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

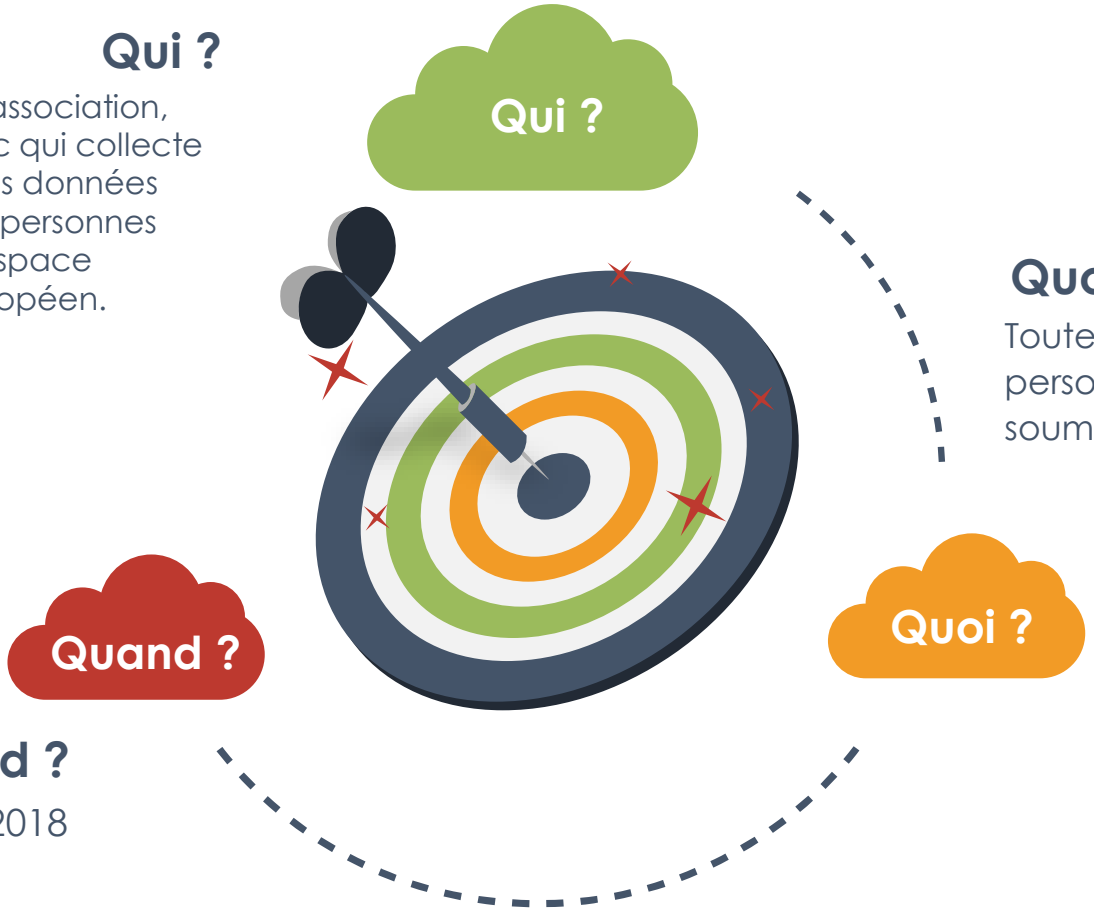
RGPD
99 articles
à respecter !

RGPD : les infos clés...

Le Règlement Européen pour la Protection des Données

Qui ?

Tout entreprise, association, organisme public qui collecte ou a collecté des données concernant des personnes résidant dans l'Espace Economique Européen.



Quoi ?

Toute donnée à caractère personnel collectée est soumise au RGPD.

Quand ?

Depuis le 25 Mai 2018

DATAVIGI PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

LES OBJECTIFS

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

Contrôle des données
Redonner aux citoyens le contrôle de leurs données personnelles tout en unifiant les règlementations relatives à la protection de leur vie privée.

Uniformiser la règlementation
Uniformiser au niveau européen la règlementation sur la protection des données.

Responsabiliser les collecteurs

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

DATAVIGI PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

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**

Deux types de données

DONNÉES STRUCTURÉS ⟷ *Données non structurés*

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

DATAVIGI PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

Quelles opérations sont soumises au RGPD ?

