RGPD : réussir son projet « Archivage & Purge », un casse-tête insoluble ?

Juin 2019

Une année après l'entrée en vigueur du RGPD, la récente nomination de Marie-Laure Denis à la tête de la Commission Nationale de l'Informatique et des Libertés (CNIL) marque résolument un tournant dans la posture de l'institution vis-à-vis de la conformité des acteurs aux nouvelles dispositions de ce Règlement visant à assurer une meilleure protection des données à caractère personnel. La récente sanction de 400 000 € imposée à SERGIC pour atteinte à la sécurité des données et non-respect des durées de conservation est en la meilleure preuve.

En avril 2019, Marie-Laure Denis déclarait que la CNIL « [avait] toujours une volonté d'accompagnement forte », mais précisait que « [c'était] la fin d'une certaine forme de tolérance » et ouvrait donc une ère de renforcement des contrôles et des sanctions à l'égard de l'ensemble des établissements de la Place.

Le nouveau positionnement de la CNIL et sa campagne de communication doivent faire prendre toute la mesure de la nécessité d'accélérer les chantiers non encore finalisés, y compris sur les dispositions complexes, telles que celles relatives à la limitation de la conservation des données.

En effet, l'obligation de mettre en place des mécanismes d'archivage et de purge des données à caractère personnel se heurte à la complexité des systèmes d'informations qui ont eu tendance à « empiler » des couches d'informations au fil des années.

Face à la complexité de ce chantier qui se révèle de grande envergure, quelles solutions déployer pour parachever sa mise en conformité ? Quelles sont les approches à adopter ?

*

Un changement de paradigme : d'une conservation sans limite des données à une restriction de la conservation.

Pour rappel, l'entrée en vigueur du RGPD ne modifie pas les exigences en termes d'archivage et de purge des données à caractère personnel. En effet, depuis la loi « Informatique & Libertés » de 1978, les établissements sont tenus de conserver les données pendant une durée limitée, en fonction des finalités pour lesquelles elles ont été collectées.

Néanmoins, certains nouveaux principes, tels que la proportionnalité des données, l'utilisation et la conservation des données strictement nécessaires aux traitements, viennent renforcer les obligations en termes de conservation des données.

Aujourd'hui, les établissements ne peuvent plus se retrancher derrière la complexité de la mise en œuvre des solutions et doivent donc lancer des projets d'archivage et de purge des données.

Comment mener son projet d'archivage et de purge des données, sans en faire un projet titanesque qui n'aboutit pas ?

Il convient, en phase préliminaire d'analyse, de répondre à trois questions structurantes :

- **Quelles sont les typologies de données et quelles sont les données dont l'établissement dispose ?** En principe, les travaux à mener pour couvrir les autres aspects de la mise en conformité au RGPD ont déjà permis de mesurer et qualifier les données (par exemple, l'identification des données sensibles), mais le chantier d'archivage et de purge des données requiert un niveau de granularité plus fin.

- **Comment les données sont-elles stockées ?** Les données d'une personne concernée peuvent être enregistrées au niveau d'un client, au niveau d'un foyer fiscal ou encore d'un contrat. Ainsi, au-delà de l'identification des données, il convient de définir les multiples emplacements d'une même donnée, considérant que la réponse à cette question orientera la stratégie retenue pour l'archivage et la purge des données.

- **Comment les données transitent-elles ?** Une fois les données référencées, il convient également d'identifier les flux de données existants entre les différents applicatifs du système d'information, ainsi que les points d'entrée et de sortie de l'ensemble des données. Une attention particulière devra être portée aux données sensibles et aux traitements à risque (par exemple, pour lesquels un DPIA a été formalisé).

Quelles approches incontournables dans le cadre d'un projet « Archivage & Purge » ?

Avancer par étape.

Le prérequis incontournable est de disposer d'une cartographie technique des données afin de recenser l'ensemble des applicatifs et des outils sur lesquels des traitements de données sont réalisés.

Une cartographie fonctionnelle des données permettra, en complément, de déterminer les données à archiver et à purger à un niveau de granularité plus fin. L'exercice permettra de mieux qualifier l'usage de la donnée et les utilisateurs de celle-ci (*data owners*, *data stewards*, …).

