Votre entreprise est-elle prête pour le RGPD ?

Le compte à rebours est déjà enclenché !

pandasecurity.com

panda

Le RGPD constitue une réponse face à la hausse des cyber-attaques et résulte d'un besoin de renforcement de la collaboration entre les entités publiques et privées pour remédier à ce problème permanent.

La création d'un cadre numérique commun constitue une barrière de sécurité supplémentaire pour un des actifs les plus stratégiques de l'entreprise : les données.

1. Introduction

Le nouveau Règlement général sur la protection des données a été approuvé par le Parlement européen et le Conseil le 27 avril 2016. Il est entré en vigueur le 25 mai 2016 et sera applicable à partir du **25 mai 2018.**

Le RGPD définit des normes visant à garantir un niveau de protection uniforme pour le traitement des données personnelles des personnes physiques au sein de l'Union européenne et pour le libre mouvement desdites données au sein des États membres.

Nous avons rédigé ce document afin de faciliter la compréhension des points les plus pertinents du nouveau cadre réglementaire et, ainsi, d'aider les entreprises et organisations à avoir une vue synthétique des changements qu'il apportera. Au final, ce document vise à aider les entreprises à s'adapter aux nouvelles exigences.

Nous encourageons le lecteur à consulter le règlement général sur la protection des données (RGPD) dans sa version intégrale, car il détaille toutes les exigences et leurs implications.

2. Principales conclusions

Le RGPD constitue une réponse face à la hausse des cyber-attaques et résulte d'un besoin de renforcement de la collaboration entre les entités publiques et privées pour remédier à ce problème permanent. La création d'un cadre numérique commun constitue une barrière de sécurité supplémentaire pour un des actifs les plus stratégiques de l'entreprise : les données.

Les entreprises doivent désormais rendre publiques toutes les violations de sécurité dont elles sont victimes et informer les utilisateurs concernés dans un délai de 72 heures. Cette exigence entraînera une augmentation du budget que les entreprises consacrent à la sécurité des réseaux. Une telle obligation existe déjà aux États-Unis.

Le cœur de la sécurité d'entreprise s'est déplacé des infrastructures vers les personnes (gestion des identités et des accès), un aspect qui n'a pas toujours été pris en compte de manière appropriée.

Le changement de modèle qui a conduit à l'adoption du RGPD découle de la double nécessité de prendre des mesures de sécurité préventives concernant la confidentialité des données et d'accréditer la conformité et la délégation de responsabilité.

De nouvelles fonctions ont émergé, notamment celle du délégué à la protection des données (DPD). Le DPD aura pour mission d'informer et de conseiller sur les obligations de l'entreprise, de surveiller la conformité et d'assurer la coopération avec l'autorité de contrôle. Il sera aussi l'intermédiaire avec les détenteurs de données.

Pour instaurer et mettre en œuvre un plan d'action permettant aux entreprises d'adapter leurs pratiques au RGPD, les solutions de cybersécurité dans l'entreprise doivent évoluer et être en phase avec le nouveau modèle, afin de passer d'une sécurité réactive à une sécurité proactive.

3. Qu'est-ce que le Réglement Général sur la Protection des Données (RGPD) ?

Ce règlement de l'Union européenne cherche à protéger les droits et libertés fondamentales des personnes physiques et ,en particulier, le droit à la protection de leurs données personnelles, que celles-ci soient traitées par des entités privées ou des autorités publiques.

Les droits d'accès, de rectification, de retrait du consentement, d'opposition, ainsi que deux nouveaux droits sont reconnus : Le droit à l' effacement, aussi appelé « droit à l'oubli », et le droit de portabilité des données.

Le règlement détaille aussi les exigences de transparence et la limitation du traitement des données personnelles aux fins d'archivage dans l'intérêt public, à des fins de recherche scientifique et historique ou encore à des fins statistiques.

Un autre ajout est la référence au traitement de données européennes par des entités établies en Europe et en dehors de l'Union européenne. Cela concerne les entités qui, même si elles ne sont pas physiquement présentes dans l'Union européenne, exercent des activités sur son territoire et traitent des données personnelles.

À cet amendement est ajoutée l'obligation pour les entités publiques de désigner dans certains cas un « délégué à la protection des données » (DPD) afin de garantir le respect des réglementations. La principale différence avec le responsable de la sécurité est que le DPD doit avoir des connaissances en droit dûment certifiées.

Cette mesure concerne aussi la majorité des entreprises privées. Bien que la présence d'un délégué dépende en principe de la quantité des données traitées et du risque d'exposition de l'entreprise aux attaques, dans ce domaine, le règlement est quelque peu ambigu.

Par ailleurs, le règlement impose l'obligation de notifier l'autorité de contrôle de la protection des données de tout incident de sécurité dont l'entreprise a souffert.

Cette agence sera même habilitée à demander à l'entreprise de rendre public les détails de ces incidents dans un délai maximum de 72 heures après en avoir pris connaissance.

4. Informations de base sur le RGPD

1. Qui est concerné ?

Le règlement concerne toute entreprise qui gère des données personnelles de personnes physiques appartenant à l'Union européenne, même si elles ne sont pas présentes physiquement sur son territoire.

Le terme « personnes physiques » désigne non seulement les clients, mais aussi les clients potentiels, ex-clients et utilisateurs de produits et services qui peuvent avoir été acquis par un tiers, ainsi que les employés et collaborateurs d'une entreprise.

2. Quelle est la durée laissée aux entreprises pour se mettre en conformité ?

Même s'il a été approuvé par le Parlement et le Conseil européen le 27 avril 2016 et s'il est entré en vigueur le 25 mai 2016, le règlement ne sera pas applicable avant le 25 mai 2018.

