Livre Blanc

Infrastructures, Cloud, sécurité et gestion des données : les entreprises françaises face au GDPR

Sponsorisé par : Juniper Networks

Karim Bahloul
June 2017

INTRODUCTION

Le GDPR (General Data Protection Regulation) a été mis en place par l'Union Européenne pour unifier la régulation des entreprises qui traitent, stockent ou collectent des données. Il a pour objectif de faire face à l'internationalisation du marché autour des données personnelles, et harmoniser les politiques entre les différents pays européens. Il concerne toutes les entreprises européennes ou non, qui détiennent des données portant sur des citoyens européens. Les entreprises doivent se mettre en conformité avant le 25 mai 2018 pour répondre aux nouvelles exigences en matière de protection des données personnelles.

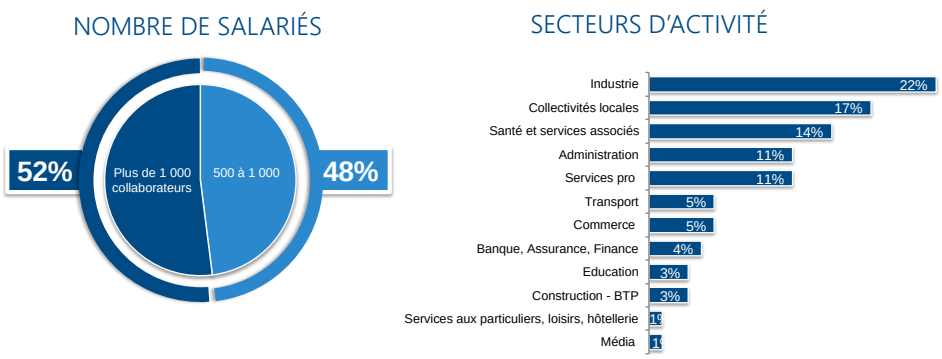
L'enquête menée par IDC auprès des entreprises privées et des organisations publiques fait le point sur l'état d'avancement des initiatives GDPR en France. Le premier enseignement est clair : toutes n'ont pas le même niveau de maturité et la perspective d'être conforme aux dispositions du GDPR s'éloigne pour nombre d'entre elles, faute d'une gouvernance et d'une feuille de route structurées. De nombreuses questions se posent alors : quelles sont les bonnes pratiques, celles retenues par les structures les plus matures ? Quels sont les impacts du GDPR sur la politique de sécurité et sur les choix informatiques ? Comment gérer sa stratégie Cloud face aux enjeux du GDPR ?

METHODOLOGIE

Pour cette étude, IDC a interrogé, en mai et juin 2017, 150 entreprises de plus de 500 salariés présentes en France.

GRAPHIQUE 1

Méthodologie



Source: IDC, 2017

Les entreprises appartiennent à tous les secteurs d'activité (secteur public et secteur privé). Plus de la moitié des entreprises interrogées ont plus de 1 000 salariés (52%), les autres disposant de 500 à 1 000 collaborateurs sur la France (48%). Afin de permettre une exploitation dans le cadre de cet observatoire et une représentativité du marché, les résultats ont été redressés conformément aux statistiques de l'INSEE.

LE GDPR EN SYNTHESE

Le GDPR (General Data Protection Regulation) a été mis en place par l'Union Européenne pour unifier la régulation des entreprises qui traitent, stockent ou collectent des données. Il représente le plus grand bouleversement de ces dernières années dans le domaine juridique de la protection et de la confidentialité des données.

Qu'est-ce qu'une donnée personnelle ?

Selon le règlement, une donnée à caractère personnel représente "toute information se rapportant à une personne physique identifiée ou identifiable. Une « personne physique identifiable » est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale"

Quelles sont les spécificités du GDPR ?

