

**Rapport pour le conseil régional
JUILLET 2022**

Présenté par
Valérie PÉCRESSE
Présidente du conseil régional
d'Île-de-France

**COMMUNICATION - ACTIONS ENTREPRISES EN RÉPONSE AUX OBSERVATIONS FORMULÉES
DANS LE RAPPORT D'OBSERVATIONS DÉFINITIVES DE LA CHAMBRE RÉGIONALE DES COMPTES
SUR LA GESTION DES SYSTÈMES D'INFORMATION (EXERCICE 2016 ET SUIVANTS)**

Sommaire

EXPOSÉ DES MOTIFS	3
---	---

EXPOSÉ DES MOTIFS

Communication - Actions entreprises en réponse aux observations formulées dans le rapport d'observations définitives de la chambre régionale des comptes sur la gestion des systèmes d'information (exercices 2016 et suivants)

Au cours de l'année 2020 la Chambre Régionale des Comptes a effectué un contrôle sur la gestion des systèmes d'information (2016 et suivants). La CRC a communiqué ses observations définitives à la Région en décembre 2020. En application de l'article L.243-6 du code des juridictions financières, ces observations ont été présentées et ont fait l'objet d'un débat à la séance de juillet 2021. Conformément à l'article L.243-9 du même code, le présent rapport présente les actions qui ont été entreprises depuis un an à la suite des observations définitives précitées.

En préambule, le rapport indique plusieurs points positifs sur les comptes et la gestion des Systèmes d'Information, notamment que la mandature 2015-2021 a mis en place une vraie stratégie informatique qui n'existait pas dans la collectivité auparavant, et, a également constaté qu'un certain nombre de mesures existaient concernant le respect des exigences du RGPD (nomination d'un DPO, documentation de la conformité) relevant que certaines nécessitaient des améliorations.

I. Les recommandations en forme de rappel au droit :

Rappel au droit n° 1 : Finaliser sans délai la mise en conformité réglementaire des traitements de données personnelles.

La protection des données personnelles est un **des principes majeurs qui guide l'action** de la Région. Elle est le socle du lien de confiance que nous construisons chaque jour avec les Franciliens. C'est pourquoi la Région a très tôt placé cette problématique comme axe essentiel de ses missions et a engagé dès avant 2018 des actions en faveur de la protection des données, renforcées lors de l'entrée en vigueur du RGPD (Nomination d'un CIL puis d'un DPO, une cartographie des traitements mis sous registre, mise en place d'outils de sensibilisation des agents, mise à jour des mentions d'information sur les sites...).

Ainsi, suite aux observations de la CRC, la Région a eu le souhait de réagir rapidement et fortement sur les points soulevés, prouvant ainsi sa volonté de conformité et d'exemplarité en suivant les six étapes de mise en conformité des traitements proposées par la CNIL :

- 1) Désigner un délégué à la protection des données (DPD ou DPO)
- 2) Cartographier les traitements de données personnelles : élaboration d'un registre.
- 3) Prioriser les actions à mener sur la base de cette cartographie
- 4) Gérer les risques identifiés le cas échéant via une analyse d'impact
- 5) Organiser les processus internes et la Gouvernance
- 6) Documenter la conformité

Sur la cartographie des traitements :

La CRC reprochait à la Région d'ignorer le nombre de traitements de données personnelles qu'elle utilise. Cette affirmation n'était pas exacte. Le nombre de traitements était connu et communiqué à

la Chambre. La Région a en revanche, suite à cet inventaire, souhaité le rationaliser et favoriser sa lisibilité et sa fiabilité autour de blocs de finalités (159 traitements vs 624 en 2021).

Sur la priorisation des actions à mener sur la base de cette cartographie :

La Région a mis en œuvre des analyses juridiques poussées et menées par le Cabinet Lexing de tous les traitements ainsi cartographiés (130 entretiens et analyses), permettant d'évaluer les écarts de conformité et identifier les plans d'actions de conformité adéquats par traitement, avec priorisation des actions selon une évaluation du risque sur les personnes concernées. Les actions ont été réalisées par les Pôles responsables des traitements concernés, avec un accompagnement du Cabinet Lexing pour sécuriser les actions et en lien avec la CNIL qui a été associée étroitement aux différentes étapes de cette démarche.

Sur la gestion des risques :

La Région a par ailleurs recensé les traitements les plus sensibles suite aux analyses précitées, et les analyses d'impacts ont été incluses parmi les plans d'actions (application des critères AIPD de la CNIL et du CEPD).

Ceux ayant des impacts les plus sévères sur la vie privée des personnes concernées ont d'ores et déjà fait l'objet d'une analyse d'impact relative à la protection des données, utilisation du logiciel de la CNIL), les autres (33 traitements) sont en cours de réalisation et pour accélérer cette étape, des ateliers sous format « Bootcamp » avec référents RGPD des Pôles, responsables Métier, équipe RGPD du Pôle Data et le DPO, ont été mis en place en avril 2022 (7 sessions sur 2 promotions).

Sur la gouvernance et les processus internes :

La Région a une volonté de renforcement continu de sa gouvernance : elle évolue au fil de l'eau et est remaniée régulièrement afin d'être adaptée aux besoins et enjeux nouveaux liés au RGPD **et à la transformation numérique de l'institution.**

Dans ce sens, elle a initié une réorganisation profonde de la gouvernance de la donnée et de son pilotage, notamment selon les actions suivantes :

- La création d'un Pôle Transformation du Numérique, qui marque une nouvelle étape de la maturité de la collectivité sur ces sujets : ce pôle concentre les directions essentielles à la maîtrise des données et des Systèmes d'Information et est composé d'experts : Data, Smart et de la DSI et d'en faire un outil stratégique ;
- Le renforcement des moyens apportés aux différents services de la Région et un encadrement des référents RGPD en place dans chaque pôle de la Région ;
- La création d'une équipe de coordination en complément de l'externalisation de la mission de DPO ;
- Un suivi systématique du sujet en comité stratégique data à compter de décembre 2020 ;
- Un chantier de contrôle est suivi au niveau du comité de direction générale sous l'autorité du Directeur Général des Services ;
- La prise en compte et l'identification de la protection des données dans la cartographie des risques stratégiques avec l'Inspection générale.