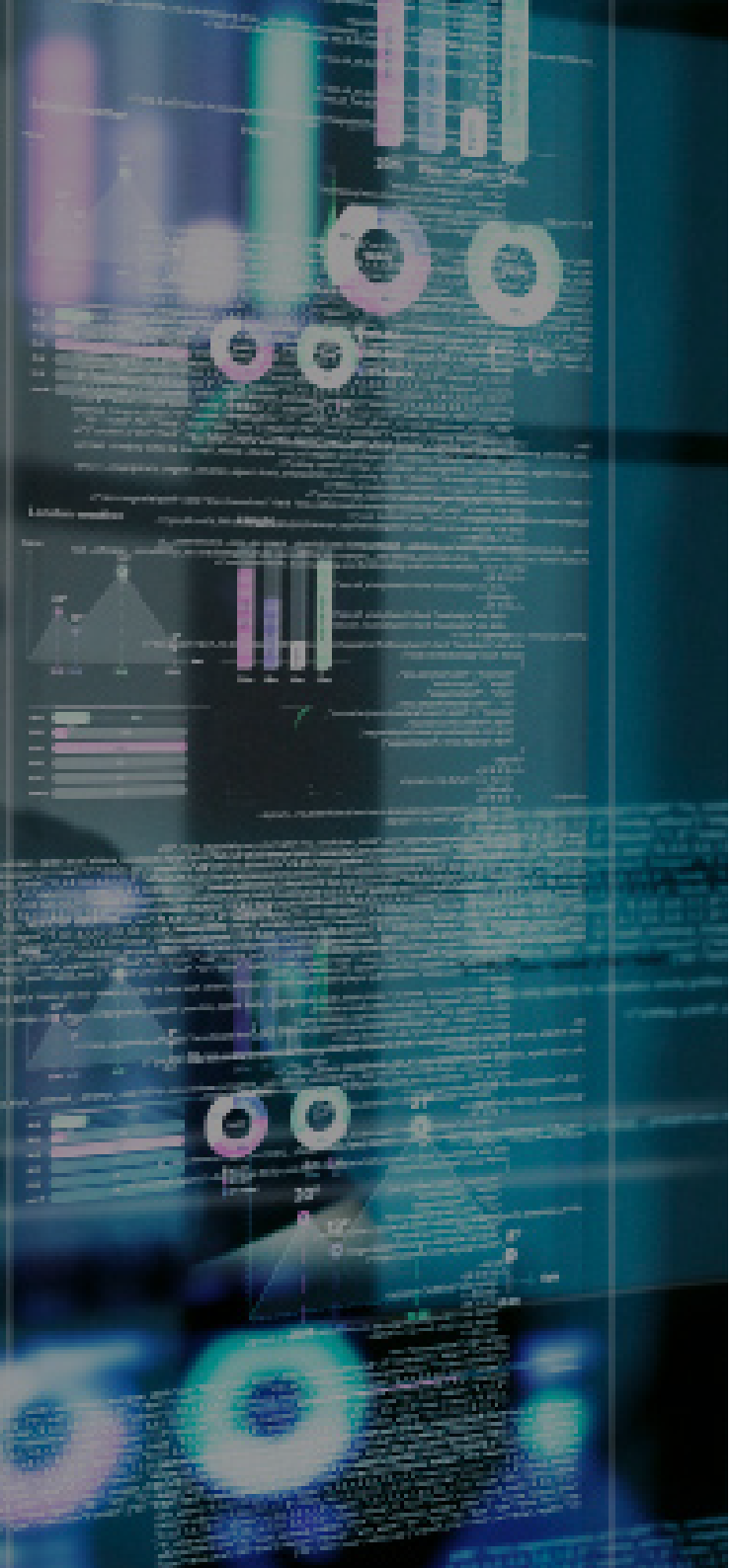
3. Que désignent les données personnelles assujetties au RGPD ?

Les données personnelles désignent toutes les informations sur une personne dont l'identité peut être attestée, que ce soit directement ou indirectement par un nom, un numéro d'identification, des données de lieu, un identifiant en ligne, ou des informations liées à l'identité physique, physiologique, génétique, économique, culturelle ou sociale de ladite personne. Le RGPD s'applique au traitement des données personnelles des personnes physiques citoyennes de l'UE. Curieusement, il est à noter que le règlement s'applique uniquement aux êtres encore vivants.

Il concerne les entreprises qui traitent **les données personnelles des personnes physiques dans les États membres de l'UE.**

Il sera applicable **à partir du 25 mai.**

Il portera sur le **traitement des données personnelles des personnes physiques dans l'UE.**



4. Que recouvrent les données personnelles sensibles ?

Le règlement établit des catégories spéciales de données qui sont considérées comme sensibles et requièrent une protection spéciale, de par leur nature ou par leur relation avec les droits et libertés fondamentales des personnes.

Le règlement interdit explicitement le traitement des données personnelles sensibles qui peuvent révéler une origine ethnique ou raciale, des opinions politiques, des croyances religieuses ou philosophiques, une affiliation à des syndicats, des données génétiques, des données biométriques qui permettent l'identification univoque d'une personne et des données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

En guise d'exception à cette interdiction, le règlement autorise le traitement de catégories spéciales de données lorsque la personne concernée a donné son consentement ou lorsque c'est nécessaire pour protéger ses intérêts vitaux, lorsque la personne a rendu ses données publiques ou encore lorsque le traitement desdites données est effectué légitimement par une organisation à but non lucratif.

Certaines données sont considérées comme sensibles et requièrent un niveau de protection specifique.

5. Quelles sont les conséquences de la violation du règlement ?

Le règlement autorise les autorités de contrôle à imposer des amendes particulièrement élevées, qui peuvent atteindre 20 000 000 € ou 4 % du chiffre d'affaires annuel total de l'exercice précédent, si ce dernier montant est plus élevé. Toutefois, comme nous le verrons ci-après, les sanctions ne seront pas les seules conséquences d'une non-conformité au RGPD lors de sa mise en application en 2018.

Les amendes peuvent aller jusqu'a **20 millions d'euros** ou **4% du chiffre d'affaires annuel global** de l'exercice précédent.

5. Quelques droits et obligations stipulés dans le RGPD

L'objectif du RGPD est de renforcer la protection des données des citoyens de l'UE. Pour ce faire, les entreprises doivent respecter un ensemble d'exigences, afin que les personnes physiques dont les données personnelles sont collectées, stockées et traitées par lesdites entreprises puissent conserver un certain nombre de droits.

Dans cette section, nous compilons des exigences clés que l'entreprise doit respecter et les droits les plus pertinents des personnes physiques mentionnées dans le nouveau règlement. La compréhension de ces aspects permettra de mieux évaluer le niveau des modifications et des prochaines mesures à prendre pour se conformer au RGPD.

1. Obligation de notification d'un incident de sécurité

Les incidents de sécurité concernant les données personnelles doivent être notifiés à l'autorité de contrôle correspondante dans les 72 heures après leur enregistrement.

La notification doit inclure ces éléments :

- Description de la nature de l'incident et de son impact.
- Nombre de personnes et des enregistrements de données personnelles concernés.
- Nom et coordonnées de contact du délégué à la protection des données.
- Description des conséquences vraisemblables de la violation des données personnelles.
- Description des mesures prises ou proposées.

2. Tâches du délégué à la protection des données (DPD)

Une entreprise devra désigner un délégué à la protection des données s'il s'agit d'une **entité publique** ou si son activité principale est le traitement à grande échelle normal et systématique de données, y compris des données personnelles ou des données liées à des condamnations antérieures ou à des infractions pénales.

Dans ce règlement, le terme «grande échelle», qui est relatif et ambigu, n'est pas défini en profondeur. Il est, par conséquent, nécessaire de désigner un DPD pour quasiment toutes les entreprises

Les fonctions du délégué sont les suivantes :

- Informer et conseiller les employés qui gèrent les données quant à leurs obligations.
- Superviser la conformité vis-à-vis du règlement, y compris l'attribution des responsabilités, le travail de sensibilisation et la formation du personnel participant au traitement, et les audits associés.
- Fournir des conseils, selon les besoins, concernant l'évaluation de l'impact de la protection des données et surveiller ses performances.
- Coopérer avec l'autorité de contrôle et servir d'interlocuteur avec celle-ci.

3. Principe de transparence et de consentement

Le principe de transparence nécessite que toutes les informations et communications liées au traitement des données personnelles soient explicites et légitimes, soient faciles d'accès et soient faciles à comprendre.

Dans ces communication, les aspects suivants doivent être parfaitement clairs :

- Les données personnelles collectées, utilisées, consultées et traitées et, en particulier, les finalités, les limites de temps envisagées, les destinataires, la logique impliquée dans tout traitement automatisé et les conséquences dudit traitement.
- Les risques, règles, protections et droits liés au traitement des données personnelles.
- La manière dont chacun peut faire valoir ses droits au regard du traitement des données personnelles.

