BearingPoint®

# RGPD : êtes-vous sur la bonne voie ?

Le RGPD est désormais en vigueur : le 25 mai, il a remplacé l'ancien dispositif de formalités préalables et introduit de nouveaux droits et obligations. Votre organisation est-elle sur la bonne voie vers la conformité ? Quelles sont les prochaines étapes ?

BearingPoint®

**Sommaire**

# « Le bonheur est dans l'ignorance » ....pas avec le RGPD

Le RGPD, c'est maintenant. Ai-je pris les bonnes options de mise en conformité ? Quelles sont les prochaines étapes ?

Le 25 mai 2018 était la date d'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD), mais où en êtes-vous de votre mise en conformité ? Et avez-vous les idées claires sur ce qu'il recouvre ?

Pour la plupart, il a été difficile ces 18 derniers mois d'échapper au tapage médiatique et aux sensibilisations liés au RGPD, ainsi qu' à la foule d'informations sur la manière de s'y préparer au mieux. Pour certaines entreprises, la mise en œuvre des obligations du RGPD s'apparente à une ascension vertigineuse ; de nombreuses organisations se posent des questions de fond « Sommes-nous prêts ? », « Ai-je pris les bonnes décisions ? », « Que pouvons-nous faire de plus ?» voire « Qu'est-ce donc que ce RGPD, exactement ? ».

Regarder autour de soi et chez ses concurrents peut donner une indication sur ce que font les autres, mais ne vous fiez pas au calme apparent de certains, car c'est à l'intérieur des organisations que l'intense travail se déroule. Processus internes, procédures, et systèmes d'information ont besoin d'être rigoureusement revus et testés pour devenir conformes au RGPD. Les faiblesses en matière de conformité ne seront pas uniquement décelées par le régulateur, mais aussi par vos clients, par des hackers, et même par vos propres employés ! Ces manquements ne vous exposeront pas seulement à des amendes significatives mais porteront atteinte à la réputation de votre organisation, et affaibliront votre position concurrentielle.

# Où en suis-je ?

Pour beaucoup d'organisations, il est difficile d'estimer le chemin restant à parcourir dans ce voyage vers la conformité au RGPD. Pour d'autres, travailler à une gestion plus efficace de la protection des données, fournir une expérience client distinctive, et finalement faire sienne la culture du « respect de la vie privée » (ou « privacy by design ») constituent déjà leurs prochaines étapes.

Quatre champs d'actions principaux ressortent dans la mise en conformité avec le RGPD :

1. **Vos collaborateurs** – Si vos collaborateurs ne comprennent pas les implications de la protection des données, le risque de non-conformité ou de violation sera élevé. Commencez par une formation de base de vos collaborateurs.
2. **Ce que vous faites** – Il s'agit de vous assurer que vous disposez des bons processus en place pour protéger la donnée et par exemple répondre aux demandes d'exercices des droits des personnes. Cela s'applique aussi bien ux données de vos employés qu'à celles de vos clients.
3. **L'aspect juridique** – Malheureusement pour vous, c'est un aspect essentiel, de la définition des politiques jusqu'à la vérification que vos contrats fournisseurs répondent aux exigences RGPD.
4. **Où est la donnée ?** – Comprendre où sont détenues toutes les données personnelles et comment fonctionne le flux de ces données au sein de votre organisation ainsi que sa gouvernance sont essentiels.

Savoir où vous en êtes est la première étape pour se préparer au RGPD. Comme lorsque l'on escalade une montagne, plusieurs chemins permettent d'arriver au sommet, mais certains sont plus durs que d'autres.

La plupart des organisations tombent dans l'un des profils ci-dessous. Quel est le vôtre ?

**Au sommet**

Vous êtes très avancé dans la mise en conformité au RGPD. D'autres challenges sont déjà en vue

**Au camp de base**

Vous êtes sur la bonne voie

**Sur les contreforts**

Vous êtes au début du voyage

**Quelle montagne ?!**

Vous devez commencer

# Quel chemin prendre ?

| | Vos collaborateurs - Formation | Ce que vous faites - Processus | L'aspect juridique - Politiques, Normes & Contrats | Où est la donnée ? - Sécurité |
|---|---|---|---|---|
| **Quelle montagne ?**<br><br>(Vous devez commencer) | • Vos employés connaissent-ils le RGPD ? | • Pouvez-vous répondre à une demande de suppression ou d'accès ? | • Les politiques requises sont-elles déjà en place dans votre entreprise ? | • Quel est votre processus de sécurité en place ?<br>• Qui traite de la donnée en votre nom ? |
| **Sur les contreforts**<br><br>(Vous êtes au début du voyage) | • Fournir une formation initiale pour sensibiliser les employés à la protection des données<br>• Pouvez-vous utiliser les nouveaux outils de formation tels que les « smartphones » dans votre organisation ?<br>• Fournir des formations spécifiques pour les équipes traitant un volume important de données personnelles | • Analyse d'écarts - où sont les écarts ? Et qui est responsable de les combler ?<br>• Quelles données personnelles traitez-vous ?<br>• Comment allez-vous assurer l'appropriation de la démarche au sein de l'entreprise ?<br>• Avez-vous besoin d'un Délégué à la Protection des Données (DPD) ? | • Mettez à jour ou créez vos déclarations de confidentialité<br>• Développez des politiques d'accès à la donnée pour les demandes d'exercice des droits<br>• Faites la revue des contrats avec les fournisseurs - Existe-il des obligations de protection de données (« remédiation contractuelle » ) | • Avec qui partagez-vous de la donnée - particulièrement en dehors de l'Union Européenne ?<br>• Avec quelle rapidité pouvez-vous identifier et répondre à une violation des données ? |
| **Au camp de base**<br><br>(Vous êtes sur la bonne voie) | • Mettre en place un programme de formation avec des formations régulières pour tous les employés | • Avez-vous un plan d'action pour mettre en œuvre vos nouveaux processus sans impacter négativement votre organisation ?<br>• Comment pouvez-vous minimiser le volume de données personnelles nécessaires au développement d'un produit ? | • Vous avez conçu vos normes, comment allez-vous les mettre en œuvre ? | • Vos contrôles de sécurité sont-ils suffisants pour répondre aux exigences du RGPD ? |
| **Au sommet**<br><br>(Vous êtes très avancé dans la mise en conformité RGPD, avec déjà d'autres challenges en vue) | • S'assurer que les processus sont en place pour contrôler et suivre le niveau de participation | • Mettre vos processus au niveau supérieur - fournissez-vous une expérience client distinctive ?<br>• Améliorer l'intégration avec vos partenaires - Comment pouvez-vous vous assurer que les changements dans les processus ne conduisent pas à une non-conformité ? | • Développer une culture de la protection de l'information ( « respect de la vie privée dès la conception » ou « privacy by design ») au sein de votre organisation<br>• Comment contrôlez-vous la conformité au sein de votre organisation et avec vos fournisseurs ? | • Remédiation de la sécurité des systèmes d'information (SI) – améliorer continuellement votre sécurité SI<br>• Optimiser votre plan de gestion de crise et entraîner les acteurs avec des scénarios innovants |

# Vos employés sont clés

En suivant l'un des chemins évoqués ci-dessus, votre organisation est assurée d'améliorer ses processus, ses politiques et sa protection des données. Cependant, améliorer la prise de conscience chez vos employés est essentiel dans tous les cas, car ils sont à la fois votre clé de voûte et votre talon d'Achille. Même si 60 % des responsables des Systèmes d'Information considèrent leurs équipes comme le plus grand facteur de risque de non-conformité au RGPD, les employés sont essentiels pour atteindre une conformité plus efficace, dans la durée. Ceux qui comprennent l'importance de cette nouvelle régulation seront plus enclin à suivre (et orienter) les nouveaux processus mis en place. En retour, ils développeront des produits, des services et une expérience client embarquant la protection des données. En cas de violation des données, les employés sensibles à la protection de celles-ci sont susceptibles d'être proactifs et de cultiver le principe de « respect de la vie privée dès la conception » (« privacy by design ») - un point capital du RGPD.

# Le moment d'entamer l'ascension

L'ascension vers le sommet n'est jamais facile. En comprenant votre situation actuelle, en choisissant le chemin le plus approprié à suivre, et sur quels domaines vous devez agir, une conformité complète au RGPD peut être atteinte dans un délai raisonnable. En progressant, une série d'autres avantages pourra être identifiées, vous permettant de développer vos employés et d'améliorer votre expérience client. Même si la concurrence s'est déjà lancée, choisir la bonne voie vous aidera à reprendre l'initiative.

BearingPoint®

BearingPoint est un cabinet de conseil en management et technologie indépendant aux racines européennes avec une couverture mondiale. Le cabinet est structuré autour de 3 activités principales : Consulting, Solutions et Ventures. Le Consulting couvre les activités traditionnelles de conseil en management. Les Solutions fournissent des logiciels dédiés à la transformation digitale, au reporting réglementaire et à l'analyse de données. L'activité Ventures est dédiée au financement et au développement des startups. BearingPoint compte parmi ses clients les plus grandes organisations mondiales publiques et privées ; fort d'un réseau international de plus de 10 000 collaborateurs, BearingPoint accompagne ses clients dans plus de 75 pays et les aide à obtenir des résultats mesurables et durables.

Pour de plus amples informations : www.bearingpoint.com

Retrouvez-nous sur twitter : @BearingPoint_FR

## Vos contacts privilégiés

**Damien Palacci**
damien.palacci@bearingpoint.com
**Philippe Mannent**
philippe.mannent@bearingpoint.com
**Yael-Stephanie Gozlan**
yael-stephanie.gozlan@bearingpoint.com

## Auteurs et équipe de rédaction

**Aloke Kapur, BearingPoint**
**Dr Baljit Sarpal PhD, Director, Sarpal Consultancy Ltd**
**Matthew Roe, BearingPoint**
**Joe Barrs, BearingPoint**
**Laura Shaw, BearingPoint**