Ce nouveau règlement, qui s'applique à tous les secteurs d'activités, et pour les organisations de tout type et de toute taille, impacte la gestion des données personnelles sur de nombreux aspects dont :

- Une protection accrue des données personnelles en termes de consentement, d'accessibilité et de portabilité.
- Les clients et utilisateurs des données des entreprises ont le droit de demander l'effacement de leurs données, ou la récupération de celles-ci dans un format clair et réutilisable.
- L'intégration des exigences de respect de la vie privée dès la conception des systèmes de traitement de données personnelles.
- Une simplification des formalités administratives pour les entreprises (avec la création d'un guichet unique).
- Une obligation pour les entreprises de démontrer la bonne application du règlement.
- L'exigence d'un représentant dans l'union.
- La désignation d'un DPO (Délégué à la Protection des Données) au sein des entreprises, qu'il soit interne ou externe.
- La notification des failles de sécurité dans les 72 heures.
- La mise en place d'un registre des traitements obligatoire pour les entreprises de plus de 250 salariés (ou pour les entreprises de moins de 250 salariés pour lesquelles le traitement des données est au cœur leur activité).
- Une sanction à hauteur de 4% de leur chiffre d'affaires pour les entreprises qui ne respecteront pas les exigences du GDPR.

GDPR : LES ORGANISATIONS FRANÇAISES SONT-ELLES PRETES ?

A première vue, les entreprises françaises sont loin d'être prêtes : seules 9% d'entre elles se disent aujourd'hui conformes aux dispositions du GDPR. Elles sont par ailleurs 19% à planifier les initiatives à mettre en place pour être conforme avant la fin 2017 tandis que 30% ont prévu les actions nécessaires pour une mise en conformité courant 2018. En définitive, près d'1 entreprise sur 2 (42%) prend tout juste conscience de l'existence du GDPR et du calendrier associé sans avoir véritablement commencé à lancer des initiatives. Ce phénomène est encore plus important au sein des PME (entreprises disposant de 500 à 1 000 collaborateurs) et des entreprises du secteur privé qui sont respectivement 47% et 46% à "découvrir" les dispositions prévues par le GDPR.

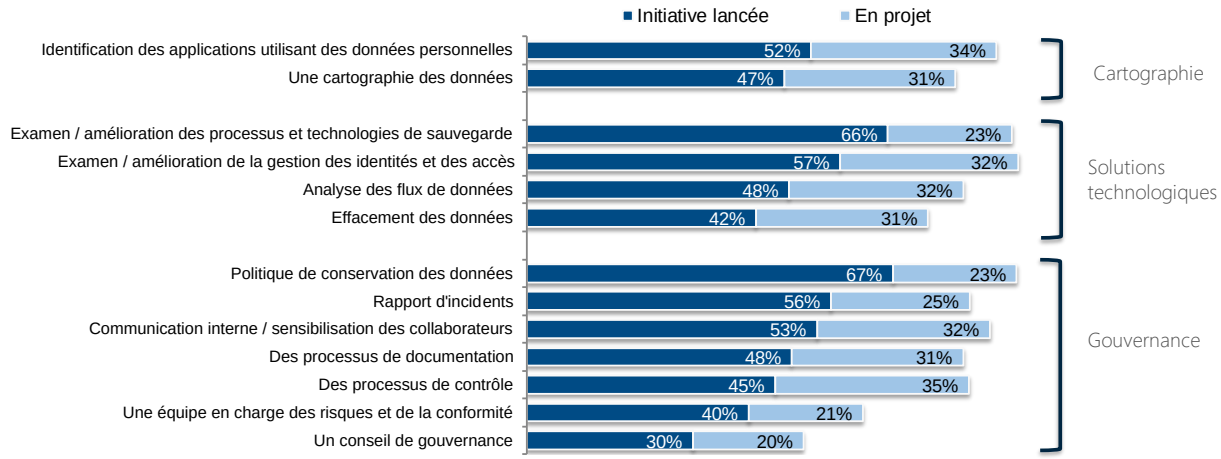
Conformité GDPR : la prime aux "first movers"

En conséquence, de nombreuses entreprises doutent de leur capacité à être conforme d'ici mai 2018 : seules 28% des structures interrogées estiment qu'elles le seront sans aucun doute possible tandis qu'à l'opposé, 27% ont la quasi-certitude qu'elles ne pourront pas l'être. Entre les deux extrêmes, 44% espèrent être le plus alignées possible sans pour autant avoir la conviction d'y arriver. Les résultats de l'enquête montrent que le retard accumulé par les entreprises depuis la signature mi-2016 du règlement européen sera difficile à rattraper. Ainsi, les entreprises qui viennent tout juste de prendre conscience du GDPR sont moins d'un tiers (32%) à considérer qu'elles seront prêtes pour mai 2018. A l'inverse, celles ayant déjà planifié des initiatives de mise en conformité sont plus de 80% à anticiper qu'elles seront prêtes dans les temps.