4. Encouragement de la pseudonymisation

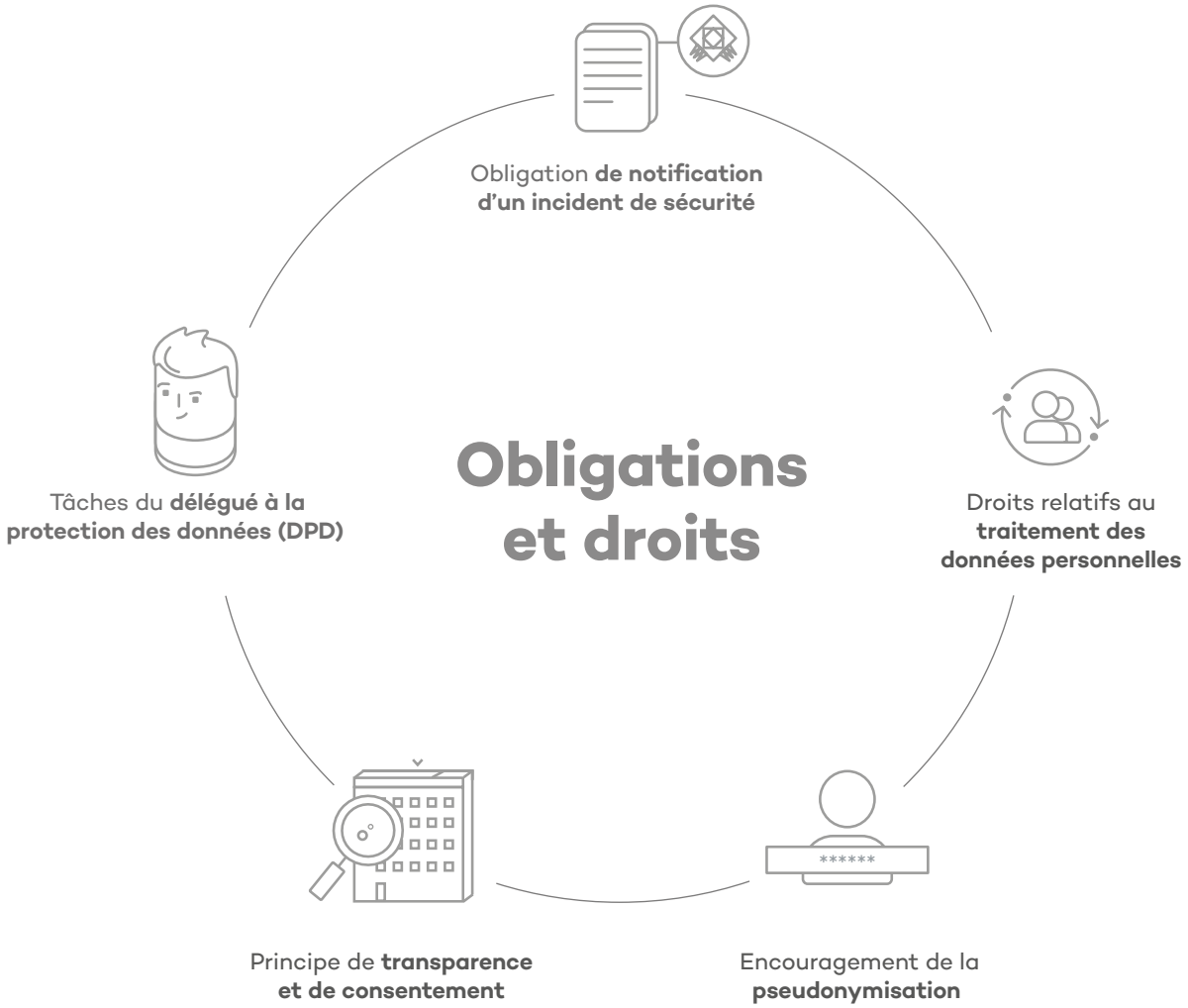
Le RGPD met l'accent sur les données liées à une personne identifiable. Le règlement ne concerne pas les données de personnes physiques non identifiées ou non identifiables.

C'est la raison pour laquelle le RGPD encourage les entreprises à pseudonymiser les données qu'elles collectent. La pseudonymisation est la séparation des données des identifiants qui permettent une identification directe des personnes physiques. La pseudonymisation peut donc réduire significativement les risques associés au traitement des données, tout en préservant son utilité. Bien que les données pseudonymisées ne soient pas entièrement exemptes du règlement, le RGPD allège plusieurs exigences pour les responsables du traitement qui utilisent cette technique.

5. Droits relatifs au traitement des données personnelles

Les entreprises doivent fournir à la partie concernée les moyens d'exercer ses droits :

1. **Le droit de demander et d'obtenir** l'accès à ses données personnelles gratuitement.
2. **Le droit de rectifier et supprimer** les données personnelles la concernant.
3. **Le droit à l'oubli,** autrement dit, le droit de faire supprimer et de faire cesser le traitement de ses données personnelles si elles ne sont plus nécessaires pour les besoins qui ont présidé à leur collecte ou à leur traitement, ou si la partie concernée a retiré son consentement pour le traitement.
4. **Le droit à ne pas faire l'objet d'un profilage.** La partie concernée a le droit de ne pas être l'objet d'une décision basée uniquement sur un profil automatisé. Le profilage est le traitement des données qui facilite l'évaluation de certains aspects personnels liés à une personne physique, en particulier qui visent à analyser ou prédire des aspects concernant les performances au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation géographique ou les mouvements de ladite personne physique.
5. **Le droit à la portabilité** des données personnelles, qui exige des entreprises qu'elles fournissent les données personnelles des parties concernées dans un format courant et qu'elles transfèrent ces données à une autre entreprise en cas de demande en ce sens.



6. Application du règlement aux entreprises

L' obligation d'adopter les pratiques de protection des données du RGPD est une réalité pour quasiment toutes les entreprises exerçant leur activité sur les marchés de l'UE.

Les entreprises qui n'adaptent pas leurs pratiques seront confrontées à des sanctions ainsi qu'à d'autres problèmes aussi sérieux. L' instauration dès que possible d'une démarche de mise en conformité doit être une priorité et, simultanément, constitue une opportunité qui aidera à avoir une plus grande visibilité et un meilleur contrôle des données, ce qui renforcera la protection et pourrait même constituer un facteur de différenciation vis-à-vis de la concurrence.

1. Sanctions et autres problèmes découlant d'une non-conformité

Si les entreprises ne respectent pas le règlement d'ici le 25 mai 2018, qui est la date de son application, elles seront confrontées aux conséquences suivantes :

- **Répercussions économiques directes ou indirectes.** Elles pourraient découler d'incidents de sécurité provenant de l'extérieur de l'entreprise ou de ses propres employés et collaborateurs.
- **Dégradation de l'image de marque.** La réputation de l'entreprise pourrait être ternie en cas d'incidents de sécurité non signalés au public de manière adaptée.
- **Une perte de clients actuels ou potentiels** pourrait survenir si l'entreprise est incapable de montrer sa conformité vis-à-vis du règlement.
- Risque de limitations ou d'interdiction de **traitement de données** imposé par des audits sur la protection des données, ce qui pourrait affecter le fonctionnement normal d'une entreprise.
- **Suspension possible des services de l'entreprise à ses clients,** ce qui pourrait les amener à la quitter, voire à engager une **action en justice**.
- **Réparations** que les parties concernées seraient en droit d'exiger en cas de violation du règlement.
- **Amendes administratives lourdes** pouvant atteindre 20 millions d'euros ou 4 % du CA annuel total de l'exercice précédent, si ce dernier montant est plus élevé.

