LE GDPR,
C'EST POUR 2018 :

Quelle perception et quels enjeux pour les entreprises françaises ?

Rédigé par :
Karim Bahloul
Yasmina Slaoui

Juin 2017

IDC
Analyze the Future

box

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

OPINION IDC

La pression réglementaire évolue et se transforme, engageant beaucoup plus les entreprises, obligeant la plupart d'entre elles à renforcer leur politique en matière de protection des données. Enjeu majeur de la vie privée et de la maîtrise des données personnelles, 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. Les entreprises n'ont plus qu'un an (jusqu'en mai 2018) pour se mettre en règle vis-à-vis de ce nouveau règlement européen et son lot de nouvelles exigences en matière de protection des données personnelles. Le GDPR a pour objectif de faire face à l'internationalisation du marché autour des données, et harmoniser la politique autour de ces données entre les différents pays européens. Il concerne toutes les entreprises européennes ou non, qui détiennent des données sur des citoyens européens.

En matière de protection des données personnelles, plusieurs législations ont précédé l'avènement du GDPR. Mais contrairement aux législations antérieures relatives à la protection des données personnelles, le GDPR prend une forme dématérialisée, et ne se limite pas aux frontières. Alors que les législations antérieures étaient du ressort des autorités nationales de chaque pays de l'Union européenne, la mise en place du GDPR concerne les données des citoyens européens quel que soit leur lieu géographique. Elle touche de nombreux domaines politiques, juridiques et business, de la sécurité renforcée et la responsabilité du collecteur de données, aux nouvelles procédures obligatoires. Face au risque de sanctions considérables, les entreprises qui traitent de la donnée se retrouvent dans l'obligation de réviser leurs procédures et d'assurer leur conformité à ce nouveau règlement.

Dans un contexte de mondialisation et de numérisation accrues, c'est à partir de 2011 que le Contrôleur Européen de la Protection des Données (CEPD) lance un grand chantier de réflexion pour réformer le cadre juridique de protection des données personnelles. Pour rappel, selon la CNIL, "une donnée à caractère personnel représente toute information se rapportant à une personne physique identifiée ou identifiable 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".

CONTEXTE ET OBJECTIFS DU GDPR

Du Safe Harbor au GDPR

Si l'affaire Edward Snowden a révélé le plus grand scandale sur l'utilisation des données personnelles à des fins d'espionnage par l'agence de renseignements gouvernementale américaine en 2013, les entreprises du secteur privé ne sont pas moins touchées par la cybercriminalité, le hacking et la fuite des données personnelles. En France, avec le vol des noms, prénoms, adresses emails et numéros de mobiles de plus d'1 million de clients, la cyberattaque qui avait visé le groupe Orange en 2014 reste dans les mémoires.

Après plusieurs cyber-scandales successifs, les politiques ont publié de nombreux textes de lois sur la protection des données personnelles en Europe, des textes qui ont générés plus de confusion sur le sujet, que d'harmonisation. D'abord le **« Safe Harbor »** (Sphère de Sécurité) en 2000, qui devait fournir un socle de confiance pour les échanges de données entre l'Union européenne et les Etats-Unis. Les principes de cet accord permettaient à une entreprise américaine de certifier qu'elle respecte la législation de l'Espace Economique Européen afin d'obtenir l'autorisation de transférer des données personnelles de l'EEE vers les Etats-Unis.

La Directive 95/46/CE sur la protection des données personnelles, entrée en vigueur en 1998, interdisait le transfert de données personnelles en dehors des États non membres de l'EEE qui protégeraient les données personnelles à un niveau inférieur à celui de l'EEE. Les États-Unis d'Amérique et l'EEE partageaient l'objectif d'améliorer la protection des données de leurs concitoyens, mais abordaient cette problématique de façon différente. Pour créer la passerelle entre ces deux approches de respect de la vie privée et permettre aux entreprises et organisations américaines de se conformer à la Directive européenne, le département du Commerce des États-Unis, en concertation avec la Commission européenne a instauré le cadre juridique du Safe Harbor (sphère de sécurité). Mais en octobre 2015, la Cour de justice de l'Union européenne invalide l'accord du Safe Harbor. La cour considérait que les États-Unis n'offraient pas un niveau de protection adéquat aux données personnelles transférées et que les États membres devaient pouvoir vérifier si les transferts de données personnelles entre cet État et les États-Unis respectent les exigences de la directive européenne sur la protection des données personnelles. Avec l'invalidation de cet accord qui avait mis en place un cadre législatif clair pour les échanges de données entre l'Europe et les Etats-Unis, les entreprises étaient confrontées à un certain flou juridique.