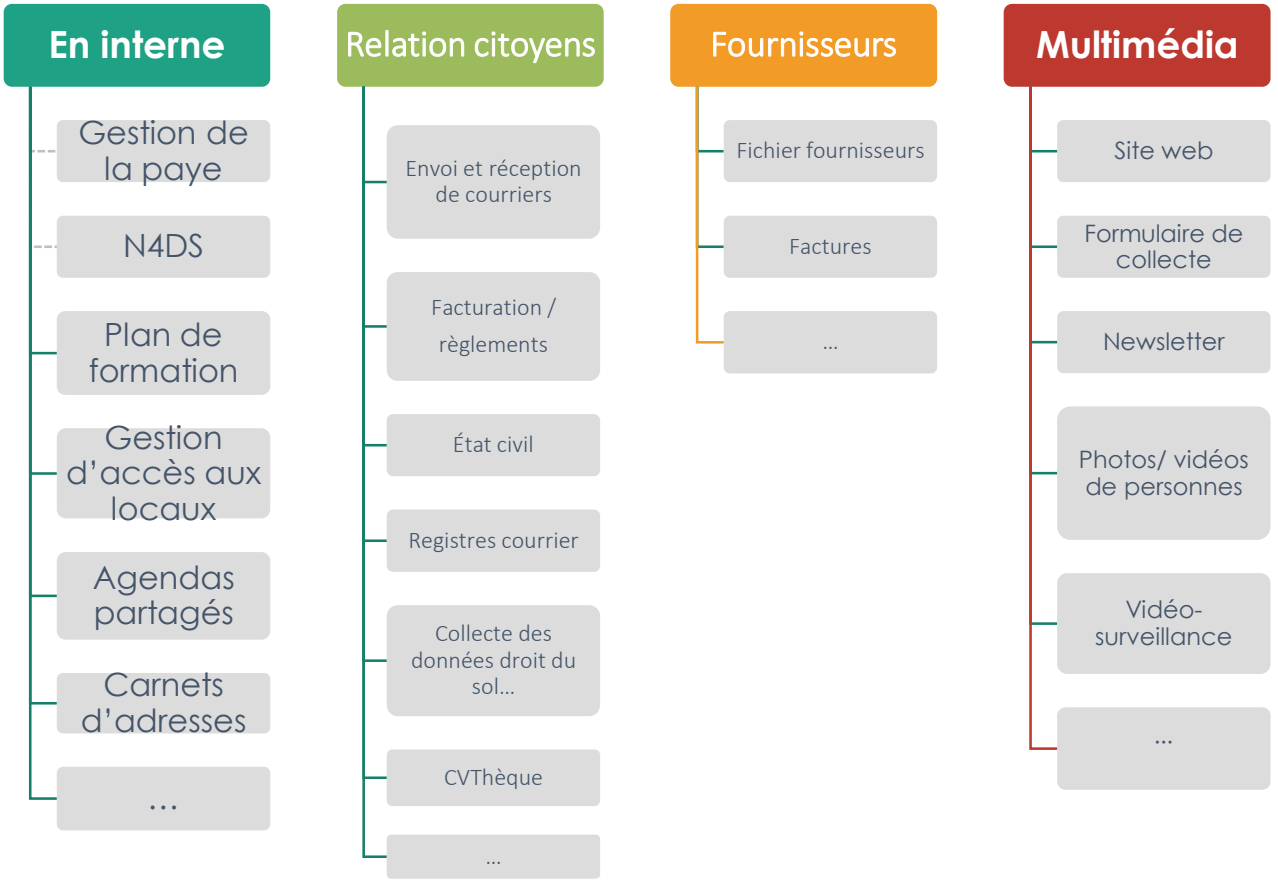
L'ensemble des traitements de données personnelles…

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 conforme 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.

