APIXIT

L'expertise augmentée

Réussir sa conformité au RGPD

Nos mesures pour garantir la disponibilité, la ocnfidentialité et l'intégrité des données traitées.

LIVRE BLANC Mars 2018

SOMMAIRE

QUI SOMMES-NOUS ?

APIXIT

APIXIT est l'union des deux spécialistes indépendants des services numériques DCI et RETIS. Expert reconnu des solutions d'infrastructures digitales, de la Digital Workplace, de la Cybersécurité, APIXIT propose un accompagnement global : audit, conseil, intégration en mode projet, services managés.Conscient que l'Innovation est une attente des clients et un atout différenciant, APIXIT est le partenaire privilégié des plus grands constructeurs et éditeurs et porte son attention et son expertise sur les enjeux des organisations et de la transformation digitale.

Animé par une solide culture de la performance, de l'innovation technologique et de la satisfaction client, le groupe APIXIT et ses 350 collaborateurs sont présents à travers toute la France.

CONTACTS

Jean-Philippe GUILLEMIN
Responsable développement d'activité Cybersécurité
jpguillemin@apixit.fr
Tél : 02 99 06 37 02

Céline SALOT
Chargée de Marketing
csalot@apixit.fr
Tél : 02 99 06 31 83

RGPD : MOINS D'UN AN POUR SE METTRE EN CONFORMITÉ !

Les entreprises sont encore dans le flou

50% ignorent les problématiques induites par la mise en conformité.

25% n'ont aucune idée de l'impact du règlement sur les processus IT de leur organisation.

33% sont à la recherche d'une démarche outillée.

Un impact lourd pour les DSI

36% des entreprises pensent que le RGPD aura un impact considérable sur la direction des systèmes d'information car, à ce stade, elles sont loin de pouvoir répondre aux exigences à venir.

33% des DSI ont anticipé certains chantiers et pensent subir un impact modéré au niveau IT.

Beaucoup de retard dans la mise en conformité

31% des entreprises pensent qu'elles seront conformes à temps.

66% des entreprises ne seront, à priori, pas prêtes à l'horizon mai 2018.

70% des entreprises n'ont pas encore nommé de DPO. (data protection officer)

Le RGPD en quelques mots

Le règlement général sur la protection des données (RGPD), également désigné en anglais par « General Data protection regulation » (GDPR), est le nouveau règlement européen en matière de protection des données personnelles. Mieux adapté aux problématiques actuelles liées au numérique, il remplacera la directive sur la protection des données personnelles en vigueur depuis 1995.

L'objectif de ce texte est de mieux encadrer le traitement et la circulation des données à caractère personnel des citoyens européens tout en simplifiant l'environnement réglementaire des entreprises. Ce texte précise donc, à l'échelle européenne, les obligations des responsables de traitements ainsi que les droits des citoyens européens. Adopté par le parlement européen le 14 avril 2016 après 4 années d'âpres négociations, celui-ci entra en vigueur dans l'ensemble des états membres de l'Union européenne à partir du 25 mai 2018.

Qu'est ce qu'une donnée à caractère personnel ?

Une donnée à caractère personnel est définie, dans l'article 4 du règlement européen, comme « toute information se rapportant à une personne physique identifiée ou identifiable », de façon directe ou indirecte (par le biais d'un identifiant par exemple). Un nom, un numéro d'identification, une donnée de localisation, et « tout autres éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » sont donc considérés comme des données à caractère personnel.

Qu'est ce qu'un traitement de données ?

Il s'agit de toute opération portant sur les données à savoir : la collecte, l'enregistrement, la conservation, la modification, l'extraction, la consultation, la communication, l'interconnexion, le transfert, le verrouillage, l'effacement et la destruction.

Quelles obligations incombent aux organisations en matière de traitement de ces données ?

Licéité, loyauté et transparence

La collecte de données doit être effectuée dans un but précis et légitime, communiqué clairement à la personne concernée.

Minimisation des données

La collecte des données doit être limitée aux seuls éléments nécessaires pour le besoin des finalités envisagées.

Limitation de finalité

Avant de collecter les données personnelles d'un individu, celui-ci doit en être informé et donner son accord de façon explicite.

Exactitude des données

Les données collectées doivent être exactes. L'organisation en charge du traitement des données est tenue de procéder à la mise à jour ou à l'effacement des données inexactes dans les plus brefs délais. En outre, les individus bénéficient d'un droit de rectification sur leurs données.

