Atelier RGPD: Etat des lieux

EIFR

10 avril 2018

Building a better working world

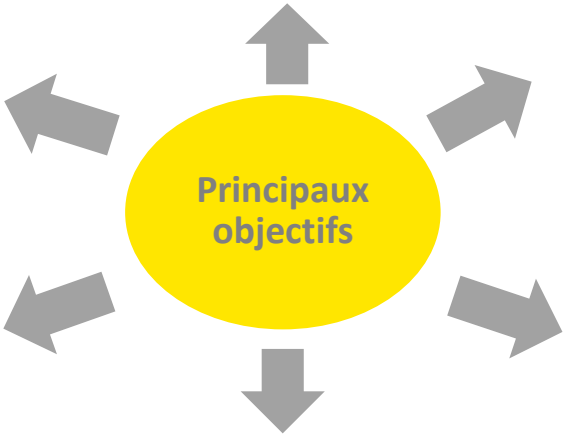
Les principaux objectifs du RGPD

Harmoniser les législations en Europe et étendre le champ d'application territorial

Renforcer les sanctions

+ Class action, indemnisation du préjudice subi

Renforcer l'information et les droits des individus



Approche par les risques

(PIA…)

Responsabiliser les acteurs

(Privacy by design, Accountability, registre des traitements…)

Règlementer de nouveaux acteurs :

- **Sous-traitants**
- **Co-responsable de traitement**
- **DPO**

Actualités
Projet de loi Informatique et Libertés

- Le projet de loi présenté le 13 décembre 2017 est en cours de revue par la Commission mixte paritaire
- L'objectif est d'intégrer les nouveautés du RGPD et d'adopter les dispositions spécifiques locales
- Les principaux impacts pour le secteur financier :
  - Le secret bancaire qui n'est plus opposable à la CNIL en cas de contrôle
  - Le maintien de certaines formalités préalables, notamment, pour les traitements utilisant le numéro de sécurité sociale (« NIR ») (régime d'autorisation)
  - Action de groupe (possibilité d'obtenir réparation du préjudice)
  - Nouveau mécanisme de certification (agrément de la CNIL ou accréditation du COFRAC)
- Les autres points importants toujours en cours de discussion :
  - Extension de l'obligation d'information (identité et coordonnées des sous-traitants)
  - Le recours au chiffrement de bout en bout lorsque cela est possible
  - Obligation de consulter la CNIL pour les traitements présentant un risque élevé pour les libertés et droits des personnes

Actualités
Autres réglementations

- **Projet de règlement « e-privacy »**
  - Objectifs : Ce projet de règlement vise à protéger la vie privée des utilisateurs personnes physiques et morales de services de communication électroniques
  - Principaux impacts pour le secteur financier :
    - Cookies et autres traceurs : Information et consentement obligatoires
    - Marketing (prospection directe) par voie électronique : Consentement obligatoire des prospects et des clients sauf en cas de réutilisation de l'adresse e-mail pour proposer des produits ou services analogues

- **DSP2**
  - Règles d'utilisation des données personnelles bancaires collectées dans le cadre de l'Open Banking
  - Règles de sécurité
  - Notification des failles de sécurité

Les messages de la CNIL à quelques mois de l'entrée en application

Un impératif : le respect des fondamentaux

La Cnil est consciente de l'ampleur de la tâche à accomplir et des nombreuses difficultés à surmonter, auxquelles elle est d'ailleurs elle-même confrontée.

Elle ne s'attend pas à une conformité intégrale sur tous les sujets dès le 26 mai 2018 et pourra écouter, sinon entendre, des arguments recevables à condition que le sujet du RGPD ait été sérieusement traité.

Pour mémoire, les contrôles CNIL portent majoritairement sur les griefs suivants :

- L'information et les droits des personnes (les plaintes sont l'un des principaux facteurs de déclenchement des contrôles de la CNIL)
- Les relations **Responsable / sous-traitant** (les contrats sont un point d'entrée classique des contrôles de la CNIL et leur absence ou insuffisance un manquement récurrent)
- La notification des **violations de sécurité** (50% des sanctions actuelles)
- Les décisions récentes illustrent ces points de vigilance du régulateur

Plan de contrôle de la CNIL à partir de mai 2018 :

La CNIL distinguera 2 types d'obligations:

- Les principes fondamentaux déjà applicables (loyauté des traitements, pertinence des données, durées de conservation, sécurité des données..)
- Les nouvelles obligations (portabilité, PIA, notification des failles de sécurité…) pour lesquelles les contrôles auront essentiellement pour but d'accompagner les acteurs dans leur mise en œuvre et n'auront normalement pas vocation à déboucher, dans les premiers mois, sur des sanctions

Les sujets/chantiers à prioriser:

