

RGPD

Enjeux et solutions

Présentation entreprise et association



**DATAVIGI
PROTECTION**
SÉCURITÉ ET CONFORMITÉ RGPD

UN POINT sur le RGPD...

.....

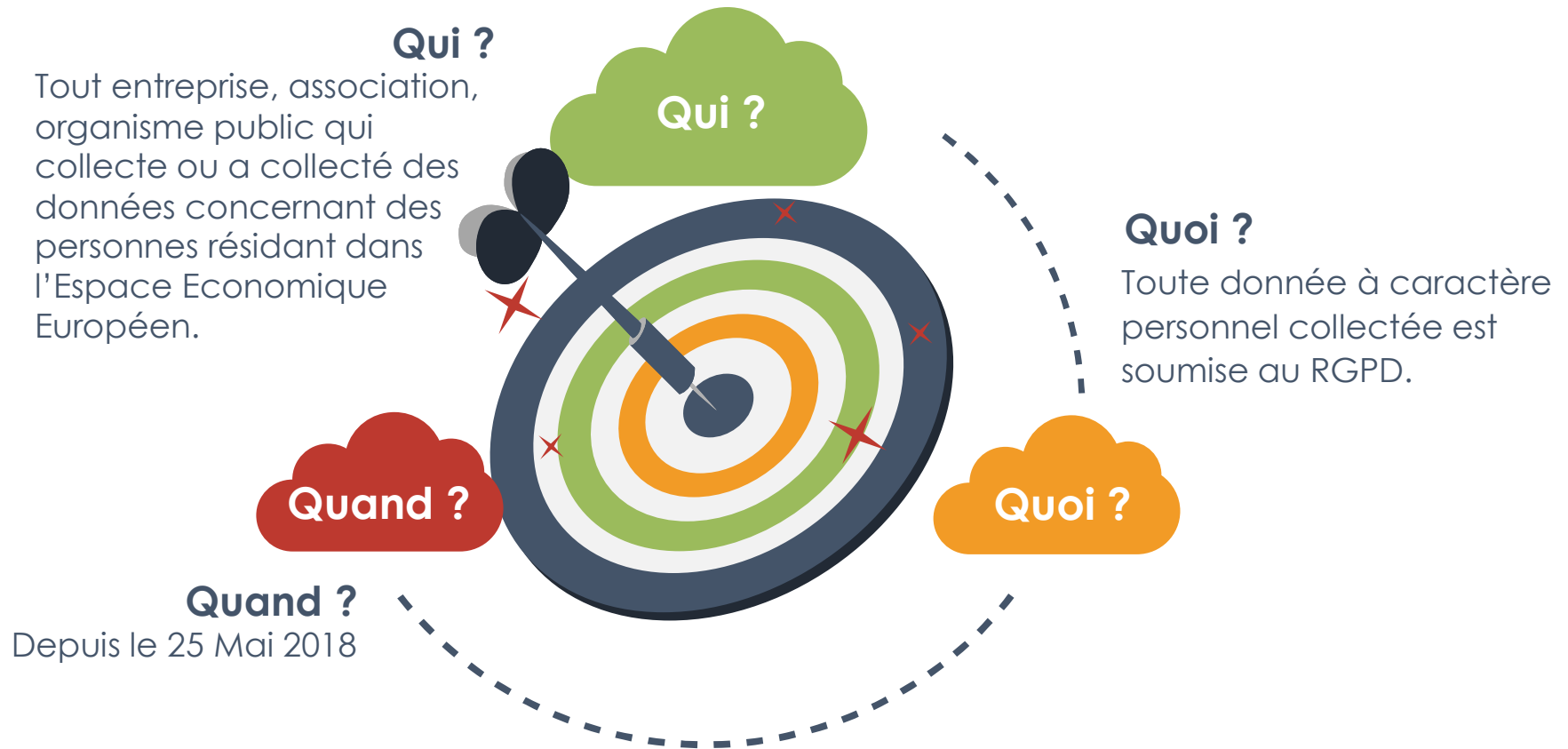
Quoi, qui, quand ?
Le CRUD
Les données
Les traitements

RGPD
99 articles
à respecter !



RGPD : les infos clés...

Le Règlement Européen pour la Protection des Données



LES OBJECTIFS

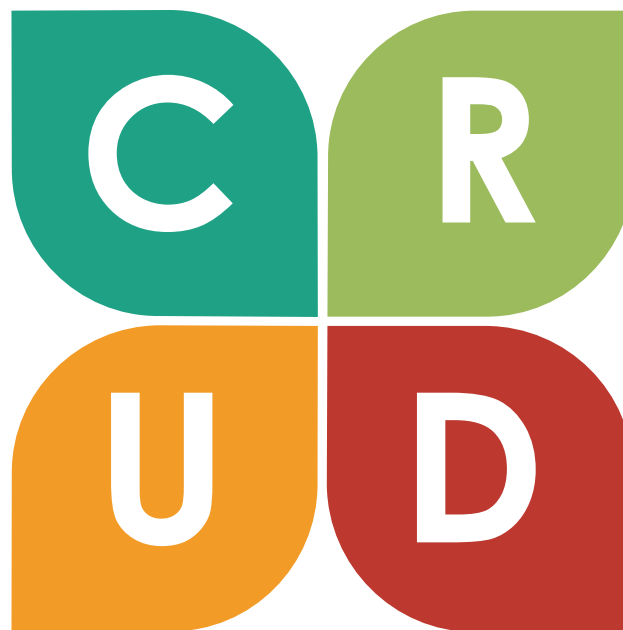
Contrôler, responsabiliser, uniformiser et démultiplier les droits du citoyen : le **CRUD**



Contrôler les données
Redonner aux citoyens le contrôle de leurs données personnelles tout en unifiant les réglementations relatives à la protection de leur vie privée



