Actions-Finance
Professionnels au service des professionnels

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) IMPACTS SUR LE SECTEUR BANCAIRE

Julie Niddam

Avocat à la cour

Correspondant informatique et liberté

Actions-Finance
Professionnels au service des professionnels

Plan

Introduction : Rappel des nouveaux concepts introduits par le RGDP

I. Sur l'accroissement du volume de données dans le secteur bancaire

II. Sur la nature particulière des données personnelles traitées par les banques et les conséquences en termes de sécurité

III. Sur les flux de données inhérents au domaine bancaire

Introduction : Rappel des nouveaux concepts du RGPD

Texte unique applicable dans tous les Etats Membres de l'UE au 25 mai 2018

Application territoriale étendue :

- Critère du pays d'établissement du Responsable de Traitement
- Critère du « ciblage » de résidents européens

« Guichet unique » et autorité chef de file pour les traitements transfrontaliers :

- Principe : le droit applicable est déterminé en fonction du lieu d'implantation de l'établissement principal
- Traitement transfrontalier : l'autorité « chef de file » est celle de l'établissement principal ou unique (« guichet unique »)

Protection des mineurs :

- L'information sur le traitement des données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre.
- Le consentement doit être recueilli auprès du titulaire de l'autorité parentale.
- Lorsque l'enfant est devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Conditions de validité des traitements de données :

- Principes applicables (limitation à des fins déterminées, minimisation des données, limitation de la durée, exactitude, sécurité, intégralité et confidentialité)
- Licéité du traitement : le consentement, à défaut :
  - *Exécution du contrat*
  - *Respect d'une obligation légale*
  - *Sauvegarde des intérêts vitaux*
  - *Exécution d'une mission d'intérêt public*
  - *Aux fins des intérêts légitimes*
- Traitement des données sensibles
  - ✓ Principe : interdiction
  - × Exposé des dérogations

- **Renforcement des obligations pour les organismes**

  - Principe de responsabilité (« *accountability* ») :

  - *Système d'autocontrôle de l'entreprise responsable de traitement* : l'entreprise doit être en mesure de démontrer que les principes généraux relatifs à la collecte et au traitement des données personnelles sont respectés.

- **Renforcement des obligations pour les organismes**
  - Partage de responsabilité :
    - *Responsabilité conjointe* : nécessité de définir clairement les obligations respectives ;
    - *Sous-traitance* : garanties que doit présenter le sous-traitant + liste des clauses à prévoir dans les contrats.

- **Renforcement des obligations pour les organismes**

  - Protection des données « dès la conception » (*Privacy by design*) et protection « par défaut » (*Privacy by default*)

    - *Privacy by design :* les mesures techniques et organisationnelles devront être mises en œuvre tant au moment de la détermination des moyens du traitement (dès sa conception) et tout au long de son cycle de vie.

    - *Privacy by default :* ces mesures devront garantir que « par défaut », seules les données nécessaires au regard de chaque finalité spécifique du traitement seront traitées.

- **Crédibilisation des sanctions**

  - Sanctions administratives

    - Prononcer un avertissement ;
    - Mettre en demeure l'entreprise ;
    - Limiter temporairement ou définitivement un traitement ;
    - Suspendre les flux de données ;
    - Ordonner de satisfaire aux demandes d'exercice des droits des personnes.

  - Amendes administratives : entre 10 et 20 millions d'€ / entre 2% et 4% du CA mondial annuel

Chapitre I

Accroissement du volume de données dans le secteur bancaire

Accroissement du volume de données dans le secteur bancaire

1. Cartographie des données :

- Spécificités du secteur bancaire :

  - **Obligation réglementaire de connaissance des clients** (*Know Your Customer – KYC)* renforcée dans le cadre de la lutte contre le blanchiment d'argent et contre le financement du terrorisme

  - Développement **des modèles d'analyses de données :**

    - Segmentation
    - Marketing digital (utilisation d'algorithmes – agrégation de données)

Accroissement du volume de données dans le secteur bancaire

- Méthodes de recensement des données (audit) :

  - Recensement des applications
  - Recensement des finalités
  - Mise en place du registre des traitements

2. Process pour le respect des droits des personnes concernées

- Principe de minimisation :
  - Collecte de données **adéquates, pertinentes et limitées** à ce qui est nécessaire pour atteindre la finalité ;
  - Mise en perspective des catégories de données par traitement avec les finalités pour lesquelles elles sont collectées (la finalité peut-elle être atteinte sans la donnée ?).