- Un plan d'action détaillé et rigoureux

Dans le cadre de ses contrôles, la CNIL a annoncé qu'elle prendra en compte la bonne foi et la coopération des acteurs concernés. La preuve de cette bonne foi passera par l'aptitude à démontrer que, même si la conformité n'est pas entièrement atteinte sur tous les sujets, l'entité contrôlée y travaille de manière effective et efficace, dispose d'un plan d'action sérieux et y consacre les moyens matériels et humains nécessaires

- L'information, le consentement et les droits des personnes

Nous recommandons de prioriser ce chantier car, outre le risque de sanction disciplinaire en cas de contrôle de la CNIL, il existe également un risque de sanction devant les Tribunaux judiciaires, renforcé par l'institution des *class action* par le RGPD; En outre, c'est sur ces aspects relatifs à la relation client que le risque réputationnel est le plus important

- La sécurité des données

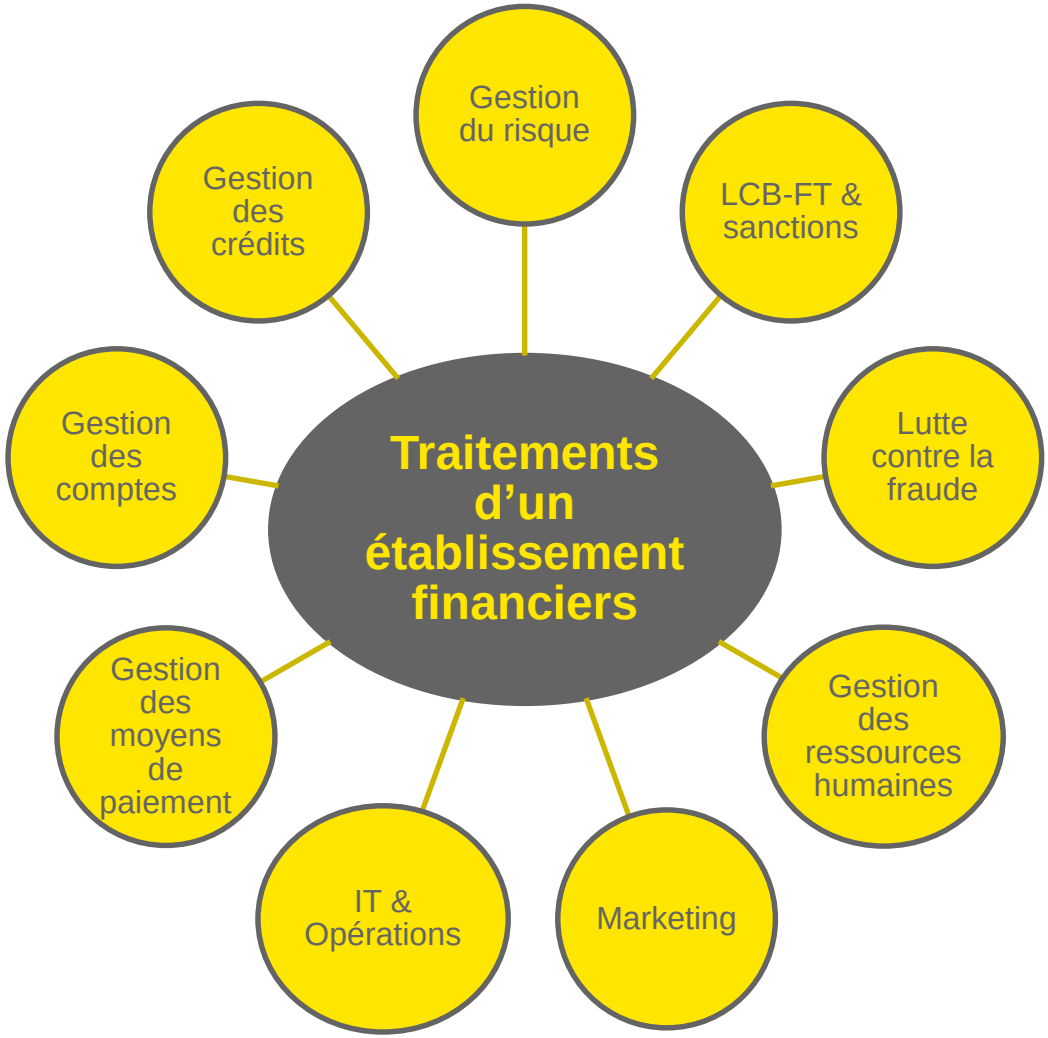
Les failles de sécurité sont au cœur des contrôle de la CNIL mais également des préoccupation de l'ACPR, notamment du fait de la dématérialisation et de la généralisation des services financiers fournis à distance. Le risque réputationnel est également très élevé dans ce domaine