En se conformant à ce règlement, les entreprises éviteront les problèmes ci-dessus, gagneront la confiance des consommateurs et, ce faisant, disposeront d'un avantage concurrentiel.

Mécanisme de certification approuvé

Les législateurs ont reconnu que pour de nombreuses entreprises, **la possibilité de démontrer qu'elles respectent le RGPD constituera un avantage.** À cette fin, des mécanismes de certification de la protection des données et des vignettes attestant de l'effective protection des données commencent à être introduits.

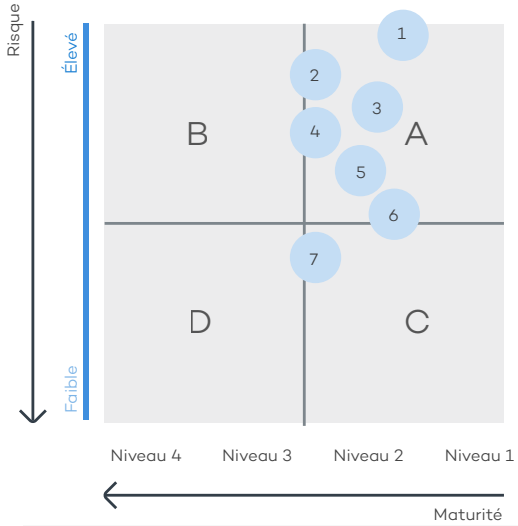
Le RGPD évoque même la possibilité d'un cachet européen commun et, même si le RGPD fournit peu de détails à ce propos, ce mécanisme devrait être développé dans les mois à venir.

2. Plan d'action en vue d'une bonne préparation pour le RGPD

Pour adapter leurs pratiques au RGPD, les entreprises doivent commencer par analyser leur situation actuelle en matière de respect du règlement. Une première étape importante consistera pour les entreprises à maîtriser leurs **procédures de traitement** des données personnelles, notamment :

- Les types de données personnelles traitées, y compris leur collecte, leur transfert et leur stockage.
- L' emplacement des informations et les personnes y accédant, y compris des tiers.
- Le moment et l'emplacement de leur transfert, y compris vers des tiers et par-delà les frontières.
- Les mesures de sécurité adoptées tout au long du cycle de vie.
- Le mode de stockage des informations afin de permettre l'identification du reste des informations.
- La manière dont l'identification, la modification, la suppression et le transfert des données sont octroyés à la partie intéressée à sa demande.
- Le mode de communication et d'archivage de la politique de confidentialité, et son mode d'utilisation pour le traitement des données

En étant sensibilisées aux lacunes en matière de conformité, les entreprises seront bien placées pour évaluer le risque de leurs pratiques de traitement des données personnelles et pour mettre en place des plans correctifs prioritaires



LEGENDE

Cercles

1. Gestion des tiers
2. Formation et sensibilisation
3. Gestion des risques
4. Politique
5. Fuite de données
6. Traitement équitable des clients
7. Gestion des incidents

Secteurs

A. Risque plus élevé
Maturité plus faible

B. Risque plus élevé
Maturité plus élevée

C. Risque plus faible
Maturité plus faible

D. Risque plus faible
Maturité plus élevée

Figure 1. Les entreprises devront relever de nombreux défis pour leur préparation au RGPD de l'UE dans les mois à venir. La première étape consiste à appréhender leur situation actuelle et à établir ce qui suit dans ce rapport pour s'engager sur la voie de la conformité.

7. Réalité du règlement pour les entreprises

Selon une étude réalisée par Dell en septembre 2016 auprès d'un total de 821 employés responsables de la confidentialité des données dans des entreprises ayant plus de 10 % de clients en Europe, les PME et les grandes entreprises ont une méconnaissance du nouveau Règlement général sur la protection des données de l'UE**.**

En résumé, les entreprises n'ont pas de plan, et ne savent pas non plus vraiment comment se préparer. Elle semblent aussi peu conscientes des répercussions que leur non-conformité pourrait avoir sur la **sécurité des données** et sur **l'entreprise** en général.

Ainsi, 82 % des professionnels responsables de la sécurité des données dans le tertiaire et le secteur informatique sont **préoccupés** par la necessité de conformité vis-à-vis du nouveau règlement. Logiquement, c'est en europe que la préoccupation est plus élevée, principalement en Allemagne et en Suède, et en particulier dans les **grandes entreprises.**

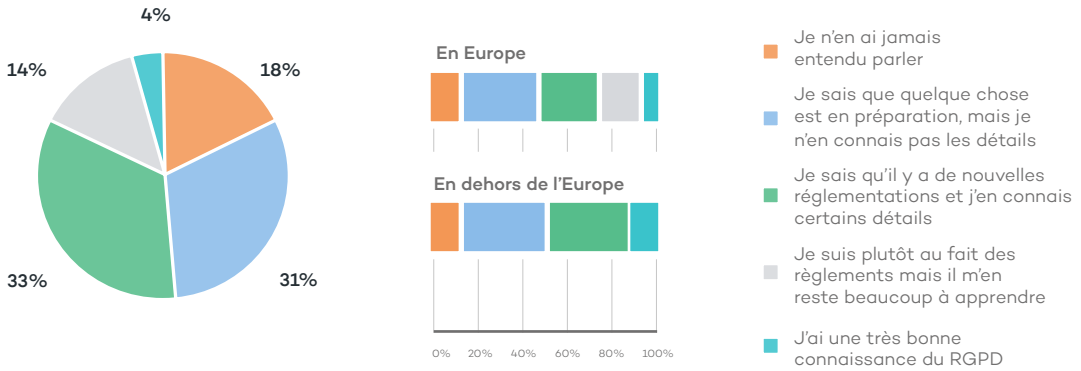


Figure 2. Comment décririez-vous votre connaissance du RGPD ?

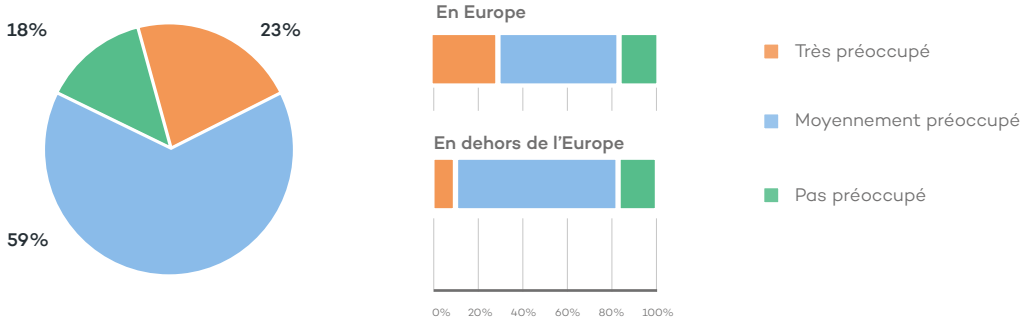


Figure 3. À quel point êtes-vous préoccupé par la conformité vis-à-vis du RGPD ?