Limitation de conservation

Les données collectées doivent être conservées pour une durée limitée et cohérente avec le traitement envisagé.

Sécurité et confidentialité

Les organisations doivent mettre en place l'ensemble des mesures nécessaires pour assurer la sécurité et la confidentialité des données collectées.

Droit à l'effacement (droit à l'oubli)

Dans les conditions prévues par le règlement, les individus peuvent demander à tout moment à faire effacer leurs données personnelles. La suppression doit alors être effectuée dans les meilleurs délais.

Portabilité des données personnelles

Les individus peuvent demander à recevoir ou à faire transférer leurs données à caractère personnel vers un autre responsable de traitement. Lorsque cela est techniquement possible, les données peuvent être directement transférées d'un responsable de traitement à un autre.

Traçabilité

Le responsable de traitement des données doit renseigner sur un registre l'ensemble des activités relatives aux données :

- D'où viennent les données ?
- Pourquoi ont-elles été collectées ?
- Dans quel contexte sont-elles utilisées ?
- Quand devra-t-on les détruire ?
- Qui a accès aux données ?
- ...

Protection des données dès la conception (data protection by design)

Tant au moment de la détermination des moyens de traitement, qu'au moment de la conception du traitement lui-même, le responsable du traitement est tenu de mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour assurer la protection des données manipulées.

Que faire en cas d'incident de sécurité ?

En cas d'incident de sécurité ayant un impact sur la disponibilité (les données sont accessibles sans failles durant les plages d'utilisation prévues et avec le temps de réponse attendu), l'intégrité (les données sont celles que l'on attend, elle ne sont pas altérées de façon fortuite, illicite ou malveillante), et/ou la confidentialité (seules les personnes autorisées ont accès aux informations qui leurs sont destinées) des données de votre organisation, vous êtes tenu d'en informer l'autorité nationale de protection désignée dans le cadre du RGPD dans les 72H. En France, il s'agit de la CNIL. Les individus concernés par la violation de leurs données (destruction, perte, altération, divulgation non autorisée, accès non autorisé…) doivent également être avertis.

Quelles sont les sanctions en cas de non-respect du règlement ?

Le règlement général sur la protection des données contient une série de sanctions administratives applicables en cas de méconnaissance ou de manquements aux dispositions énoncées. La CNIL, autorité en charge de faire appliquer le RGPD en France, pourra donc, en fonction de la gravité du manquement, infliger les sanctions suivantes :

- Prononcer un avertissement, communiqué ou non au public
- Mettre en demeure l'organisation de remédier aux manquements constatés
- Limiter temporairement ou de manière définitive le traitement des données
- Suspendre les flux de données
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes
- Ordonner la rectification, la limitation ou l'effacement de certaines données

En outre, l'organisation qui aura failli dans le traitement de ses données pourra se voir infliger une lourde amende. Selon la catégorie de l'infraction, celle-ci pourra atteindre, au maximum, le montant le plus élevé entre 20 millions d'euros ou 4% du chiffre d'affaire annuel mondial groupe.

Au delà des sanctions importantes qui pourraient être prononcées par la CNIL, prendre des mesures pour assurer la sécurité des données est essentiel pour garantir la pérennité de votre organisation. En effet, on considère que le coût moyen d'un vol de données s'élève à 4 millions de dollars. Cette menace est d'autant plus importante que le risque d'occurrence d'une cyberattaque est élevé. Entre 11 et 21 cyberattaques affectant des organisations françaises sont recensées chaque jour en France.

Entrer en conformité en cinq étapes

Etape 1
Nommer un délégué à la protection des données

La question de la nomination d'un délégué à la protection des données doit être le point de départ de votre démarche de sécurisation des données personnelles. En effet, la désignation d'un délégué à la protection des données est obligatoire dans certains cas (traitement de données à grande échelle notamment). Son rôle sera de coordonner la mise en place des mesures de mise en conformité au RGPD et de s'assurer du respect, sur le long terme, des règles instaurées. Successeur naturel du CIL (correspondant informatique et libertés), le délégué aura un rôle de conseil et de sensibilisation prépondérant sur l'ensemble des questions relatives à la protection des données.

Etape 2
Faire un état des lieux de vos traitements de données

Avant de planifier la moindre action de mise en conformité, il est nécessaire de réaliser un audit des activités de votre entreprise orienté sur la nature des données que vous traitez et les impératifs de sécurité qui y sont liés.