Le nouvel accord présenté en février 2016, le « **Privacy Shield** » (Bouclier de Protection) a été vivement critiqué lors de sa présentation, et très mal accueilli par le Contrôleur Européen de Protection des Données (CEPD) qui juge le texte trop complexe. Selon lui, cet accord ne prend pas suffisamment en compte toutes les garanties appropriées pour protéger le droit européen des individus à la vie privée et à la protection des données, notamment en ce qui concerne le recours juridictionnel. Le CEPD considérait que des améliorations significatives étaient nécessaires dans l'hypothèse où la Commission Européenne souhaiterait adopter cette décision d'adéquation. Cet accord ne constituait pas un traité international, mais se composait d'une série de dispositions qui réglementaient la protection des données personnelles transférées depuis un Etat membre de l'Union Européenne vers les Etats-Unis.

2000

Mise en place du « SafeHarbor » entre les USA et l'UE

2015

Le SafeHarbor devient invalide

2016

Mise en place du « Privacy Shield »

2017

CEPD

Mauvais accueil par le CEPD et réflexion sur un nouveau traité européen, le « GDPR »

En octobre 2016, plusieurs associations françaises, dont le Quadrature du net ont déposé un recours devant le Tribunal de l'Union Européenne pour annuler cet accord. Au même moment, une association irlandaise, Data Rights Ireland a attaqué le texte en justice. Pendant ce temps, de nombreuses entreprises utilisent les « clauses contractuelles types » pour poursuivre leurs échanges avec les Etats-Unis, ce qui était défini dans le cadre de la 1ère directive de 1995, la Directive 95/46/CE. Ces clauses sont des règles internes aux entreprises connues aussi sous le nom de « **BCR** » (Binding Corporate Rules).

35%

des entreprises se contentent de demander un consentement aux personnes concernées

Le graphique suivant (graphique 1) présente les réglementations qui sont utilisées aujourd'hui par les entreprises françaises en matière de protection des données personnelles selon notre dernière enquête menée en Mai 2017 auprès de 150 entreprises de plus de 500 salariés basées en France. Les résultats de l'étude révèlent que plus d'un un tiers (35%) des entreprises se contentent de demander un consentement aux personnes concernées, et plus de la moitié (54%) utilisent des clauses contractuelles. Ces clauses contractuelles constituent un bon code de conduite définissant la politique d'une entreprise en matière de transfert de données personnelles. Mais ces clauses sont amenées à disparaître au profit du GDPR qui impose un seul règlement pour toutes les données européennes et toutes les entreprises qui les collectent, les hébergent et les manipulent.