GRAPHIQUE 2

Les initiatives en matière de protection des données personnelles

Q. Quelles sont les initiatives que vous avez mises ou prévoyez de mettre en place ?



Source: IDC, 2017

Le chantier qui permettra aux entreprises d'être conformes aux prérogatives du règlement européen est dense. Mais dans la réalité, presqu'aucune entreprise ne part véritablement de zéro. Toutes ont déjà lancé des chantiers qui répondent aux exigences du GDPR sans pour autant les avoir systématiquement initiés dans ce but. Les chantiers les moins avancés et ceux pour lesquels les entreprises interrogées témoignent de réelles difficultés sont plus particulièrement liés à la gouvernance d'une initiative GDPR (mise en place d'un conseil de surveillance et d'une équipe en charge des risques et de la conformité).

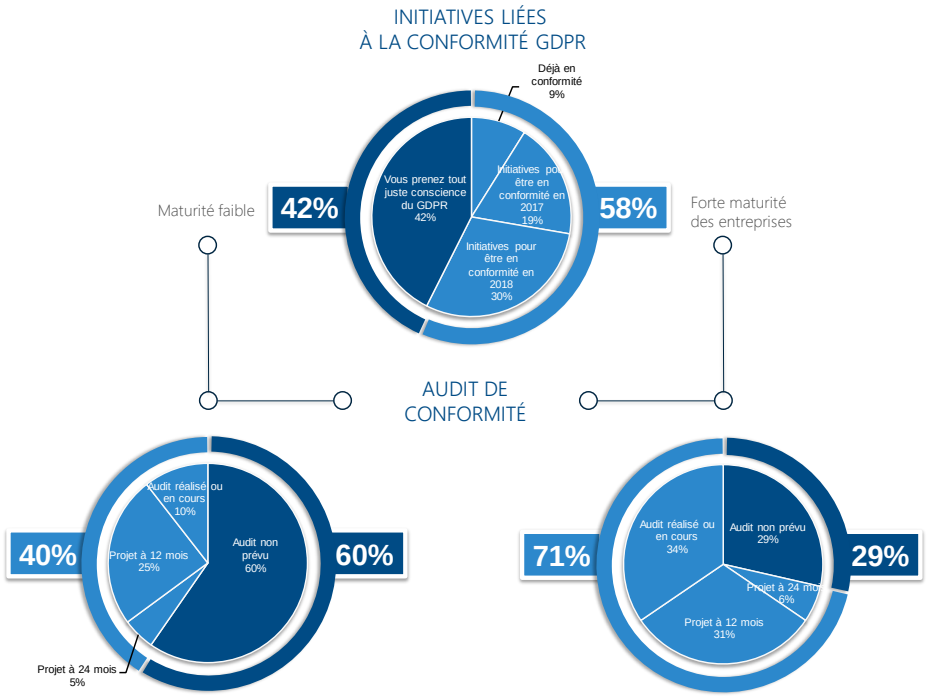
L'audit, point de départ d'une mise en conformité GDPR

La difficulté à faire le lien entre les exigences du GDPR, les initiatives déjà lancées et le trajet restant à parcourir est surtout liée au fait que peu d'entreprises ont aujourd'hui pleinement conscience de leur point de départ. Moins d'1 entreprise sur 4 a procédé à un audit interne global destiné à évaluer leur position actuelle et leurs besoins pour se mettre effectivement en conformité. Les entreprises du secteur privé sont les plus matures : les deux tiers d'entre elles ont déjà réalisé un audit (31%) ou projettent de le faire dans les prochains mois (35%) afin de déterminer leur feuille de route. A l'inverse, moins d'1 structure publique sur 2 (49%) s'inscrit dans une telle démarche : 17% ont déjà réalisé cet audit tandis que 34% le projettent dans les prochains mois.