Pour un audit de sécurité exhaustif et rigoureux, votre attention devra porter sur les éléments suivants :

- Classification : les données collectées sont-elles des données à caractère personnel ?
- Finalité : dans quel but collectez-vous ces données ?
- Traitement : quel traitement subissent ces données ?

- Droits d'accès : qui peut accéder et traiter les données ?
- Durée de conservation : avez-vous défini une durée de conservation pour chaque type de données ? Comment vous assurez-vous de l'effacement des données à l'issu de ce délai ?
- Risque sécuritaire : quelle est la maturité de votre organisation en termes de cybersécurité? Les mesures prises vous permettent-elles de faire face aux menaces (internes et externes) auxquelles votre activité vous expose ?
- Partenariats : des prestataires externes accèdent-ils à tout ou partie de vos données ? Si oui, les clauses de confidentialité qui régissent vos relations sont-elles adaptées ?
- Transparence : vos clients/utilisateurs, savent-ils que vous collectez des données les concernant?
- Traitement hors UE : envisagez vous de transférer des données hors Union Européenne ?
- Stratégie de réponse : disposez-vous d'une stratégie en cas de perte de contrôle de vos données?

Cet état des lieux doit vous permettre d'obtenir une solide compréhension du cycle de vie des données que vous traitez : de leur collecte à leur suppression en passant par leurs sauvegardes et les différentes modifications et actualisations (usages, transmissions internes comme externes…). Vous devez désormais parfaitement cartographier vos traitements de données et consigner l'ensemble des informations relatives à cette collecte au sein d'un registre de traitements.

En cas d'incident de sécurité, ce document sera un premier élément de preuve auprès de la CNIL de votre bonne mise en conformité.

Etape 3
Définir un plan d'action

L'état des lieux réalisé lors de l'étape précédente vous permet de dresser le bilan de votre situation et de mesurer l'écart (gap analysis) qu'il vous faudra combler pour vous conformer aux nouvelles règlementations.

Fort de cette analyse vous pouvez désormais construire un plan d'action destiné à combler cet écart. En premier lieu, il vous faudra lister l'ensemble des actions à mener. Ces dernières devront ensuite être priorisées en tenant compte :

- des risques que font peser vos traitements sur les droits et les libertés des personnes concernées,
- des ressources et des compétences nécessaires à leur mise en œuvre.

Ainsi identifiées, les actions à mener seront concrétisées sous la forme de projets et intégrées dans votre planning.

Pour les données identifiées comme « sensibles », des processus de traitement spécifiques doivent être prévus dans le plan d'action. En effet, le responsable de traitement sera tenu de mener une étude d'impact sur la vie privée (EIVP, PIA) présentant les caractéristiques du traitement, les risques qui lui sont associés ainsi que les mesures adoptées pour prévenir toute perte de contrôle sur les données. Les résultats de l'étude d'impact pourront impliquer des mesures de gestion des données plus drastiques.

Etape 4
Adapter les processus de votre entreprise

C'est à cette étape que vous mettez en œuvre l'ensemble des mesures listées dans votre plan d'action en fonction de leur degré de priorité. Cette phase peut prendre plusieurs mois et modifier considérablement les habitudes de travail des collaborateurs de l'entreprise. Il vous faudra donc accorder une importance toute particulière à l'accompagnement au changement afin que les nouvelles mesures techniques et organisationnelles prises soient réellement adoptées.

En outre, l'implication de l'ensemble du management dans le processus de mise en conformité s'avère prépondérant. En effet, le respect de la nouvelle règlementation n'est pas l'apanage de la seule direction des systèmes d'information. L'ensemble des organes décisionnels de votre organisation doit être intégré à la réflexion menée sur le traitement des données à caractère personnel.

Etape 5
Documenter votre mise en conformité

Votre organisation se doit de constituer une base documentaire afin d'attester de sa conformité au règlement européen. Bien entendu, il est essentiel que ces documents soient régulièrement réexaminés et mis à jour pour assurer une protection continue des données traitées. En cas d'incident de sécurité, ces derniers pourront être soumis à la CNIL dans le cadre d'une procédure de contrôle.

Ci-dessous les documents que vous devez être en mesure de fournir :

La documentation relative au traitement des données personnelles :

- Le registre des traitements : à réaliser par les responsables de traitement et les sous-traitants,
- L'analyse d'impact sur la protection des données : à réaliser pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes,
- L'encadrement des transferts : à réaliser pour les transferts des données hors Union européenne
- La documentation des durées de conservation, des politiques d'archivage et des destructions de données.

La documentation relative à l'information des personnes :

- Les mentions d'information
- Le recueil du consentement : lorsque ce consentement est nécessaire, une preuve que les personnes concernées par le traitement de leurs données ont bien donné leur accord.
- Les procédures mises en place pour l'exercice des droits : droit de rectification, droit à l'oubli, portabilité des données personnelles…
- Les contrats définissant les rôles et responsabilités des acteurs :
- Les contrats avec les sous-traitants : définissant les rôles, les responsabilités et les droits et devoirs de chacune des parties.
- Les procédures décrivant les actions à mener en cas de violation de données.
- Les obligations applicables à vos salariés : charte informatique, procédures internes de gestion des données.

NOS EXPERTS

La sécurité IT : un enjeu juridique et économique

— Par Anne Laure Gaillard, CEO – Withlaw

Chacun est responsable des données à caractère personnel qu'il collecte et qu'il utilise. En cas d'atteinte à la sécurité de ces données, votre responsabilité ne pourra être écartée que si vous aviez fait tout le nécessaire pour les protéger.

Votre organisation dispose également d'autres catégories de données qui doivent faire l'objet d'une protection rigoureuse : ce sont notamment vos données stratégiques ainsi que les informations confidentielles de vos clients et partenaires. En détaillant les processus devant être respectés pour protéger les données à caractère personnel, le RGDP et les autorités de protection des données à caractère personnel (notamment la CNIL) créent l'opportunité d'une véritable prise de conscience qui va nous permettre d'adopter les bons réflexes et de protéger l'ensemble des données détenues par nos organisations.

Saisissons-nous de cette démarche ! Du fait de l'accroissement considérable des risques depuis ces derniers mois, la protection des informations est devenue un véritable enjeu économique. La crédibilité, la compétitivité et la pérennité de votre organisation en dépend.

LES ESSENTIELS DE VOTRE PROTECTION

Adopter une démarche de sécurité globale

La sécurité IT n'est pas uniquement une affaire « technique ». Sans pilotage et vision globale de l'état de la protection du SI de l'entreprise portée par le RSSI, le DSI ou tout responsable IT, la plupart des mesures et solutions de sécurité seront vaines. Il est nécessaire d'adopter une démarche de sécurité globale, allant de la mise en place d'une Politique de Sécurité du Système d'information (PSSI) à l'administration sécurisée du SI, en passant par une politique cadrée de mises à jour (ex : processus de gestion des arrivées et des départs des différents collaborateurs). Une fois la démarche de sécurité rigoureusement définie, il vous faudra également porter une attention toute particulière à sa déclinaison opérationnelle (actions méthodologiques, organisationnelles, procédurales…)

Accompagné du DPO qui veillera au bon respect des règlements relatifs à la sécurité des données, le responsable IT devra prévoir des contrôles et audits réguliers afin de tester la sécurité de son système d'information et ainsi de s'assurer de l'efficacité de la couverture des risques jugés inacceptables par l'entreprise. En outre, l'équipe qui pilote la sécurité IT de votre organisation devra mettre en place un système d'alerte et de veille technologique afin de maintenir dans le temps un haut niveau de sécurité et son efficacité dans le temps.

Protéger dynamiquement et surveiller

Trop souvent négligée, la surveillance en continue des évènements qui rythment la vie de votre système d'information (SI) est pourtant essentielle. Cette surveillance constitue, en effet, un premier rempart face aux cyber-attaques dont vous êtes potentiellement la cible. Grâce à la supervision rigoureuse de vos équipements et de votre SI, vous serez en mesure de détecter de façon proactive les attaques contournant votre périmètre de défense et infiltrant votre environnement interne. Vous pouvez ainsi agir avant même qu'un incident de sécurité se produise (ex : tentative d'accès frauduleux, exécution de virus, prise de contrôle à distance…). Les première minutes consécutives à une cyber-attaque étant déterminantes, en cas d'incident de sécurité avéré, vous pourrez prendre les mesures qui s'imposent avec une réactivité accrue.

63 Jours sont nécessaires en moyenne pour constater et réparer les dégâts causés par une cyber-attaque.

Source : Cabinet ISIE, 2017

La supervision de l'ensemble d'un système d'information requiert d'importants moyens, humains notamment. De nombreuses entreprises font donc le choix d'externaliser la surveillance de leur SI auprès d'acteurs experts de la cybersécurité. Ces derniers disposent de services experts et d'outils technologiques aux fonctionnalités avancées intégrés au sein d'un SOC (Security Operation Center / Centre opérationnel de Sécurité en français).

Outre la surveillance et la détection de menaces, il convient de mettre en place une politique de réaction appropriée aux évènements. C'est l'objet d'une politique de gestion des incidents de sécurité. Cette politique doit indiquer les bonnes pratiques à suivre en termes de signalement, de remontée d'information et de réponse aux incidents. Cette dernière doit être connue de tous les collaborateurs de l'entreprise, des rappels réguliers des procédures sont donc nécessaires.

NOS EXPERTS

La sécurité des données dans les applications

— Par Hervé LE GOFF, CEO – Yagaan Software Security

La sécurité applicative revêt une importance cruciale dans la protection des données personnelles. Avec le RGPD, le nouvel enjeu des développements logiciels est d'adopter les approches «privacy by design» et de justifier que les données personnelles seront correctement protégées dès la première mise en service des applications. Cela passe par la détection au plus tôt des vulnérabilités logicielles connues (pendant les phases de codage et lors des revues de code en particulier, ou lors d'audits de code pour les applications legacy), et leur correction lorsque nécessaire. Les enjeux de la détection des vulnérabilités et l'analyse de leur criticité métier sont critiques, il est en particulier nécessaire :

- de cartographier les données personnelles dans les applications « legacy »
- d'adapter l'analyse selon le contexte métier de l'application et sa stratégie de protection globale : par exemple une variable nommée Numero_Insee pourra contenir un identifiant INSEE chiffré correctement, et sera non confidentiel, ou bien elle contiendra un identifiant INSEE en clair et aura un besoin de confidentialité fort.
- de tracer exhaustivement les traitements qui manipulent les données sensibles pour vérifier tous les "flux de données" susceptibles de mener à une fuite d'information telle que le stockage d'un mot de passe dans un fichier de log, ou l'envoi de données insuffisamment protégées à des applications tierces.
- de justifier et de documenter les actions de vérification qui auront été menées.

Chez YAGAAN, nous tirons parti des technologies d'intelligence artificielle pour une analyse des codes sources plus efficiente et obtenir une bien meilleure efficacité dans l'obtention de la "privacy by design".

Gérer la mobilité des collaborateurs

Selon une récente étude menée par Sharp, 75% des professionnels travaillent régulièrement en situation de mobilité. Incontournable pour certains métiers de l'entreprise, cette mobilité doit faire l'objet de mesures de sécurité spécifiques, destinées à protéger le patrimoine informationnel stocké et manipulé par les collaborateurs.

En outre, la flotte des équipements IT d'une entreprise ne s'arrête plus aujourd'hui aux simples postes de travail. Elle intègre désormais un ensemble hétérogène de terminaux mobiles (smartphones, tablettes…), qui traitent, eux aussi, des informations liées aux activités de l'entreprise. Les partages d'informations induits par l'utilisation simultanée et complémentaire de plusieurs terminaux (la redirection d'une messagerie professionnelle sur mobile par exemple), bien qu'apportant plus de confort et de souplesse au quotidien, amènent avec eux de nouveaux enjeux que les directions IT ne peuvent plus se permettre d'ignorer.

Pour bien protéger votre organisation dans un tel contexte, mettre en place une protection périmétrique de type antivirus ne suffit plus. Il est essentiel de renforcer les architectures de sécurité de votre système d'information avec la mise en place d'une solution de contrôle d'accès réseau. Ainsi, vos équipes informatiques pourront identifier plus simplement les terminaux et les utilisateurs qui ont accès au réseau et leur adosser des droits d'accès adéquats.

81%

des employés consultent régulièrement des documents professionnels lorsqu'ils sont en déplacement

Source : Sharp, octobre 2017

L'implémentation d'une plateforme de gestion des terminaux (MDM) leur apportera également plus de visibilité concernant la gestion des accès au réseau d'entreprise. Grâce à ce type de solutions, vous pourrez acquérir une meilleure compréhension des risques (ex : téléchargement d'applications non pilotée par le SI) et des vulnérabilités qui vous exposent.