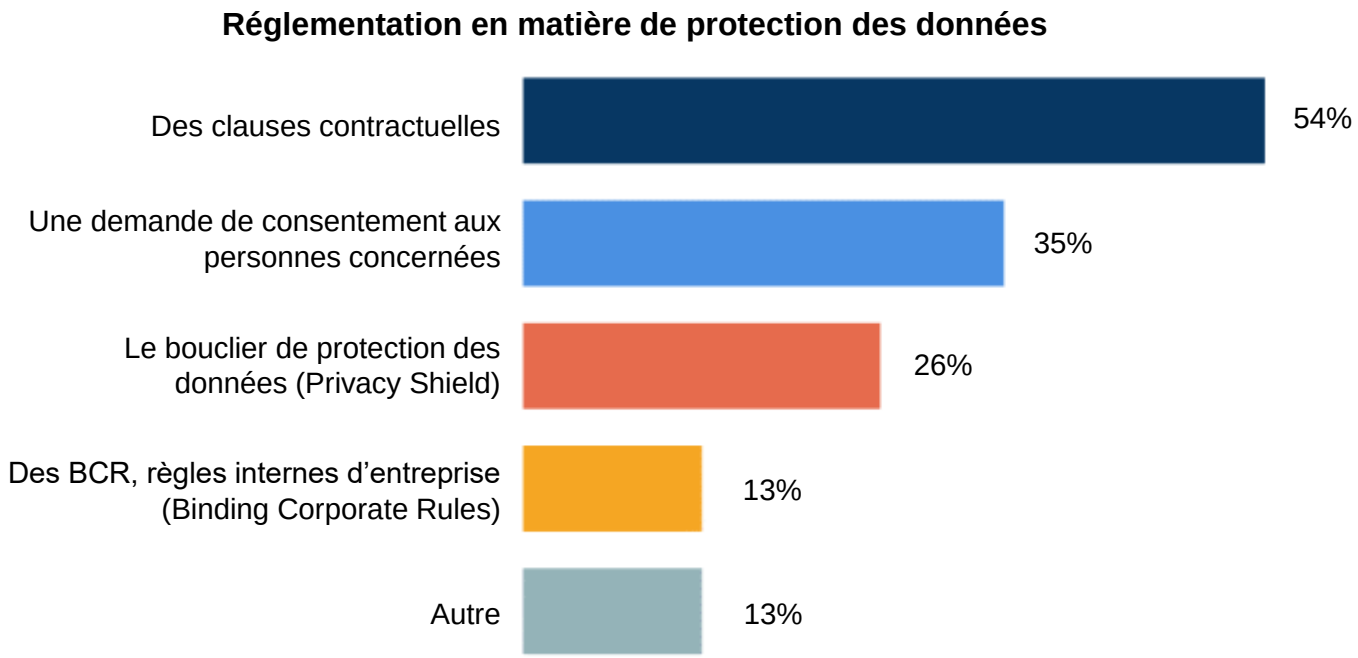
54%

utilisent des clauses contractuelles

Graphique 1

Réglementations en matière de protection des données utilisées par les entreprises en France

Parmi les outils suivants, quels sont ceux utilisés par votre entreprise en matière de transfert de données personnelles vers d'autres pays que ceux de l'Union européenne ?



Source : Enquête France Observatoire GDPR, IDC Mai 2017
N=150

Les principales implications 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.

LES ENJEUX ET OPPORTUNITÉS DU GDPR

Le rôle d'un système d'information centré sur les données

Les derniers entretiens menés par IDC ont permis d'identifier l'importante évolution en cours dans un certain nombre d'entreprises qui visent à passer d'une approche centrée sur les processus à une approche centrée sur les données. Cette approche modifie et impacte les systèmes d'informations mais aussi les directions métiers. Il s'agit en effet de passer de la gestion d'un patrimoine applicatif par la DSI à la gestion d'un patrimoine fonctionnel, qui dépend donc du responsable de ce domaine fonctionnel. Cette évolution amène à repenser les rôles et les responsabilités autour de la donnée au sein des entreprises, à lever les contraintes liées au silotage des données au sein du système d'information, tout en garantissant une meilleure sécurité et une meilleure conformité des données.

Placer la donnée au cœur de ces approches signifie également placer le client au cœur de la stratégie des entreprises. Le traitement des données clients devra respecter les nouvelles réglementations autour des données personnelles telles que le GDPR, tant pour les données internes que pour les données externes ou agrégées, mais aussi continuer à respecter les exigences du législateur sur certains processus tels que Know Your Customer (KYC). La gestion de ces enjeux parfois contradictoires renforcera le rôle de la gouvernance de la donnée et l'émergence de pôles Data au sein des entreprises, regroupant les activités de collecte, de Data Science ou encore de gouvernance.

Les opportunités du GDPR

De nombreuses entreprises ne se rendent pas encore compte de l'impact qu'aura le GDPR sur leur organisation, résultant d'un état d'esprit encore trop focalisé sur un effort minimum nécessaire à fournir pour être en conformité. Hors les entreprises qui retiennent ce type d'approche passent à côté d'une véritable opportunité. Le GDPR implique un environnement dans lequel le risque, la confidentialité et la sécurité sont au cœur de leur métier. Par exemple, « la protection de la donnée par design et par défaut » obligent les entreprises à prendre en compte les exigences relatives au risque associé aux données au fur et à mesure que les nouveaux processus métiers sont conçus et non pas comme une réflexion à posteriori.

Y aurait-il une opportunité relative au GDPR à saisir pour les entreprises ou les individus ? Aucun doute pour les entreprises qui ne sont pas des opérateurs d'importance vitale, celles-ci répondent positivement.

