Expert Insights

Protection de la vie privée et des données :

un catalyseur de changement

IBM

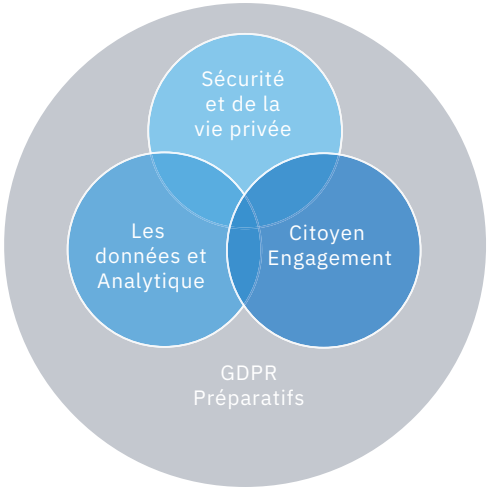
1

–

Vers un nouveau départ

Les pouvoirs et organisations publics peuvent-ils profiter du défi de la conformité pour initier une transformation plus profonde ?

Une grande part des problèmes que doivent affronter aujourd'hui les entités publiques pouvoirs et organismes publics a trait aux données. Nombre de ces organisations en récoltent beaucoup trop de ces données. De plus, elles sont gérées de manière cloisonnée, tout en étant difficiles à consolider et à analyser. Cet état de fait provoque un manquement important : les organisations sont incapables d'analyser adéquatement leurs données et de tirer profit de leur valeur.
Dans le même temps, les nouvelles réglementations ont un impact majeur sur les structures publiques organisations et les individus. Grâce à ces nouvelles règles, toute personne qui transmet ses informations personnelles données se voit accorder de nouveaux droits. Et c'est un nouveau défi qui se pose donc aux autorités et aux fournisseurs de services publics qui Les organisations ont finalement intégré la nouvelle règlementation dans leur réalité. Et elles cherchent désormais à tirer parti de l'investissement consenti pour répondre à ces exigences. Car l'attentisme n'est plus une attitude tenable. Et les méthodes traditionnelles d'analyse des données ne sont plus suffisantes.
Les systèmes méthodes d'analyse « smart » basées sur l'intelligence artificielle et l'apprentissage automatique sont une des pistes de solution. Mais de nombreuses institutions ne savent pas par où commencer ou quelle approche leur conviendrait convient le mieux. Par ailleurs, un grand nombre d'organisations ont réalisé plus d'investissements pour répondre aux enjeux de la « compliance » que ce qu'elles n'en retirent comme bénéfices. Et cela doit changer.
Une vision à plus long terme ainsi qu'une approche plus mature de la sécurité et de la protection de la vie privée, des données et des analyses, mais aussi l'implication et la confiance des citoyens : voici quelques-uns des éléments qui peuvent aider les organisations à relever le défi de la digitalisation. Grâce à une approche globale et holistique, il est possible d'améliorer sur le long terme un certain nombre de facteurs. Des exemples ? Une meilleure collaboration organisationnelle, la rationalisation des processus et de la gestion des informations privées données, une meilleure sécurité et des relations plus étroites avec les citoyens *(voir graphique 1).*
Le fait d'aller au-delà du simple respect des obligations légales ouvre de nouvelles opportunités pour votre organisation. Et c'est particulièrement vrai lorsqu'il est question de la manière dont peut évoluer la relation avec ceux qui transmettent leurs données. Avec leur accord et dans le respect de la réglementation, les pouvoirs et organismes publics ont la possibilité de créer des produits et services plus personnalisés… et donc aussi de faire évoluer les rapports qu'ils entretiennent déjà avec les citoyens et les parties prenantes.



Graphique 1 - GDPR et confiance digitale

Sécurité et protection de la vie privée - données et analyses – implication du citoyen - préparation du GDPR

- Créez une confiance digitale forte et une stratégie qui améliore la collaboration au sein des organisations.
- Renforcez la sécurité et la protection de la vie privée ainsi que l'implication des citoyens.
- Trouvez de nouvelles façons d'améliorer la sécurité et la protection de la vie privée et faites-en un élément de différenciation de votre entreprise qui vous donne un avantage concurrentiel.

2

–

L’impact de la sécurité des données :

Ce n’est pas seulement une question IT

Nous avons déjà expliqué combien il est important pour les autorités et les organismes publics de relever le défi de la digitalisation. Même si ça a toujours été le cas, les mesures que nous devons prendre maintenant sont plus complexes et doivent s’appliquer à tous les niveaux de l’organisation. Dans ce contexte, nous considérons la sécurité comme une chaîne de mesures : son niveau de robustesse équivaut à celui de son maillon le plus faible.