Chiffrer et anonymiser vos données

L'utilisation d'outils cryptographiques est incontournable pour la protection de vos données. En effet, ceux-ci garantissent la confidentialité (l'information n'est accessible qu'à ceux dont l'accès est autorisé) et l'intégrité (garantie que l'information n'a pas été modifiée) des informations manipulées par votre SI. Ces outils de chiffrement peuvent être intégrés à plusieurs maillons de la chaine de traitement de l'information, comme par exemple le chiffrement des flux de communications, qu'ils soient internes ou externes, ou encore le stockage et la sauvegarde.

Former et sensibiliser vos collaborateurs

Dans son rapport annuel « Le facteur humain 2017 », Proofpoint note que les cybercriminels s'appuient de plus en plus sur des techniques de hameçonnage plutôt que sur des failles logicielles pour mener leurs attaques. Depuis 2015, cette tendance ne cesse de se renforcer. A titre d'exemple, le rapport indique, que les messages d'attaque BEC (Business Email Compromise) ont augmenté de 41% entre 2015 et 2016. Au total, cela représente un coût supérieur à 5 milliards de dollars pour les entreprises dans le monde.

Mettre en place des mesures de protection techniques avancées ne suffit plus. Il est essentiel de sensibiliser vos collaborateurs en mettant à leur disposition une documentation complète des procédures de sécurité (charte informatique) et en procédant à des actions de sensibilisation régulières (démonstrations de cyber-attaque, serious game…).

FOCUS EXPERT

Le cas des traitements des données à caractère personnel entrainant un risque élevé pour les droits et libertés des personnes physiques

Lorsque vous traitez des données sensibles, vous êtes dans l'obligation de réaliser une analyse d'impact sur la protection des données (PIA). Sont concernés les cas suivants :

- Vous traitez des données de certains types : origine raciale ou ethnique, opinion politique, philosophique, ou religieuse, appartenance syndicale, données de santé, orientation sexuelle, données génétiques ou biométriques, données relatives aux infractions ou aux condamnations pénales.
- Votre traitement a pour objet ou pour effet : la surveillance systématique et à grande échelle d'une zone accessible au public. L'évaluation systématique et approfondie d'aspects personnels sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

D'une manière générale, lorsque vous traitez des données personnelles, pensez à :

Qui ?

- Mentionner dans le registre de conformité au règlement européen les coordonnées du responsable de traitement et, le cas échéant, celles du délégué à la protection des données.
- Identifier l'ensemble des responsables de services opérationnels intervenant dans le traitement des données au sein de votre organisme.
- Répertorier, dans votre registre, tous les sous-traitants qui peuvent avoir accès à vos données personnelles.

Quoi ?

- Identifier les différents types de données traitées (identification par catégories de données)
- Identifier les données susceptibles de présenter un risque particulier en raison d'une sensibilité accrue (données de santé par exemple).

Pourquoi ?

- Préciser la ou les finalités pour lesquelles vous collectez ces données (gestion de la relation commerciale, gestion RH, …).

Où ?

- Indiquer dans votre registre le lieu où les données sont collectées.
- Si vos données sont transférées, préciser le pays de destination

Jusqu'à quand ?

- Pour chaque catégorie de données, préciser la durée de conservation des données.

Comment ?

- Préciser quelles mesures de sécurité vous mettez en place pour minimiser les risques liés à une perte de contrôle de vos données (notamment accès non-autorisés).

APIXIT

L'expertise augmentée

Ce Livre Blanc est un document d'information rédigé par la société APIXIT.
Il n'a pas vocation à servir de support de prestation de conseil.

APIXIT ne serait être tenu responsable en cas de cyber-attaque ou de manquements aux obligations présentes dans le règlement général sur la protection des données.

SIEGE SOCIAL

Les Conquérants
Immeuble Annapurna
1 avenue de l'Atlantique
91940 LES ULIS

RENNES

Espace Jacques Cartier
CS 96031
35360 MONTAUBAN
DE BRETAGNE

LILLE

Village Créatif
10 rue de la Cense
59650 VILLENEUVE D'ASCQ

QUIMPER

3 allée Emile Le Page
29000 QUIMPER

PARIS

Immeuble AXIUM
22/24 rue du Gouverneur
Général Félix Eboué
92130 ISSY LES MOULINEAUX

NANTES

Les Espaces Océane
4 rue Jack London
44400 REZÉ

REIMS

13 rue Desbureaux
51100 REIMS

TOULOUSE

32 rue des Cosmonautes
31400 TOULOUSE

LYON

Immeuble Woodclub
97, allée Alexandre Borodine
69800 SAINT-PRIEST

5D chemin du Jubin
69570 DARDILLY

www.apixit.fr