Ce constat concorde avec le fait que les **Allemands** sont les plus préparés à appliquer le RGPD (4 %), tandis que les personnes interrogées au **Benelux** (Belgique, Pays-Bas et Luxembourg) indiquent être les **moins préparées.**

En fait, plus de **80 % des personnes répondent qu'elles ont une connaissance réduite voire nulle** des implications et seulement **3 % des professionnels de l'informatique y sont préparés.**

Selon l'étude, même si les entreprises réalisent qu'une violation du RGPD peut avoir un **impact sur la sécurité des données et leurs résultats, elles ne sont pas sûres de l'étendue** des changements à mettre en œuvre, ni de la gravité des sanctions en cas de non-conformité.

Seulement 23 % s'attendent à des changements majeurs dans leurs pratiques concernant la sécurité des données et sur leur technologie.

Plus de 80 % des personnes interrogées **en savent très peu** sur le nouveau règlement, n'ont pas de plan de mise en œuvre du nouveau règlement et ne sont pas préparées. **Seulement 3 % ont un plan pour sa mise en œuvre.**

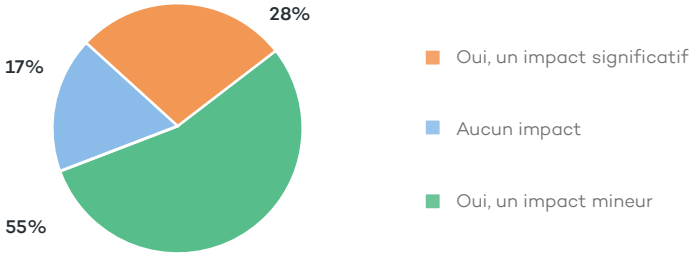


Figure 4. À votre avis, le RGPD aura-t-il un impact sur votre approche de la sécurité des données ?

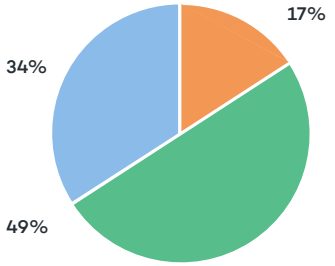


Figure 5. À votre avis, le RGPD aura-t-il un impact sur les résultats de votre entreprise ?

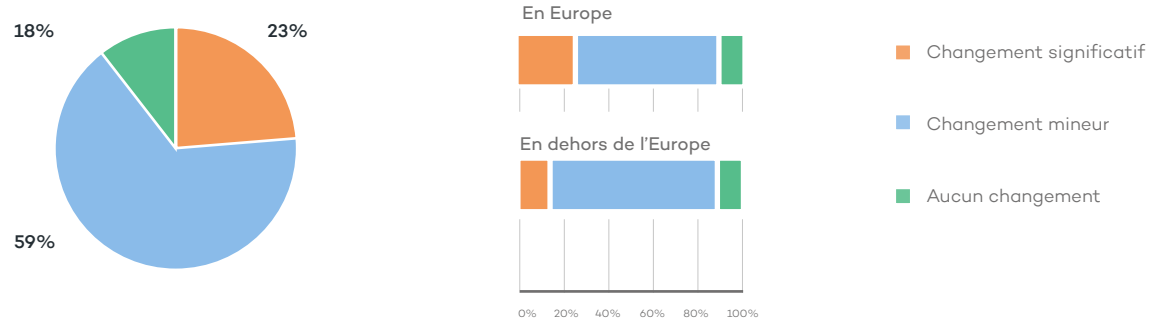


Figure 6. Jusqu'à quel point pensez-vous que les technologies et pratiques actuelles devront changer du fait du RGPD ?

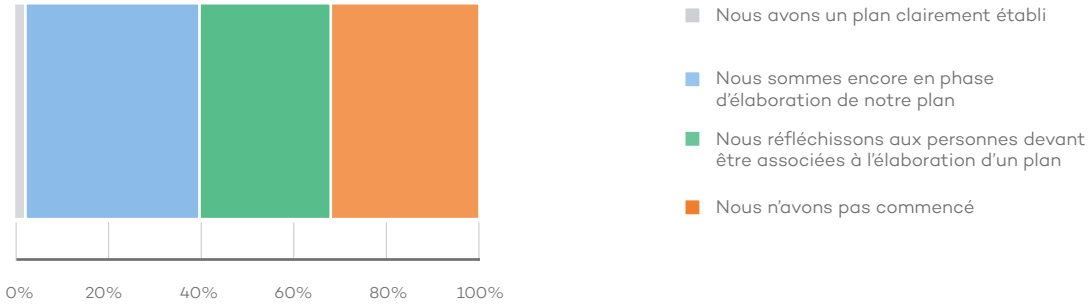


Figure 7. Votre entreprise a-t-elle un plan de préparation au RGPD ?

8. Panda Adaptive Defense peut vous aider à vous mettre en conformité avec le RGPD

Comme nous venons de le voir, il existe, d'une part, **un besoin d'adapter les pratiques en matière de sécurité des données et les technologies** sous-jacentes aux exigences du nouveau règlement, et, d'autre part, une méconnaissance de la part des entreprises de leurs nouvelles obligations, de l'impact potentiel sur leur organisation et des risques économiques induits.

Une fois que les entreprises prendront conscience de ces aspects, le processus d'assimilation recessitera un effort considérable de sensibilisation, de formation, d'analyse et de mise en œuvre des nouvelles pratiques et technologies. Tout ce travail risque d'être vain si les choix effectués sont erronés. Une erreur humaine peut aboutir à une défaillance du système de sécurité et les données gérées par l'entreprise peuvent aussi être perdues ou volées.

Les conséquences peuvent être pires encore : sanctions économiques directes et indirectes, dégradation de la réputation, perte de clients, limites imposées aux opérations, plaintes de clients et demandes d'indemnisation.

Panda Adaptive Defense réduit au minimum ces risques et aide les entreprises à respecter le RGPD, en s'appuyant sur deux piliers fondamentaux : la sécurité et la gestion des informations.

Ils constituent les deux axes stratégiques.

1) Contrôle des données collectées, stockées et traitées dans les différents départements de l'entreprise (RH, marketing, etc.), sur les postes de travail et les serveurs,

2) Adoption des mesures de sécurité nécessaires pour les protéger des pirates.

Une fois que les entreprises prendront conscience de ces aspects, le processus d'assimilation nécessitera un effort considérable de sensibilisation, de formation, d'analyse et de mise en œuvre de nouvelles pratiques et technologies.

À partir de ces bases, il est possible de déduire trois domaines d'action garantissant la sécurité des données :

1. Préparation

Une attitude proactive est très importante. La disponibilité d'un système au moment d'effectuer des analyses a posteriori détaillées est cruciale pour neutraliser une attaque le plus rapidement possible.

Adaptive Defense inclut un système d'audit interne qui **vérifie le statut de sécurité de l'infrastructure informatique** à tout moment, même avant le déploiement de la solution. Il se révèle un outil très précieux pour l'implémentation du plan d'action de conformité vis-à-vis du RGPD ou pour des utilisations régulières.