Uniformiser au niveau européen la réglementation sur la protection des données



Responsabiliser les collecteurs

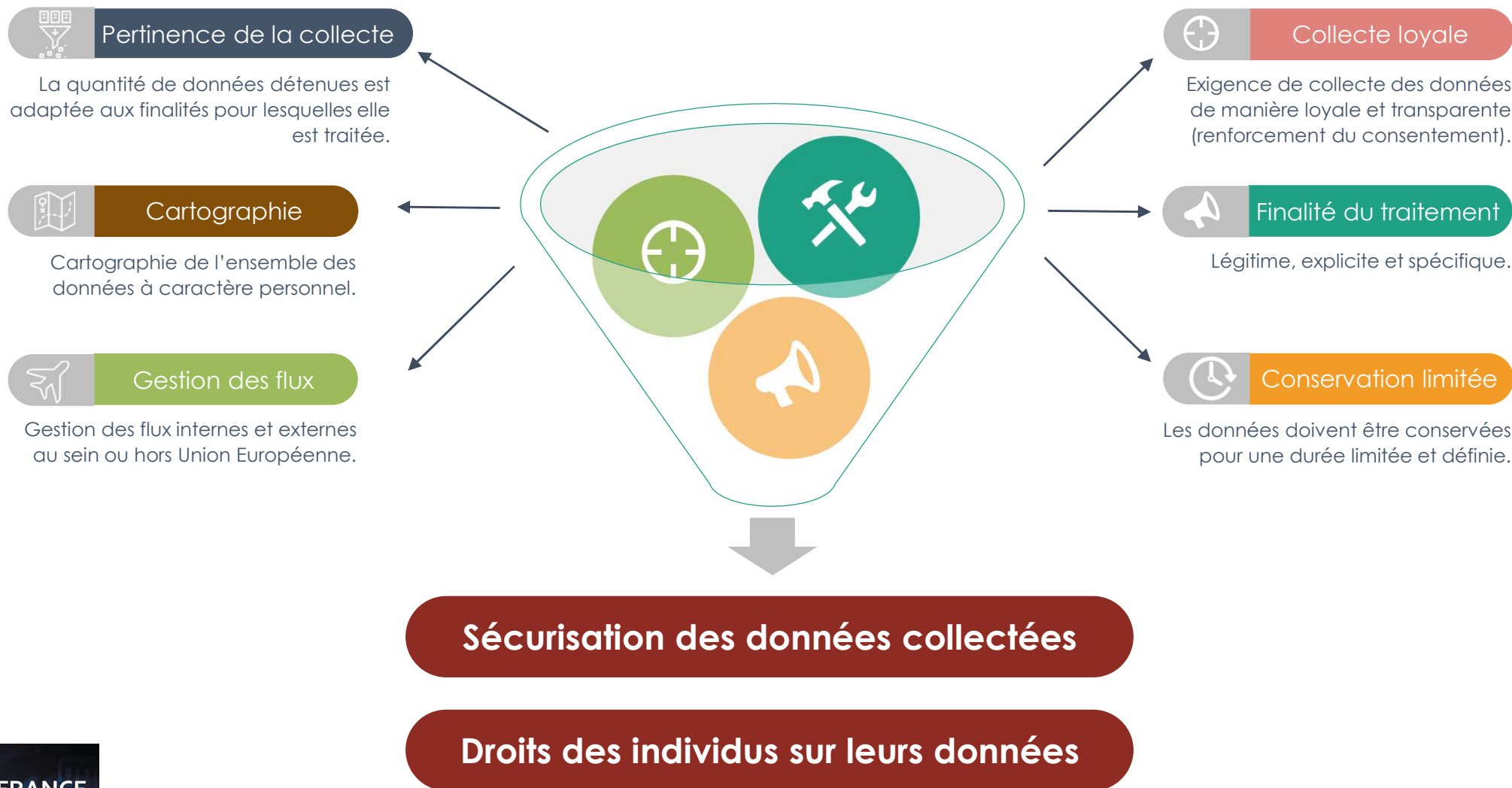


Démultiplier et renforcer le droit des personnes (**droit à l'accès, droit à l'oubli, droit à la portabilité...**)

Principes et objectifs

du RGPD

6 grands principes qui permettent de viser 2 objectifs majeurs



Quelles sont les données concernées ?

L'ensemble des données personnelles...

Constitue une donnée à caractère personnel, toute information permettant d'identifier directement ou indirectement une personne physique que ce soit par l'intermédiaire d'éléments informatisés ou pas.

Par exemple :

- **Nom**
- **Prénom**
- **Photo**
- **Adresse mail**
- **Numéro de téléphone**
- **CV**
- **Images de vidéosurveillance**
- **Numéro de sécurité sociale**
- **Plaque d'immatriculation**
- **Adresse IP**
- **RIB**
- **Situation familiale**
- ...

Ces données peuvent être stockées au sein de bases de données structurées (logiciel métier par exemple) ou dans de simples fichiers (Word, PDF...). On parle dans ce cas de données non structurées.

Que les données soient structurées ou non, le RGPD s'applique.



Quelles opérations sont soumises au RGPD ?

L'ensemble des traitements de données personnelles...

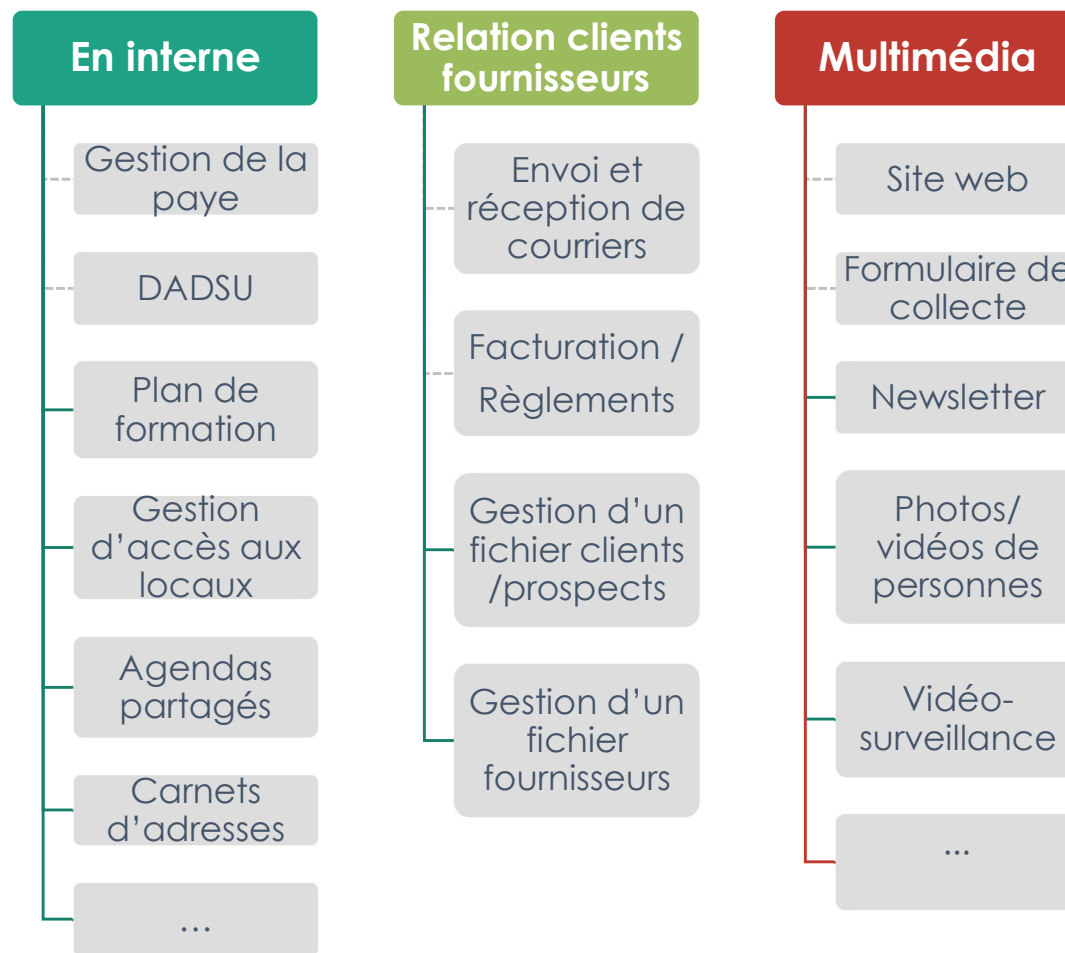
Toutes les opérations effectuées sur des ensembles de données à caractère personnel sont soumises au RGPD et notamment :