A titre d'exemple, la date de décès d'un client est une donnée structurante pour déterminer la fin de la relation contractuelle et ouvrir, ainsi, le délai d'archivage des données. Partant de ce principe, l'établissement dispose-t-il de cette information en interne ? Fait-il appel à un *data provider* externe (dans notre exemple, interrogation du RNIPP) ? Dans tous les cas, pour pouvoir utiliser cette donnée, celle-ci doit être présente dans les systèmes de manière exhaustive et homogène.

Constituer le référentiel des durées de conservation.

Les établissements bancaires et assurantiels disposent de marges de manœuvre extrêmement limitées dans les durées de conservation des données, considérant que celles-ci sont encadrées par de nombreuses règlementations préexistantes : le Code Monétaire et Financier pour les valeurs mobilières, le Code des Assurances pour les contrats d'assurance, le Code du Travail pour les relations avec les collaborateurs… La cohérence des règles entre les différents droits n'est, par ailleurs, pas garantie.

Dès lors, le référentiel des durées de conservation doit être constitué sur la base des produits distribués par l'établissement, mais ne doit pas omettre les durées de conservation applicables aux candidats et aux collaborateurs de l'établissement. Ce référentiel est une étape chronographe mais indispensable, qui doit associer l'ensemble des acteurs concernés, sous l'égide du DPO.

Par ailleurs, il faut avoir à l'esprit que les durées de conservation ne sont pas figées, les droits applicables en la matière pouvant évoluer. Ainsi, le référentiel requiert de faire l'objet d'une mise à jour régulière. Charge à tous les acteurs concernés de sensibiliser les équipes informatiques aux évolutions régulières et à leurs impacts sur la solution.

Constituer la liste des évènements déclencheurs.

Si le référentiel des durées de conservation indique les délais durant lesquels les données seront conservées, il convient d'identifier clairement le point de départ de ce délai, autrement dit, les **évènements déclencheurs**.

A titre d'exemple, si un client clôture un contrat d'assurance, l'établissement devra-t-il, dès la clôture, archiver les données relatives à ce contrat ou faudra-t-il attendre que le client ait clôturé l'intégralité des contrats détenus avant de procéder à l'archivage, puis à la purge des données ? L'établissement doit-il attendre le départ d'un collaborateur pour procéder à l'archivage de l'intégralité des données de ce dernier ? Par ailleurs, pour une assurance-vie, la durée de conservation

dépend des modalités de dénouement du contrat (rachat, décès, …). Des pratiques de Place peuvent même se constituer, pour certaines plus contraignantes que le droit.

Sur la base d'une revue exhaustive, la liste des évènements déclencheurs peut être longue et doit prendre en compte les liens entre les évènements pour garantir une solution globalement cohérente.

Construire sa solution informatique.

La phase de définition des spécifications fonctionnelles de la solution ne doit pas être décorrélée de la phase de définition des spécifications techniques : une approche Agile peut s'avérer pertinente.

En effet, les Métiers et la DSI doivent, en cohérence, construire la solution pour respecter les principes structurants suivants :

- **Disposer d'une solution flexible.** Les spécifications fonctionnelles étant amenées à évoluer dans le temps, la solution informatique se doit d'être souple. L'intégration de nouvelles données dans le SI ou des évolutions règlementaires conduisant à l'application de nouvelles durées de conservation auront des impacts sur la solution technique.

  Dès lors, la solution informatique doit être conçue, *by design*, de manière à intégrer ces contraintes (par ex., facilité de paramétrage des durées de conservation ou d'ajout d'une nouvelle règle).

- **S'assurer de la qualité des données.** Dans la majorité des établissements, le chantier « Archivage & Purge » conduira inéluctablement à soulever des problématiques liées à la qualité des données. Selon les orientations fonctionnelles, une phase de mise en qualité des données, quelle que soit son périmètre, peut devenir un pré-requis. Une approche DMO, en complément de RGPD, doit être considérée comme une valeur ajoutée.

- **Identifier les *pain points* pour définir les solutions de contournement.** A titre d'exemple, une migration informatique antérieure aurait pu altérer des données du SI. Une co-construction de la solution entre les Métiers et la DSI permet d'identifier, en amont, ces *pain points* et de définir des solutions de contournement afin de ne pas engendrer de retards sur la livraison d'un lot ou de la solution dans sa globalité.

Une approche longue et structurante pour la suite des travaux.

La complexité et le temps nécessaire à la réalisation des étapes précédentes ne doivent pas être sous-estimés : les travaux soulèveront nécessairement des questions de fond pour lesquelles les réponses devront être proprement qualifiées et justifiées.