2. Protection

Une véritable solution de sécurité doit combiner des technologies sophistiquées avec l'intelligence humaine et informatique. En d'autres termes, il faut combiner l'apprentissage machine et le savoir-faire des experts en sécurité. Pour être prise au sérieux, la solution de sécurité doit offrir le type de prévention, de détection, de visibilité et d'intelligence capable d'arrêter et de prévenir inlassablement les cyber-attaques de toutes sortes.

Les exigences de protection d'une entreprise, y compris celles requises par le RGPD, imposent aux solutions de sécurité de couvrir les aspects suivants,qui sont pris en charge par **Adaptive Defense** et **Adaptive Defense 360** :

- **Surveillance continue,** en enregistrant et en surveillant toutes les activités des processus en cours, afin d'empêcher le démarrage de logiciels non fiables au moment de l'exécution, de détecter des menaces avancées en temps réel, de réagir en quelques secondes et de rétablir le fonctionnement normal instantanément.
- **Détection de l'exécution de fichiers non fiables,** afin de réduire le périmètre des attaques menées contre l'entreprise. L' entreprise doit vérifier que la solution de sécurité recherchée puisse classifier comme fiables ou malveillantes toutes les applications qui s'exécutent sur ses appareils.
- **Détection intelligente des menaces**
  Une menace est toujours plus rapide que l'appareil à protéger, quel qu'il soit. Par conséquent, ce n'est pas à l'utilisateur de s'atteler à la tâche de surveillance de la réponse. Les solutions de sécurité efficaces doivent être capables de fonctionner en autonomie et de s'adapter automatiquement à l'environnement d'exploitation, unique, de chaque entreprise.
- **Réponse rapide et automatisée.**
  Les organisations sont saturées par le volume d'événements et d'alertes générés par leurs systèmes, mais une fois le cybercriminel infiltré, quelques secondes peuvent lui suffire pour dérober des informations. Par conséquent, la solution de sécurité choisie doit être capable d'identifier rapidement une attaque en cours, de prendre des mesures pour éviter des dommages et d'alléger la charge de travail des systèmes. Ainsi, l'entreprise peut réduire les coûts et automatiser des tâches dont l'exécution nécessitait auparavant plusieurs jours.

3. Visibilité et contrôle

Les données sont comme la matière vivante. Elles croissent, changent, et plus encore. Leur gestion en conformité avec le nouveau règlement constitue seulement un début.

Une fois que tout est en place pour une gestion efficace, il reste encore la question du suivi constant et des méthodes pour identifier toute anomalie susceptible de se produire.

Le module optionnel **Advanced Reporting Tool (ART)** d'Adaptive Defense est un outil de sécurité intelligent qui génère automatiquement des rapports sur l'activité de tous les postes clients.

Ce système intelligent donne aux entreprises la capacité d'identifier des comportements inhabituels et des attaques, ainsi que les éventuels écarts de conduite en interne. Il se base sur la surveillance constante des événements se produisant sur les postes clients, lesquels événements sont envoyés à la plate-forme Adaptive Defense pour l'enrichir. Le module ART offre aux entreprises les possibilités suivantes :

- **Supervision et contrôle** de l'utilisation inappropriée des ressources de l'entreprise.
- **Réception d'alertes** concernant les indicateurs de sécurité et l'utilisation des ressources d'entreprise, ainsi que les fichiers contenant des données personnelles.
- **Exécution d'analyses** sur les aspects critiques concernant les incidents de sécurité et les anomalies d'accès aux fichiers de données personnelles.
- **Calculs de rapports et visualisation graphique** concernant l'activité détectée sur les postes clients et serveurs.

Si le service de sécurité informatique d'une entreprise utilise un outil de gestion des informations et des événements de sécurité (**SIEM**), la nature ouverte de la plate-forme Adaptive Defense facilite l'intégration en temps réel des informations d'activité recueillies sur les postes clients dans l'ensemble des journaux d'évenement (logs) gérés par le SIEM.

Cette approche permet aux équipes de sécurité de l'entreprise ou au centre d'opérations de sécurité (SoC) externe d'effectuer les actions suivantes :

- **Étendre leur approche de sécurité intégrale** en englobant non seulement le réseau périphérique, mais aussi les postes clients.
- **Obtenir une vue privilégiée des attaques et de leur impact global,** pour des analyses en profondeur a posteriori.
- **Exploiter au mieux** les informations collectées afin de mieux apprécier la situation de l'infrastructure informatique de l'entreprise et mettre en place des stratégies d'amélioration.
- **Enrichir les données SIEM** en les corrélant avec des données supplémentaires provenant des postes clients, afin d'introduire plus d'information d'entreprise dans les systèmes.


TOP10 accessed Files from endpoints

MACHINE	CHILDPATH	COUNT	%
BIOIGIL	SYSTEMDRIVE | \Users\igil\AppData\Local\Google\Chrome\User Data\Default\Login Data	21	0.055%
BIOIGIL	DESKTOPDIRECTORY | \CAU_gestinven_II.mdb	20	0.053%
BIOMARTINEZ	APPDATA | \Mozilla\Firefox\Profiles\u7tq2np1.default\places.sqlite	19	0.050%
BIOIGIL	INTERNET_CACHE | \Content.Outlook\1ZE6EX4F\Visual Studio 2013 and MSDN Licensing Whitepaper - January 2015 (BG).pdf	19	0.050%
BIOIGIL	INTERNET_CACHE | \IE\609EM7I5\Office_365_Addons_Customer_Overview.pdf	19	0.050%
BIOIGIL	RECYCLED | \S-1-5-21-20473081-1892483688-328166375-9156\$I3ARFTK.pptx	19	0.050%
BIOPDELACASA	DESKTOPDIRECTORY | \redes_escalados.pdf	18	0.048%
BIOSAUCIO	DESKTOPDIRECTORY | \20160302_secure.pandasoftware.com.pfx	18	0.048%
BIOJCORDERI	PROFILE | \AppData\LocalLow\LastPass\sites.dat	18	0.048%
BIOIGIL	TEMP | \Temp\B83567864E4EA54582971867#D9DFCE\fullppt.ppt	18	0.048%

Figure 8. Exemples de visibilité fournie par le module ART.

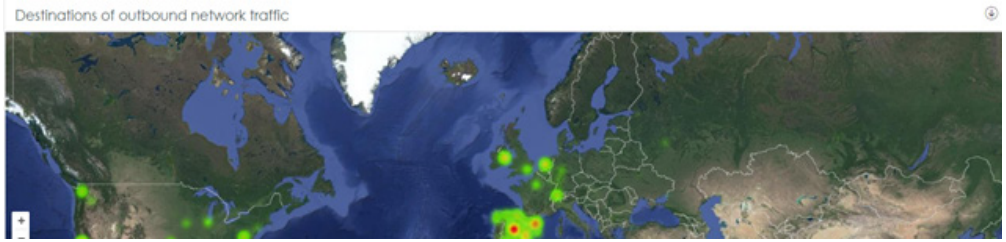


Figure 9. Géolocalisation du trafic sortant d'une entreprise.

Panda Adaptive Defense assure avant tout la sécurité de l'entreprise et de ses données. Les entreprises qui ont placé leur confiance dans Adaptive Defense sont déjà bien avancées sur le chemin de la conformité au RGPD. Adaptive Defense a apporté à ces entreprises les atouts suivants :

- **Protection** des données personnelles traitées sur les systèmes de l'organisation, en empêchant par exemple le démarrage de tout processus non fiable.
- **Réduction des risques, indicateurs d'activité clé et statut des postes clients,** afin de faciliter la mise en place de protocoles de sécurité et d'informer les administrateurs des appareils vulnérables, des activités réseau internes et externes anormales, etc.