Le GDPR peut être une occasion de mettre la cyber sécurité au cœur des préoccupations stratégiques. Pour les autres (banques, assurances et autres OIV), le GDPR ne change rien de plus puisque la sécurité et la protection des données sont déjà à un niveau élevé au sein de ces organisations. S'appuyer sur le registre du Correspondant informatique et libertés (CIL), s'il en existe déjà un dans l'entreprise, peut résoudre certains des problèmes. Certaines entreprises perçoivent également le GDPR comme une occasion de renforcer leurs relations avec leurs clients, notamment en termes de confiance. Quelle que soit l'opportunité, le GDPR représente un levier fondamental en termes de protection des données, et par extension de sécurité. Le GDPR bouleverse véritablement les règles du jeu et pose de nouvelles exigences sur les processus opérationnels de sécurité, et plus généralement sur les considérations IT.

80%

des entreprises perçoivent le GDPR comme une opportunité importante pour améliorer la sécurisation et la confidentialité des données

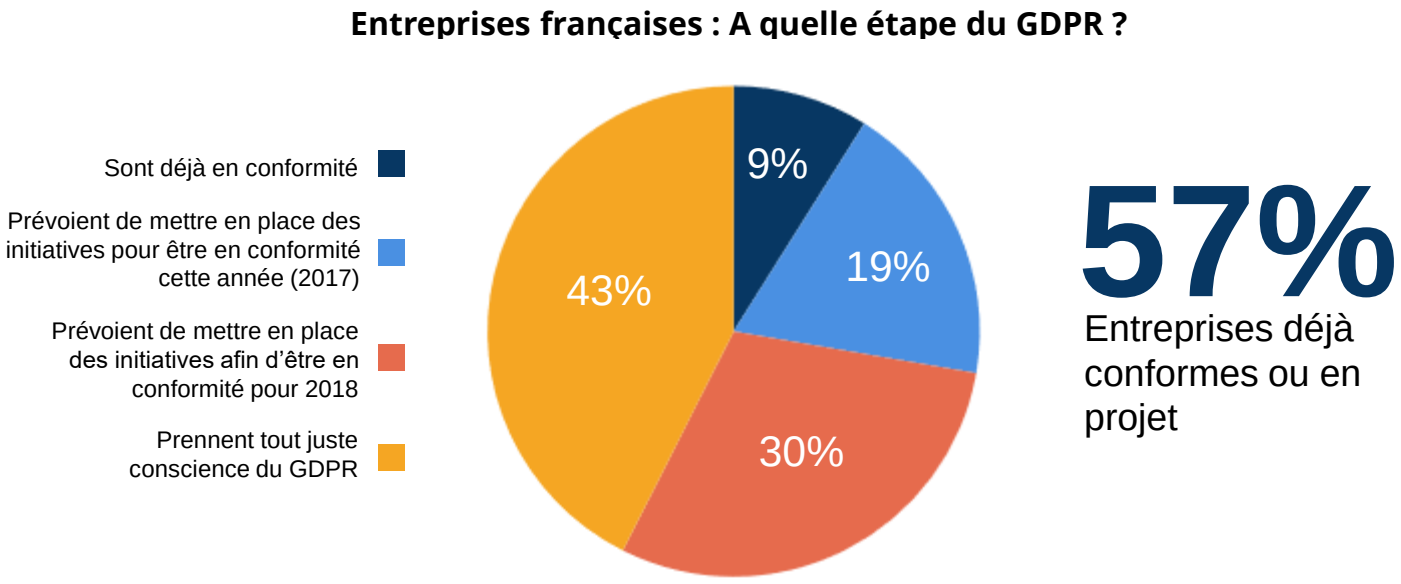
L'opportunité du GDPR est peut-être plus un état d'esprit qu'une certitude. Cela pourrait se faire à différents niveaux : utiliser le GDPR pour sécuriser le budget, utiliser la protection des données par design et par défaut pour influencer l'innovation, réorganiser la sécurité pour répondre aux nouvelles exigences du GDPR et à un environnement où les menaces sont en perpétuelle évolution. L'enquête révèle que 80% des entreprises perçoivent le GDPR comme une opportunité importante pour améliorer la sécurisation et la confidentialité des données. Cette opportunité est perçue de façon plus importante au sein des plus petites entreprises, 83% des entreprises de 500 à 1000 salariés, contre 77% des entreprises de plus de 1000 salariés. Près des deux tiers des entreprises interrogées associent également le GDRP à une opportunité importante d'améliorer la gestion du cycle de vie des données. Les entreprises perçoivent aussi d'autres opportunités, une meilleure image auprès des clients grâce à la certification GDPR, l'amélioration de la collaboration entre les directions métiers et la direction informatique, mais aussi une meilleure relation avec leurs partenaires.

