Le Guide de référence pour la conformité GDPR

Contenu

Introduction

Êtes-vous préparé au nouveau règlement européen en matière de protection des données personnelles ?

Le concept de la « protection en amont » (« Privacy by design ») vise à agir de manière proactive et préventive, avant qu'une nouvelle technologie, qui faciliterait le traitement de données personnelles, ne favorise les failles de sécurité et la violation de ces données.

Le 25 mai 2018, le Règlement Général européen sur la Protection des Données (RGPD ou GDPR) entrera en vigueur. Il remplacera toutes les réglementations de protection des données nationales au sein de l'Union Européenne, et tout entrepreneur du marché unique devra s'y conformer. Cela comprend également les entreprises hors UE qui travaillent avec des clients de l'Union Européenne.

Selon le GDPR, toute violation de données personnelles doit être signalée dans les 72h suite à sa prise de connaissance. Le défaut de signalement – ou de preuve apportée qu'il n'y a pas eu négligence – peut entraîner des amendes allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires global (le plus élevé de ces deux montants).

Heureusement, les mesures requises pour la protection des données de la société dans son ensemble permettront aussi de préserver les données clients. L'approche de la sécurité multi-niveaux que nous recommandons déjà chez HP permettra d'assurer la « conformité GDPR ».

Dans cet eGuide sont détaillés les éléments essentiels du GDPR que doivent connaître les professionnels de l'informatique, et les enjeux des programmes de sécurité des terminaux basés sur les appareils.

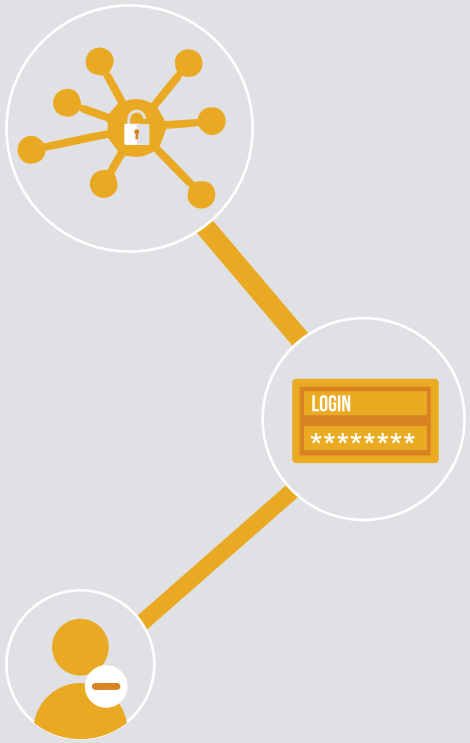
Présentation du GDPR européen

L'essentiel à retenir pour les services informatiques

Le GDPR s'articule autour de deux grands axes : la protection des droits des citoyens européens et la protection de leur vie privée. Tous deux ont des implications technologiques.

Voici les points à retenir pour les responsables informatiques :

1. **Les violations doivent être signalées dans un délai de 72 heures**
   Selon le GDPR, toute violation de données personnelles doit être signalée dans les 72 h suite à sa prise de connaissance. Les pénalités pour défaut de signalement sont élevées (voir « Quelles sont les pénalités pour non-conformité ? »).
2. **Le droit à l'oubli**
   Tout citoyen de l'UE a le droit à l'oubli. S'il vous le demande, vous devez effacer ses données, ainsi que toutes les copies de celles-ci.
3. **Le droit à la portabilité des données**
   Les résidents de l'UE ont le droit de contrôler leurs données personnelles. Sur demande, vous devez leur fournir les données les concernant dans un format accessible et transférable à un tiers.
4. **Transferts internationaux**
   Le transfert de données personnelles vers une autre juridiction de protection des données (c'est-à-dire en dehors de l'UE) ne peut être effectué qu'avec le consentement explicite de la personne, et seulement aux organismes de régulation considérés comme « appropriés », ou avec des mesures de protection supplémentaires[1]
5. **Protection en amont (« Privacy by design »)**
   Les sociétés doivent adopter une approche de protection en amont intégrant la sécurité des données aux produits, processus et services par défaut[2]



À qui s'applique le GDPR ?