Au-delà de cet audit global qu'il est nécessaire de réaliser pour s'assurer de la trajectoire à suivre, les résultats de l'enquête montrent que les entreprises mènent des initiatives souvent déconnectées les unes des autres, sans véritable cohérence d'ensemble : alors qu'1 entreprise sur 2 en moyenne a procédé à une cartographie pour identifier la nature des données dont elles disposent (personnelles ou pas), leurs criticités, leurs localisations, les droits utilisateurs et les usages qui leurs sont associés, elles ne sont que 38% à l'avoir intégrée dans un audit plus général de leur position. Il en est de même pour l'identification des applications utilisant des données concernées par le GDPR : 52% des entreprises ont lancé des initiatives en ce sens, mais seules 40% d'entre elles les ont intégrées à un audit de plus grande envergure.

GRAPHIQUE 3

Audit de conformité et maturité des entreprises



Source: IDC, 2017

Les résultats de l'enquête révèlent (figure 3) par ailleurs une différence de perception entre les entreprises ayant une maturité avancée sur le sujet (initiatives GDPR lancées ou panifiées) et celles prenant tout juste conscience de la problématique GDPR. Ces dernières ne sont que 40% à prévoir la réalisation d'un audit préalable. Les entreprises plus matures sont presque deux fois plus nombreuses à s'inscrire dans cette démarche (71%), la considérant comme indispensable à la

définition de la bonne trajectoire. Selon IDC, le risque pour les entreprises moins matures est d'accumuler des retards face au manque de visibilité sur les initiatives à mener, faute d'un diagnostic clairement établi.

LE GDPR IMPOSE-T-IL DE MODIFIER SA STRATEGIE D'INFRASTRUCTURE ?

Penser GDPR, c'est réfléchir à l'ensemble de son système d'information afin d'évaluer s'il permet de répondre aux contraintes imposées par le règlement européen. Les solutions de sécurité qui vont permettre de protéger les données, de gérer les accès et de crypter les données sont bien entendu en première ligne. Mais tout autant, l'entreprise doit se poser la question de ses infrastructures et plus généralement de l'architecture de son système d'information : les infrastructures serveurs et stockages hébergent et traitent les données tandis que les réseaux se chargent de conduire les données d'un point à un autre.

Conformité GDPR et stratégie Cloud : que décident les entreprises ?

Le premier élément de réflexion porte sur la stratégie Cloud : faut-il continuer à utiliser les services Cloud face aux impératifs réglementaires du GDPR ? Les données personnelles (portant sur les collaborateurs, les clients ou les partenaires) hébergées ou utilisées par les services Cloud sont-elles pleinement protégées ? Qui est responsable en cas de défaillance du partenaire Cloud ? Autant de questions que se posent aujourd'hui les entreprises.