Si les entreprises sont bien conscientes des opportunités qu'apportent le GDPR et qu'elles n'ont plus qu'un an pour se mettre en conformité, les résultats de notre étude montrent clairement que les entreprises françaises ne sont pas encore prêtes. Plus de 4 entreprises sur 10 (43%) prennent tout juste conscience du GDPR (graphique 2), et moins de 10% sont déjà conformes aujourd'hui. Cependant, près de 50% d'entreprises supplémentaires travaillent sur le sujet pour être conformes au GDPR d'ici l'échéance 2018.

Graphique 2

Où en sont les entreprises dans leur approche GDPR ?

Parmi les propositions suivantes, laquelle décrit le mieux l'approche de votre organisation en matière de GDPR ?



Source : Enquête France Observatoire GDPR, IDC Mai 2017
N=150

LES PRINCIPAUX IMPACTS DE LA MISE EN PLACE DU GDPR POUR LES ENTREPRISES

L'impact du nouveau règlement sur les organisations en France varie selon la taille, la portée et la nature des organisations ainsi que leurs activités. Ce qui est cependant certain, c'est qu'il y a un impact, mais celui ci est moins important pour les opérateurs d'importance vitale que pour les autres entreprises.

La nécessaire mise en place d'un DPO

Les entreprises françaises sont aujourd'hui nombreuses à avoir mis en place un Chief Information & Security Officer (CISO) ou un Correspondants Informatique et Liberté (CIL). Ce CISO ou CIL pourra aussi, pour certaines entreprises, endosser le nouveau rôle de responsable de la protection des données personnelles ou DPO (Data Protection Officer). Cette fonction devient obligatoire au sein des entreprises avec la mise en place du GDPR. Le rôle du DPO est de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données est effectué conformément au GDPR. S'il est clair que la mission du DPO consistera à la protection des données, sa fonction n'est pas encore clairement définie, et son périmètre d'intervention et son entité de rattachement ne sont pas encore précisés. Il semble tout de même bien plus probable que le DPO soit rattaché à une direction de la conformité par exemple, qu'à la direction de la Data.

Entreprises déjà conformes

38%

sont en cours ou ont déjà nommées un DPO au sein de leur organisation

30%

prévoient de mettre en place un DPO dans les prochains mois

Les résultats de l'étude montrent que parmi les 57% d'entreprises qui sont déjà conformes au GDPR ou qui prévoient de se mettre en conformité d'ici 2018, près de 4 entreprises sur 10 (38%) sont en cours ou ont déjà nommées un DPO au sein de leur organisation (graphique 3), et près de 30% prévoient de mettre en place un DPO dans les prochains mois. Cependant, alors que la mise en place du DPO devient obligatoire avec le GDPR, un tiers des entreprises qui se disent déjà conformes ou qui s'y préparent, ne projettent pas de nommer un DPO.

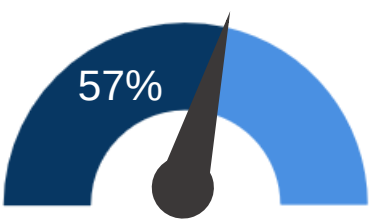
Graphique 3

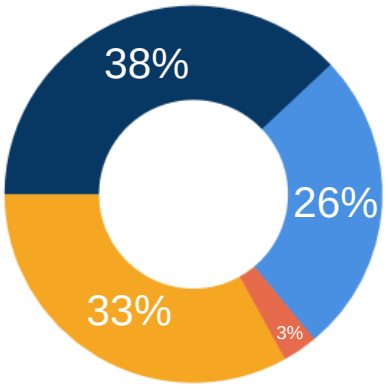
Mise en place d'un DPO au sein des entreprises françaises

Votre entreprise a-t-elle ou va telle nommer un délégué en charge de la protection des données (DPO) ?