- Encadrement du profilage :
  - Principe : interdiction des décisions individuelles automatisées ;
  - Exceptions : consentement, autorisation légale, décision nécessaire à la conclusion ou l'exécution d'un contrat.

- Principe de limitation de la durée : mettre en place des politiques d'archivage intermédiaire et d'effacement des données.

Mise en œuvre des droits des personnes concernées

- **Droit d'accès précisé** : indépendamment de l'obligation spontanée d'information qui incombe au RT, toute personne aura le droit d'obtenir de celui-ci la confirmation que des données personnelles le concernant sont traitées ou non, d'accéder à ces données et de recevoir certaines informations.
- **Droit de rectification maintenu** : la personne concernée pourra obtenir du RT la rectification des données **inexactes ou incomplètes**.
- **Droit d'opposition plus restrictif** : toute personne peut s'opposer, pour des motifs tenant à sa situation particulière, à des traitements nécessaires à l'exécution **d'une mission d'intérêt public** ou aux fins des **intérêts légitimes** poursuivis par le RT ou par un tiers, y compris un profilage.

Mise en œuvre des droits des personnes concernées

- **Droit à l'oubli / droit à l'effacement** : sous certaines conditions le RT devra effacer, dans les meilleurs délais, certaines données.
- **Droit à la portabilité** : permet aux personnes concernées de recevoir les données qu'elles ont fournies au RT **« dans un format structuré, couramment utilisé et lisible par machine »** afin qu'elles soient transmises à un autre responsable, sans que le responsable initial ne puisse s'y opposer (art. 20).
- **Droit à la limitation du traitement** : la personne concernée a le droit de demander au responsable de traitement de geler le traitement.

Informations des personnes concernées

- Rappel des principes de la Loi Informatique et Libertés
  - Identification du responsable du traitement et coordonnées du DPO
  - Données collectées, finalités, et fondement juridique du traitement
  - Existence de droits pour la personne concernée
  - Destinataires et transfert vers un pays tiers le cas échéant
  - Durée ou critères de détermination de la durée de conservation des données

Informations des personnes concernées

- Ajouts du règlement
  - Droit de réclamation auprès de l'autorité de contrôle
  - Précisions sur la question de savoir si la collecte de saisie des données personnelles conditionne la conclusion d'un contrat, et les conséquences du refus le cas échéant
  - Existence et « logique » d'une prise de décision automatisée
  - Nouveaux droits : portabilité et limitation

Chapitre II

Sur la nature particulière des données personnelles traitées par les banques et les conséquences en matière de sécurité