- la collecte
- l'enregistrement
- l'organisation
- la structuration
- la conservation
- la modification
- l'extraction
- la consultation
- l'utilisation
- la communication
- la diffusion
- le rapprochement
- l'effacement
- la destruction
- ...



Exemples de traitements

devant être conformes au RGPD



EN RÉSUMÉ

Toute donnée à caractère personnel qu'elle soit informatisée ou non et quelle qu'en soit l'utilisation envisagée doit être traitée conformément au RGPD.

Nota Bene : Une entreprise bénéficiant d'une certification ISO, ou autre certification qualité, doit impérativement documenter sa conformité au risque de perdre sa certification

VERS LA MISE EN CONFORMITÉ



Les 4 étapes clés
Sanctions et risques
Les erreurs à éviter

UNE EXPERTISE NÉCESSAIRE

A white icon consisting of a downward-pointing arrow inside a dashed circular border, centered in the bottom right corner of the dark blue box.

Les 4 étapes clés

Pour une mise en conformité réussie...



Nommer un référent RGPD ou un DPO



Auditer l'entreprise



Agir pour la mise en conformité



Analyser pour assurer votre conformité dans le temps



Référent ou DPO ?

Il est nécessaire de disposer d'une personne ressource...

La nomination d'un DPO « officiel » **devient obligatoire pour les entreprises qui traitent une « quantité importante de données personnelles »**. La notion de « quantité importante » reste pour le moment assez floue.

Il appartient donc à l'entreprise de déterminer si la nomination d'un DPO est nécessaire ou pas.

Le DPO (Délégué à la Protection des Données) **est le « chef d'orchestre » de la conformité** en matière des données au sein de son organisme. Il n'est pas responsable de la conformité, cette responsabilité est supportée par les responsables des traitements (le chef d'entreprise). Le DPO doit être libre et indépendant pour mener sa mission et ne doit pas être placé en situation de conflit d'intérêts.

Même si l'entreprise ne collecte que peu de données et que le DPO n'est pas obligatoire, **nous conseillons fortement de définir un référent RGPD** dont la mission principale sera de documenter la mise en conformité RGPD de l'entreprise. Au même titre que pour le DPO, 3 missions principales lui incomberont :

Informer

Informer et conseiller les responsables de traitement (la direction de l'entreprise) et/ou les sous-traitants ainsi que ses employés.

Analyser

Le DPO ou le Référent analysera tout au long de l'année les actions menées par l'entreprise afin de documenter sa conformité. En cas de contrôle, il coopèrera avec la CNIL.

Analyser



Auditer

Auditer

Réaliser un audit initial de la structure qui permettra de vérifier le respect du règlement et du droit en matière de protection des données. Le DPO ou le référent déterminera alors les actions à mener en les priorisant.

Quel profil pour le DPO ou le Référent ?

Ni informaticien, ni juriste...

Un métier à part entière ?

Un DPO ou un Référent RGPD doit disposer de sérieuses compétences en matière :



De droit



Du RGPD



D'informatique



Il doit être indépendant et ne doit pas être placé en situation de conflit d'intérêts.

Le temps à consacrer à la mission dépendra de la taille de l'entreprise et de la quantité et du type de données collectées. Une formation initiale exhaustive, une veille continue et de bons outils sont nécessaires pour assurer la mission correctement.



DPO ou Référent interne VS DPO externalisé

Deux possibilités à étudier

	DPO/ Référent interne	DPO externalisé
Avantages 	<ul style="list-style-type: none">• Connaissance de l'entreprise et des collaborateurs• Réactivité	<ul style="list-style-type: none">• Expertise assurée• Tranquillité (y compris en cas de remplacement)• Absence de couts de formation• Cout maitrisé, car connu à l'avance• Confidentialité et neutralité• Veille règlementaire assurée• Absence de conflits d'intérêts et indépendance totale
Inconvénients 	<ul style="list-style-type: none">• Temps à consacrer à la mission inférieur à 35h/semaine• Difficulté de recrutement• Formation initiale couteuse : 3500€ minimum• Profil de poste difficile à trouver• Risque de conflits d'intérêts important• Indépendance impossible à obtenir• Difficultés en cas de remplacement• Coût indirect difficilement quantifiable	<ul style="list-style-type: none">• Temps d'adaptation au fonctionnement de l'entreprise• Dépense supplémentaire

La nomination d'un DPO externalisé est une solution qui vous apporte la tranquillité, un niveau d'expertise élevé et des coûts maîtrisés.

Auditer et Agir

Démarrer la mise en conformité



1

Recenser et cartographier les données

- Recensement des différents traitements de données personnelles
- Recensement des différentes catégories de données personnelles
- Validation des objectifs poursuivis par les opérations de traitements de données
- Recensement des acteurs (internes ou externes) qui traitent ces données. Les contrats et clauses de confidentialité des sous-traitants doivent être actualisés
- Recensement des flux de données en indiquant l'origine et la destination des données

2

Constitution des registres obligatoires

Auditer et Agir

Mener les actions de mise en conformité



3

Mise en place des actions de mise en conformité

- Identifier les actions à mener pour chaque traitement
- S'assurer que seules les données strictement nécessaires sont collectées et traitées (purge de toutes les autres données)
- Validation du fondement juridique du traitement (ex: consentement de la personne, intérêt légitime, contrat, obligation légale)
- Vérification que les sous-traitants connaissent les nouvelles obligations et leurs responsabilités
- Mise en place de l'exercice des droits des personnes concernées (droit d'accès, droit de rectification, portabilité, consentement, droit à l'oubli...)