57%

Entreprises déjà conformes ou en projet de conformité d'ici 2018





Source : Enquête France Observatoire GDPR, IDC Mai 2017
N=150

Par ailleurs, même les petites entreprises devront nommer une personne responsable du traitement de la donnée qui puisse assumer différentes fonctions :

- Avoir toute l'information nécessaire sur le GDPR et ses contraintes. Il aura à sa disposition un code de conduite et de certifications pour former ses collaborateurs.
- Vérifier et valider les propositions commerciales des partenaires et sous-traitants ainsi que leur niveau de services contractuels (SLA / Service Level Agreement). Il doit notifier les failles de sécurité dans les 72 heures, être l'interlocuteur dédié pour les fournisseurs et pouvoir être joignable facilement en cas d'incident.
- S'assurer que les partenaires n'effectuent aucun traitement des données, excepté sur instruction du responsable du traitement.
- Vérifier et valider les pratiques de traitement des données en interne, en particulier avec le marketing, et les ressources humaines en particulier) pour s'assurer de la mise en œuvre de politiques appropriées en matière de protection des données. Il veillera en particulier à faire respecter le fameux « droit à l'oubli » qui oblige toute entreprise à effacer les données d'un prospect ou d'un client sur sa simple demande.
- Vérifier la pertinence des procédures liées au traitement des données et tenir à jour des procédures écrites et consultables. L'UE se réserve le droit de les consulter sur simple demande.
- S'assurer qu'un plan de continuation, de reprise de l'activité et de rétablissement après désastre a été mis en place et validé avec les sous-traitants potentiels et au sein de l'entreprise.

L'impact sur le Shadow IT

Pour être conforme au GDPR, les entreprises doivent pouvoir démontrer un niveau de sécurité adéquat pour toute donnée européenne collectée et hébergée par une entreprise. La problématique du Shadow IT, - "informatique de l'ombre" – devient alors cruciale. IDC qualifie de Shadow IT les projets informatiques financés et gouvernés par les métiers sans le concours de la DSI, et sans que celle-ci n'en soit informée. La dernière enquête IDC sur les budgets informatiques des entreprises menée sur une population de directions informatiques et décideurs IT, révèle que 61% des projets informatiques sont aujourd'hui financés par les directions métiers. Pour 23% de ces projets, l'IT bien qu'informé, n'est pas inclus dans la gouvernance des projets, et 17% des projets sont financés et mis en œuvre par les métiers sans que la DSI n'en soit informée. La part des collaborateurs qui décident d'utiliser une solution non référencée par l'entreprise (un outil de Web conférence, une solution SaaS métier type plateforme de mass emailing, etc.) est alors non négligeable, et présente un nouveau danger légal avec une couche de complexité à un problème déjà important.

61%

des projets informatiques sont aujourd'hui financés par les directions métiers

17%

de ces projets sont financés et mis en œuvre par les métiers sans que la DSI n'en soit informée.