Le GDPR s'applique à toute société recueillant et/ou traitant les données personnelles de citoyens européens. Cela comprend les sociétés basées en-dehors de l'Union européenne, mais exerçant à l'intérieur de celle-ci.

[1]https://www.lesechos.fr/idees-debats/cercle/cercle-162490-gdpr-un-tournant-dans-le-traitement-des-donnees-personnelles-2042117.php#is33TD2GBGpbhldr.99
[2]http://www.journaldunet.com/ebusiness/crm-marketing/1191593-reglement-europeen-sur-la-protection-des-donnees/

Présentation du GDPR européen

Qu'entend-on par « données personnelles » ?

Selon le GDPR, les « données personnelles » comprennent « toutes données permettant d'identifier une personne ».

Cela comprend les informations génétiques, mentales, culturelles, économiques et sociales, mais aussi celles habituellement considérées comme moyen d'identification.

Des sociétés qui ne relevaient pas jusqu'à présent de la Législation sur la protection des données peuvent ainsi se retrouver dans le champ du GDPR.

Quelles sont les pénalités pour non-conformité ?

L'amende maximale est de 20 millions d'euros ou 4 % du chiffre d'affaires global (le plus élevé de ces deux montants). Elle concerne les délits les plus graves aux termes de cette réglementation, comme le défaut de signalement d'une violation de sécurité dans les 72 heures suite à sa prise de connaissance.

Les délits moins graves entraînent une amende maximale de 10 millions d'euros ou 2 % du chiffre d'affaires global, ce qui représente un coût élevé pour les sociétés.

Checklist de procédures GDPR

Dans le cadre de votre gouvernance pour la protection des données, vous aurez besoin de procédures explicites pour :

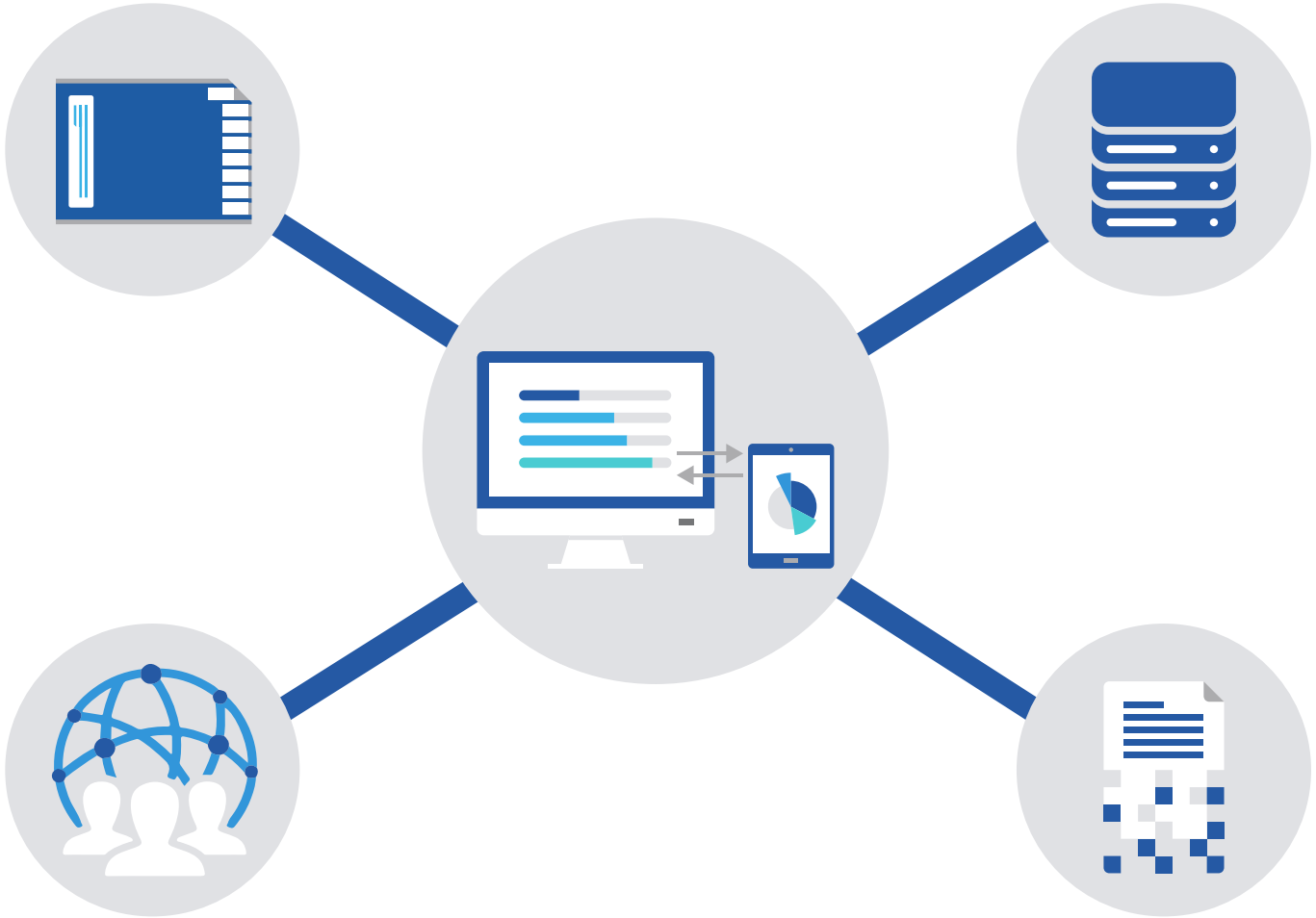
- Informer les personnes concernées de la manière dont leurs données sont recueillies, stockées et traitées.
- Obtenir des personnes concernées leur consentement explicite.
- Fournir aux personnes concernées leurs informations dans un format accessible.
- Effacer toutes les données personnelles d'une personne concernée, y compris les copies.
- Transférer des données vers un autre contrôleur ou processeur de données.
- Transférer des données en-dehors de l'UE – y compris au sein de la société.