Il n’est donc plus possible de réduire exclusivement ce défi à des devoirs IT. C’est une priorité que se partagent les politiciens, les dirigeants des instances exécutives et le management de leur département informatique organisation IT. Mais dans la pratique, les règles sont pourtant souvent appliquées de manière très technique et ad hoc, sans tenir compte du reste de la chaîne de sécurité.
La dure réalité, c’est que les services IT des instances et organisations publiques doivent travailler avec des budgets de plus en plus serrés. Plutôt qu’élaborer des solutions trop spécifiques, ils ont besoin d’une plateforme intégrée capable de délivrer des fonctionnalités avancées, comme, par exemple, des informations de sécurité, ce qui produirait rapidement de la valeur ajoutée. Dans le même temps, cette fonctionnalité doit être suffisamment évolutive et fonctionnelle pour pouvoir répondre facilement à de nouvelles exigences.

La sécurité de l’accès aux données est un défi majeur, mais c’est désormais aussi le cas de la localisation de l’information, qui, jusqu’à il y a peu, les données étaient hébergées était hébergée sur des systèmes centraux, avec à la clé un défi majeur concernant en termes de sa sécurité de ces données. La logique du stockage en silo de l’information, en silo, soulève inévitablement des interrogations : qui détient quoi quelle information et Et où se trouve-telle ? Et ceci Cela génère bien d’autres difficultés.

La fuite des données est devenue un problème récurrent. Ce sont généralement les entreprises qui sont confrontées au problème. Mais que se passerait-il si l’organisme en charge du chômage, la police ou les autorités fiscales divulguaient à grande échelle les données qu’elles traitent ? Cela porterait un coup majeur à la confiance que nous accordons aux autorités publiques et à leur rôle de gardien de nos informations personnelles des données.
Comment éviter que la digitalisation à grande échelle et la facilité que nous voulons dans nos contacts avec les autorités soient entravées par la fuite des données, le vol d’identité et la fraude ? Comment contrôler en temps réel des données sans créer des barrières infranchissables et limiter les développements futurs de la digitalisation ?

3

–

Préparation pour l’avenir

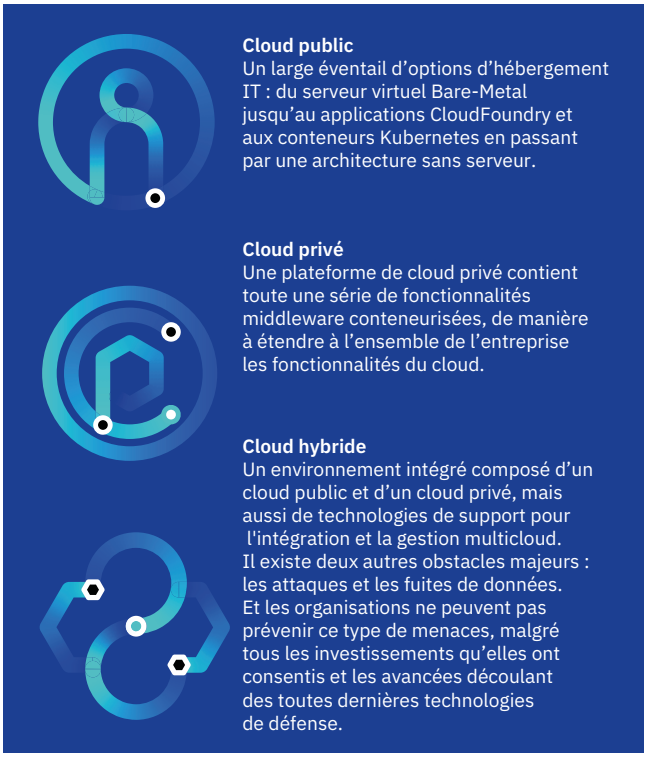
Pour que les mesures de sécurité soient efficaces, il faut une vision

De nombreuses autorités et organisations publiques n'ont recours ni au cloud ni à d'autres services technologiques modernes. Ce n'est pas encore un problème, même s'il faut s'attendre à ce que certains services informatiques ne soient bientôt plus disponibles que via une application cloud.