4

Prioriser les actions à mener

Auditer et Agir

Sécuriser et former...



5

Sécuriser les données

- Réalisation d'un audit de sécurité interne
- Vérification des mesures de sécurité en place et des outils à disposition pour lutter contre les vols ou l'altération des données personnelles

6

Sensibiliser et conseiller

- Action de sensibilisation à destination des responsables de l'entreprise
- Conseil en matière de sécurité et d'organisation des traitements et des collectes
- Appui en cas de contrôle par la CNIL

Analyser

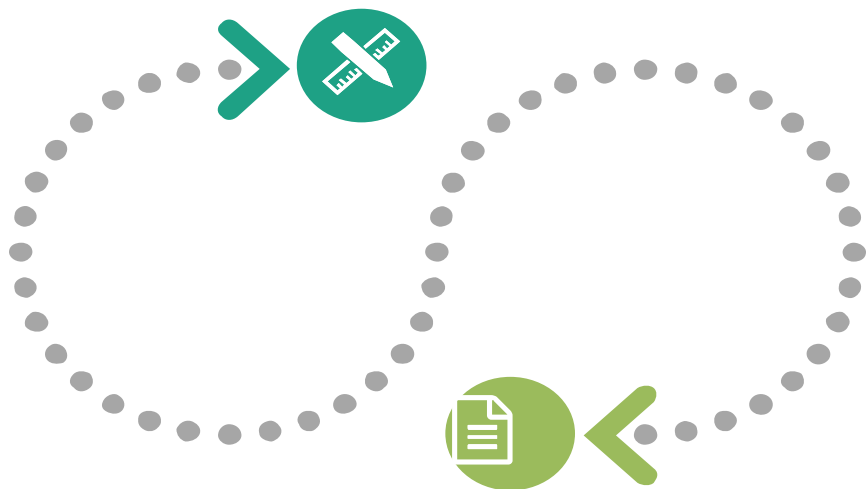
Pour assurer votre conformité dans le temps



Assurer un suivi de la mise en conformité

Une analyse continue des actions mise en place permet de s'assurer la mise en conformité dans le temps. Il est important :

- De sensibiliser et d'organiser la remontée d'information grâce à la mise en place d'un plan de formation et de communication interne
- De traiter les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits
- D'anticiper les violations de données



Documenter votre mise en conformité

Pour prouver la conformité au règlement, une base documentaire doit être constituée. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. Le dossier doit comporter à minima les pièces suivantes :

- Les mentions d'information aux personnes
- Les modèles de recueil de consentement des personnes concernées
- Les preuves que les personnes concernées ont donné leur consentement
- Les analyses d'impacts sur la protection des données
- L'encadrement des transferts de données
- Les procédures de mise en place pour l'exercice des droits
- Les contrats avec les sous-traitants
- Les procédures internes en cas de violation des données

La mise en application du RGPD nécessite donc une véritable expertise et des outils et procédures appropriés.

Sanctions et risques

A ne surtout pas sous-estimer



SANCTIONS

En cas de non-conformité avérée les sanctions financières encourues peuvent aller **jusqu'à 4% du CA annuel global de l'entreprise.**



RISQUES

Le risque contentieux est à prendre au sérieux. 15 jours après la mise en application du RGPD, plusieurs milliers de plaintes avaient déjà été déposées auprès de la CNIL. Un client mécontent ou un collaborateur en froid avec l'entreprise pourra se retourner contre cette dernière et demander réparation en cas de non-respect du caractère personnel des données le concernant.



IMAGE

Au-delà du risque financier pesant sur les entreprises qui ne seraient en règle avec le RGPD, la dégradation de son image pourrait également être très préjudiciable pour les responsables de l'entreprise en cas de sanction, de non-conformité ou de contentieux. L'effet boule de neige pourrait vite devenir incontrôlable et ouvrir la voie à d'autres sanctions ou d'autres contentieux.

La CNIL fait office de gendarme en matière de RGPD. Ses pouvoirs sont étendus tout comme son périmètre d'action. La CNIL peut ainsi perquisitionner sans demande préalable le siège d'une entreprise entre 6h du matin et 21h.

Quelques erreurs

à ne pas commettre...

20



Imaginer que votre entreprise est déjà conforme sans vous pencher sur la question !

Le RGPD a introduit et/ou renforcé un certain nombre de règles. Imaginer que seules les très grosses entreprises doivent fournir des efforts pour se mettre en conformité est une erreur. Toutes les entreprises sont soumises au RGPD et l'immense majorité devra consacrer du temps et des moyens pour se mettre en conformité.



Subir le RGPD, plutôt que s'en servir !

Ne nous le cachons pas, le RGPD est, sous certains aspects, contraignant. Il nécessite un niveau d'expertise élevé pour se mettre en conformité, ce qui induit nécessairement des coûts et ce, quelle que soit la méthode de mise en conformité employée. Mais le RGPD peut aussi devenir une opportunité. Sur le plan marketing, une entreprise conforme au RGPD peut facilement s'en prévaloir et utiliser cet argument pour renforcer son image auprès de ses clients. Sur le plan de la sécurité, c'est aussi une opportunité de faire un point sur la situation de l'entreprise et se prémunir ainsi des attaques informatiques et du vol ou de l'altération de ses données.



Sous-estimer le poids du risque pesant sur la sécurité de vos données !

Peut-être avez-vous eu la chance de ne jamais subir une attaque informatique vous privant d'un accès à vos données, mais ne faites pas l'erreur de penser que cela n'arrive qu'aux autres. En cas d'attaques informatiques ciblées ou non, votre responsabilité pourra être recherchée si des données personnelles ont été volées et que vous n'aviez rien envisagé pour leur protection.

Au-delà de la responsabilité, un vol ou une altération de données peut vite s'avérer catastrophique pour une entreprise. Que se passera-t-il si une attaque informatique vous prive de toutes vos données clients et comptables ?