Les défis technologiques de la conformité

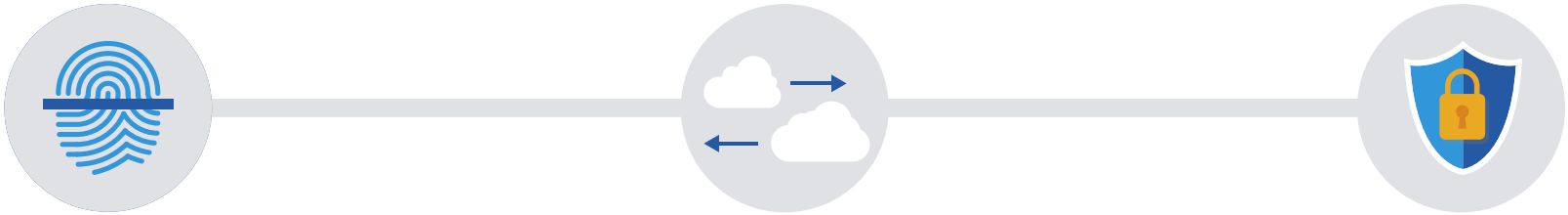
Les plus grands défis posés par le GDPR sont d'ordre technique.

Mettre en place la portabilité et la protection des données d'une personne, lui accorder un droit à l'oubli nécessitent une cartographie complète des données et des collaborateurs y ayant accès à chaque niveau.

La menace de la cybercriminalité augmentant chaque année, assurer une sécurité absolue est un défi de plus en plus complexe.



Les défis technologiques de la conformité



Tenir à jour la liste des appareils

Pour être conforme à la portabilité des données et au droit à l'oubli, un registre détaillé de toutes les données personnelles détenues par la société est nécessaire.

Vous devez connaître :

- Tout appareil contenant des données personnelles
- Tout appareil permettant d'accéder à des données personnelles

C'est le seul moyen de vous assurer de pouvoir récupérer et/ou effacer les données personnelles détenues par la société.

Tenir à jour la liste des services hébergés dans le Cloud

Une entreprise européenne utilise en moyenne 608 applications, un chiffre sous-estimé dans environ 90 % des cas. Les employés utilisent souvent des applications Cloud à l'insu du service informatique.[3]

Pour être conforme au GDPR, le Cloud doit être limité aux services suivants :

- intra-européens, donc conformes par définition au GDPR
- relevant de la juridiction d'un organisme de régulation de la protection des données considéré comme « adéquat » par l'UE

Tout autre service risquerait de violer la réglementation des transferts internationaux. Et si le droit à l'oubli venait à être invoqué, vous devez savoir quels services Cloud utilisent vos employés.

Mettez vos données à l'abri

Si la menace de la cybercriminalité grandit, c'est partiellement en raison de la prolifération des réseaux et des appareils personnels non sécurisés.

Les failles de sécurité sont presque inévitables. L'UE en a conscience, mais pour éviter une amende conséquente, vous devez :

- Mettre en place un outil de surveillance des événements d'incidents système (SIEM), pour pouvoir signaler toute violation dans les 72 heures.
- Mettre en place une sécurité des terminaux multi-niveaux ; pour pouvoir apporter la preuve de l'audit préalable et éviter les violations.

Les utilisateurs doivent être sensibilisés aux risques d'utiliser des appareils ou réseaux non protégés.

[3]http://www.journaldunet.com/solutions/expert/63233/gdpr---des-nuages-noirs-sur-le-cloud-en-europe.shtml

La menace de la cybercriminalité

La menace du cybercrime est bien réelle, et elle s'accentue de jour en jour

68 %

des entreprises françaises ont déclaré avoir été victimes d'une fraude au cours des 24 mois précédant l'étude. (Alors que ce chiffre n'est que de 36% pour les entreprises dans le monde et intérrogées au cours de la même étude)[4]

80 %

des grandes entreprises françaises ont déjà fait l'objet d'une rançon via une cyberattaque.

71 %

des cyberattaques se font par le biais des points d'extrémité.[5]

69 %

des employés utilisent plusieurs appareils mobiles dans le cadre du BYOD.

62 %

des entreprises estiment que ce sont ses collaborateurs qui sont à l'origine de certaines attaques subies.

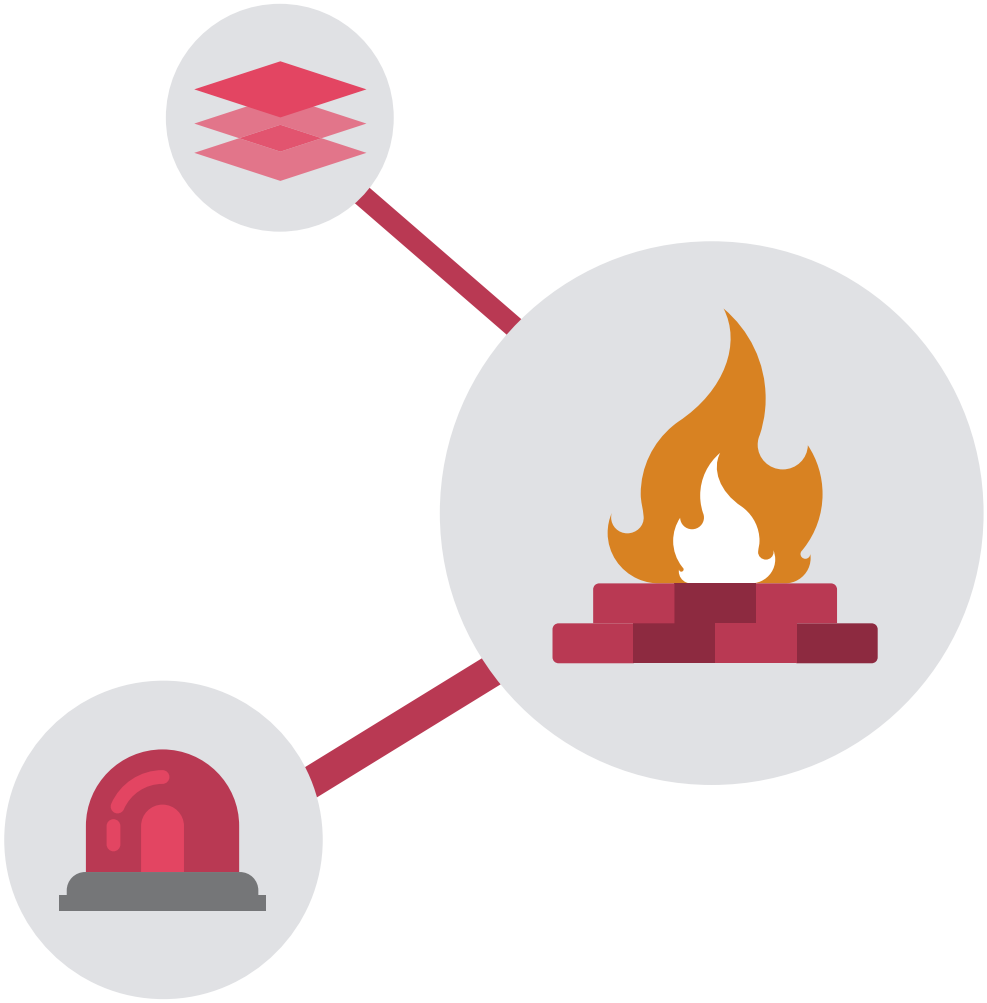
[4]Global Economic Crime Survey 2016 – PwC France https://www.pwc.fr/fr/assets/files/pdf/2016/03/pwc_ad_fraude_mars2016_v3.pdf
[5]https://h30657.www3.hp.com/t5/BusinessBlog-fr/Les-risques-de-sécurité-aux-points-d-extrémité-sont-en-hausse-y-êtes-vous/ba-p/9044