Pourquoi est-il si important d'implémenter ces technologies ?
Pour ne pas se faire surprendre par l'obligation de passer sans délais aux services cloud ou de type cognitif, il est important que tous les pouvoirs et organismes publics créent ensemble les conditions d'un basculement sûr et fiable.
La croissance exponentielle des données et l'obligation de les conserver font grimper les coûts de stockage. Les technologies embarquées chargées de réduire la leur quantité de données et un stockage rentable du « data offloading » sont donc aujourd'hui plus cruciales que jamais.
Ce sont les données qui font la différence. Vous avez donc besoin des solutions adéquates pour les stocker. Une idée qui tient la route ? Utiliser une plateforme pour les applications et l'infrastructure, une plateforme basée sur 2 ou plusieurs composants du cloud public, du cloud privé et de l'IT on-site. C'est ce que nous appelons l'hybrid multicloud : une solution permettant d'accéder, d'utiliser et de les gérer les données rapidement, de manière productive et flexible, tout en les hébergeant dans une infrastructure de stockage sécurisée. Grâce à cette solution flexible, économique et intelligente, les entreprises peuvent plus facilement moderniser leurs applications actuelles, mais aussi en intégrer de nouvelles *(voir graphique 2)*.

Pourquoi ?
Parce que trop d'événements de sécurité se produisent trop vite pour que l'on puisse les détecter. Et la quantité de données est trop importante pour que l'on puisse les investiguer et les gérer. Il n'y a pas assez de personnes chargées du suivi de ceci. Même en mettant en place une analyse pointue, il est difficile de distinguer failles de sécurité pures et activités suspectes. Un exemple parmi d'autres ? Chaque année, des milliers d'heures sont gaspillées à gérer à courir derrière des faux positifs alors que dans le même temps de vraies cyberattaques restent invisibles pendant des mois.
Avec des solutions cognitives telles que l'intelligence artificielle et le « machine learning », vous disposez des meilleures options pour renforcer votre défense et bâtir un " système immunitaire". Ces solutions rendent le combat plus équitable en donnant aux analystes le renforcement de la sécurité dont ils ont besoin pour prévenir les menaces. En chargeant la technologie cognitive de passer au peigne fin d'énormes quantités de données et de trouver des liens pertinents pour identifier les principales menaces, on permet aux experts en sécurité de se concentrer sur l'essentiel : le traitement rapide, précis et évolutif des menaces réelles.
La transformation digitale est un processus irréversible.
Ce que les citoyens attendent des pouvoirs publics ? Une expérience équivalente à celle qu'ils connaissent lorsqu'ils effectuent leurs transactions en ligne habituelles. Les utilisateurs veulent que les choses soient faciles. Cela oblige les autorités publiques à privilégier une approche différente, et ce en tenant compte d'un cadre budgétaire limité et du risque d'augmentation des (cyber)menaces. Le temps est donc venu de transformer l'ensemble des modes de fonctionnement, les processus et la culture des pouvoirs publics. Mettre en pratique une approche digitale innovante dans cette nouvelle ère est un objectif ambitieux. Mais c'est la seule manière de prendre en compte l'évolution du monde et de répondre aux attentes toujours plus élevées des gens.

Graphique 2 – Les différents types de cloud



Par où commence-t-on ?

Voici ce que toutes les autorités et organisations publiques doivent mettre en œuvre à chaque étape du processus de compliance pour atteindre leurs objectifs, aussi bien à court qu'à moyen terme :

Collaboration et implication	Bâtir les bases de la transformation	Le processus de digitalisation
Déterminez qui s'occupe de la digitalisation au sein de votre organisation.	Mettez-vous tous d'accord sur le contenu de la roadmap.	Mettez en œuvre.
Informez tous les acteurs clés de l'organisation du processus de digitalisation.	Définissez quels éléments sont à court terme impactés par des situations à risque dans le paysage actuel.	Appliquez.
Améliorez votre stratégie de digitalisation.	Définissez une approche centrée sur les données et l'information.	Évaluez régulièrement les progrès obtenus.
Assurez-vous que toutes les parties prenantes (et leurs ressources : budget, personnel, temps, etc.) sont impliquées dans la stratégie.	Affirmez votre engagement à suivre cette direction.	Ajustez et continuez.

IBM Government can help organizations leverage new business models, innovative capabilities and the wealth of data available to create a robust and efficient public infrastructure, help ensure safety and security, support the needs of individuals, facilitate sustainable economic growth and build stronger communities.

Authors & contributors
Diana Corredor Suárez, Security consultant
specialized in Privacy and Data Protection, IBM Security
Ralf Verberne, Managing Consultant
IT Risk Management, IBM Security
Kim Boermans, IBM Associate Partner
for Security Services Benelux, IBM Security

More information
https://ibm.biz/government-nl
https://ibm.biz/government-be
https://ibm.biz/secteurpublic-be