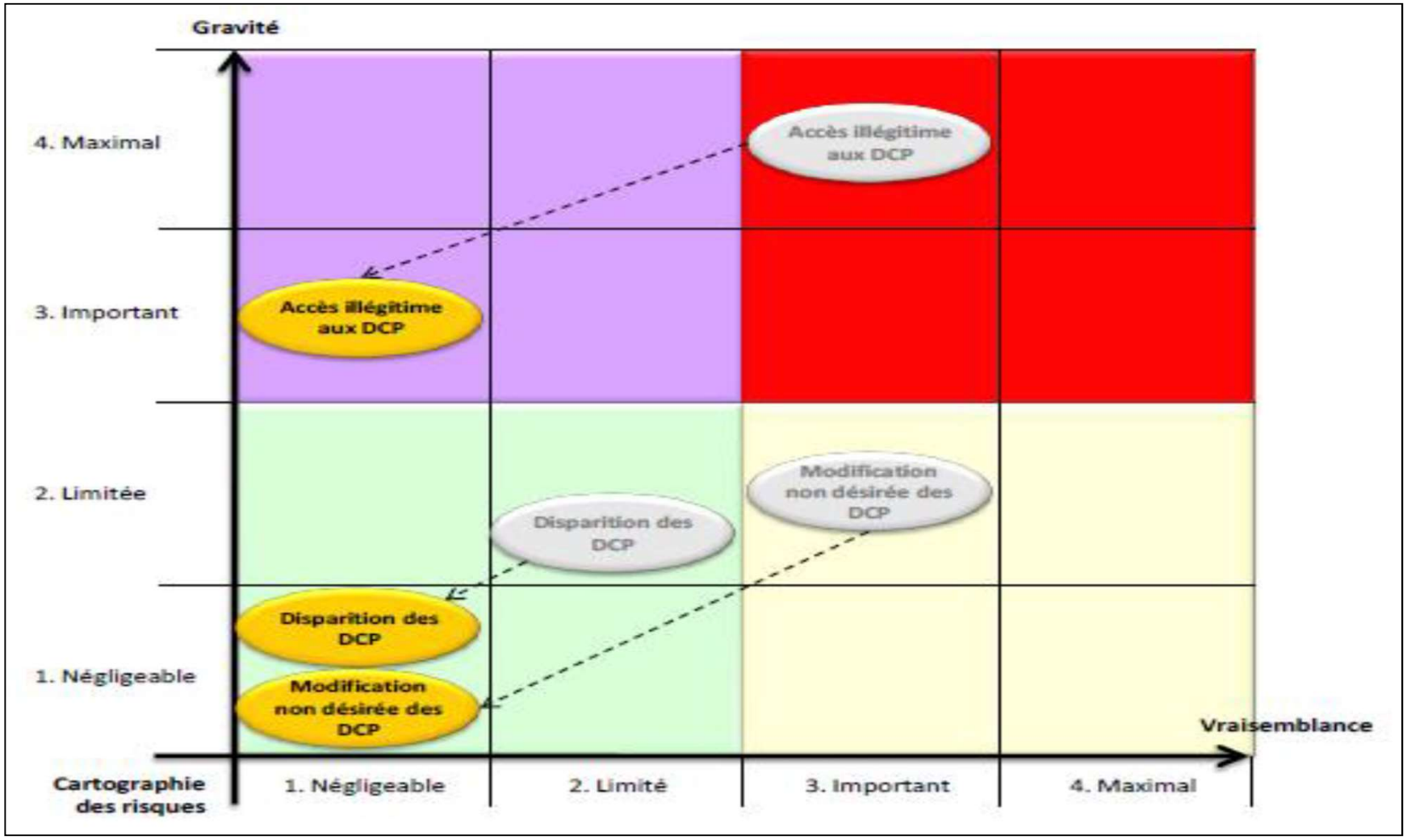
1. Sur l'audit de sécurité

Caractère impératif d'une analyse des risques – méthode :

- Recensement des traitements des données
- Identification des supports de stockage
- Recensement des menaces : confidentialité, disponibilité, intégralité
- Impacts potentiels sur les droits et libertés des personnes concernées : gravité et vraisemblance

Sur la nature particulière des données personnelles…

AUDIT DE SECURITE



Actions-Finance
Professionnels au service des professionnels

Nécessité accrue de mener, en matière bancaire, des études d'impact « *Privacy Impact Assessment* » (PIA)

➢ Règlement (Art. 35) :

- Traitement expose les droits et libertés des personnes à un **risque élevé,** notamment du fait du **recours à de nouvelles technologies.**
- Hypothèses particulières visées par le règlement :
  - Traitement destiné au **profilage ;**
  - Traitement à grande échelle de **données sensibles ou relatives aux condamnations pénales et aux infractions ;**
  - **Surveillance** à grande échelle d'une zone accessible au public.