Mettre en place la sécurité des terminaux

L'approche multi-niveaux de la sécurité des terminaux HP

L'approche de cybersécurité défense/protection – pare-feu et antivirus - n'est pas suffisante. « Dans un véritable environnement, un fichier ne serait scanné qu'une fois par un antivirus », explique une étude de l'agence Dambella. « Si une équipe de sécurité moyenne reçoit 17 000 alertes par semaine, ou 2 430 par jour, un logiciel antivirus en raterait 796 par jour »[6]

Le point de vue de HP est que la cybersécurité doit être multi-niveaux, opérant au niveau du réseau, des appareils et des utilisateurs, avec plusieurs lignes de défenses à chaque niveau. L'approche de « détection et réponse » doit être privilégiée, prioritairement à l'approche de « protection et défense », déjà dépassée.



Les contrôles de sécurité critiques (CSC)

Le Centre de Sécurité Internet (CIS – Center of Internet Security) a défini 20 contrôles de sécurité critiques (CSC) internationalement reconnus, affinés et validés par les plus grands experts de la sécurité informatique au monde. Ces contrôles sont considérés comme des réflexes de cyber-hygiène essentiels pour chaque société.

Nous n'avons retenu que les principaux contrôles, car ce sont des directives utiles pour la conformité au GDPR, mais l'ensemble des CSC est disponible en ligne. Consultez-les sur le site du CIS.