- **Outils** permettant de respecter l'exigence d'**informer les autorités des incidents de sécurité dans les premières 72 heures après une violation.** Grâce aux outils d'analyse a posteriori, aux alertes, à la visibilité et au contrôle total fournis par Adaptive Defense/Adaptive Defense 360, l'entreprise disposera en permanence des ressources appropriées pour générer rapidement un rapport et mettre en place un plan d'action afin d'éviter de futurs incidents.

- **Mécanismes de contrôle et gestion des données pour le délégué à la protection des données,** afin que celui-ci soit informé en temps réel des incidents de sécurité mais aussi du fait qu'ils concernent ou non des fichiers de données personnelles compromis. Le module ART, via les alertes temps réel, la console d'administration et les rapports, et les systèmes de notification SIEM d'entreprise alerteront le délégué de toute activité anormale impliquant un accès à des fichiers de données personnelles.

9. Questions les plus fréquentes concernant le RGPD

1. Qui sont les entités et agents principaux concernés par le RGPD ?

Le Comité européen de la protection des données. Le Comité est constitué d'une autorité de contrôle de chacun des vingt-huit États membres et du Contrôleur européen de la protection des données. Le rôle du Comité est d'examiner les pratiques efficaces et inefficaces, ou encore de fournir des conseils et des directives.

Autorité de contrôle de la protection des données. Autorité publique indépendante mise en place par un État membre pour appliquer la législation locale.

Sous-traitant des données. Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement. Le sous-traitant ne détermine pas la finalité et les moyens du traitement. Il se contente de traiter les données à la demande du responsable du traitement.

Exemple : Une société de gestion externalisée de la paie ou un fournisseur de services de cloud tel que Microsoft Azure™, où les données sont collectées, stockées et traitées.

Si un prestataire agit conformément aux exigences, il constitue un responsable de traitement. Selon l'ancienne directive, une amende était imposée uniquement en cas de non-conformité vis-à-vis du responsable du traitement.

Avec le nouveau règlement, le sous-traitant doit aussi respecter ses propres obligations, notamment en prenant des mesures de sécurité appropriées.

Responsable du traitement. La personne ou le département chargé de définir les données personnelles dont l'entreprise a besoin et leur finalité. Ensuite, l'entreprise demande les données auprès des personnes (employés, clients, public, etc.). Une page Web qui demande un nom et une adresse pour envoyer un colis en est un exemple. L'entreprise qui demande les informations et établit la finalité de leur utilisation est responsable des données.

Le responsable du traitement doit non seulement se conformer au règlement, mais aussi apporter la preuve de sa conformité. Ce point est l'une des principales différences entre ce règlement et les autres. Le responsable devra être en mesure de démontrer la conformité à tout moment, à la demande de l'autorité de contrôle ou de la partie concernée.

2. Que deviennent les lois sur la protection des données des États membres ?

Le règlement ne les abroge pas et elles ne sont pas abrogeables, car elles relèvent de la compétence de chaque État membre. Le règlement provoque le déplacement normatif des lois des États membres pour tout ce qui entre en conflit avec le règlement européen. Néanmoins ces lois demeureront en vigueur jusqu'à ce qu'elles soient complètement abrogées ou modifiées pour les adapter au RGPD.

Par conséquent, il sera nécessaire de prendre en compte le RGPD mais aussi la loi de l'État membre. En cas de conflit entre les deux, le RGPD prévaudra sur la loi de l'État membre.

3. Les entreprises doivent-elles revoir leurs avis de confidentialité ?

La réponse est oui. Dans les informations fournies aux parties concernées, le règlement prévoit l'inclusion d'aspects qui n'étaient pas forcément obligatoires selon le règlement et de nombreuses lois nationales qui se recoupent. Par exemple, il sera nécessaire d'expliquer les bases légales du traitement des données, de définir leur période de conservation et d'informer les parties concernées qu'elles peuvent adresser leurs réclamations aux autorités de protection des données si elles pensent qu'il existe un problème concernant le mode de traitement de leurs données. Il est

important d'avoir à l'esprit que le règlement exige expressément que les informations fournies soient faciles à comprendre et soient présentées dans un langage clair et concis.

4. Cela change-t-il le mode d'obtention du consentement ?

Un des fondements du traitement des données personnelles est le consentement. Le règlement exige que celui-ci soit, en général, volontaire, informé, spécifique et sans équivoque. Pour pouvoir considérer le consentement comme sans équivoque, le règlement exige une déclaration de la part des parties concernées ou une indication positive selon laquelle la partie concernée a donné son consentement. Le consentement ne peut pas être déduit du silence ou de l'inaction des clients ou d'autres personnes physiques.

Les entreprises doivent examiner le mode d'obtention et d'enregistrement du consentement.

Il est à noter que le consentement doit être vérifiable et que les personnes collectant des données personnelles doivent être capables d'apporter la preuve du consentement donné par la personne concernée. Il est donc important d'examiner les systèmes d'enregistrement des consentements afin de pouvoir assurer leur vérification par un audit.

5. Est-il possible d'externaliser ou de scinder les responsabilités du DPD ?

Les entreprises dont le budget est limité peuvent externaliser ou partager les tâches du DPD. En Allemagne, la loi fédérale sur la protection des données (BDSG) impose aux entreprises de plus de 9 employés de nommer un DPD, mais une externalisation de cette fonction auprès de sociétés spécialisées dans les données ou de cabinets d'avocats est fréquente.

Le règlement stipule qu'un groupe d'entreprises peut nommer un DPD unique à condition que celui-ci soit accessible facilement à partir de chaque établissement.
Si l'entreprise choisit l'externalisation du DPD, il sera nécessaire d'établir un contrat de niveau de service (SLA), afin de garantir le respect du RGPD. La conformité passe non seulement par la case DPD, mais aussi en veillant à ce que le DPD puisse répondre à tout moment aux différentes requêtes des parties concernées.

6. Quand, comment et à qui signaler un incident de sécurité ?

Quand ? Un incident de sécurité doit être notifié chaque fois qu'il affecte les données personnelles de personnes physiques, indépendamment du fait qu'il entraîne une perte ou un vol ou qu'il s'agit simplement d'un accès aux données.