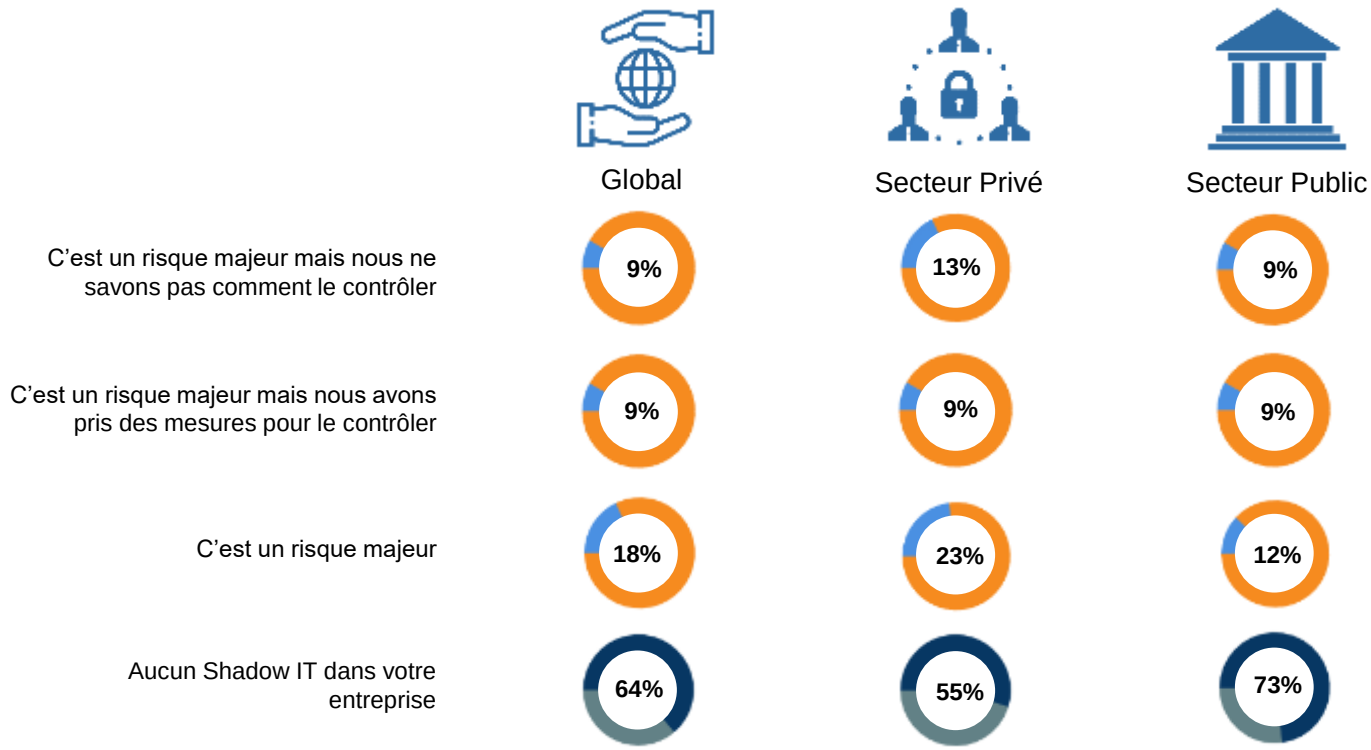
Les résultats de l'enquête montrent que seules 36% des entreprises de plus de 500 salariés confirment le risque de Shadow IT au sein de leur entreprise. Pour 64% des entreprises, la pratique du Shadow IT est inexistante (graphique 3). Les organisations du secteur privé sont plus nombreuses à percevoir le risque que représente le Shadow IT dans leur entreprise (45%) que les organisations du secteur privé (27%). Par ailleurs, parmi les entreprises qui reconnaissent le Shadow IT comme un risque pour leur organisation, la moitié évaluent ce risque comme un risque mineur. Pourtant les études IDC montrent que le Shadow IT est largement répandu dans les entreprises. Pour les départements IT, il est difficile de mesurer réellement le risque que représente le Shadow IT au sein des départements métiers. En sous-estimant le risque réel de cette pratique, il est difficile de prendre les mesures nécessaires pour le contrôler. D'après les résultats de l'étude, parmi les entreprises qui reconnaissent le Shadow IT comme un risque majeur (18%), seule la moitié prennent les mesures nécessaires pour le contrôler.

Les principaux risques associés à la pratique du Shadow IT sont aujourd'hui bien connus. En tête de file de ces risques : la sécurité des données de l'entreprise. Car si le Shadow IT est un phénomène qui touche l'ensemble du système d'information, le cœur de la problématique se situe bien au niveau de la donnée. Le choix des solutions mis en place pour répondre aux besoins métiers, qui traduit la capacité de la DSI à comprendre les attentes des collaborateurs de l'entreprise, apparaît évidement comme un moyen naturel d'endiguer la pratique du Shadow IT. En effet, plus une solution est en mesure de répondre au besoin du métier, tant d'un point de vue fonctionnel que d'un point de vue de l'expérience utilisateur, moins la tentation du Shadow IT sera élevée. Le choix de la solution apparaît donc crucial, d'autant plus qu'elle doit permettre d'assurer dans un même temps la sécurité des données de l'entreprise.

Graphique 4

Shadow IT, quel risque pour le GDPR ?