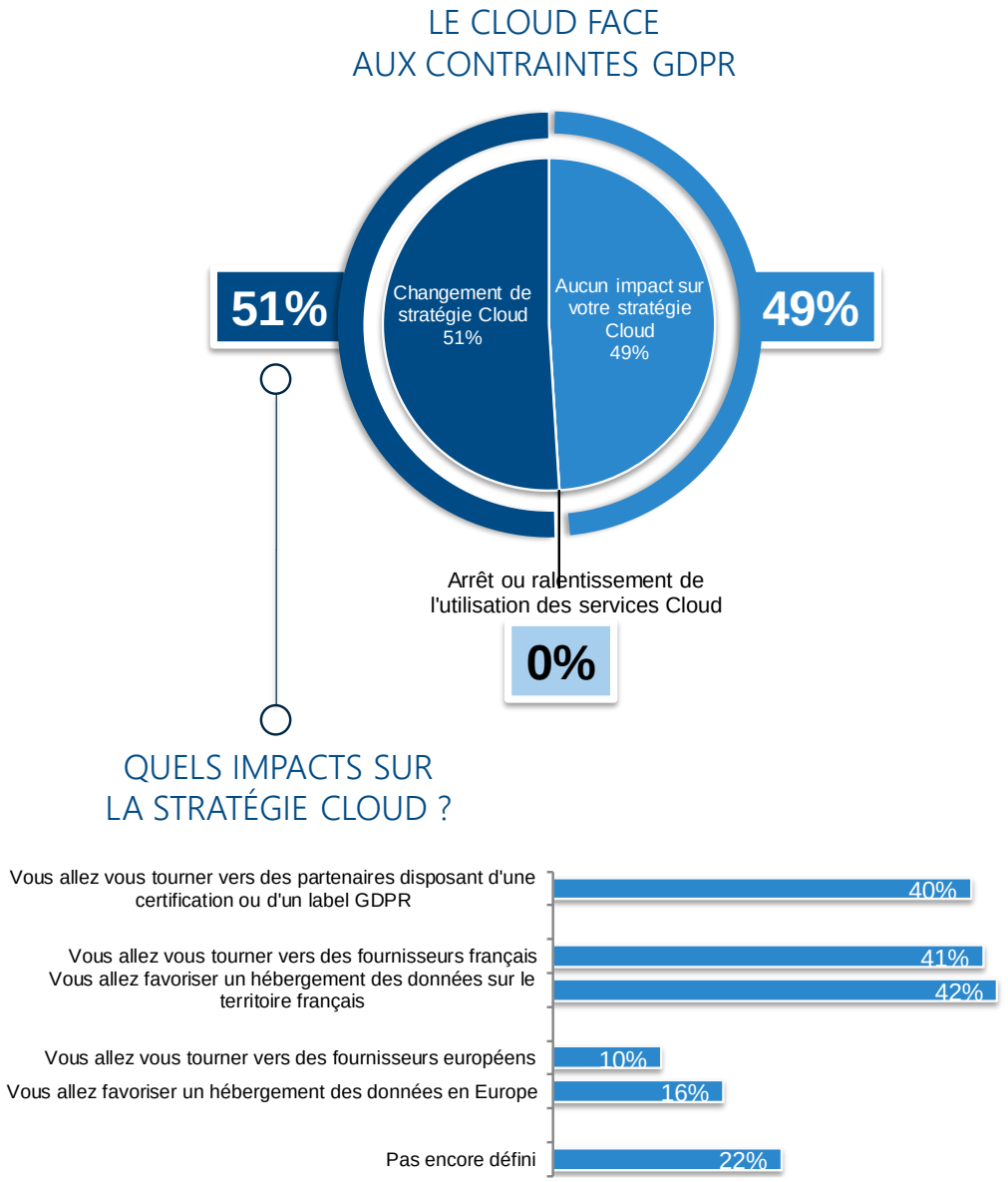
L'article 22 du règlement européen précise que "***tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ("controller") ou d'un sous-traitant ("processor") sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même ait lieu ou non dans l'Union***". La responsabilité du sous-traitant, en l'occurrence le fournisseur Cloud, est donc bien engagée. Dans le même temps, l'article 81 du règlement précise que le responsable du traitement (en d'autres termes l'entreprise confiant ses données à un fournisseur Cloud) " ***ne devrait faire appel qu'à des sous-traitants présentant des garanties suffisantes (…) pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont aux exigences du présent règlement, y compris en matière de sécurité du traitement***".

L'enquête menée par IDC montre que les structures interrogées ne prévoient pas de faire machine arrière concernant leur recours aux services Cloud : elles vont continuer à utiliser les services de Cloud public ou de Cloud privé hébergé. Pour la moitié d'entre elles, elles vont conserver leurs partenaires actuels et les modèles de Cloud qu'elles utilisent aujourd'hui. Pour l'autre moitié (51%), il est nécessaire d'adapter leur stratégie Cloud (sans pour autant la freiner) aux enjeux et aux risques que représente le GDPR. Les organisations les plus matures (celles ayant déjà engagé des initiatives GDPR) sont d'ailleurs plus régulièrement convaincues qu'elles doivent faire évoluer leur stratégie Cloud (60%, contre 44% pour les moins matures).

Les principaux axes de réflexion consistent à privilégier des acteurs français proposant des services Cloud ou ceux, quelle que soit leur nationalité, proposant des capacités d'hébergement sur la France. D'ailleurs, plusieurs fournisseurs américains (Amazon, Microsoft et SalesForce) ont annoncé courant 2016 l'ouverture dès 2017 de centres de données sur la France pour à la fois améliorer la performance de leurs services (latence) mais également pour répondre aux enjeux de la localisation des données.

GRAPHIQUE 4

Quelles stratégies Cloud face aux contraintes du GDPR ?