EN RÉSUMÉ

- Nommer un DPO ou un Référent RGPD n'est pas toujours une obligation légale mais cela s'avère indispensable en pratique
- La complexité du RGPD nécessite un niveau d'expertise élevée et de bons outils pour assurer une mise en conformité réelle

NOTRE OFFRE DE SERVICE



Une solution globale, clés en main, sur mesure
DPO mutualisé
Logiciel dédié RGPD
Solutions de sécurité intégrale de vos données

UNE SOLUTION
GLOBALE



Une solution globale

clés en main et sur mesure...

Une solution globale, pourquoi ?

Tout simplement parce que la mise en conformité nécessite une expertise technique, juridique et informatique, et que sans outils adaptés la mise en conformité réelle est impossible !

Spécialistes en sécurité informatique depuis plus de 25 ans, nous avons développé des méthodes et des outils spécifiques permettant une mise en conformité réelle au RGPD.



DPO MUTUALISÉ

Nous mettons à votre disposition, nos équipes de DPO (délégués à la protection des données). Véritables chefs d'orchestre, nos DPO organisent au sein de votre structure, la mise en conformité.

DPO FORMÉ PAR UN ORGANISME DE FORMATION LABÉLISÉ CNIL



OUTILS INFORMATIQUES DÉDIÉS

Développés en partenariat avec « Panda Security » un des leader mondial de la sécurité informatique, nos outils permettent **une mise en conformité réelle** avec le RGPD contrairement à ce que propose l'immense majorité de nos confrères.

DÉTECTION DES DONNÉES NON STRUCTURÉES

LOGS



PROTECTION RENFORCÉE CONTRE LE PIRATAGE INFORMATIQUE

La mise en conformité RGPD requiert bien plus qu'une simple « cartographie » des données personnelles que vous collectez. Vous devez pouvoir prouver que tout est mis en œuvre pour garantir la sécurité des données. Nos outils le permettent !

PROTECTION CONTRE LE VOL DE DONNÉES

ANTIVIRUS

DPO MUTUALISÉ

Un chef d'orchestre à votre disposition !



Le DPO mutualisé c'est :

- Un DPO suivant des formations continues labellisées par la CNIL
- Un DPO avec un quota limité de clients afin d'assurer à bien sa mission
- La garantie d'indépendance et de neutralité
- La sensibilisation de vos collaborateurs
- L'intervention immédiate auprès de la CNIL en cas de violation de données
- L'analyse et les compétences juridiques, techniques et informatiques
- La vérification et l'exécution des correctifs
- L'accompagnement permanent
- La disponibilité et la réactivité immédiate

IMPORTANT : Pour mener à bien sa mission, le DPO devra disposer d'outils et de moyens le lui permettant

AUDIT RGPD

L'étape primordiale !

Extrait d'un rapport d'audit

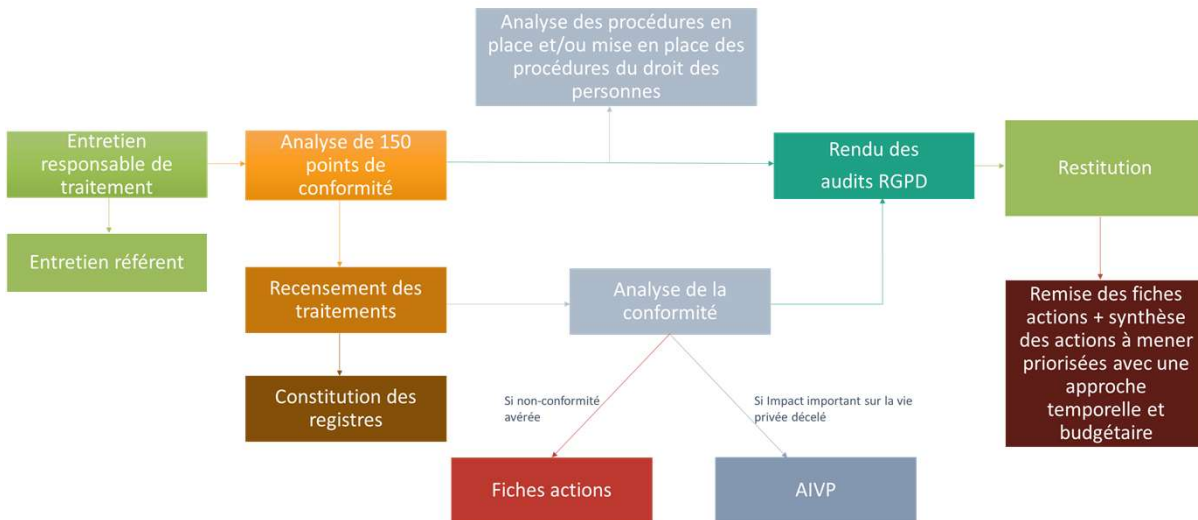


+ de 150 points de contrôle et une analyse de la sécurité du réseau informatique de nos clients

L'audit permet d'analyser la conformité au RGPD sur près de 150 points de contrôle. Chaque point analysé fait l'objet de recommandations personnalisées. Nous analysons également le niveau de sécurité du réseau informatique afin de déceler de potentielles failles.

A l'issue de ce travail une synthèse des actions à mener est présentée aux responsables de traitements afin d'établir une liste d'actions prioritaires à mettre en œuvre.

Méthodologie de base d'audit



Q : Des données sur des informations de santé ou par rapport à l'orientation sexuelle sont-elles traitées ?
Aucune donnée concernant des informations de santé ou par rapport à l'orientation sexuelle n'est traitée

Q : Des données à caractères sensibles (origine ethnique, opinions politiques, convictions religieuses, appartenance syndicale, données génétiques ou biométriques) sont-elles traitées ?
Aucune donnée à caractère sensible (origine ethnique, opinions politiques, convictions religieuses, appartenance syndicale, données génétiques ou biométriques) n'est traitée

Q : Des données à caractères sensibles relatives à des condamnations pénales ou infractions sont-elles traitées ?
Aucune donnée à caractère sensible relative à des condamnations pénales ou infractions n'est traitée

Q : Le traitement de vos données est-il nécessaire à la sauvegarde des intérêts vitaux des personnes concernées ?
Le traitement des données n'est pas nécessaire à la sauvegarde des intérêts vitaux des personnes concernées

Q : Ces traitements de données sont-ils nécessaires, et justifiés dans le cadre de vos activités ?
Ces traitements de données sont nécessaires et justifiés dans le cadre des activités de l'organisation

Réponse non communiquée

Q : Détenez-vous des listes de membres d'associations ou de C.E ?
Un ou des listes de membres d'associations ou de C.E sont détenues dans l'organisation

Q : Dans le cadre de détention et de traitement de listes de membres d'associations ou de C.E, une méthodologie particulière doit être utilisée afin que les données à caractère personnel soient stockées et accompagnées avec l'enregistrement du consentement, et des préférences de communication des personnes concernées. Si plusieurs outils ou logiciels sont utilisés, il sera alors impossible d'avoir une vue à 360 degrés des données collectées et des consentements associés, ce qui nuit à l'exercice des droits des personnes concernées et des moyens mis à disposition par le responsable du traitement pour tenir à jour ces données.

Q : Dans vos logiciels, des zones de commentaires libres pour y stocker des données personnelles sont-elles utilisées ?
Des zones de commentaires libres dans les logiciels sont utilisées pour y stocker des données personnelles

Q : Il n'est pas recommandé d'utiliser des zones de commentaires libres pour y stocker des données à caractère personnel, dans quelque logiciel que ce soit. Cela dans le respect de la confidentialité des données et dans le respect des droits des personnes concernées ; plus les données seront structurées, plus les droits des personnes pourront être exécutés dans des conditions sécuritaires et organisationnelles optimales.

Q : Une surveillance systématique d'une zone accessible au public via une caméra est-elle pratiquée ?
Aucune surveillance systématique d'une zone accessible au public via une caméra n'est pratiquée

Q : Le responsable du traitement peut-il prouver que le consentement de chaque utilisateur l'informant de la mise en place d'un logiciel de sécurisation et de traçabilité informatique sur son poste de travail, et ses finalités, a été recueilli ?
Le responsable de traitement peut prouver qu'il a recueilli le consentement de chaque utilisateur l'informant de la mise en place d'un logiciel de sécurisation et de traçabilité informatique sur son poste de travail, et de ses finalités

Q : C'est parfait, dans le respect de la réglementation en vigueur et dans le respect des droits des personnes comme stipulé dans le règlement RGPD, chaque utilisateur d'un poste du système d'information doit être informé de l'utilisation d'un tel logiciel de sécurisation, ainsi que de ses finalités précises. Ainsi, il est donc primordial de recueillir le parfait consentement à ce sujet, de chaque utilisateur, par écrit. Vous pouvez reprendre le modèle de consentement présent en annexe du présent audit.



Q : Des données sur des informations de santé ou par rapport à l'orientation sexuelle sont-elles traitées ?
Aucune donnée concernant des informations de santé ou par rapport à l'orientation sexuelle n'est traitée

Q : Des données à caractères sensibles (origine ethnique, opinions politiques, convictions religieuses, appartenance syndicale, données génétiques ou biométriques) sont-elles traitées ?
Aucune donnée à caractère sensible (origine ethnique, opinions politiques, convictions religieuses, appartenance syndicale, données génétiques ou biométriques) n'est traitée

Q : Des données à caractères sensibles relatives à des condamnations pénales ou infractions sont-elles traitées ?
Aucune donnée à caractère sensible relative à des condamnations pénales ou infractions n'est traitée

Q : Le traitement de vos données est-il nécessaire à la sauvegarde des intérêts vitaux des personnes concernées ?
Le traitement des données n'est pas nécessaire à la sauvegarde des intérêts vitaux des personnes concernées

Q : Ces traitements de données sont-ils nécessaires, et justifiés dans le cadre de vos activités ?
Ces traitements de données sont nécessaires et justifiés dans le cadre des activités de l'organisation

Réponse non communiquée

Q : Détenez-vous des listes de membres d'associations ou de C.E ?
Un ou des listes de membres d'associations ou de C.E sont détenues dans l'organisation

Q : Dans le cadre de détention et de traitement de listes de membres d'associations ou de C.E, une méthodologie particulière doit être utilisée afin que les données à caractère personnel soient stockées et accompagnées avec l'enregistrement du consentement, et des préférences de communication des personnes concernées. Si plusieurs outils ou logiciels sont utilisés, il sera alors impossible d'avoir une vue à 360 degrés des données collectées et des consentements associés, ce qui nuit à l'exercice des droits des personnes concernées et des moyens mis à disposition par le responsable du traitement pour tenir à jour ces données.

Q : Dans vos logiciels, des zones de commentaires libres pour y stocker des données personnelles sont-elles utilisées ?
Des zones de commentaires libres dans les logiciels sont utilisées pour y stocker des données personnelles

Q : Il n'est pas recommandé d'utiliser des zones de commentaires libres pour y stocker des données à caractère personnel, dans quelque logiciel que ce soit. Cela dans le respect de la confidentialité des données et dans le respect des droits des personnes concernées ; plus les données seront structurées, plus les droits des personnes pourront être exécutés dans des conditions sécuritaires et organisationnelles optimales.

Q : Une surveillance systématique d'une zone accessible au public via une caméra est-elle pratiquée ?
Aucune surveillance systématique d'une zone accessible au public via une caméra n'est pratiquée

Q : Le responsable du traitement peut-il prouver que le consentement de chaque utilisateur l'informant de la mise en place d'un logiciel de sécurisation et de traçabilité informatique sur son poste de travail, et ses finalités, a été recueilli ?
Le responsable de traitement peut prouver qu'il a recueilli le consentement de chaque utilisateur l'informant de la mise en place d'un logiciel de sécurisation et de traçabilité informatique sur son poste de travail, et de ses finalités

Q : C'est parfait, dans le respect de la réglementation en vigueur et dans le respect des droits des personnes comme stipulé dans le règlement RGPD, chaque utilisateur d'un poste du système d'information doit être informé de l'utilisation d'un tel logiciel de sécurisation, ainsi que de ses finalités précises. Ainsi, il est donc primordial de recueillir le parfait consentement à ce sujet, de chaque utilisateur, par écrit. Vous pouvez reprendre le modèle de consentement présent en annexe du présent audit.

DPO MUTUALISÉ

Un chef d'orchestre à votre disposition !