VERS LA MISE EN CONFORMITÉ

- Les 4 étapes clés
- Sanctions et risques
- Les erreurs à ne pas commettre

UNE EXPERTISE NÉCESSAIRE

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

DATAVIGI PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

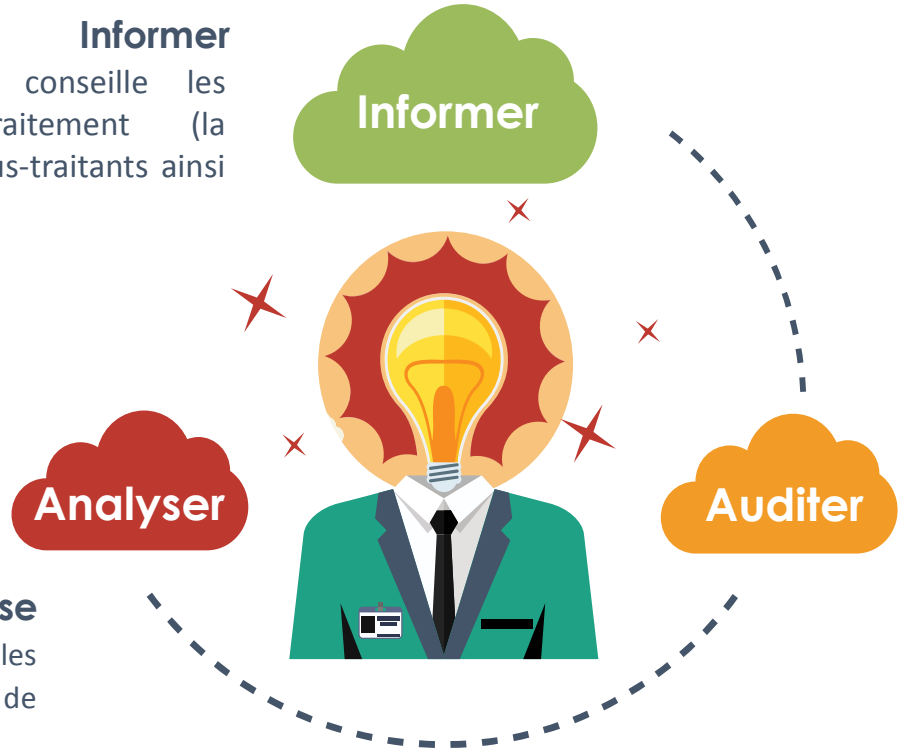
Que fait le DPO ?

Le chef d'orchestre !

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 est obligatoire pour une collectivité de nommer un DPO. Il n'est pas responsable de la conformité, celle-ci est supportée par les responsables des traitements. Le DPO doit être libre et indépendant pour mener sa mission et ne doit pas être placé en situation de conflit d'intérêts.

Informer

Le DPO informe et conseille les responsables de traitement (la collectivité) et/ou les sous-traitants ainsi que ses employés.



Auditer

Le DPO réalise l'audit initial de la structure. Il contrôle ainsi le respect du règlement et du droit en matière de protection des données. Il détermine les actions à mener et les priorise.

Analyse

Le DPO analyse tout au long de l'année les actions menées par la collectivité. En cas de contrôle, il coopère avec la CNIL.

Quel profil pour le DPO ou le Référent ?

Ni informaticien, ni juriste…

Un métier à part entière ?

Le DPO doit disposer de sérieuses compétences en matière :

De droit

Du RGPD

D'informatique

Le DPO 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 la collectivité. Une formation initiale exhaustive, une veille continue et de bons outils sont nécessaires pour assurer la mission correctement.

Autant d'éléments qui complexifient la nomination d'un DPO en interne !

DPO ou Référent interne VS DPO externalisé

Deux possibilités à étudier

	DPO/ Référent interne	DPO externalisé
Avantages	• Connaissance de l'entreprise et des collaborateurs • Réactivité	• 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	• 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	• Temps d'adaptation au fonctionnement de l'entreprise • Dépense supplémentaire

La nomination d'un DPO externalisé est la solution la plus adaptée (voire la seule) pour les collectivités de petite et moyenne taille.

Auditer et Agir

Une fois nommé, le DPO entre en action…

1. **Recenser et cartographier les données**
2. **Constitution des registres obligatoires**
3. **Mise en place des actions de mise en conformité**