Source: IDC, 2017

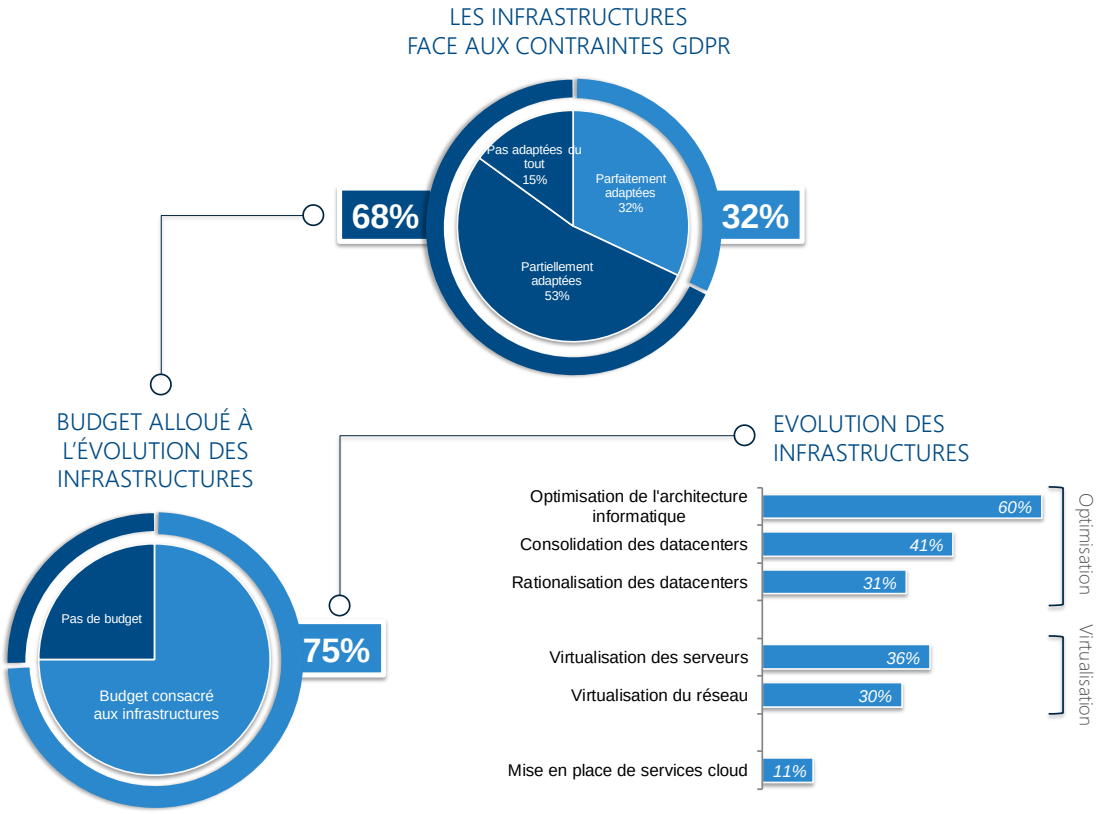
Le même article 81 stipule que "***l'application par un sous-traitant d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à démontrer le respect des obligations incombant au responsable du traitement***". Les entreprises interrogées en ont bien conscience : 40% de celles qui anticipent une évolution de leur stratégie Cloud souhaitent changer de partenaire pour se tourner vers un fournisseur ayant adhéré à un label ou disposant d'une certification GDPR. Ce label ou cette certification lui permettront de s'assurer - et d'assurer à ses clients finaux - que les données personnelles sont effectivement protégées conformément aux dispositions du GDPR. Cela représente par ailleurs un véritable enjeu pour les fournisseurs de services Cloud et ceux proposant des services d'hébergement dans la mesure où ce label, cette certification, deviendront des éléments différenciateurs sur le marché. A moins que cela ne soit l'inverse : ceux n'en disposant pas seront progressivement évincé du marché.

GDPR : 75% des entreprises projettent de faire évoluer leurs infrastructures IT

Au-delà des choix liés à l'externalisation Cloud, nombre d'entreprises se posent la question de leurs propres infrastructures : sont-elles adaptées aux contraintes imposées par le GDPR ? Faut-il les faire évoluer ou faut-il juste y apposer des couches supplémentaires de sécurité ? Les résultats de l'enquête montrent que seules 1/3 des entreprises considèrent leurs infrastructures (serveurs, stockage et réseaux) comme étant parfaitement adaptées pour supporter les enjeux du GDPR. Dans la majorité des cas (53%), les infrastructures ne sont que partiellement adaptées. Elles sont même considérées comme totalement inadaptées par 15% des structures interrogées.