70 points de contrôle et une analyse de la sécurité

• Applications vulnérables

MACHINE / APPLICATION	VERSION	CRITIQUE
MACHINE : POSTE 1		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	18.11.20040.281318	Non
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	67.0.3396.87	Non
C:\Program Files (x86)\Java\jre1.8.0_60\bin\java.exe	8.0.600.27	Non
C:\Program Files (x86)\Java\jre1.8.0_60\bin\javaws.exe	11.60.2.27	Non
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	12.0.7601.23517 (win7sp1_ldr160812-0732)	Non
C:\Program Files\Internet Explorer\EXPLORE.EXE	100.9600.16428 (winblue_gdr131013-170C)	Non
C:\Program Files\Microsoft Office 15\Root\Office15\EXCEL.EXE	15.0.5031.1000	Non
C:\Program Files\Microsoft Office 15\Root\Office15\WINWORD.EXE	15.0.4997.1000	Non
C:\Windows\system32\mstsc.exe	9600.16415 (winblue_gdr_oob131001-09)	Non
MACHINE : POSTE 2		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	18.11.20040.281318	Non
C:\Program Files (x86)\Internet Explorer\EXPLORE.EXE	30.812.16421 (WIN7_I9_RTM.110308-033)	Non
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	12.0.7601.23517 (win7sp1_ldr160812-0732)	Non
C:\Program Files\Internet Explorer\EXPLORE.EXE	100.9600.16428 (winblue_gdr131013-170C)	Non
C:\Windows\system32\mstsc.exe	6.1.7601.18540 (win7sp1_ldr140716-1508)	Non
MACHINE : POSTE 3		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	18.11.20040.281318	Non
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	67.0.3396.87	Non
C:\Program Files (x86)\Java\jre1.8.0_25\bin\java.exe	8.0.25.18	Non
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	12.0.7601.23517 (win7sp1_ldr160812-0732)	Non
C:\Program Files\Internet Explorer\EXPLORE.EXE	100.9600.16428 (winblue_gdr131013-170C)	Non
C:\Program Files\Java\jre1.8.0_25\bin\java.exe	8.0.25.18	Non
C:\Program Files\Java\jre1.8.0_25\bin\javaws.exe	11.25.2.18	Non
C:\Program Files\Microsoft Office 15\Root\Office15\EXCEL.EXE	15.0.5031.1000	Non
C:\Program Files\Microsoft Office 15\Root\Office15\WINWORD.EXE	15.0.4997.1000	Non
C:\Windows\system32\mstsc.exe	9600.16415 (winblue_gdr_oob131001-09)	Non
MACHINE : POSTE 4		
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe	11.0.23.22	Non
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	67.0.3396.87	Non
C:\Program Files (x86)\Microsoft Office\Root\Office10\EXCEL.EXE	16.0.9330.2087	Non
C:\Program Files (x86)\Microsoft Office\Root\Office10\WINWORD.EXE	16.0.9330.2087	Non
C:\Program Files (x86)\Java\jre1.8.0_25\bin\java.exe	8.0.25.18	Non
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	12.0.7601.23517 (win7sp1_ldr160812-0732)	Non
C:\Program Files\Internet Explorer\EXPLORE.EXE	100.9600.16428 (winblue_gdr131013-170C)	Non
C:\Program Files\Java\jre1.8.0_25\bin\java.exe	8.0.25.18	Non
C:\Program Files\Java\jre1.8.0_25\bin\javaws.exe	11.25.2.18	Non
C:\Program Files\Microsoft Office 15\Root\Office15\EXCEL.EXE	15.0.5031.1000	Non
C:\Program Files\Microsoft Office 15\Root\Office15\WINWORD.EXE	15.0.4997.1000	Non
C:\Windows\system32\mstsc.exe	9600.16415 (winblue_gdr_oob131001-09)	Non
MACHINE : POSTE 4		
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe	11.0.23.22	Non
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	67.0.3396.87	Non
C:\Program Files (x86)\Microsoft Office\Root\Office10\EXCEL.EXE	16.0.9330.2087	Non
C:\Program Files (x86)\Microsoft Office\Root\Office10\WINWORD.EXE	16.0.9330.2087	Non
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	12.0.17134.1 (WinBuild.160101.0800)	Non
C:\Program Files\Internet Explorer\EXPLORE.EXE	11.00.17134.1 (WinBuild.160101.0800)	Non
C:\Windows\system32\Macromed\Flash\Flash.ocx	30	Non
C:\WINDOWS\system32\mstsc.exe	10.0.17134.103 (WinBuild.160101.0800)	Non
C:\Windows\SysWOW64\Macromed\Flash\Flash.ocx	30	Non

Extrait du rapport de sécurité mettant en évidence les failles de sécurité (ici l'obsolescence des versions de logiciels utilisés)

LOGICIEL DÉDIÉ

Pour vous assurer une mise en conformité réelle.

01 INVENTAIRE DES FICHIERS SUR L'ENSEMBLE DU RÉSEAU

Le logiciel recherche dans l'ensemble des fichiers de votre réseau des données à caractère personnel. Il les identifie afin de retrouver facilement les données.

Cela vous permet, par exemple de répondre très rapidement à toute demande de droits à l'oubli (article 17).

Toute correspondance avec un client doit en effet être retrouvée si ce dernier vous demande d'effacer les données le concernant.

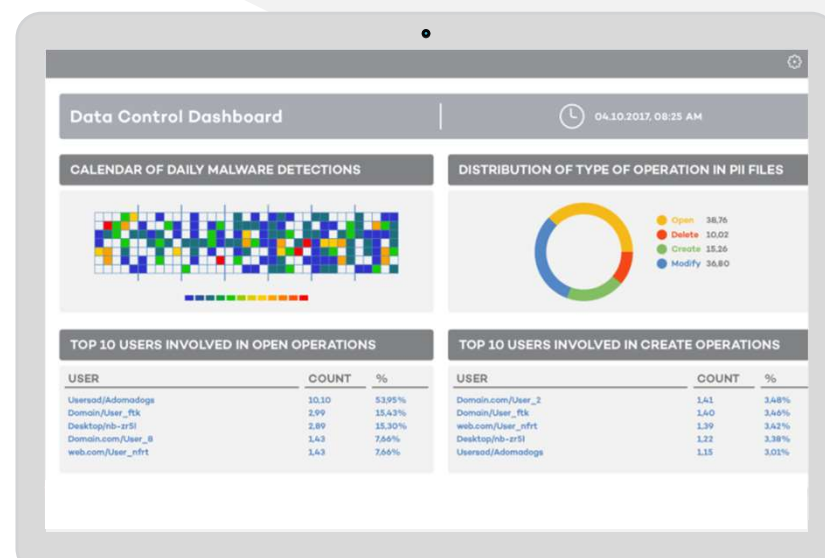
02 REALISATION DE L'AUDIT DE SÉCURITÉ

Le logiciel met en évidence les failles potentielles de sécurité afin d'éviter tous vols ou altérations des données. Vous répondez ainsi à l'obligation de « sécurité du traitement » de l'article 32 du RGPD.

03 GESTION DES LOGS AVANCÉS

En cas de fuites ou d'altérations de données, vous savez qui en est à l'origine grâce à l'enregistrement des actions effectuées sur les fichiers contenant des données personnelles.