Nécessité accrue de mener, en matière bancaire, des études d'impact « *Privacy Impact Assessment* » (PIA)

➢ Rapport du groupe de travail « article 29 »

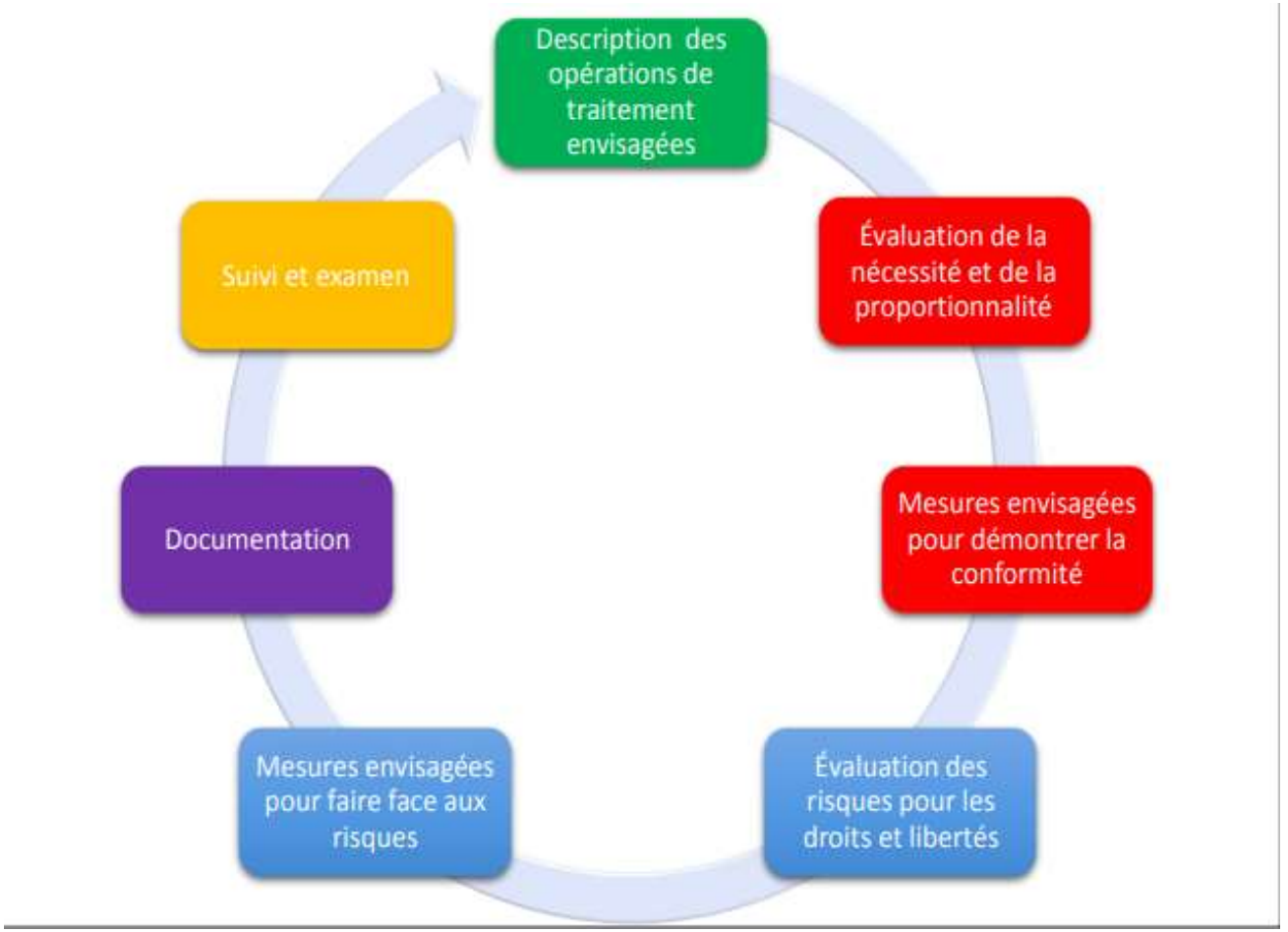
▲ **Critères à prendre en compte pour évaluer la nécessité de procéder à un PIA :**

- Evaluation et notation
- Prise de décision automatisée
- Surveillance systématique
- Données sensibles ou à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données
- Données concernant des personnes vulnérables
- Utilisation de nouvelles solutions technologiques
- Opérations visant à autoriser/modifier/refuser l'accès à un service ou un contrat