GRAPHIQUE 5

Les impacts du GDPR sur les infrastructures informatiques



Source: IDC, 2017

Il est alors nécessaire, pour les 3/4 de ces entreprises, de faire évoluer leurs infrastructures pour les rendre plus agiles et pour casser des silos encore trop présents. L'objectif est alors de faciliter la gestion d'un environnement souvent considéré comme très complexe à travers une approche d'optimisation (architecture, consolidation) et de virtualisation serveurs et réseaux. L'évolution vers une infrastructure "Software Defined" doit permettre de disposer d'une vision centralisée des ressources (serveurs, stockage et réseaux), beaucoup plus précise et systématique, permettant de mieux maîtriser les données (identification, localisation) et les flux qui y sont liés.

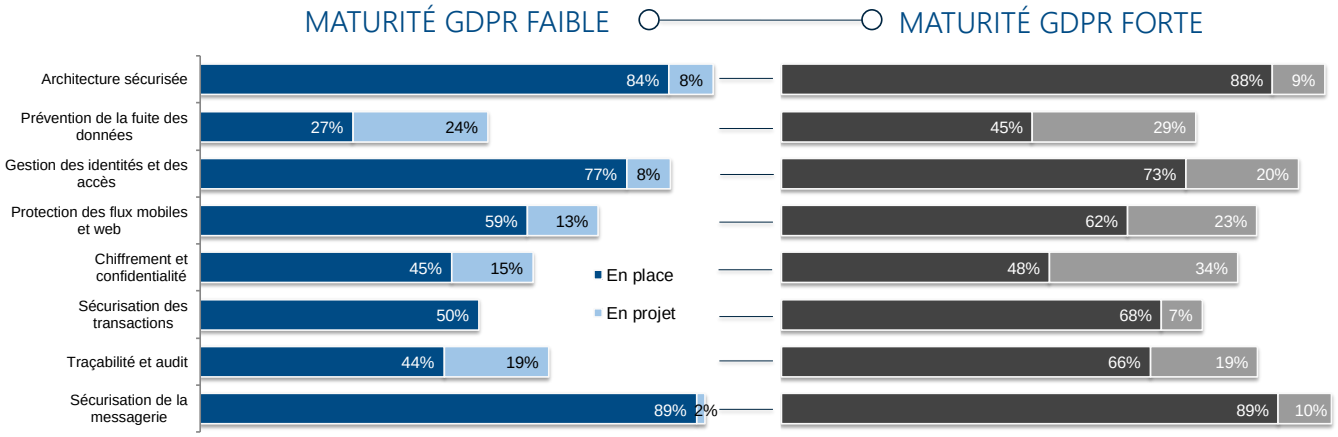
GESTION DES IDENTITIES ET DES ACCES, CHIFFREMENT, DLP : VERS UNE NOUVELLE VAGUE D'INVESTISSEMENT

L'évolution des infrastructures informatiques de l'entreprise est bien entendu insuffisante pour répondre aux prérogatives du GDPR sur la protection des données personnelles. Le cœur de l'action porte sur les mesures de sécurité et de gouvernance que les entreprises mettent en place pour assurer la protection des données.

Ici aussi, les résultats de l'enquête montrent que les entreprises ne partent pas de zéro, elles peuvent fortement capitaliser sur les initiatives déjà lancées par le passé, notamment celles liées à la gestion des identités et des accès (IAM), à la protection des flux mobiles et web (pour éviter le détournement de données) ou encore à la sécurisation de la messagerie qui voit transiter de nombreuses données personnelles. Mais de nombreux chantiers sont encore à explorer : prévention contre la fuite des données, chiffrement et confidentialité des données, audit et traçabilité des données. Même si elles s'inscrivent dans le cadre du GDPR, ces initiatives débordent du champ des données personnelles pour renforcer la sécurisation de l'ensemble des données de l'entreprise. D'ailleurs, la réglementation GDPR est perçue par 80% des entreprises comme une véritable opportunité d'améliorer globalement le niveau de sécurité et de confidentialité des données et de renforcer l'image de l'entreprise auprès de ses clients (41%).