Auditer et Agir

Une fois nommé, le DPO entre en action…

4 **Prioriser les actions à mener**

5 **Sécuriser les données**

6 **Sensibiliser et conseiller**

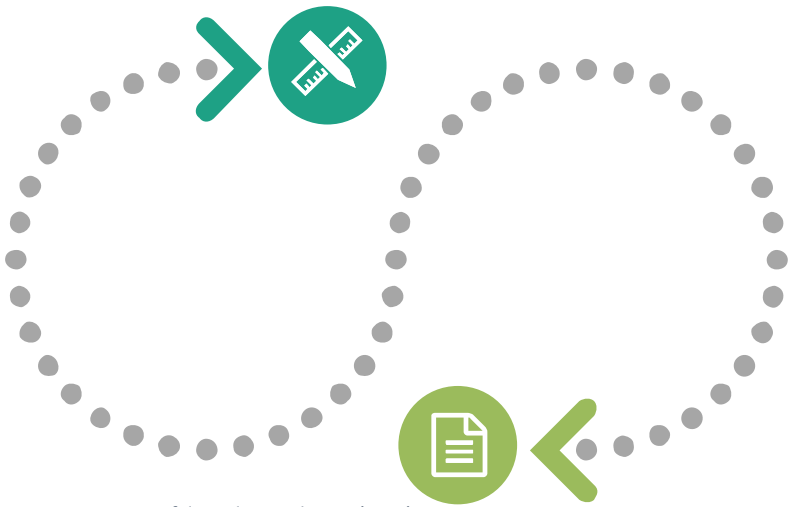
Analyser

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

Sanctions et risques

A ne surtout pas sous-estimer

SANCTIONS

4% du CA annuel globale de l'entreprise.

De 10 millions en cas d'absence de DPO ou de registre de données à jour, à 20 millions d'euros pour les organismes n'ayant prévu aucun traitement pour les données sensibles ou ayant transféré des données hors de l'UE.

RISQUES

Le risque contentieux est à prendre au sérieux. **15 jours après la mise en application du RGPD**, plus de **12 000 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…

- **Imaginer que la nomination d'un DPO vous garantit la mise en conformité !**
- **Imaginer que votre entreprise est déjà conforme sans vous pencher sur la question !**
- **Laissez votre DPO seul !**
- **Sous-estimer le poids du risque pesant sur la sécurité de vos données !**
- **Sous-estimer le risque contentieux et le chemin à parcourir pour s'en prémunir !**

EN RÉSUMÉ

- L’externalisation de la mission DPO est quasi inévitable

- La vigilance lors du choix d’un prestataire RGPD doit être de mise.La seule nomination d’un DPO ne vous garantit pas la mise en conformité.
- Le DPO doit être formé et doté d’outils et de moyens lui permettant d’assurer sa mission.

NOTRE OFFRE
DE SERVICE

UNE SOLUTION GLOBALE

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

Une solution globale

clés en main et sur mesure…

Une solution globale, pourquoi ?

- Nécessite une expertise technique, juridique et informatique
- Outils adaptés la mise en conformité réelle est impossible !

Spécialistes en sécurité informatique depuis plus de 25 ans

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

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 prouver que tout est mis en œuvre pour garantir la sécurité des données.

PROTECTION CONTRE LE VOL DE DONNÉES

ANTIVIRUS

DPO MUTUALISÉ

Un chef d'orchestre à votre disposition !

Le DPO mutualisé

- 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

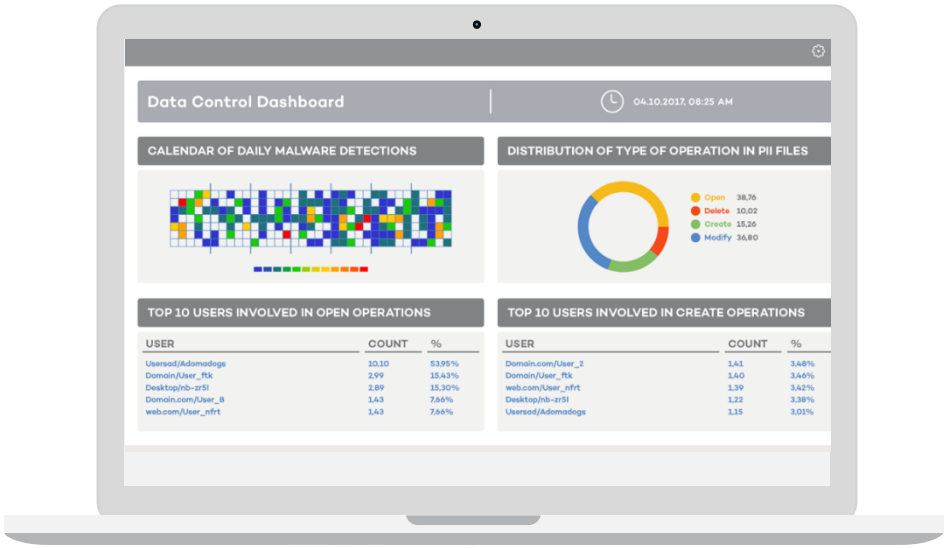
IMPORTANT : Pour mener à bien sa mission, le DPO devra disposer d'outils et de moyens le lui permettant.