Par ailleurs, la mise à disposition d'outils de sensibilisation à tous les agents (ateliers de formation générales et d'autres spécifiques, espaces dédiés Teams et sous intranet, tutoriels, ...) a permis une accélération d'une acculturation à la protection des données personnelles

Concernant les process internes, pour rappel, plusieurs process existaient au sein de la Région avant le rapport de la CRC : encadrement des nouveaux traitements (des analyses de conformité préalables, des clauses dans les marchés/conventions, des mentions d'informations systématiquement préparées), procédure de gestion des demandes des personnes concernées

dans le respect des délais et de gestion des incidents de sécurité (coopération RSSI/DPO, évaluation des impacts, mémorandum établissant les formalités à suivre en cas de violation). Des référentiels sur les durées de conservation et des modes opératoires sont également déployés (qualification des acteurs, obligations des sous-traitants...).

Ces éléments font l'objet d'amélioration en continue et d'une industrialisation grandissante.

Dans cette logique d'amélioration contenue de la conformité, des chantiers sont en cours parmi lesquels : un référentiel de classification des données, la mise en place de réunions de gestion de crises coordonnées entre le DPO, le RSSI, les services de l'urbanisme et de la data, mise à disposition des agents de « kits RGPD » par thématique et la mise à jour de la politique de la sécurité.

Sur la documentation de la conformité :

La Région a un souhait de conformité continue et élevée : elle a donc mis à jour son Registre des Traitements, et elle tient également un Registre des Violations de sécurité comme demandé par le RGPD. Un process permet le respect des droits de personnes (gestion des réponses aux demandes, mentions d'informations, gestion des sous-traitants...). Des référentiels existent et sont revus de manière régulière afin de correspondre aux besoins.

Enfin, la Région a une volonté forte de conformité et de bonne gestion des données, de transparence et de proactivité, en collaborant avec la CNIL avec qui elle a déjà pu échanger dès novembre 2021, et souhaite maintenir ce suivi avec la Régulateur (réunion prévue en juillet 2022 avec le Service DPO de la CNIL).

II. Les autres recommandations adressées par la CRC

Recommandation n° 1 : Mieux articuler la fonction informatique avec l'ensemble des missions de la Région en vue d'en faire un outil stratégique

Au cours de ces 6 dernières années la Région, a posé les bases d'une première étape de sa transformation numérique. Le déménagement, avec la mise en place du télétravail, la création d'Île-de-France smart services et du CRM sans oublier le développement du THD sur tout le territoire et la transformation numérique des lycées avec le wifi, les PC aux élèves et les tablettes aux agents, ont été des éléments puissants de transformation de la région.

Une deuxième étape a été actée avec la création du nouveau Pôle Transformation Numérique au 1^{er} janvier 2022 et qui s'appuie à la fois sur les recommandations de la CRC de faire du numérique et de l'informatique un outil stratégique au service de la collectivité régionale.

En se réorganisant, il s'agit de mieux tirer parti des opportunités offertes par les outils numériques et par une meilleure utilisation de nos données afin de faire de ce pôle un outil permettant de simplifier la vie des franciliens et le travail des agents.

Ce pôle permet de renforcer l'**infrastructure informatique et la cybersécurité**, d'investir dans nos grands systèmes d'information (D.R.H., Finances, lycées, formation professionnelle ...) et urbaniser ces systèmes d'information. Il permettra de mieux organiser la circulation de la donnée et la création de tableau de bords décisionnels.

Le regroupement des différents services hier localisés dans différentes directions et la réorganisation de la DSI répondent à ces grands principes.

Ce nouveau pôle est structuré en 3 grands directions :

La direction des Systèmes d'Information qui a trois grandes missions :

- La responsabilité des infrastructures et de la production
- La bureautique et le service aux utilisateurs qui va inclure la gestion des écrans des salles de réunion
- La gestion des grands systèmes d'information

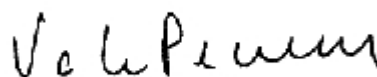
La direction Smart, Numérique et Innovation qui se découpe en trois grandes missions :

- La mission du numérique dans les lycées.
- La mission Connaissance, Lab, Design et innovation qui structure le pilotage des grands projets d'innovation en se centrant sur la gestion de la connaissance, l'utilisateur et le design.
- La mission grands projets numériques qui vise à ***améliorer la qualité de service aux usagers (agents et citoyens) par le développement, la gestion ou l'appui au déploiement de plateformes numériques de services agrégeant des données et des informations internes et externes.***

La direction de la donnée rassemble l'ensemble des savoir-faire et compétences autour de la donnée en soutien des pôles qui portent la connaissance métier, et portera les missions suivantes :

- Développer et porter la gouvernance de la donnée en interne et en lien avec les partenaires de la région.
- Porter une nouvelle offre d'accompagnement des directions dans l'élaboration et la mise en œuvre de leurs feuilles de routes, pour rendre la donnée accessible là où elle peut apporter de la valeur ajoutée et être vectrice d'innovations dans la production des politiques publiques régionales
- Concevoir l'architecture et mettre en œuvre l'outillage permettant à la région de tirer pleinement partie du potentiel de la donnée.

**La présidente du conseil régional
d'Île-de-France**



VALÉRIE PÉCRESSE