3 fonctionnalités primordiales pour une mise en conformité réelle



SÉCURISEZ TOUTES VOS DONNÉES

Avant qu'elles ne soient détruites, volées ou cryptées...

En plus des fonctionnalités dédiées au RGPD, notre logiciel vous permet de sécuriser l'ensemble de vos données contre les menaces informatiques.



Protection contre les « ransomwares » et les « ransomhacks »

Les ransomwares et les ransomhacks sont des menaces informatiques de plus en plus répandues. En cliquant simplement sur une pièce jointe dans un email ou un lien sur internet, le contenu de votre ordinateur se crypte et devient inaccessible. Vous recevez alors une demande de rançon pour déverrouiller votre appareil ou éviter que le pirate ne publie les informations collectées pour prouver votre non-conformité. **Notre logiciel intervient avant la contamination et vous garantit l'intégrité des données.**



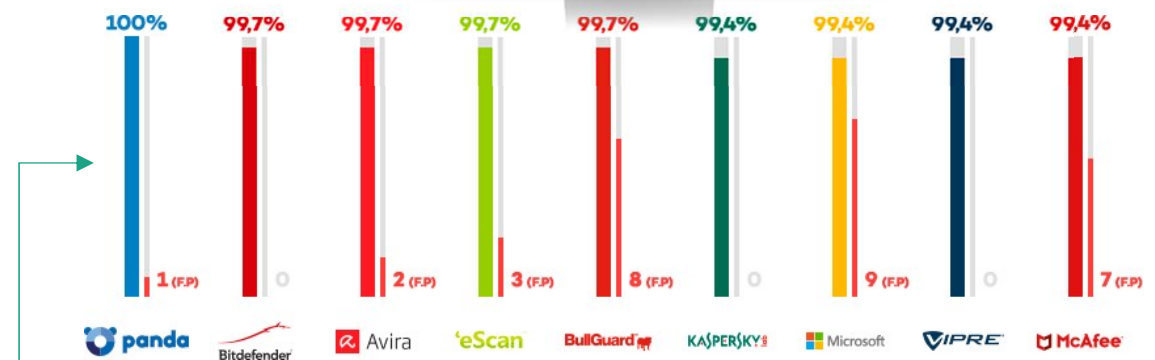
Mise à jour en temps réel

Le logiciel s'adapte en temps réel aux nouvelles menaces, vos données sont constamment protégées !



Informations détaillées

Informations détaillées sur les failles de sécurité potentielles et les attaques déjouées.



Un taux de détection de **100%** selon le test de protection en situation réelle

PLATEFORME RGPD EN LIGNE

Centraliser, analyser, agir...

Afin de pouvoir centraliser, analyser et suivre les actions à mettre en œuvre dans le cadre de la mise en conformité, nous mettons à disposition de nos clients une plateforme en ligne dédiée au RGPD.



La plateforme permet notamment :

- D'accéder à l'ensemble de vos traitements et à ses caractéristiques. Il est possible de les éditer et d'en créer de nouveaux
- D'éditer les registres des traitements
- De centraliser les demandes relatives aux droits des personnes et de suivre l'état des demandes jusqu'à l'archivage
- De gérer la procédure de violation des données
- D'accéder et de piloter les actions de mise en conformité préconisées
- D'accéder à des ressources techniques (vidéos, articles, veille réglementaire...)
- De centraliser les demandes d'assistance (helpdesk)
- D'afficher des indicateurs clés (demandes en attente, actions en cours, nombre de traitements...)



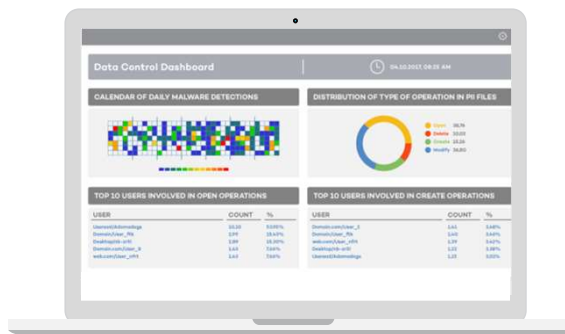
Vue du tableau de bord de la plateforme en ligne

TARIFS

Transparents et tout compris !



DPO mutualisé



Logiciels dédiés RGPD



Sécurité informatique renforcée

TARIF 2018*

Nombre de postes informatiques Redevance mensuelle HT/poste

De 2 à 10 postes	22€
De 11 à 25 postes	19€
De 26 à 50 postes	15€
Au-delà de 50 postes	Nous consulter

*sur la base d'un engagement de 36 mois

Notre solution est compatible avec la plupart des solutions antivirus concurrentes. Si vous souhaitez conserver votre antivirus actuel, merci de nous le préciser

Notre offre globale comprend :

- La mise à disposition d'un DPO mutualisé qui vous accompagnera dans le processus de mise en conformité
- Les logiciels dédiés RGPD
- La partie antivirus pour une sécurité accrue de vos données
- L'audit approfondi de sécurité
- L'audit approfondi RGPD
- L'édition du rapport « correspondant »
- La présentation du rapport et des propositions d'actions correctives
- L'accès à la plateforme en ligne
- ...

EN RÉSUMÉ

Posez-vous les bonnes questions :

1. Est-il plus judicieux de perdre du temps et de l'argent à former un Référent RGPD ou un DPO interne à l'entreprise, plutôt que d'externaliser la mission ?
2. Comment assurer la mise en conformité des données non structurées sans outils logiciels ?
3. Comment garantir la sécurité des données informatiques sans outils logiciels ?

Notre offre globale vous permet de répondre à ces questions et vous assure une mise en conformité **réelle** en toute tranquillité

Pour quelles raisons nous choisir ?

Nous assurons votre tranquillité

et votre mise en conformité

Une offre de service complète

DPO mutualisé, outils dédiés et mise en sécurité de vos données

Des outils dédiés

permettant une mise en conformité réelle

Une équipe à votre écoute

Des DPO experts

Formés par un organisme de formation labélisé CNIL

Des tarifs maîtrisés

Une politique tarifaire compétitive sans surprise, sans frais caché

Votre Interlocuteur Local



France-RGPD est une marque de SPINVEST, partenaire d'Hiteo pour l'installation technique de ses produits informatiques



SPInvest est une entreprise bordelaise spécialisée dans la distribution de la solution éditée par DataVigiProtection

Philippe ALCANTARINI

Email : contact@france-rgpd.com