#LOGICIEL RGPD

LOGICIEL DÉDIÉ

Pour vous assurer une mise en conformité réelle.

3 fonctionnalités primordiales pour 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.

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.

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.

DATAVIGI PROTECTION
SÉCURITÉ ET CONFORMITÉ RGPD

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 »

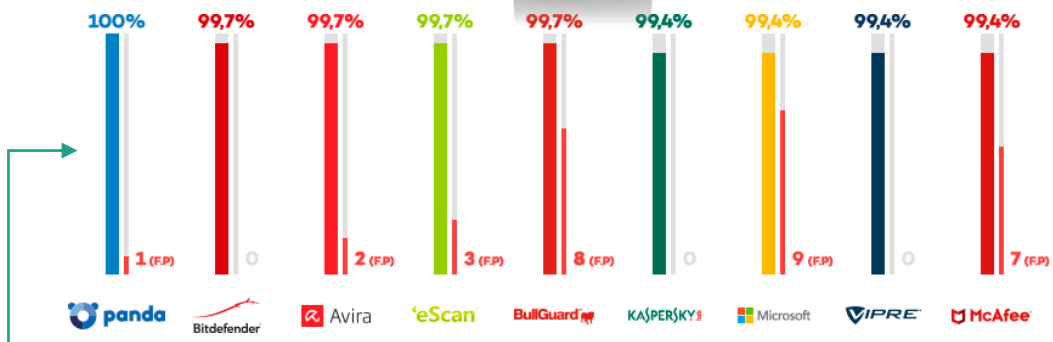
Les ransomwares et les ransomhacks sont des menaces informatiques de plus en plus répandues.
Notre logiciel intervient avant la contamination et vous garantit l'intégrité des données.

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

"Real World Protection Test" AV Comparatives | Juillet 2017 www.av-comparatives.org (F.P.) = Fausses alertes

EN RÉSUMÉ

- Une offre globale qui vous assure mise en conformité réelle et tranquillité
- Posez-vous les bonnes questions :

1. Comment assurer la mise en conformité des données non structurées sans outils logiciels ?
2. Comment garantir la sécurité des données informatiques sans outils logiciels ?

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 DPO experts

Formés par un organisme de formation labélisé CNIL

Des outils dédiés

permettant une mise en conformité réelle

Des tarifs maitrisés

Une politique tarifaire compétitive sans surprise, sans frais caché

Une équipe à votre écoute

15 collaborateurs basés dans les Hauts de France à votre service, sourire compris !

Résumé de l'offre

Pour prouvez votre bonne foi à la CNIL

	CRITÈRES	SOLUTIONS
1.	Sensibiliser les utilisateurs	Devoir de conseil revendeur/ Charte informatique
2.	Authentifier les utilisateurs	AD
3.	Gérer les habilitations	Comptes/Gestion des droits
4.	Tracer les accès et gérer les incidents	Cartographie et gestion des logs
5.	Sécuriser les postes de travail	Antivrus/Politique de sécurité
6.	Sécuriser l'informatique mobile	Antivirus
7.	Protéger le réseau informatique interne	Firewall
8.	Sécuriser les serveurs	Firewall + Pièces sécurisées + Antivirus
9.	Sécuriser les sites web	AV.Firewall
10.	Sauvegarder et prévoir la continuité d'activité	NAS/Politique de sauvegarde
11.	Archiver de manière sécurisé	NAS/Politique de sauvegarde
12.	Encadrer la maintenance	Contrat, comité de pilotage
13.	Gérer la sous traitance	Comité de pilotage
14.	Sécuriser les échanges avec d'autres organismes	Politique de sécurité
15.	Protéger les locaux	Alarmes
16.	Encadrer les développements informatique	Politique de sécurité/Charte informatique, comité de pilotage
17.	Utiliser des fonctions cryptographiques	Politique de sécurité/Charte informatique, comité de pilotage

OFFRE

Package

Software "panda security adaptibe defense"*

panda

+

Installation

Questionnaire en ligne des 17 critères

+

=

Audit général

*Offre disponible sans antivirus