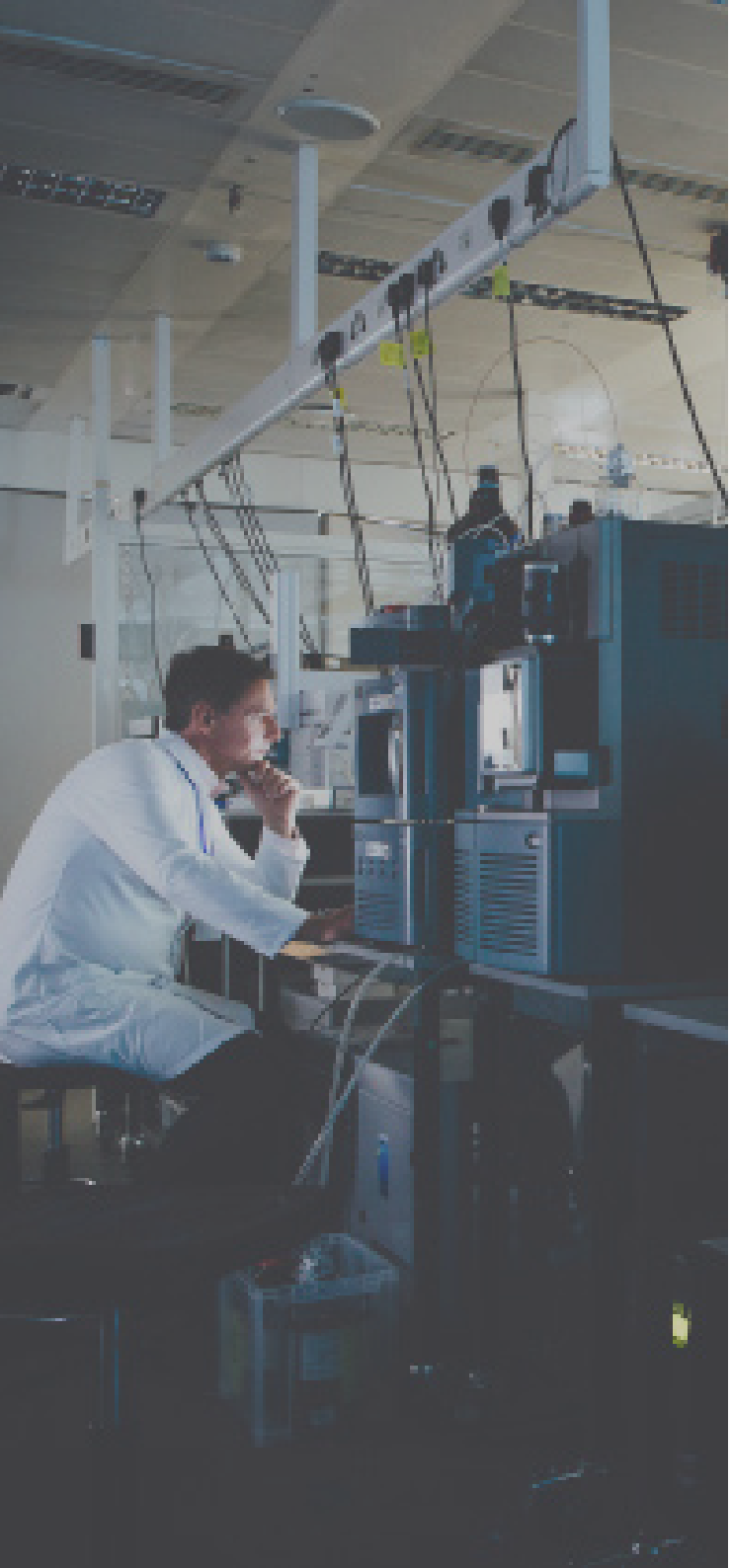
L' absence de signalement rapide de l'incident peut donner lieu à des amendes jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel.

À qui notifier ? Il est important d'avoir à l'esprit l'existence de deux seuils différents, un pour notifier les clients ou le public, et un autre pour alerter l'autorité de contrôle de la protection des données.

- Si les données personnelles ayant fait l'objet d'un accès incluent un identifiant, par exemple une adresse e-mail, un ID de compte en ligne ou une adresse IP, il sera nécessaire de notifier les personnes physiques concernées.
- Si les données contiennent des informations monétaires à savoir des numéros de compte bancaire ou d'autres identifiants financiers, l'incident est susceptible de porter préjudice à la personne et l'autorité de contrôle doit être notifiée.

Comment ? Outre la description de la nature de l'incident, la notification doit mentionner les types de données, le nombre de personnes et le nombre d'enregistrements exposés. L'entreprise doit décrire les conséquences possibles de la non-conformité, ainsi que les actions d'atténuation à mettre en place.

Quel est le délai ? La notification à l'autorité de contrôle doit intervenir dans les 72 heures après l'incident.



Comment se préparer à cet événement ? L'entreprise doit s'assurer qu'elle a une procédure interne pour le reporting d'incident et qu'elle dispose de tous les détails de l'incident, en particulier en cas d'accès à des données personnelles. Elle ne doit pas oublier de soumettre un dossier des mesures correctives mises en place. Pour ce faire, il faut présenter des informations sur les voies d'entrée du pirate, sur la configuration des postes de travail attaqués et leur vulnérabilité, sur les systèmes affectés, etc. Cela facilitera les décisions concernant la notification au public et à l'autorité de contrôle. Au vu des délais réduits de signalement d'un incident, il est important d'avoir une détection robuste des attaques, des capacités d'analyse a posteriori, des alertes temps réel et des rapports d'analyse détaillés à présenter au public ainsi qu'à l'autorité de contrôle.

Panda Adaptive Defense est le meilleur allié de l'entreprise dans le processus d'assimilation du RGPD, car il offre les atouts suivants :

- Protection des données personnelles traitées sur les systèmes de l'entreprise.
- Réduction de l'exposition aux attaques.
- Outils facilitant le respect de l'obligation de notification des incidents de sécurité dans les premières 72 heures.
- Mécanismes de contrôle et de gestion des données pour le DPD, permettant les notifications en temps réel des incidents de sécurité, mais aussi des incidents pouvant porter sur des fichiers contenant des données personnelles.

7. Les entreprises doivent-elles commencer la mise en place immédiate des mesures prévues par le règlement ?

Pas nécessairement. Le règlement est en vigueur, mais il ne sera pas applicable avant le 25 mai 2018.

Néanmoins, il peut être utile de commencer à évaluer la mise en œuvre de certaines des mesures prévisibles :

- Exécution d'une analyse des risques des systèmes de données de l'entreprise, à commencer par une identification du type de traitement qu'ils réalisent.
- Mise en place d'archives de traitement des données.
- Implémentation d'évaluations d'impact ou de toute autre mesure prévisible.
- Conception et mise en œuvre de procédures pour notifier correctement aux autorités ou parties concernées de tout incident de sécurité potentiel.

Panda Adaptive Defense veille à la sécurité de l'entreprise et de ses données, et facilite la gestion des informations. Les entreprises qui font confiance à Adaptive Defense sont déjà bien avancées dans leur démarche de conformité vis-à-vis du RGPD.

10. À propos de Panda Security

Ce rapport utilise les données collectées par l'équipe pluridisciplinaire de Panda Security. Il s'agit d'un réseau d'experts créé en 1990 et ayant pour mission de simplifier la complexité en créant des solutions innovantes et performantes pour protéger la vie numérique de ses utilisateurs.

Nous partageons ouvertement les connaissances de nos techniciens experts du PandaLabs, le laboratoire qui traite les menaces et les neutralise en temps réel. Nous sommes des développeurs spécialisés dans la cybersécurité avancée, ainsi que des experts dans le domaine des solutions logicielles, du cloud, du big data et du machine learning.

Nous voulons réinventer la cybersécurité et la mettre à la portée de tout le monde.

panda

Pour plus d'information :

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46 84 20 00
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 87 32 32 10
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SOUTH AFRICA
+27 21 683 3899
sales@za.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44(0) 800 368 9158
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

Pour plus d'information :

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda