Etude économique de la mise en conformité au RGPD

Rapport - V2

8 février 2022

Agenda

01 Introduction

Objectifs de l'étude

Trois ans après l'entrée en vigueur du Règlement général sur la protection des données (RGPD), le **Laboratoire d'innovation numérique de la CNIL** (LINC) souhaite faire un **bilan de la mise en conformité au RGPD selon un angle économique**. Il s'agit pour cela de mettre en regard les **gains** de la mise en conformité pour les entreprises (augmentation de la confiance client, meilleure qualité des données…) et les **coûts directs et indirects** (mise en place de nouveaux processus, évolutions des applications, recueil de nouveaux consentements...).

Cette étude vise pour le LINC à identifier les leviers pour mieux **valoriser les opportunités lors de l'adoption et du maintien** de la conformité et ainsi à **alimenter les dispositifs d'accompagnement des organismes par la CNIL** (proposition d'outils ou de guides, communication positive autour de la conformité, etc.).

Opportunités de gains

- Gain d'évitement de data-breach (amélioration de la sécurité des données…)
- Meilleure efficacité opérationnelle de la gestion des données (économie sur le volume de données traitées, augmentation de la qualité des données…)
- Meilleure efficacité opérationnelle des processus métiers (exercice des droits…)
- Valorisation de la confiance auprès des clients
- Prise en compte de la valeur de la donnée en tant qu'asset de l'entreprise
- …

Postes de coûts

- Coût de mise en place des activités réglementaires (registre, PIA…)
- Coût de mise en conformité de l'IT & data (évolutions des applications…)
- Coût de mise en conformité sur la transformation métier (recueil des consentements, exercice des droits…)
- Coût récurrent de l'exercice des droits (accès, portabilité, effacement, etc.)
- Coût indirect lié à l'impact sur le modèle d'affaires (retrait du consentement…)
- …

Conduite de l'étude

Une série de **17 entretiens** est conduite entre novembre et décembre 2021 auprès d'entreprises issues de différents **secteurs représentatifs :**

14

Grandes entreprises et ETI

Banques & assurances, Industrie / BTP (B2B), Transports / Industrie / Energie (B2C), Retail, Santé (secteur privé), Services numériques, Culture / médias / jeux vidéos, Médico-social

3

TPE / PME

Présentation du document

- Ce document constitue la **synthèse** des entretiens réalisés. Les **entreprises concernées sont anonymisées**.
- Ce document aborde :

Les coûts de la mise en conformité

Les gains de la mise en conformité

Grandes entreprises et ETI

02.1 Mise en conformité RGPD: gouvernance et coûts de mise en œuvre

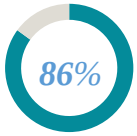
1/ Démarche de mise en conformité

- Toutes les entreprises interviewées se sont organisées en programme pour piloter la mise en conformité au RGPD
    - Certaines ont démarré leur programme tardivement (en 2018) du fait d'une prise de conscience tardive des enjeux et d'un manque de maturité de leur organisation I&L

- Dans quasiment tous les cas, le programme a fait l'objet d'un suivi par le top management :
    - Le niveau de sponsorship se situe au niveau du Comité Exécutif, de la Direction Générale, du Secrétariat Général, avec la contribution d'une ou plusieurs autres directions (Direction juridique, Direction du Digital/IT…)
    - Le niveau de sponsorship est d'autant plus fort que la protection des données fait partie de l'ADN de l'entreprise

- En général, la 1ère étape pour enclencher la conformité a consisté à nommer un DPO en charge de la démarche de conformité
    - Un directeur de programme a pu également être nommé pour piloter opérationnellement la démarche

- Pour certains grands groupes, le DPO en central met à disposition des outils communs et assure la coordination et les BU sont en charge de se doter des budgets nécessaires et de mener leurs actions de mise en conformité



Des programmes ont été soutenus par le top management de l'entreprise

2/ Mise en place de l'organisation Privacy

Le 1er chantier a constitué à mettre en place / renforcer l'organisation de la Privacy au sein de l'entreprise

L'organisation Privacy est généralement constituée de :