▲Cas dans lesquels le PIA n'est pas obligatoire

- Le traitement n'engendre **pas de risque élevé** pour les droits et libertés des personnes concernées ;
- La nature, la portée, le contexte et les finalités du traitement sont très **similaires à un traitement ayant déjà fait l'objet d'un PIA ;**
- Le traitement a fait l'objet d'un **examen par une autorité de contrôle ;**
- Le traitement a pour objet le **respect d'une obligation légale**, et qu'un PIA a déjà été réalisé pour établir cette base légale ;
- Le traitement figure dans la **liste des opérations de traitement dispensées de PIA** établie par l'autorité de contrôle.

Méthodologie du PIA



2. Sur la mise en place de mesures techniques et organisationnelles

- Sécurité organisationnelle :
  - Mettre en place une Politique de Sécurité des Systèmes d'Information (PSSI) :
    - *Charte informatique*
    - *Clause de confidentialité dans les contrats de travail*
  - Sensibiliser les salariés : formations, notes internes sur la sécurité ;
  - Gérer les authentifications :
    - *Règles de générations, stockage et renouvellement de mots de passe*
  - Mettre en place une procédure de gestion des habilitations :
    - *Encadrer la sous-traitance*
    - *Sécuriser l'archivage*

2. Sur la mise en place de mesures techniques et organisationnelles

- Sécurité technique :
  - ➢ Sécurité physique
    - *Mettre en place des systèmes anti-intrusion*
    - *Protéger l'accès aux salles serveurs et locaux techniques*
    - *Restreindre ou désactiver les prises réseau dans des zones accessibles au public*
    - *Protéger les matériels informatiques*

Sur la nature particulière des données personnelles…

- Sécurité logique

  - Traçage des accès
  - Sécurisation des postes de travail
  - Sécurisation de l'informatique mobile (*bring your own device*)
  - Protection du réseau informatique interne
  - Sécurisation des serveurs
  - Sécurisation des sites web
  - Prévoir la continuité d'activité (PCA)
  - Sécurisation de l'archivage
  - Encadrement de la maintenance
  - Encadrement de la destruction des données
  - Gestion de la sous-traitance
  - Sécurisation des échanges
  - Encadrement des développements informatiques
  - Surveillance de la sécurité du SI

Chapitre III

Sur les flux de données inhérents au domaine bancaire

1. Modèles de circulation des données :

- Obligation légale d'échange de données au sein des groupes bancaires dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme
- *Offshoring*
- *Back offices* mutualisés
- *Outsourcing*
- Partenariats

2. Mise en place de mesures adaptées à ces modèles bancaires « multi-pays »

- Règles générales applicables :
  - **Principe** : le RT ne peut procéder au transfert que si l'Etat tiers assure **un niveau de protection adéquat** des droits et libertés des personnes à l'égard du traitement dont les personnes font l'objet ou vont faire l'objet après le transfert.
- Comment évaluer le niveau de protection d'un pays tiers ? (Le principe de la décision d'adéquation)
- En l'absence de décision d'adéquation, quelles garanties appropriées ?
  - Que doivent contenir les *Binding Corporate Rules (BCR)* ?
  - Comment mettre en place des *clauses contractuelles types* ?

2. Mise en place de mesures adaptées à ces modèles bancaires « multi-pays »

➢ Dérogations :

- Le consentement de la personne concernée ;
- L'exécution d'un contrat entre la personne concernée et le RT ;
- La conclusion ou l'exécution d'un contrat conclu, dans l'intérêt de la personne concernée, entre le RT et une autre personne ;
- Les motifs importants d'intérêt public ;
- La constatation, l'exercice ou la défense de droits en justice ;
- La sauvegarde d'intérêts vitaux ;
- La consultation, par le public ou toute personne justifiant d'un intérêt légitime, d'un registre destiné à fournir des informations au public.

➢ Exception de l'exception

CONCLUSION

Conclusion

Importance de désigner un « *Data Protection Officer* » (DPO) pour la mise en place d'un programme de mise en conformité.

Actions-Finance
Professionnels au service des professionnels

Merci pour votre attention

Questions ?