En effet, un établissement ne peut pas prendre le risque de non-conformité en conservant des données au-delà des durées légales ou en supprimant des données toujours nécessaires à l'activité de celui-ci.

Quelques pistes et bonnes pratiques pour mener à bien son projet « Archivage & Purge ».

Documenter ses travaux.

Pour la majorité des établissements, le déploiement d'une solution complète d'archivage et de purge des données s'effectuera dans un horizon long. Partant de ce principe, il conviendra de constituer une documentation exhaustive de l'ensemble du projet afin de disposer d'une preuve de l'avancement des travaux en cas de contrôle du régulateur. En outre, une documentation complète et détaillée permettra de maintenir plus facilement la solution dans la durée.

Adopter le bon niveau de granularité dans les règles de conservation des données.

Les règles à mettre en place, basées sur les évènements déclencheurs et les durées de conservation des données, doivent être les plus génériques possibles, tout en couvrant l'exhaustivité des cas fonctionnels. Si les règles sont trop fines, elles deviendront tentaculaires et incompréhensibles dans le temps.

Traiter les archives physiques.

Les archives physiques peuvent être étroitement liées aux données détenues dans les outils informatiques : une référence stockée informatiquement peut permettre d'identifier l'emplacement d'un document détenu uniquement sur un support physique. Il faut donc veiller à ne pas dissocier les supports (informatique et physique) dans la phase d'analyse. En revanche, il peut s'avérer utile, voire nécessaire, de décorréler les deux approches pour les phases de déploiement pour permettre de réaliser des avancées.

Lotir les travaux.

Afin d'obtenir des résultats plus rapides et d'assurer, pas à pas, la mise en conformité de l'établissement à la limitation de la conservation des données, il convient de lotir les travaux (par typologie de personnes concernées, par typologie de produits, …). Le déploiement des premiers lots permettra également de sécuriser les solutions retenues pour les lots ultérieurs. Planifier les travaux selon la « règle du 80/20 » permettra de concentrer les efforts de développement et de tests sur les secteurs où se situeront les risques les plus élevés.

Identifier les adhérences avec les autres projets.

La complexité du chantier « Archivage & Purge » réside également dans le fait que le périmètre des travaux est mouvant : le lancement d'un nouveau produit, la mise en place d'un nouvel outil conduira, *de facto*, à élargir le périmètre initial et peut ainsi retarder la mise en production de la solution. En amont du lancement des travaux, il convient d'identifier toutes les adhérences possibles afin de les inclure, au plus tôt, dans le périmètre.

Néanmoins, une robuste procédure *Privacy by Design* pourrait permettre d'éviter cet écueil en ne sélectionnant que des outils (internes ou du marché) proposant, nativement, la possibilité de restreindre l'accès des données à certains groupes d'utilisateurs ou de supprimer les données, directement dans l'outil.

*

Si l'ampleur des travaux et les budgets requis pour les exécuter peuvent décourager les établissements, désormais le régulateur n'accepte plus qu'aucune action ne soit lancée, comme en témoigne la récente sanction de SERGIC.

Si ce n'est déjà fait, un projet « Archivage & Purge » doit impérativement être lancé et doit bénéficier des ressources et du budget nécessaires à son déroulement.

*

Fort de nombreuses missions de cadrage et de mise en conformité au RGPD auprès des principaux d'établissements de la Place, Ailancy vous accompagne dans l'ensemble des phases de votre projet : du cadrage jusqu'au déploiement ou la réalisation d'un audit de conformité aux nouvelles dispositions du Règlement.

Virginie Thomsen, Senior Manager
Virginie a supervisé les travaux de cadrage et de mise en conformité au RGPD de plusieurs acteurs de la Place. Elle est chargée de l'offre RGPD au sein d'Ailancy.

Florian Hallant, Consultant Senior
Florian a mené, pendant plus d'un an, les travaux de mise en conformité au RGPD d'un acteur bancaire spécialisé de la Place.

Ailancy, cabinet de conseil indépendant spécialisé dans les métiers de la banque de la finance et de l'assurance vous accompagne pour relever vos enjeux métiers, accompagner vos réflexions et mener à bien vos projets de transformation.

Ailancy
32, rue de Ponthieu
75008 Paris
Tel : +33 (0)1 80 18 11 60
www.ailancy.com