires de services de paiement devraient classer comme majeurs les incidents opérationnels ou de sécurité qui remplissent :

a. Un ou plusieurs critères au «niveau d'impact supérieur», ou

b. Trois critères ou plus au «niveau d'impact inférieur»

Tableau 1: Seuils

Critères	Niveau d'impact inférieur	Niveau d'impact supérieur
Opérations affectées	> 10 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) **et** > 100 000 EUR	> 25 % du volume habituel des opérations du prestataire de services de paiement (en nombre d'opérations) **ou** > 5 millions EUR
Utilisateurs de services de paiement affectés	> 5 000 **et** > 10 % des utilisateurs de services de paiement du prestataire de services de paiement	> 50 000 **ou** > 25 % des utilisateurs de services de paiement du prestataire de services de paiement
Interruption du service	> 2 heures	Sans objet
Impact économique	Sans objet	> Max. (0,1 % des fonds propres de catégorie 1*, 200 000 EUR) **ou** > 5 millions EUR
Niveau élevé d'escalade interne	Oui	Oui, et un mode de «crise» (ou équivalent) est susceptible d'être déclenché
Autres prestataires de services de paiement ou infrastructures pertinentes potentiellement affectés	Oui	Sans objet
Impact en termes de réputation	Oui	Sans objet

*Fonds propres de catégorie 1 tels que définis à l'article 25 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012.

RISQUES OPERATIONNELS

Orientations de l'EBA du 12/01/2018 relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liés aux services de paiement dans le cadre de la directive DSP2

Diagnostic à réaliser

Gouvernance (Cadre de gestion des risques opérationnels et de sécurité, Modèles de contrôle et Externalisation)

Evaluation des risques

Mesures préventives

Détection

Continuité d'activité

Tests des mesures de sécurité

Connaissance des situations et formation continue

Gestion des relations avec les utilisateurs des services de paiement

Authentification forte du client et API

Le Règlement Délégué 2018/389 de la commission EU complétant la DSP 2 (UE) 2015/2366 relatif à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication.

Exigences

- protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement
- Les prestataires de services de paiement mettent en place des mécanismes de contrôle des opérations qui leur permettent de déceler les opérations de paiement non autorisées ou frauduleuses aux fins de la mise en œuvre des mesures de sécurité visées à l'article 1er, points a) et b) du règlement.
- Les prestataires de services de paiement garantissent une identification sécurisée lors des communications entre le dispositif du payeur et les dispositifs du bénéficiaire visant à accepter les paiements électroniques, notamment.
- Un prestataire de services de paiement gestionnaire de comptes qui propose à un payeur un compte de paiement accessible en ligne met en place au moins une interface. Aux fins de l'authentification de l'utilisateur de services de paiement, l'interface API permet aux prestataires de services d'information sur les comptes et aux prestataires de services d'initiation de paiement de s'appuyer sur l'ensemble des procédures d'authentification proposées par le prestataire de services de paiement gestionnaire du compte à l'utilisateur de services de paiement.

Dérogations à l'authentification forte

Quelques situations de dérogations listées par le règlement délégué 2018-389 :

- Information sur le compte de paiement
- Paiement effectué par l'intermédiaire d'instrument de paiement anonymes
- Les paiements récurrents aux mêmes bénéficiaires créés ou confirmés par le payeur
- Opérations initiées à partir d'automates de paiement des frais de transport et de parking
- Paiement sans contact de faible valeur
- Achat en ligne en faible valeur
- Bénéficiaire de confiance
- Procédures et protocoles de paiement sécurisés utilisés par les entreprises

Dérogations à l'authentification forte

- Le taux de fraude global lié à chaque type d'opération est calculé comme étant la valeur totale des opérations à distance non autorisées ou frauduleuses, dont les fonds ont été récupérés ou pas, divisée par la valeur totale de l'ensemble des opérations à distance pour le même type d'opération, authentifiées par une authentification forte du client ou exécutées au titre d'une dérogation, sur une base trimestrielle glissante (90 jours).

Valeur-seuil de dérogations	Paiements électronique à distance liés à une carte	Virements électroniques à distance
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015

Suspension de la dérogation :

- Les prestataires de services de paiement cessent immédiatement de faire usage de la dérogation pour tout type d'opération de paiement à distance, lorsque le taux de fraude qu'ils contrôlent dépasse pendant deux trimestres consécutifs le taux de référence en matière de fraude applicable à cet instrument de paiement ou à ce type d'opération de paiement à l'intérieur d'une fourchette de 100 EUR à 500 EUR.

Délai de traitement des réclamations - Ordonnance 9 août 2017

Ordonnance 9 août 2017 – Section 16 « *Traitement des réclamations* »

« **Art. L. 133-45.-** Les prestataires de services de paiement mettent en place et appliquent des procédures destinées au traitement des réclamations des utilisateurs de services de paiement portant sur le respect des dispositions de la section 5 du chapitre II du titre Ier du livre Ier, du chapitre III du titre III du livre Ier, du chapitre IV du titre Ier du livre III et du chapitre Ier du titre II du livre V.

« Ces procédures sont accessibles dans une des langues officielles de l'Etat membre concerné ou dans une autre langue si le prestataire de services de paiement mentionné à l'alinéa premier et l'utilisateur de services de paiement en sont convenus ainsi.

« Les prestataires de services de paiement mentionnés à l'alinéa premier répondent sur support papier ou, s'ils en sont convenus ainsi avec l'utilisateur de services de paiement, sur un autre support durable, aux réclamations des utilisateurs de services de paiement.

« Cette **réponse aborde tous les points soulevés dans la réclamation** et est **transmise dans les meilleurs délais** et au plus tard dans les **quinze jours ouvrables suivant la réception de la réclamation**.

« Dans des situations exceptionnelles, **si une réponse ne peut être donnée dans les quinze jours ouvrables pour des raisons échappant au contrôle du prestataire de services de paiement, celui-ci envoie une réponse d'attente motivant clairement le délai complémentaire nécessaire pour répondre à la réclamation et précisant la date ultime à laquelle l'utilisateur de services de paiement recevra une réponse définitive**. En tout état de cause, l'utilisateur de services de paiement reçoit une réponse définitive **au plus tard trente-cinq jours ouvrables suivant la réception de la réclamation.**

Textes	Dates d'application	Notes
DSP2 2015/2366 transposée par l'ordonnance du 9 août 2017	13 janvier 2018	Cf. Référentiel de contrôle : Thèmes 1 et 3
Orientations EBA (2017/10) sur la notification des incidents majeurs en vertu de la directive (UE) 2015/2366 (DSP2)	13 janvier 2018	Cf. Référentiel de contrôle : Thème 2
Orientations EBA (2017/17) relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liés aux services de paiement dans le cadre de la directive (UE) 2015/2366 (DSP2)	13 janvier 2018	Cf. Référentiel de contrôle : Thème 4
Le Règlement Délégué 2018/389 de la commission EU complétant la DSP 2 (UE) 2015/2366 relatif à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication	**14 mars 2019** : Test **14 septembre 2019** : Application finale	Le prestataire de services de paiement gestionnaire du compte devrait proposer un dispositif permettant aux prestataires de services de paiement **de tester les solutions techniques au moins six mois avant la date d'application des présentes normes de réglementation** ou, **si le lancement a lieu après la date d'application des présentes normes, avant la date à laquelle l'interface sera lancée sur le marché**. Afin de garantir l'interopérabilité des différentes solutions de communication technologiques, l'interface devrait utiliser des normes de communication mises au point par des organisations européennes ou internationales de normalisation.