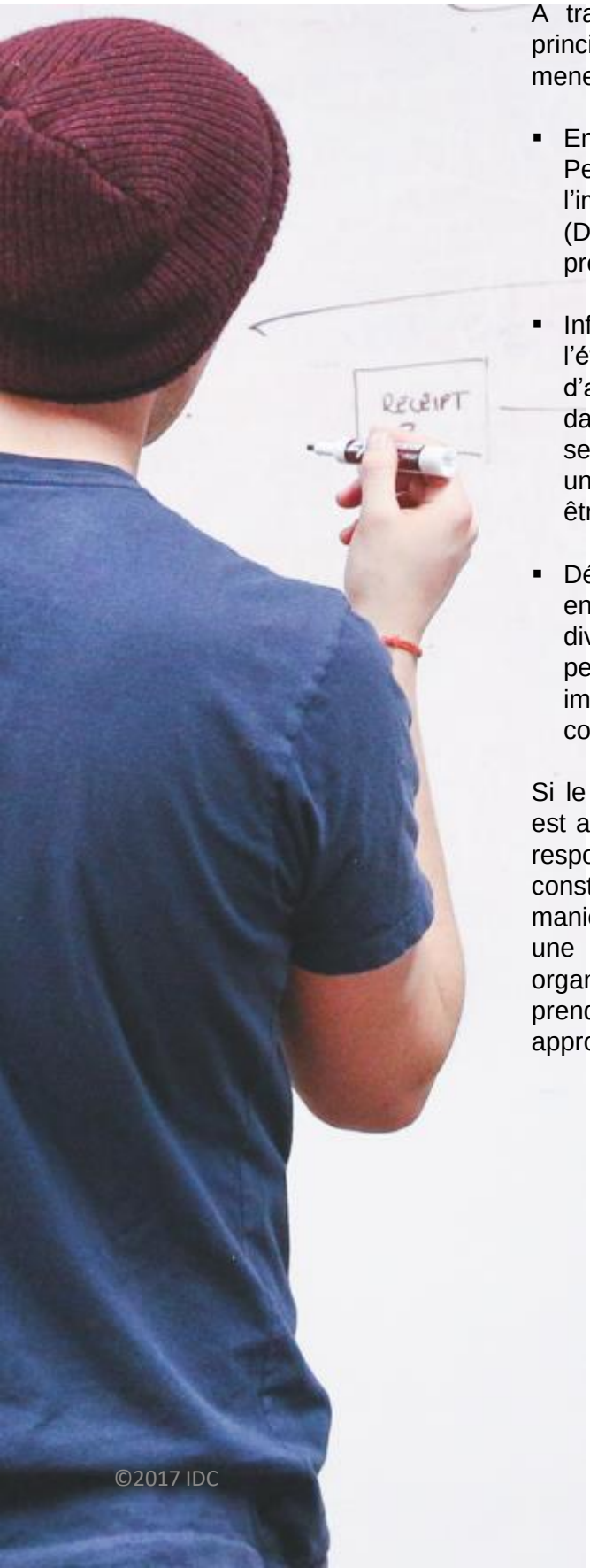
Selon vous, le Shadow IT représente-t-il un risque majeur face aux exigences de conformité GDPR ?



Source : Enquête France Observatoire GDPR, IDC Mai 2017
N=150

©2017 IDC

CONCLUSION : RECOMMANDATIONS POUR ALLER VERS LE GDPR



A travers cette étude, nous pouvons mettre en exergue trois principales recommandations relatives au GDPR que doivent mener les DSI et CISO :

- Engager un programme (et non un projet) concernant le GDPR. Peu importe la provenance du programme dans l'entreprise, l'importance résulte dans le fait de nommer un responsable (DPO), et que celui-ci doit s'appuyer sur toutes les parties prenantes de l'entreprise.

- Informer votre entreprise sur la compréhension des termes de l'état de l'art. Consultez vos pairs, fournisseurs, ainsi que d'autres acteurs de l'industrie, et si cela est possible, collaborer dans l'optique de fournir ensemble une définition propre à votre secteur. Soyez prêts à défendre votre définition, peut-être, face à une cour de justice ou une cour d'opinion public. La CNIL devrait être une bonne source de conseils dans ce domaine.

- Décidez si le GDPR représente une opportunité pour votre entreprise dans sa globalité, ou bien pour votre division/département, ou pour vous en tant qu'individu. Il n'y a peut-être aucun autre règlement de cette ampleur qui aura un tel impact sur votre organisation que le GDPR. Toutes les décisions concernant le GDPR ne dépendent que de vous.

Si le GDPR représente une charge très importante, ce règlement est aussi un agent de changement important reconnu par tous les responsables. La mise en place du GDPR est essentielle à la construction d'un environnement de confiance qui exploitera de manière de plus en plus massive les données, et peut représenter une opportunité de différenciation importante entre les organisations les plus avancées, et celles qui au contraire prendront du retard dans la mise en place des meilleures approches.

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
LinkedIn : IDC France
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.