1. **Une équipe DPO dédiée**
    - L'équipe a été créée ou renforcée dans le cadre de la mise en conformité
    - Cette équipe est composée de juristes, souvent accompagnés d'experts IT
    - Parfois, existence de ressources AMOA dédiées aux projets de conformité
    - Les effectifs ont généralement cru entre 2018 et maintenant (mise en route des processus d'accompagnement au sein de l'entreprise)

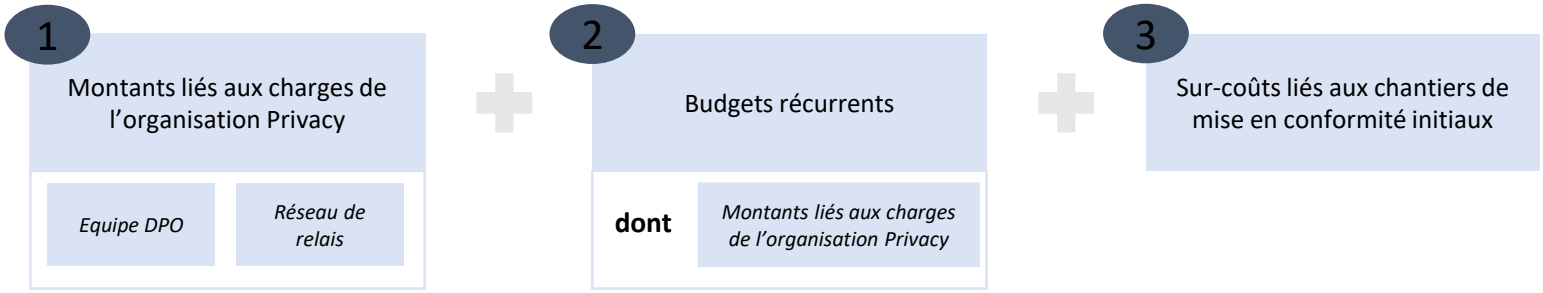
2. **Un réseau de relais, à temps partiel en général**
    - Dans les branches / BU ; dans les marques / pays ; dans les établissements / magasins
    - Le nombre de relais peut être très important en fonction de l'organisation de l'entreprise (ex: +600 relais au sein des établissements)
    - Le taux de mobilisation des relais sur les sujets Privacy est généralement compris entre 5% et 15% de leur activité
    - Le réseau a généralement été formé à la Privacy lors de sa mise en place
    - Les DPO interrogés indiquent que les référents ne sont pas toujours assez disponibles sur les sujets de Privacy

Les ratios en terme d'effectifs Privacy (dédiés + relais) par rapport aux effectifs totaux des entreprises se situent entre **1/150 et 1/5000**

- Les ratios les plus forts se trouvent pour les entreprises dont le cœur de métier est digital
- Pour la majorité, le ratio se situe entre 1/1000 et 1/2500
- Quelques entreprises aux alentours de 1/5000 : notamment dans l'industrie et le retail

3/ Evaluation des coûts de mise en conformité

Trois types de montants ont été considérés dans l'étude :



Points d'attention :

Les résultats obtenus en terme d'évaluation des coûts sont variables en fonction des éléments fournis lors des interviews (niveau de détails des interlocuteurs, changements de postes des interlocuteurs clés depuis le programme, etc.).

La comparaison des résultats n'est pas toujours possible pour les raisons suivantes :

- La consolidation budgétaire globale a rarement été réalisée par les entreprises et le DPO n'a pas la vue complète
- Les montants consolidés ne sont pas toujours homogènes selon les entreprises
    - Assez rarement, le DPO pilote le budget d'évolution des applications ;
    - Plus généralement, ce budget est porté par la DSI / dans les projets et n'est pas consolidé
- La frontière est parfois floue entre ce qui relève de la mise en conformité initiale lors du programme et du mode récurrent

3/ Evaluation des coûts de mise en conformité

En terme de coûts récurrents :

- Le budget du DPO comprend généralement :
  - Le coût humain lié à la constitution de l'équipe DPO et du réseau de relais (ressources internes et/ou externes)
  - Un budget conseil / audit
  - Des frais d'avocats dans le cas de contentieux / d'expertise juridique
  - Le coût de l'outillage spécialisé de la conformité (outil de registre, etc.)
- Les projets prennent en charge le coût de la conformité dans les projets (notamment dans les projets IT) au titre du Privacy-by-Design

En terme de sur-coûts initiaux :

- Le financement du programme a été réalisé de plusieurs manières :
  1. Dans 29 % des cas, un budget global a été alloué ; il consolide à la fois la mise en conformité documentaire et l'évolution des SI
  2. Dans 36 % des cas, le budget du programme RGPD comprend la mise en conformité documentaire ; l'évolution du SI est intégrée dans les budgets de la DSI / Direction Numérique
  3. Dans 36 % des cas, pas de budget global initial, mais une allocation des moyens et des ressources au fil de l'eau selon les besoins
- Toutes les entreprises ont alloué des ressources pour la constitution / le renforcement de l'équipe DPO ainsi qu'un budget d'accompagnement externe (création de la documentation) et un budget pour l'outillage de la conformité
- Lorsque des chantiers d'évolutions des SI ont été réalisés, les budgets sont généralement portés côté DSI et sans vision consolidée du DPO
- Les chantiers cités comme ayant généré le plus de coût sur l'IT cités sont :
  - La revue du cycle de vie et la mise en cohérence des consentements
  - La purge des données et le respect des durées de rétention

02.2 Points de complexité dans la mise en conformité

Points de complexité de mise en œuvre

1/ Points de complexité organisationnelle

Les points de complexité suivants ont été soulignés :

1. Difficulté de faire prendre conscience des enjeux de conformité pour l'entreprise et de développer une culture privacy en l'absence de gains économiques

2. Ambiguïté du rôle du responsable de traitement et du DPO : le responsable de traitement ne se sent pas vraiment « responsable ». Dans la pratique, le DPO endosse le rôle de responsable de traitement et donc sa responsabilité va au-delà de ce que le RGPD définit.

3. Difficulté à assurer la conformité à tous les niveaux dans des contextes de grandes entreprises décentralisées (réseau d'établissements / filiales / marques / pays)

- Certaines entreprises ont des réseaux de plus de 650 correspondants au sein des établissements
- La maîtrise de ce qui est localement est complexe pour le central
- Difficultés de recenser les différents traitements au sein des nombreuses filiales et entités

NB : les leviers identifiés pour mieux maitriser la conformité dans les entités sont les suivants :

- Homogénéiser les processus de conformité
- Homogénéiser certaines pratiques métiers (ex: gouvernance des sites Web)
- Demander aux relais de lever les alertes
- Faire des contrôles dans les entités

4. Problématique budgétaire pour les projets dans le cadre du Privacy-by-Design : le DPIA peut coûter relativement cher pour les petits projets

Points de complexité de mise en œuvre

2/ Points de complexité sur de l'expertise RGPD (1/2)

Des points de complexité récurrents ont été mentionnés :

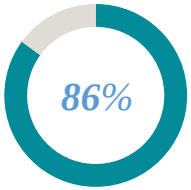
1. La gestion contractuelle avec les tiers

A la fois en tant que client :

- Equipes juridiques et commerciales de certains sous-traitants peu sensibilisées aux attentes sur le sujet RGPD: difficulté dans les négociations
- Difficulté dans la gestion des contrats avec les fournisseurs/éditeurs sur certaines clauses (transferts de données, niveaux de sous-traitance, demande de droits d'accès)
- Complexité lors de la contractualisation avec de grandes entreprises (notamment globales de type GAFAM) qui imposent leurs propres annexes RGPD (clauses génériques quelque soit le logiciel, volonté de limiter la clause de responsabilité, niveaux de sous-traitance, etc.) et leur définition de la notion de responsable de traitement
- Complexité de la qualification en tant que RT, co-responsable ou ST et manque de modèle de convention en cas de co-responsabilité
    - Certains sous-traitants ne veulent pas être qualifiés ainsi car ils portent la relation avec les clients (volonté marketing)
    - Certaines entreprises qui éditent des logiciels en SaaS considèrent qu'elles sont responsables des données en ligne
    - pour des multinationales avec des équipes multi-pays : compliqué de refléter la réalité des échanges avec seulement les notions de responsable de traitement et sous-traitants

Et en tant que fournisseur: impacts sur la charge de travail dans les activités commerciales de réponse aux appels d'offres des clients :

- Exigences renforcées des clients lors des négociations contractuelles (ex : demande de garanties sur la protection des données) et contrôles et audits plus complexes et plus longs



citent la gestion contractuelle comme complexe

Points de complexité de mise en œuvre

2/ Points de complexité sur de l'expertise RGPD (2/2)

2. La définition et application des durées de conservation (purge et archivage)

- Difficultés à définir certaines durées de conservation au regard de la multiplicité des réglementations et des incohérences entre certains textes
- Besoin d'anonymisation pour pouvoir conserver les données et piloter l'activité
- Coûts très importants de mise en place des archives courantes, intermédiaires, définitives
- Complexité et coûts très importants sur la suppression des archives papier

3. Interprétation du RGPD parfois différente selon les autorités dans les pays soumis au RGPD : donc difficulté à être conforme dans tous les pays

- ex: sur les durée de conservation des données des prospects, gestion des cookies, ce qui doit être notifié…
- Il y a des zones d'interprétations locales (autres pays européens) qui rendent problématiques les activités des entreprises
- Certaines autorités font des demandes d'information sur des traitements transfrontaliers (selon leur propre modèle) et une entreprise a nommé des DPO locaux pour y répondre

4. Complexité de la prise en compte des autres réglementations sur les DCP dans les pays hors zone UE

- Ex: notion de données sensibles, durées de conservation, réglementations dans le secteur de la santé, etc.

5. Difficultés de faire évoluer les SI et coûts importants :

- Complexité de faire évoluer les outils legacy : les entreprises profitent du remplacement de certaines applications pour bénéficier d'un progiciel conforme au RGPD et réaliser la purge des données

02.3 Impacts sur le modèle d’affaires et coûts indirects

4/ Impacts sur le modèle d'affaires

Dans **86 % des cas**, les entreprises n'ont pas vu d'impacts sur le modèle d'affaires et n'ont pas cherché à le mesurer.

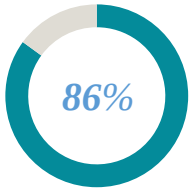
- Les équipes Marketing ont fait part de leurs inquiétudes sur la réduction des bases de client adressables et sur les cookies collectés, mais aucun impact notable n'a été mesuré sur les opérations et les activités
- L'impact des changements sur les politiques cookies n'a pas encore été évalué
  - Les entreprises ont constaté une réduction de l'acceptation des cookies de 90% à 50-60% d'opt-in
- Une entreprise a noté que le fait que les communications à destination des clients soient moins abondantes incite à mieux les cibler grâce à une meilleure exploitation des données des clients qui ont donné leur consentement

Deux entreprises ont noté un impact important sur le modèle d'affaires :

1. Pour une entreprise avec un modèle de vente sur Internet, la mise en conformité au RGPD a entraîné :
   - Des parcours clients moins fluides à cause de cases supplémentaires à cocher
   - Des veto sur certains projets d'affaires (ex: ventes de données pour entraîner des algorithmes…)
2. Pour une entreprise très internationale avec des fonctions informatiques en near-shore, l'arrêt SCHREMS II engendre une impossibilité d'opérer dans certains pays, obligeant l'entreprise à rapatrier certaines de ses fonctions et à augmenter les coûts pour les outils impactés
3. Il a aussi été noté que pour des activités de type « location de bases clients », il est nécessaire d'ajouter de nombreuses mesures de sécurité complémentaires

Par ailleurs, des coûts indirects ont été exprimés en terme de charges supplémentaires et de délais de mise en œuvre des projets à cause de la complexité des négociations commerciales liées :

- Au niveau d'exigences des clients et aux contrôles demandés
- Au manque de maturité des fonctions achats des tiers sur les sujets GDPR (soit sous-traitants, soit clients)



n'ont pas vu d'impacts sur le modèle d'affaires

Eléments quantitatifs

Impact Schrems II : sur-coûts évalués entre 10 à 15 millions € / an pour rapatrier des activités en Europe

02.4 Identification des gains de la mise en conformité et valorisation

1/ Evaluation des gains de mise en conformité

Dans **100% des cas**, les entreprises n'ont pas identifié de gains de mise en conformité au préalable à la démarche.

Aucune évaluation chiffrée n'a été réalisée, ni avant, ni après le projet.

La démarche reste motivée par la réduction du risque de sanctions et il est difficile d'établir des gains au service du business.

Gains en externe

Certaines entreprises ont exprimé des gains en externe :

1. **Gains d'un point de vue commercial**

Dans **21 % cas**, le respect de la Privacy est vu comme un atout concurrentiel sur le marché en B2B :

- Dans les appels d'offres (dont les AO publics), la conformité au RGPD est un point différenciant
- Pour les prospects de certains secteurs, la Privacy est un « must have » pour conclure de nouveaux contrats et les acteurs cherchent à se différencier sur ce sujet
- Les contraintes internes de conformité peuvent être valorisées vers les clients et les prospects : la documentation produite et les audits de conformité ont pu être valorisés pour être fournie aux clients

A l'inverse, en B2C, l'avantage concurrentiel est plus difficile à matérialiser.

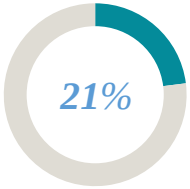
2. **Confiance client plus importante**

Dans **55 % des cas**, les entreprises ont estimé que la démarche génère une meilleure confiance des clients, mais le gain opérationnel est difficile à mesurer.

Dans certains cas, l'augmentation de la confiance des clients a été mesurée par :

- La satisfaction exprimée par les clients lors de la mise place d'un centre d'appel pour répondre aux personnes victimes d'une fuite de DCP
- Une amélioration de l'expérience client grâce à la centralisation des consentements et à une meilleure transparence du traitement des données à caractère personnel
- Une économie sur le nombre de téléconseillers en charge de répondre aux demandes des clients (économie de plusieurs dizaines de téléconseillers)

3. **Un meilleur ciblage des communications vers les clients** du fait d'avoir recueilli les consentements pour faire du ciblage et d'avoir purgé les bases commerciales



estiment que la mise en conformité est un atout concurrentiel

1/ Evaluation des gains de mise en conformité

Gains en interne

Des gains sur des processus internes ont également été exprimés :

1. **Levier pour renforcer la sécurité du SI**

Dans **36 % des cas,** la démarche RGPD a constitué un levier pour renforcer la sécurité de leur système d'information

- Mise en place d'un SMSI
- Augmentation du budget de la sécurité
- Dans un cas, levier pour la création du poste de RSSI

2. **Levier pour homogénéiser la gouvernance de certains processus métiers**

La démarche a permis de mettre en évidence des processus internes perfectibles du point de vue de la gouvernance :

- Ex: Meilleure gestion des données (RH, etc.)
- Ex: Amélioration du processus de lancement de produits
- Ex: Actualisation des contrats sur d'autres types de clauses
- Ex: Meilleur suivi des sous-traitants

Ou bien de travailler sur l'homogénéisation de certains processus à l'échelle de l'entreprise afin de mieux garantir le respect des bonnes pratiques RGPD :

- Ex: Homogénéisation des processus de gestion des sites Web
- Ex: homogénéisation de l'utilisation d'un outil de gestion des campagnes marketing

3. **Green Privacy**

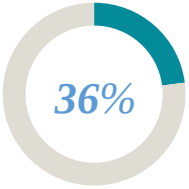
La purge de données a permis de réduire le volume de données traitées

- Ex: suppression de plusieurs To de données

4. **Levier pour la valorisation de la donnée (démarche de data management)**

La cartographie des traitements a permis de mieux comprendre la gestion des données en interne

5. **Facilitation de la mise en conformité du fait que tous les partenaires soient soumis aux mêmes obligations (notamment pour les activités intermédiées)**



indiquent que la démarche RGPD a constitué un levier pour renforcer la sécurité de leur SI

2/ Valorisation de la démarche de conformité

Valorisation en externe

Dans **57 % des cas**, les entreprises ont cherché à valoriser leur démarche vers l'extérieur : clients, partenaires, écosystème.

Vers l'écosystème ou le B2B :

1. Contribution / pilotage de travaux et réflexions au niveau de leur secteur d'activité pour développer la Privacy (productions de guides, de labels, etc.)

2. Valorisation de l'action du DPO de l'entreprise :

- Prix attribué à un DPO qui a reçu un prix pour son action : crédibilisation la démarche et démonstration de la performance de l'entreprise sur la Privacy
- Certification AFNOR du DPO

3. Certification et notation de l'entreprise :

- Certification ISO 27701
- Notation des agences européennes de notation sur les aspects de la Privacy

4. Publication sur les sites institutionnels de l'entreprise de la prise en compte de la Privacy en tant que « valeur du groupe »

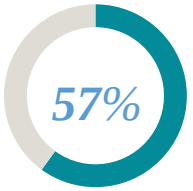
5. Mentions de la Privacy dans les rapports annuels ou RSE

Vers les consommateurs (entreprises B2C) :

- Pas de démarche spécifique dans notre panel

Pour les entreprises qui ne cherchent pas à valoriser la démarche, les raisons peuvent être les suivantes :

- La protection des données personnelles est tellement ancrée dans la relation client qu'il n'est pas nécessaire de s'en valoriser (ex: secteur bancaire)
- L'entreprise manque encore de garantie sur le respect des exigences Privacy sur tous les périmètres de l'entreprise
- La Privacy n'est pas un sujet de préoccupation pour le type de consommateurs de l'entreprise (consumer goods)



Ont prévu de communiquer dans le rapport annuel / rapport RSE

2/ Valorisation de la démarche de conformité

Valorisation en interne

En pratique, la valorisation de la conformité est peu valorisée en interne :

Elle est généralement mise en visibilité à travers les programmes de formations / sensibilisations menés par les collaborateurs, avec parfois un mot d'engagement du COMEX sur le sujet.

Une entreprise a réalisée une auto-évaluation en interne pour mesurer le niveau de conformité au sein des entités et des pays et pour factualiser les résultats.

TPE & PME

Démarche de mise en conformité

La démarche de mise en conformité au RGPD au sein des TPE / PME est variable en fonction des enjeux

1. Pour les entreprises **qui n'ont pas de forts enjeux autour des données à caractère personnel** (DPC en B2B, peu de SI, traitements standards), la démarche de mise en conformité est **souvent limitée** :

- Le SI est limité à quelques logiciels : ERP, CRM, logiciels de comptabilité et de paie, de bureautique, logiciels spécialisés dans leur activité.
- Elles sont faiblement sensibilisées aux enjeux du RGPD et se sentent peu concernées par les enjeux de mise en conformité
    - Informations via un service d'abonnement à un service d'actualités juridiques et réglementaires
- Seules quelques actions sont menées : mention d'informations sur le site, éventuellement purge des bases de données clients les plus anciennes
- Pour celles qui sont le plus sensibilisées : formalisation d'un registre, revue des droits sur les systèmes, actions de sécurité complémentaires

2. Pour les entreprises qui connaissent **de forts enjeux autour des données à caractère personnel** (visibilité, type de données, cotation), la démarche de mise en conformité est **proche de celle des plus grandes entreprises**.

- Organisation en mode programme
- Organisation de la filière Privacy avec la nomination d'un DPO
- Allocation de ressources pour la mise en conformité :
    - Le coût humain de l'équipe DPO
    - Un budget conseil / audit ; frais d'avocats dans le cas de contentieux / d'expertise juridique
    - Outillage spécialisé de la conformité (outil de registre, etc.)…
- Lancement de chantiers de documentation et IT au sein de l'entreprise

Evaluation des gains de mise en conformité

Comme pour les grandes entreprises, les TPE / PME n'ont pas identifié de gains de mise en conformité au préalable à la démarche.
Aucune évaluation chiffrée n'a été réalisée, ni avant, ni après le projet.

Pour la PME ayant de forts enjeux, les gains identifiés sont similaires à ceux des grands groupes :

- Rapprochement de la Direction conformité avec les collaborateurs : échanges plus nombreux entre la hiérarchie et l'ensemble des employés de l'entreprise
- Amélioration de l'image de l'entreprise par un meilleur ciblage des clients (moins de mails, des informations et des relances)
- Levier d'amélioration de la sécurité

Pour une PME dont les clients sont sensibles au sujet (secteur public), la conformité au RGPD a eu un impact commercial :

- La protection des données personnelles est nécessaire pour répondre aux AO pour les entreprises publiques (ex: collectivités territoriales, etc.)
- La conformité RGPD a contribué aux critères pour obtenir le label «expert-cyber» de Cyber-malveillance
- Mise en avant de la démarche de conformité vis-à-vis des clients dans le cadre des appels d'offres publics