



ÉDITION 2019

Un an après, comment  
le RGPD permet  
**de créer de la valeur ?**

**TNP<sup>1</sup>**

ACCÉLÉRATEUR DE PERFORMANCE



## Avant-propos

Guy LETURCQ,  
Directeur général, TNP

---

Un an après l'adoption du RGPD (Règlement Général pour la Protection des Données), le 25 mai 2018, où en sont les entreprises, quelles sont les difficultés auxquelles elles sont confrontées, quels bénéfices peuvent-elles escompter et quelles sont leurs perspectives de création de valeur ?

Les organisations ont pris la mesure de l'ampleur de la transformation qu'elles doivent opérer pour se mettre en conformité avec le RGPD et le rester de manière pérenne. Cependant, cette réglementation implique **un profond changement de culture** car l'objectif de ce règlement est avant tout de **protéger les personnes des risques liés aux traitements de leurs données personnelles** par les organisations publiques ou privées.

D'abord, la transposition opérationnelle du RGPD oblige les organisations à **faire évoluer leur gouvernance de la donnée** et leur système d'information, voire à investir dans des solutions technologiques ad hoc. TNP vient de publier son livre blanc annuel sur le sujet.

Ensuite, s'appuyant sur ces obligations réglementaires, des Directions Générales de grands groupes se tournent vers une organisation **« data-centric »** pour renforcer leur compétitivité et chercher à **créer de la valeur par la data**, mettant ainsi en exergue l'indispensable maîtrise de la qualité de données. On passe plus de temps dans les entreprises à chercher et à préparer les données (80% du temps) qu'à les utiliser pour créer de la valeur (20%). C'est devenu **un enjeu de « désilotage » des organisations** et d'efficacité opérationnelle. C'est ainsi que l'on voit se renforcer un peu partout les fonctions de **« Chief Data Officer »** et de Data Management Office. À titre d'illustration, on trouve plus de 10.000 profils **« Chief de Data Officer »** en France en 2019 dans LinkedIn contre 4.000 en 2016.

TNP est un cabinet indépendant spécialisé dans la définition et la mise en place de programmes de transformation avec :

- **Des équipes multisectorielles et multi-spécialistes,**
- **Des démarches outillées s'appuyant sur la capitalisation de ses missions.**

TNP dispose d'une **offre RGPD de bout en bout**, depuis la phase de diagnostic jusqu'à la mise en œuvre opérationnelle des mesures de conformité et de sécurité. Cette offre passe par **l'intégration de la protection des données dès la phase de conception des projets** (Privacy by Design), par un accompagnement dans la transformation des systèmes d'information et dans le choix de solutions technologiques.

TNP développe son pôle **« Data for Business »** réunissant ses savoir-faire en Data protection, Data gouvernance, Data Architecture et Data Analytics.

# Sommaire

## Paroles d'experts

<b>Florence BONNET</b> , <i>Directrice, TNP</i>	...5
<b>Elisabeth QUILLATRE</b> , <i>DPO, Christian Dior Couture</i>	...7
<b>Gwendal LE GRAND</b> , <i>Director of technology and innovation, CNIL</i>	...9
<b>Fabienne NAIME</b> , <i>Axa Partners Group DPO</i>	...11
<b>Boyan YANKOV</b> , <i>Partner, TNP</i>	...14

## TNP en bref

<b>L'offre TNP Data 4</b>	...17
<b>Vos interlocuteurs TNP</b>	...18

# Paroles d'experts





# Un an après, comment le RGPD permet-il de créer de la valeur ?

Florence BONNET, Directrice, TNP

▣ **Avant de parler de création de valeur, ne devrait-on pas d'abord aborder les difficultés rencontrées par les entreprises dans le déploiement du RGPD ?**

**60% des entreprises se disent prêtes par rapport à la mise en œuvre du RGPD.**

Je serais moins optimiste. Le principe d'«*accountability*» va bien au-delà de la seule documentation des processus et impose de pouvoir en démontrer l'efficacité. Nous n'en sommes pas là.

Le RGPD (Règlement Général sur la Protection des Données) a pour objectif de protéger les personnes des risques pour leurs droits et libertés. C'est une approche qui diffère de la gestion des risques pour l'entreprise. Tant dans ses fondements que dans sa mise en œuvre, cette nouvelle réglementation implique un changement de culture.

Avec le RGPD, chaque directeur d'établissement, chaque responsable de «*Business Units*» doit veiller à son niveau à gérer les risques sur la vie privée liés aux traitements et à l'application effective des mesures de protection des données personnelles qu'elles soient juridiques ou techniques.

La mise en place d'une gouvernance de la protection des données avec des rôles et des responsabilités clairs, un processus d'escalade et une chaîne de validation bien définis ne sont pas toujours évidents en raison notamment du manque de ressources et de sensibilisation sur le sujet.

La transposition opérationnelle des exigences du RGPD, oblige les organisations à faire évoluer leur système d'information voire à investir dans de nouvelles solutions technologiques afin de s'assurer de leur conformité dans le temps. La suppression des données personnelles tout comme leur

anonymisation sont des sujets complexes en pratique.

▣ **Pouvez-vous nous expliquer ce que recouvre la notion de «*RGPD lineage*» ?**

Le «*RGPD lineage*» correspond à une cartographie des liens dans le système d'information. Il permet de visualiser le cycle de vie de la donnée personnelle en vue de répondre aux questions suivantes : de quelle source provient la donnée ? qui en est le destinataire ? sous quelle forme est-elle accessible ?

La finalité du «*RGPD lineage*» est de faciliter les processus de protection des données : droits d'accès, droit à l'oubli, portabilité, gestion des durées de conservation...

▣ **Pensez-vous que les entreprises puissent retirer des bénéfices de la mise en œuvre du RGPD ?**

Le RGPD représente d'abord un enjeu en termes de confiance.

Rappelons quelques constats. Plus de 60% des Français pensent que les entreprises font un usage détourné de leurs données et 38% les suspectent de les revendre. Les études montrent que la réaction des personnes face à une utilisation détournée de leurs données est beaucoup plus importante que face à une faille de sécurité. Il est intéressant de noter que le manque de transparence, l'absence de consentement et la violation des règles du RGPD font de plus en plus l'objet de dénonciations sur les réseaux sociaux.

Des chercheurs ont démontré que la mise en place de mesures de protection des données permettait de réduire la perception du risque liée à la transmission de ses données personnelles. Cela augmente la confiance des

clients et donc la quantité et la qualité des informations qu'ils sont prêts à divulguer. Ensuite, nous constatons chaque jour avec nos clients qu'un bon niveau de conformité est indéniablement un avantage concurrentiel en B2B. Pouvoir justifier d'une démarche de «*Privacy by Design*» ou de certification, crée un avantage compétitif pour les éditeurs de solutions et pour les prestataires de services qui traitent ou qui fournissent des données.

On peut aussi imaginer que si le consommateur est à même de paramétrer ses choix concernant l'utilisation de données personnelles le concernant, il sera d'autant plus attentif à une publicité ciblée a priori plus pertinente. C'est donc tout le parcours client qui est impacté.

Il a aussi été démontré que lorsque les entreprises étaient préparées à la gestion des violations de données personnelles, les coûts liés à ces incidents étaient moins élevés.

J'ajoute que le niveau de protection des données est enfin de plus en plus présent parmi les critères d'évaluation des entreprises et de leurs produits et services. Ce mouvement devrait prendre de l'ampleur dans les années à venir et il n'est pas utopique d'imaginer que le niveau de protection des données aura un impact sur la valorisation d'une entreprise.

## ▀ Quelles sont les prochaines étapes ?

Pour garantir leur conformité de manière pérenne, les entreprises auront besoin de s'appuyer sur les technologies, s'engager dans des démarches de certification et adhérer à des codes de bonne conduite tels que prévus par le RGPD.

On voit également apparaître de nouveaux besoins en dehors de l'Union Européenne notamment en Afrique où TNP est présent dans des entreprises soumises pour partie au RGPD mais aussi à d'autres législations de protection des données, avec la volonté de déployer un niveau homogène de protection des données au niveau mondial.

De leur côté, les autorités de régulation vont développer leur coopérations, sur

le modèle de la CNIL et de l'autorité de la concurrence en France ou du Financial Conduct Authority («*FCA*») et de l'ICO au Royaume-Uni par exemple.

Enfin, je pense que l'IoT (Internet of Things) associé au big data, l'IA (Intelligence Artificielle) et la blockchain représentent un énorme enjeu pour l'usage des technologies au travail ou du développement des démocraties, notamment dans le cadre des smart cities.

Je pense que les individus n'ont pas conscience de la quantité de données qui peut être utilisée pour leur bien mais aussi à leur rencontre.

Pour le Gartner par exemple, l'un des risques les plus importants auxquels les entreprises seront confrontées au cours des prochaines années résiderait dans l'atteinte à la vie privée des personnes due à l'utilisation de blockchains publiques.

## ▀ Comment le cabinet TNP accompagne-t-il ses clients dans la mise en œuvre du RGPD ?

TNP a une offre RGPD de bout en bout, depuis la phase de diagnostic jusqu'à la mise en œuvre opérationnelle des mesures de conformité et de sécurité, soit en tant que DPO externe soit en support du DPO interne de nos clients.

Cette offre passe, notamment, par l'intégration de la protection des données dès la conception des projets, par défaut et tout au long du cycle de vie («*Privacy by Design*»), par un accompagnement dans la transformation des systèmes d'information et dans l'aide au choix et au déploiement de nouvelles solutions technologiques tant pour la gestion de la conformité que pour la cartographie et la gouvernance des données ou la sécurité.

À ce sujet, pour la 3<sup>ème</sup> année consécutive, TNP a réalisé un benchmark des outils pour les DPO (Data Protection Officer) et les CDO (Chief Digital Officer).



## Interview Elisabeth QUILLATRE

*DPO, Christian Dior Couture*

### ■ Est-ce la seule peur de la sanction qui a guidé la démarche de mise en conformité avec le RGPD de votre groupe? Quel niveau de conformité avez-vous visé à court et moyen termes?

Christian Dior Couture a toujours considéré que les données personnelles de ses clients étaient précieuses. Avec l'adoption du RGPD, Christian Dior Couture a vu l'opportunité d'aller plus loin en améliorant la relation avec ses clients et en renforçant la confiance de ces derniers, notamment par plus de transparence et la nomination d'un DPO en interne pour piloter la mise en conformité en interne et vis-à-vis des tiers.

La sanction théorique des 4% est bien connue de tous en interne et a permis de rappeler quels étaient les enjeux financiers en cas de non-conformité, mais elle n'a pas guidé la démarche de mise en conformité de la Maison.

### ■ Depuis quand et comment vous y êtes-vous prise pour gérer ce programme de mise en conformité avec le RGPD?

Il y a tout d'abord eu une phase d'observation et d'inventaire qui a eu lieu en 2017. Une fois l'inventaire réalisé, le programme de mise en conformité a été déterminé et a fait l'objet d'une présentation et validation par tous les sponsors internes, indispensables pour le succès du programme.

Ce programme a été divisé en plusieurs phases, dont une prioritaire qui avait un timing très serré puisque les actions correspondantes avaient pour date butoir le 25 mai 2018.

Afin de s'assurer que les interlocuteurs clés étaient bien impliqués dans le programme,

un réseau de privacy champions a été nommé dans les différents Métiers mais également dans les différentes zones géographiques, y compris en dehors de l'Union Européenne, les clients de la Maison étant internationaux.

### ■ Quelles sont les difficultés rencontrées pour vous mettre en conformité avec le RGPD?

Comme partout, tous les Métiers ont été impactés par les actions de mise en conformité à mettre en place, augmentant pour certains considérablement la charge de travail, et impactant de ce fait les roadmaps des projets existants. Il a donc été nécessaire de revoir les priorités entre les besoins business et les actions de mise en conformité impératifs.

La plupart des filiales de la Maison étant situées dans des pays ayant déjà adopté des réglementations en matière de protection des données qui reprennent pour l'essentiel les principes de RGPD, il nous a semblé naturel d'avoir un socle commun de principes de protection des données partout dans le monde. L'implémentation du programme de conformité hors UE s'est fait plus rapidement dans certaines zones/pays que d'autres, mais l'enjeu business d'offrir une expérience client similaire partout dans le monde a été le fil conducteur.

### ■ Avez-vous une bonne visibilité des impacts IT du RGPD dans votre entreprise?

Assez bonne maintenant oui, qu'il s'agisse des outils existants qu'il a fallu faire évoluer ou des nouveaux outils qu'il a fallu implémenter, mais aussi et surtout la charge de travail que cela a représenté et représente encore pour les équipes.

## ■ Sur le plan opérationnel, comment avez-vous mis en œuvre les processus de protection des données? Est-ce que cela s'inscrit dans une politique de gouvernance des données?

Pour ce qui concerne l'exercice des droits de personnes, nous avons décidé dans un premier temps d'adopter des process adéquats pour chaque Métier au regard de la structure IT concernée. Nous avons ensuite décidé de faciliter cet exercice en mettant à jour les outils existants et/ou en déployant de nouveaux outils pour permettre aux personnes concernées de suivre en direct leur demande (ex. pour les candidats) ou d'être alertées lorsque leur demande est traitée (ex. pour les clients). À titre d'exemple, pour les clients, nous avons déployé pour notre call center un outil en interne permettant de logger et traiter chaque demande, incluant l'envoi d'AR automatique lorsque pertinent. Tous ces process s'accompagnent bien sûr d'une évolution des outils IT impliqués pour permettre le respect des droits de bout en bout, qu'il s'agisse du droit à la suppression/à l'oubli, du droit d'accès, ou encore du droit de s'opposer à recevoir des offres commerciales (personnalisées ou non).

## ■ Envisagez-vous de recourir à des solutions technologiques soit pour le pilotage de votre conformité RGPD, soit pour la gouvernance des données, soit encore pour répondre à des exigences de sécurité?

Nous utilisons déjà certains outils pour gérer une partie de notre conformité, dont notamment les SAR (demandes des personnes concernées en lien avec leur données) ou les RPA (Registre des traitements).

## ■ Est-ce que le RGPD a été l'occasion de déceler des opportunités de nouveaux «business»?

La confiance générée par la transparence sur la protection de la vie privée a un impact très positif sur la qualité des informations partagées par les clients - y compris leur actualisation, permettant ainsi une meilleure personnalisation de la communication de la Maison.

## ■ Avez-vous mis en place une démarche de privacy-by-design sur un plan technique (au-delà des aspects organisationnels et juridiques)?

À titre d'exemple, nous avons pris le parti de créer des modules de formation Maison afin de montrer concrètement les enjeux de la protection des données des clients de Dior. Une nouvelle application sera prochainement mise à disposition de tous les collaborateurs amenés à collecter des informations sur nos clients en boutique, intégrant un module de formation dédié à la protection des données, ponctué de quizz et se terminant par une animation synthétisant le cycle de la donnée client chez Dior, de sa collecte à sa suppression.

Par ailleurs, par soucis de transparence qui est un principe du RGPD, la collecte des informations de contact et des choix en matière de réception d'offres personnalisées s'inscrit désormais complètement dans le cérémonial de vente depuis la mise à disposition en boutique de la carte client «GDPR» digitalisée sur iPhone. Chaque sales associate a sa façon d'utiliser et de présenter la carte client digitalisée au client: il la complète lui-même et demande au client de vérifier les informations, il propose au client de compléter lui-même ses informations via l'iPhone, ils le font ensemble.





## Interview Gwendal Le Grand

*Director of technology and innovation, CNIL*

■ **On a beaucoup parlé du RGPD ces derniers mois. Cependant, un autre texte très important est en cours de discussion au niveau européen, la proposition de règlement ePrivacy. Quels sont les enjeux de ce texte ? Qu'est-ce qu'il va changer pour les entreprises et leurs modèles économiques ? Dans quels délais pourrait-il être adopté et entrer en vigueur ?**

La proposition de règlement eprivacy concerne des aspects essentiels dans le domaine de la confidentialité des communications: il inclut les nouveaux acteurs proposant des services tels que skype ou whatsapp afin qu'ils garantissent un niveau équivalent à celui des opérateurs traditionnels; il révisé les règles concernant la confidentialité des communications (méta données et contenu); il modernise les règles relatives au dépôt de cookies, ainsi que les règles de protection s'agissant du spam (par email, SMS ou automate d'appel); enfin, il adapte les pouvoirs des autorités. En particulier, il s'agit de remettre sur un pied d'égalité toutes les entreprises du numérique, quelle que soit leur taille ou leur localisation.

Les acteurs internationaux seront soumis aux mêmes obligations de recueil du consentement que les entreprises européennes; l'alignement du champ d'application territorial et des sanctions avec celles du RGPD (pourcentage du chiffre d'affaires et gouvernance) permettra aux régulateurs d'appliquer réellement le texte. Quant au délai d'application, si la Commission européenne et le Parlement européen

ont adopté leur version du texte, les discussions sont toujours en cours au Conseil. La CNIL et ses homologues, réunis au sein du CEPD, ont récemment réaffirmé leur demande de ne pas abaisser le niveau de protection et de voir les travaux aboutir rapidement.

■ **La récente décision à l'encontre de Google a fait grand bruit. Elle est principalement axée autour de deux griefs, la transparence et le consentement. Sur le premier point, nous avons la sensation que la CNIL a voulu faire référence à la notion de «*design*» que l'on retrouve dans l'obligation de «*privacy by design*».**

Dans le cas de cette sanction, c'est l'architecture générale de l'information qui a été pointée du doigt, mais aussi le manque de transparence et l'absence de consentement valable pour la personnalisation de la publicité. Des informations essentielles étaient excessivement disséminées dans plusieurs documents et l'information pertinente n'était accessible qu'après plusieurs étapes, impliquant parfois jusqu'à 5 ou 6 actions de l'utilisateur. Et les informations délivrées n'étaient pas toujours claires et compréhensibles. Or, le principe de transparence exige que toute information et communication relative aux traitements de données à caractère personnel soit aisément accessible, facile à comprendre et formulée en des termes clairs et simples. Cela passe par l'architecture et le design des interfaces.

D'une certaine manière, le design et le consentement sont liés, soit en positif lorsque les pratiques de design visent à

améliorer la capacité des individus à faire un choix, soit en négatif lorsqu'elles visent à tromper par des pratiques de design abusives. Ces notions sont d'ailleurs explorées plus en détail dans notre dernier cahier IP, intitulé La forme des choix.

**■ Dans une économie numérique, les périmètres d'intervention des différentes autorités de contrôle peuvent parfois se chevaucher. Doit-on envisager une nouvelle forme de coopération entre la CNIL et les différents régulateurs (ADLC, ARCEP, DGCCRF, CSA, ACPR...)? Si oui, quels pourraient être les contours et les modalités de cette nouvelle forme d'interrégulation ?**

L'efficacité de la régulation exige une coopération approfondie avec les autres régulateurs intervenant dans ces mêmes équilibres afin d'apporter aux citoyens et aux opérateurs une réponse publique cohérente et efficace. Cette interrégulation méritera d'être renforcée dès 2019, à un double titre. D'une part, parce que la

question des données dépasse le simple cadre de leur protection: on pense, ici, à leur valeur dans une logique concurrentielle. D'autre part, parce que la protection des données peut être une partie d'une régulation plus globale – par exemple, les réflexions liées à la régulation des plateformes numériques. Dès lors, la CNIL entend renforcer ses liens avec les autres régulateurs concernés (Autorité de la concurrence, CSA, ARCEP, ACPR, etc.). Cela s'est notamment traduit par la signature, le 31 janvier 2019, d'un nouveau protocole de coopération entre la DGCCRF et la CNIL. Les deux autorités ont décidé de mettre à jour la convention initialement signée en janvier 2011 afin de renforcer leur collaboration et de l'adapter aux nouveaux enjeux numériques.



## Interview Fabienne NAIME

*Axa Partners Group DPO*

### ▣ Est-ce la seule peur de la sanction qui a guidé la démarche de mise en conformité avec le RGPD de votre groupe ? Quel niveau de conformité avez-vous visé à court et moyen termes ?

AXA est le premier groupe d'assurance au monde à avoir adopté un ensemble de Règles internes d'entreprise («BCRs») qui ont été approuvées par la CNIL et par 15 autres autorités européennes en charge de la protection des données à caractère personnel. Aujourd'hui les sociétés AXA ayant adhéré aux BCRs représentent 97% du chiffre d'affaires total consolidé du Groupe. Lorsque les discussions autour du RGPD ont commencé à émerger au sein du WP29, le Groupe AXA a été très sensibilisé et c'est de façon naturelle que le Groupe a décidé de mettre en place un programme de conformité au sein d'AXA. Ce programme a été défini au niveau du comité exécutif du Groupe AXA. Chaque CEO a reçu pour instruction de déployer au sein des entités dans son périmètre un programme de conformité, avec l'obligation de reporter les statuts d'avancements et KPIs au Groupe de façon régulière.

Comme pour toute société, le montant significatif de la sanction nous a effectivement encouragé à anticiper cette réglementation et à mettre en place toutes les mesures appropriées afin d'être en conformité.

Toutefois, au-delà du montant de la sanction, nous savons que le respect de la confidentialité des données à caractère personnel est essentiel pour conserver la confiance de nos clients. Ainsi l'enjeu phare d'AXA a toujours été de nous assurer (i) que les données de nos clients disposent d'un niveau de protection adéquat et (ii) que nos clients

puissent accéder à une information claire et transparente.

Toutes les mesures que nous sommes en train de mettre en place, notamment au sein d'AXA Partners, ont vocation à s'inscrire sur le long terme. La protection des données personnelles faisant progressivement partie intégrante de notre modèle business.

### ▣ Depuis quand et comment vous y êtes vous prise pour gérer ce programme de mise en conformité avec le RGPD ?

Le programme RGPD a été lancé au sein d'AXA en 2016. Au sein d'AXA Partners, courant 2017, nous avons identifié plusieurs chantiers divisés en 2 grandes sections :

**1.**La partie fonctionnelle: mise en place des politiques et procédures de protection des données personnelles (politique de protection des données, procédure de gestion des incidents de sécurité des données, procédure de droits d'accès, etc); sensibilisation des employés; définition de standards (DPIA, templates de clauses); mises à jour des mentions d'informations.

**2.**La partie IT: cartographie des flux de données; identification des systèmes applicatifs; analyse de profondeur de l'historique des données; implémentation des capacités de purge sur le plan technique.

### ▣ Quelles sont les difficultés rencontrées pour vous mettre en conformité avec le RGPD ?

Les difficultés que nous avons rencontrées sont assez communes je pense :

• **Créer l'adhésion en interne sur le sujet :** le montant des sanctions aura de toute

évidence été l'argument clé pour susciter l'adhésion et expliquer les risques encourus si on ne s'inscrit pas dans une démarche collective et rapide.

- **Ressources:** le RGPD a impliqué une augmentation des tâches, qui sont très chronophages et nécessitent d'avoir un dispositif robuste pour pouvoir tout gérer. Pour autant, il faut faire avec les moyens dont nous disposons car nous ne pouvons raisonnablement avoir une armée de DPO et cela nous incite à réfléchir de façon pragmatique et optimale.

- **Budget:** des budgets assez significatifs ont été débloqués au sein de chaque société AXA pour faire du GDPR l'une des priorités. Ces budgets ont permis de faire appel à des cabinets de conseil pour nous assister dans la mise en œuvre du programme. Comme dans toute entreprise, les budgets ne sont pas illimités. Il a fallu faire des arbitrages et définir une approche par les risques.

### ■ Avez-vous une bonne visibilité des impacts IT du RGPD dans votre entreprise ?

Oui, je pars du principe qu'un bon DPO doit avoir une certaine appétence pour des sujets sécurité et IT, sinon il passe à côté du sujet. Sur le volet IT, nous avons au sein d'AXA Partners un Chef de Projet GDPR dédié à la partie IT qui vérifie l'état d'avancement des purges application par application. Nous avons travaillé avec les équipes IT, Data Management et Gestion des Risques pour définir ensemble une méthodologie afin d'identifier les applications éligibles et définir les étapes à suivre :

1. Nous avons élaboré un questionnaire dans lequel nous avons défini un ensemble des critères (nature de la donnée; historique de la donnée; durée de conservation applicable; volume de données; etc) et associé des poids à chaque critère. En fonction du résultat obtenu cela nous a permis d'iden-

tifier les applications les plus critiques et éligibles au programme GDPR.

2. Le Chef de projet a travaillé en continu avec les équipes IT et DPO des différents pays pour collecter les durées de conservation; définir et valider les règles de purge; et s'assurer que les purges sont réalisées, en cours, ou planifiées à une date donnée.

### ■ Sur le plan opérationnel, comment avez-vous mis en œuvre les processus de protection des données? Est-ce que cela s'inscrit dans une politique de gouvernance des données?

Le RGPD doit vraiment être vu comme une opportunité pour créer de la valeur et mettre la donnée au centre de notre business. Nous travaillons équipe Privacy et Data Management de façon très étroite sur la mise en place d'un modèle de gouvernance de la donnée, assuré par de nouveaux rôles, qui sont les CDO (Chief Data Officers), Data Owners, Data Managers, Data stewards, etc. Il s'agit d'un réseau de personnes, responsables de façon opérationnelle de la donnée. Ce modèle est toujours en cours d'implémentation au sein d'AXA Partners, car c'est un sujet complexe. Complexe en raison de notre large rayonnement géographique; du volume de données traitées; de la diversité de nos activités et de l'existence d'applications historiques. Tous ces paramètres nécessitent d'avoir une stratégie affinée et en phase avec notre organisation.

### ■ Envisagez-vous de recourir à des solutions technologiques soit pour le pilotage de votre conformité RGPD soit pour la gouvernance des données ou pour répondre à des exigences de sécurité ?

Oui. Sur la gouvernance de la donnée et le registre des traitements, nous avons

développé sur la base d'une technologie tierce notre propre outil, qui a vocation à être utilisé par toutes nos entités dans le monde. L'objectif étant d'avoir en central, une vue d'ensemble sur les traitements opérés dans nos filiales, d'avoir un process homogène au sein de notre organisation, des zones de contrôle et enfin une bonne gestion de la donnée. Cet outil a vocation à être utilisé par le réseau (CDO, Data Owners, Data Managers, Data stewards) en charge de la gouvernance de la donnée et les DPO locaux. Il est actuellement en phase de pilote en Europe, pour aboutir vers un déploiement mondial, à moyen terme.

### ▣ Avez-vous mis en place une démarche de Privacy by Design sur un plan technique (au-delà des aspects organisationnels et juridiques) ?

Le Privacy by Design est un concept innovant, intéressant et complexe à la fois.

- **Innovant:** Ce concept implique de faire de la protection des données personnelles, non pas un sujet réglementaire, juridique, conformité, mais un sujet opérationnel. Comment faire d'un texte réglementaire un chantier opérationnel ?

- **Intéressant:** Qu'est-ce que ça veut dire concrètement ?

- **Complexe:** On commence par quoi ?

Au sein d'AXA Partners, nous sommes encore en train de réfléchir à ce concept et voir comment on peut le faire évoluer. Dans les grandes lignes, les mesures que nous avons déjà prises sont les suivantes :

- Chaque traitement de données doit faire l'objet d'une pré-analyse. Cette analyse permet d'identifier si nous sommes ou pas sur un traitement représentant un risque pour l'individu dont les données sont traitées :

- **S'il n'y a pas de risque:** la pré-analyse est complétée et finalisée sur la base des recommandations et validations du DPO, de l'IT et la sécurité.

- **S'il y a un risque:** le chef de projet doit, après la pré-analyse, compléter avec l'équipe opérationnelle une analyse d'impact sur la vie privée (DPIA). Dans cette étude, tous les critères du RGPD sont analysés de façon approfondie (notamment : base légale du traitement ; mesures appliquées aux données sensibles ; mention d'information ; respect du principe de minimisation des données ; durée de conservation ; mode de collecte du consentement ; règles de suppression des données).

- Chaque chef de projet doit faire valider son projet dans un Comité d'Architecture auquel assistent les équipes IT, Sécurité, Data Management, Privacy, Juridique, Opérationnelles et donnent leur avis, recommandations, approbations ou décision de rejet.

- Il est de la responsabilité du chef du projet et son équipe de s'assurer que tous les éléments demandés ont bien été pris en compte avant que le projet soit en production. À titre d'exemple, si l'objectif est de mettre en place un nouvel outil pour la gestion des sinistres. Cet outil doit dans son design être conforme avec les exigences du RGPD, ce qui implique un travail collaboratif avec les équipes IT, opérationnelles et Privacy.



# La création de valeur grâce à l'exploitation des données

Boyan YANKOV, Partner, TNP

## ❑ Où en est le marché concernant l'exploitation des données par les entreprises ?

Depuis 5 à 6 ans, les entreprises ont réalisé que l'exploitation de leur patrimoine de données était insuffisante. Elles ont mis en place des initiatives pour créer de la valeur et mieux exploiter leurs données : urbanisation, traitement, mise en qualité mise à disposition aux métiers qui amène notamment la meilleure connaissance des clients...

Les entreprises se rendent compte qu'elles sont assises sur un « trésor » inexploité. Leurs initiatives s'accroissent, notamment sous l'effet des opportunités technologiques.

## ❑ Quel est le rôle de la data dans les « business models » ?

Les entreprises ont conscience que nous allons vers un modèle davantage orienté vers les clients et les services. Cette orientation va faire pivoter les « business models ». Les données sont des matières premières qui peuvent être façonnées de différentes manières pour créer de la valeur.

Mais si les données ne sont pas correctement collectées, vérifiées et connectées entre elles, le « tas d'or » n'est en réalité qu'un « tas de plomb ».

## ❑ Comment la mise en place d'une gouvernance de la donnée permet-elle de répondre au droit à l'oubli des personnes ou à la portabilité des données ?

Pour n'importe quel type de données, la mise en place d'une gouvernance est la pièce maîtresse de la connaissance de la donnée, de sa traçabilité et de sa qualité mais ceci n'est possible qu'à la condition

de respecter un certain nombre de règles d'utilisation de ces données tout au long de leur cycle de vie. Les exigences du RGPD et de sécurité doivent être prises en compte afin non seulement de ne pas traiter la donnée de manière contraire à la loi mais aussi afin de répondre aux processus de protection des données qui imposent d'être en capacité de répondre aux demandes de droit d'accès, de droit à l'oubli ou de portabilité par exemple.

## ❑ Avez-vous un exemple d'enrichissement de produits ou de services existants grâce aux données ? Quelle est la valeur des analytics au service de l'humain ?

Sur la base de la connaissance des clients, les entreprises peuvent adapter leurs offres et créer des produits sur mesure en fonction des besoins des clients.

Pour une institution financière travaillant en BtoB, nous avons l'exemple d'un projet consistant à mieux connaître les clients via des interactions avec eux, dans le but de concevoir et de proposer des services en fonction de l'anticipation de leurs besoins. Cet exemple illustre la capacité de gérer la relation client au quotidien et d'être pro-actif pour pousser une proposition de valeur, comme par exemple la possibilité pour le client de gérer le risque collatéral (son exposition en risque de contrepartie).

## ❑ Comment TNP peut-il aider les clients à se poser les bonnes questions et à mettre en œuvre une stratégie data ?

TNP apporte des réponses sur l'intégrité du traitement des données, depuis la connaissance des données en terme de

structuration, d'évaluation de leur valeur, de mise en place d'une gouvernance et de règles de data management structurées autour d'outils basés sur des technologies innovantes.

Les points forts de TNP portent sur la connaissance des métiers pour lesquels les données apportent de la valeur et le traitement des données dans leur intégralité.

Nous pouvons citer l'exemple d'une intervention dans une banque privée avec la construction d'un référentiel de données, l'évaluation de la valeur des données, la cartographie, le choix d'un outil, la prise en compte de la gestion des données par rap-

port au RGPD et à la législation des autres pays.

### ■ Comment utiliser les bons leviers pour sécuriser et valoriser les datas ?

TNP réalise l'évaluation de la maturité de l'entreprise sur la manière dont elle traite les données. Puis, les consultants évaluent l'entreprise sur une échelle de 1 à 10 et effectuent un travail collaboratif pour définir la cible de maturité. Vient ensuite la définition des axes à améliorer et les leviers à activer, par exemple en termes de qualité et de mise à disposition.



# TNP en bref





# L'offre TNP Data 4

## Notre équipe

Notre équipe Data 4 Business est composée de **70 consultants** et Data Scientists (dont 25 experts RGPD). Elle est l'interlocuteur privilégié des organisations souhaitant mettre en place une stratégie en matière de data management.

- **Data protection (RGPD)**
- **Data Governance & Quality**
- **Data Architecture & Solutions**
- **Data Science & Analytics**

## Notre objectif

**Faire de la data un véritable levier de croissance et de compétitivité, en toute sécurité.**

Les quatre défis de nos clients :

- 1 **Intégrer la protection des données** dès la conception et par défaut tout au long du cycle de vie de la data (Privacy by Design);
- 2 **Faire de la data un axe majeur** créateur de valeur et de compétitivité;
- 3 **Concilier les exigences** liées aux différentes réglementations (BCBS 239, RGPD, etc.) que les entreprises doivent mettre en place;

## TNP en chiffres

**450**  
consultants

**40%**  
de croissance  
annuelle depuis  
2008

**70m€**  
de chiffre  
d'affaires

## 4 Transformer le système d'information et la gouvernance des données

et trouver des solutions technologiques pour permettre au DPO de piloter la conformité, au Chief Data Officer de gérer la donnée et au RSSI de la protéger.

## Nos missions

- 1 **Faire comprendre** à nos clients les enjeux de la donnée;
- 2 **Mettre en place** les moyens nécessaires pour la valoriser et l'exploiter;
- 3 **Conseiller** nos clients sur leurs enjeux de transformation pour mettre la data au cœur de l'entreprise et de sa stratégie.

## Nos exemples de missions

- **Diagnostic et accompagnement GDPR**
- **DPO externe**
- **Construction d'un socle de données hétérogènes** permettant de prédire les dysfonctionnements de processus facturiers
- Mise en place d'une **plateforme API**
- **Analyse sémantique** et dynamic pricing
- Mise en place de **gouvernance**
- **Politique de sécurité** au service des ventes et du marketing

## NOS BUREAUX

Paris, Lyon, Marseille, Luxembourg, Genève, Cochin, Casablanca, New Delhi.

## ▣ Vos interlocuteurs TNP



**Guy LETURCQ**  
*Directeur général  
cofondateur*  
guy.leturcq@  
tnpconsultants.com



**Florence BONNET**  
*Directrice*  
florence.bonnet@  
tnpconsultants.com



**Boyan YANKOV**  
*Partner*  
boyan.yankov@  
tnpconsultants.com



**Matthieu LEBEURRE**  
*Associate partner*  
matthieu.lebeurre@  
tnpconsultants.com



**Stéphane HOZÉ**  
*Partner*  
stephane.hoze@  
tnpconsultants.com

## ▣ Nous contacter

📍 TNP, 31 rue du Pont, 92200 Neuilly-Sur-Seine

☎ 01 47 22 43 34 ✉ [commarket@tnpconsultants.com](mailto:commarket@tnpconsultants.com)

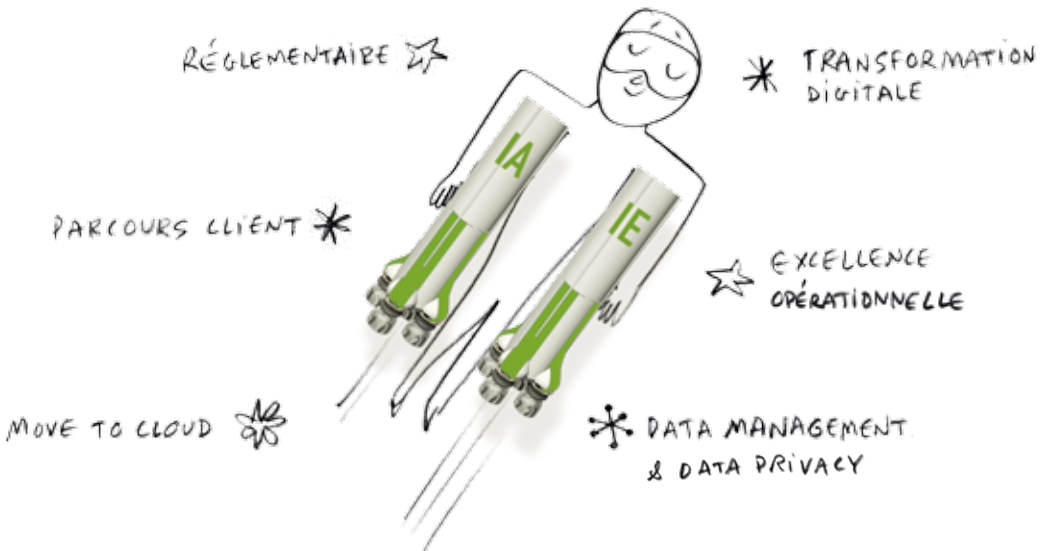
[blog.tnpconsultants.fr](http://blog.tnpconsultants.fr)    

[www.tnpconsultants.com](http://www.tnpconsultants.com)

# TNP<sup>1</sup>

ACCÉLÉRATEUR DE PERFORMANCE

MENEZ AVEC TNP LES TRANSFORMATIONS  
OÙ **INTELLIGENCE ARTIFICIELLE ET INTELLIGENCE  
ÉMOTIONNELLE** FERONT LA DIFFÉRENCE



TNP accompagne depuis 10 ans les leaders  
de l'économie dans leurs programmes  
de transformation à forts enjeux métiers et humains.

---

**BUSINESS HUMAN TECHNOLOGY**

[www.tnpconsultants.com](http://www.tnpconsultants.com)