Mise en conformité avec le RGPD

Exemple de méthodologie

Cadrage et sensibilisation	► La définition du périmètre fonctionnel et territorial du RGPD est une phase fondamentale pour la réussite du projet ► La mise en conformité doit suivre une approche par les risques, pour permettre avant tout une sécurisation de l'entreprise, au niveau protection des données et au niveau conformité
Analyse d'écart	► La mise en conformité passe par un état des lieux et une analyse des écarts de l'existant sur de multiples axes qui composent les activités de l'entreprise et plus particulièrement les traitements de données personnelles ► La pluridisciplinarité du sujet, impose une implication forte de l'ensemble des métiers de l'entreprise (juristes, IT et métiers)
Définition de la feuille de route	► La feuille de route, est l'occasion de positionner la donnée personnelle au centre de la stratégie d'entreprise et de transformer la contrainte réglementaire en une opportunité de business.
Implémentation	► La feuille de route, doit prendre en compte les diverses contraintes opérationnelles de l'entreprise (délais de développement, processus de changement, …) et intégrer les initiatives et les projets en cours impactant les données personnelles
Monitoring et revue	► Le principe d' « Accountability » est un sujet clé du RGPD, la phase projet de mise en conformité fait partie de ce principe et il convient de prendre les mesures nécessaires pour pouvoir démontrer les réalisations en cas de contrôle de l'autorité, par exemple

Traitements d’un établissement financier



Focus : Mise en place d'une gouvernance de la protection des données

- Points clés à prendre en considération :

1. La nomination conseillée d'un délégué à la protection des données conformément à l'article 37 du Règlement sur la protection des données et/ou à la réglementation locale applicable en matière de protection des données

2. La mise en place d'un réseau approprié de délégués à la protection des données (si nécessaire et/ou décidé par le groupe) et/ou de contacts/personnel chargé de la protection des données qui seront les contacts au sein du groupe afin de gérer les questions de protection des données.

3. Le choix d'un modèle approprié de gouvernance de la protection des données en fonction de la structure de l'établissement :

   - Centralisation avec un DPO Groupe disposant de relais ou de correspondants dans chacune des entités locales ;
   - Décentralisation avec un DPO dans chacune des entités locales, chapeauté par un DPO central ayant un rôle d'animateur de réseaux ;
   - Une approche mixte avec une mutualisation régionale ou fonctionnelle, ou prenant en compte le degré d'indépendance des entités composant un même Groupe

Focus: Information, Consentement et Droits des personnes

Exigences	Actions
Information ➢ ***Des nouvelles obligations d'information*** : • Coordonnées du DPO • Base juridique du traitement et intérêt légitime poursuivi • Droits créés par le RGPD • Possibilité de retirer son consentement • Possibilité d'introduire une réclamation devant la CNIL • Le cas échant, l'existence d'une prise de décision automatisée (y compris un profilage) • Le cas échéant, éventuelles finalités ultérieures différentes • La possibilité d'organiser le sort des données après la mort	**Information** • Recenser les mentions d'informations existantes (contrats, site internet, bulletins d'adhésion, jeux concours…) • Mesurer l'écart avec les nouvelles exigences • Mettre à jour les clauses contractuelles existantes • Prévoir une procédure interne permettant d'insérer systématiquement une partie protection des données lors de la création d'une mention légale • Notice d'information des clients
Consentement ➢ ***De nouvelles modalités de recueil du consentement :*** • Une action positive claire et non-ambigue du client (opt-in) • Distinguer la collecte du consentement des autres informations • Etre compréhensible et accessible • Ne pas subordonner la conclusion du contrat à la collecte des données non nécessaires à son exécution	**Consentement** • Recenser les traitements basés sur un consentement • Identifier une éventuelle procédure de collecte • Mettre en place une procédure de gestion du consentement • Prévoir une procédure de retrait du consentement, le cas échéant, dématérialisée • Diffuser la nouvelle procédure / sensibiliser les collaborateurs • Collecter à nouveaux les consentements si les exigences nouvelles n'étaient pas respectées
Exercice des droits des personnes ➢ ***De nouveaux droits conférés aux personnes :*** • Droit à la portabilité des données • Droit à « l'oubli » • Droit à la limitation du traitement ➢ ***De nouvelles modalités pour les droits existants*** (délai et réponse dématérialisée)	**Exercice des droits des personnes** • Identifier les périmètres des nouveaux droits et les données concernées • Procédure de gestion des demandes d'exercice des droits • Implémenter une solution technique pour rendre les données portables (interopérabilité des données, transferts sécurisés…)