GRAPHIQUE 6

Les investissements réalisés ou planifiés en solution de sécurité : comparaison entre les structures disposant d'une maturité GDPR faible et forte



Source: IDC, 2017

Un focus plus précis sur les résultats de l'enquête montre que toutes les entreprises ne sont pas égales face à la sécurisation de leurs données. En effet, celles considérées comme les plus matures – elles ont une bonne connaissance du GDPR et ont défini une feuille de route – sont également celles qui investissent le plus fortement dans les solutions de sécurité qui leur permettront d'être "compliant".

- Les entreprises les plus matures sur le sujet GDPR ont commencé à investir (66%) dans des approches leur permettant de disposer d'une bonne vision de leurs données à travers un audit (***cartographie des données***) et la mise en place de solutions de ***traçabilité*** permettant de suivre les données, leur localisation, les accès (personnes physiques et applications).

- Ainsi, elles projettent de renforcer de manière importante leurs investissement dans les ***solutions de chiffrement et de confidentialité*** des données (34% des entreprises ont des projets, 48% ont déjà investi dans des solutions de ce type).

- De même, la ***gestion des identités et des accès*** devient une priorité pour ces entreprises : 20% projettent de s'équiper de solutions professionnelles dans les prochains mois.

- Les solutions ***DLP (prévention contre la fuite de données)*** sont également un levier important permettant d'éviter que les données protégées ou confidentielles ne quittent le système d'information de l'entreprise, que cela soit de manière non-intentionnelle ou malveillante. Les entreprises les plus matures sur le sujet GDPR projettent de renforcer leurs investissements (29% d'entre elles) afin de réduire l'exposition au risque.

Selon IDC, l'écart se creuse entre les entreprises "matures" sur le sujet GDRP et les autres. Les plus matures ont déjà capitalisé sur les solutions de sécurité déployées par le passé et continuent à investir pour disposer d'une approche sécuritaire plus complète. Inversement, les entreprises les moins matures, alors qu'elles sont soumises aux mêmes engagements et aux mêmes pénalités que les autres, restent encore sur la réserve et limitent leurs investissements en solutions de sécurité. Ces dernières prennent un risque non négligeable : ne pas pouvoir justifier auprès du régulateur leur bonne volonté pour se mettre en conformité.

CONCLUSION : VERS UNE NOUVELLE GOUVERNANCE DE LA DONNEE

Les entreprises et les structures publiques interrogées dans le cadre de cet observatoire témoignent de nombreuses difficultés lorsqu'il s'agit de se mettre en conformité avec le Règlement Général sur la Protection des Données (GDPR). La première d'entre elles repose sur la capacité de l'entreprise à notifier une violation sur les données personnelles dans un délais de 72h. Une approche qui nécessite ici aussi de revoir les modèles de détection des failles de sécurité et une forte automatisation des capacités de réponse de l'entreprise.

Assurer, de manière automatisée, la portabilité des données est également une difficulté majeure (65%). Cette disposition nécessite d'avoir une vision détaillée des données (cartographie) et d'être en mesure techniquement de les réunir quels que soient leur localisation, leur nature (structurée, non structurée) et les systèmes dont elles dépendent (parfois très anciens).

Pour répondre aux nombreux enjeux (cryptage des données, effacement des données, droit à l'oubli, service de demande d'accès aux données …), les entreprises doivent rapidement prendre conscience que le GDPR n'est pas une option. La nouvelle gouvernance de la donnée (cartographie, traçabilité, sécurisation) impose la mise en place d'une gouvernance spécifique aux initiatives GDPR. C'est d'ailleurs le cas dans 52% des entreprises matures sur le sujet GDPR (contre 23% pour les entreprises moins matures). C'est à cette condition que l'entreprise pourra avancer de manière structurée vers une mise en conformité à l'horizon 2018. Cette gouvernance permettra de structurer l'approche GDPR : nomination d'un DPO (en place dans 38% des entreprises, en projet dans 29% des entreprises), réalisation d'un audit de conformité, mobilisation d'une enveloppe budgétaire liée au GDPR (c'est le cas dans 71% des entreprises), actions de communication en direction des collaborateurs en interne (53% l'ont réalisé, 31% le projettent dans les prochains mois).

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

IDC France

13 Rue Paul Valéry
75116 Paris, France
+33.1 56.26.26.66
Twitter: @IDCfrance
idc-community.com
www.idc.com / www.idc.fr

Copyright

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2017 IDC. Reproduction is forbidden unless authorized. All rights reserved.