Focus: Accountability, Privacy by design / by Default

Exigences	Actions
Accountability Mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données personnelles et d'apporter la preuve, sur demande de l'autorité de contrôle, que les mesures appropriées ont été prises	➢ **Prévoir des outils, politiques, méthodologies et procédures opérationnelles notamment sur les sujets suivants:** • Registre des traitements et méthodologie de mise à jour • Politique interne de protection des données personnelles (obligations du responsable des traitement, description des programmes mis en place, rôles et responsabilité des intervenants…) • Politique externe de protection des données personnelles (information des tiers sur les engagements pris par le responsable de traitements en matière de collecte et de traitement des données personnelles) • Politique de Privacy by Design (destinée à aider les intervenants à intégrer les exigences du RGPD dès la conception des produits et services: rappel des règles, principaux points à prendre en compte, identification des parties prenantes…) • Politique de contractualisation avec les sous-traitants • Référentiel des durées de conservation • Paramétrage des logiciels aux fins de minimisation des données collectées • Procédure de traitement des réclamations clients • Politique d'audit (méthodologie de conduite des audits: périmètre, fréquence, liste des points clés à auditer, rôles et responsabilités, communication des résultats)
Privacy by design Mettre en œuvre des mesures techniques et organisationnelles pour prendre en compte de façon effective les principes relatifs à la protection des données, lors de la phase de conception des projets et pendant le cycle de vie des outils et applications	
Privacy by Default Mettre en œuvre des mesures techniques et organisationnelles pour garantir que, par défaut, ne seront traitées que les données nécessaires pour les finalités du traitement	

Focus: Sécurité et approche par les risques

Exigences	Actions

Analyse d'impact sur la vie privée (PIA)
• Réaliser une PIA lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes (ex: évaluation/scoring/profilage); décision automatisée avec des effets juridiques ou similaires; données sensibles; surveillance systématique; croisement de données; personnes vulnérables; usage d'une nouvelle technologie…)
• L'étude doit au moins contenir une description du traitement, une évaluation de sa nécessité et de sa proportionnalité, une évaluation des risques pour les droits et libertés et les mesures envisagées pour y faire face
	Analyse d'impact sur la vie privée (PIA)
	• Recenser les traitements entrainant un risque pour les personnes concernées
	• Créer une procédure pour évaluer la gravité du risque
	• Identifier les traitements pour lesquels un PIA doit être effectué (risque élevé pour les personnes)
	• Créer une ou plusieurs méthodologies d'analyse d'impact en :
	  ○ Définissant et adoptant une procédure commune d'évaluation du risque au niveau du groupe (standardiser)
	  ○ Prévoyant la possibilité de faire un PIA dématérialisé
	• Créer une procédure de consultation de la CNIL en cas de risque résiduel élevé (équipe dédiée, stratégie…)

Anonymisation, pseudonymisation, chiffrement • L'anonymisation permet de conserver des données personnelles au-delà de leur durée de conservation. • La pseudonymisation permet de sécuriser des données toujours nécessaires au regard de la finalité poursuivie (remplacer un identifiant par un pseudonyme) • Le chiffrement des données sensibles ou confidentielles est une mesure de sécurité supplémentaire (collecte, stockage, échange)	**Anonymisation, pseudonymisation, chiffrement** • Anonymisation : Utiliser un procédé irréversible • Pseudonymisation : utiliser un procédé grâce auquel les données sont toujours identifiantes pour l'émetteur, mais rendues anonymes pour les destinataires (tables de correspondance) • Vérifier que la technique de chiffrement utilisée n'est pas corrompue
Notification des failles de sécurité • Notifier aux autorités de protection des données compétentes les incidents de sécurité qui présentent un risque pour les droits et libertés des personnes • En cas de risque élevé, notifier les incidents de sécurité aux personnes concernées	**Notification des failles de sécurité** • Prévoir une procédure d'évaluation des incidents de sécurité pour identifier les incidents présentant un risque • Prévoir une procédure de réponse aux incidents avec un caractère multidisciplinaire (IT, juridique, communication…) • Prévoir une procédure de notification aux autorités et aux personnes concernées • Réfléchir à l'opportunité de souscrire à une assurance

Exemples de bonnes pratiques

Gouvernance

- Mise en place d'un réseau data protection
- Organisation des trois lignes de défense (définition des rôles et responsabilités)

Droits des personnes

- Notices d'information pour les différentes catégories de data subject
- Portail client

Registre des traitements

- Registre des traitements effectués en qualité de responsable de traitement
- Registre des traitements effectués en qualité de sous-traitant
- Définition des rôles et responsabilités pour faire vivre le registre des traitements

PIA

- Délai de 3 ans pour les traitements régulièrement mis en œuvre
- Outil CNIL PIA
- Liste des traitements pour lesquels une PIA est requise