[6]https://www.tomsguide.fr/actualite/antivirus-malwares,46524.html

Sécurité du réseau

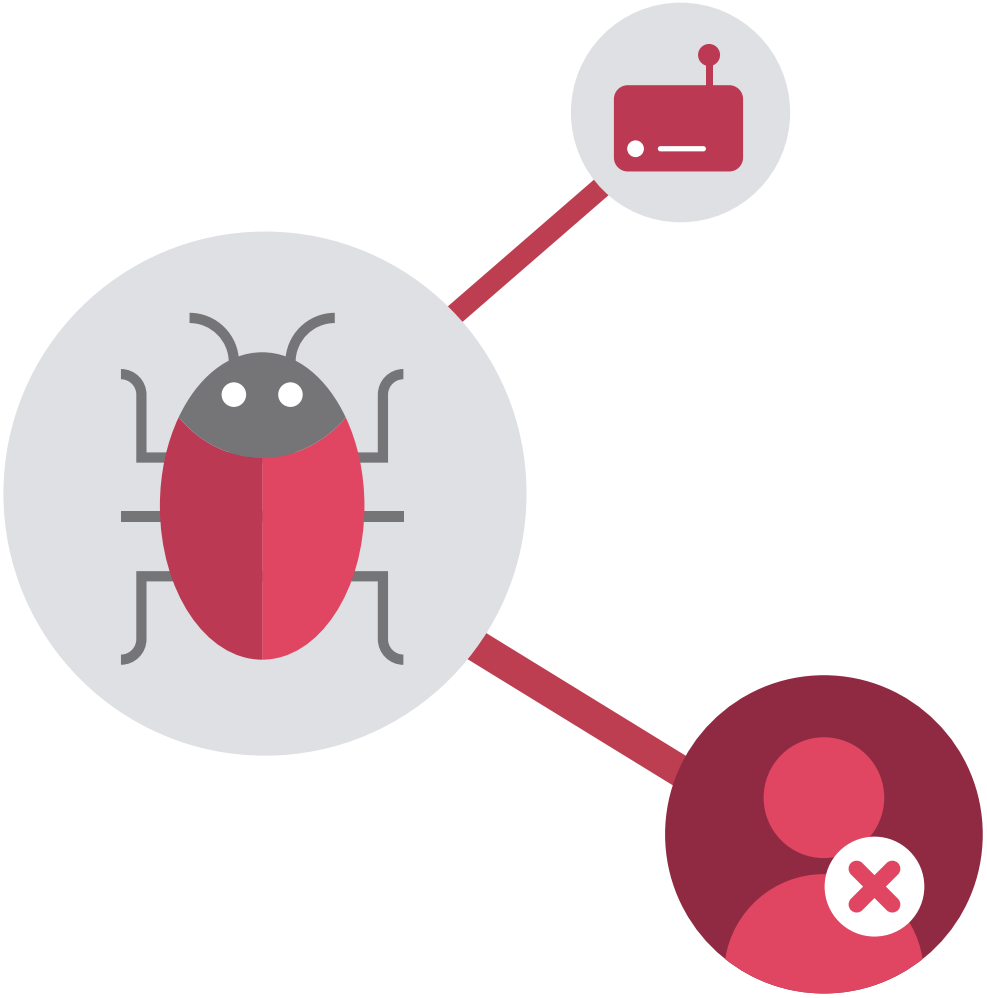
Les piratages les plus sévères exploitent généralement un point d'entrée unique, pour obtenir l'accès à l'ensemble du réseau. C'est pourquoi la sécurité doit être basée sur ce point d'entrée.

- **Contrôlez les privilèges administratifs (CSC 5)**
  Limitez l'autorisation de changer les paramètres et les mots de passe à un minimum de personnes.
- **Contrôlez l'accès selon ce que l'on a besoin de savoir (CSC 14)**
  Hiérarchisez l'accès aux informations sensibles selon l'utilisateur, l'appareil et la localisation. Mettez en balance le risque de sécurité et la sensibilité des données.
- **Limitez et contrôlez les ports réseaux, les protocoles et les services (CSC 9)**
  Fermez tous les points d'accès (virtuels et physiques) inutiles, y compris FTP, Telnet et services d'impression.
- **Maintenance, surveillance et analyse des journaux d'audit (CSC 6)**
  Passez régulièrement en revue les journaux d'audit pour analyser les comportements du système et détecter toute activité suspecte.
- **Évaluez et traitez en permanence les failles (CSC 4)**
  Votre équipe informatique doit évaluer en permanence l'environnement afin de détecter toute vulnérabilité et de prendre des mesures correctives pour réduire le nombre de failles.

L'objectif est d'obtenir un réseau sous-divisé selon le degré de sensibilité des informations. Les demandes d'accès sont évaluées selon les risques de sécurité qu'elles présentent. Les appareils non reconnus, les utilisateurs et les demandes provenant de réseaux non sécurisés sont exclus de l'accès aux informations les plus sensibles. La politique BeyondCorp de Google en est un bon exemple.[7]

[7] http://www.lemagit.fr/etude/BeyondCorp-Google-detaille-son-approche-de-la-securite-sans-perimetre

Sécurité du réseau



Chaque appareil de l'entreprise ou personnel représente une vulnérabilité potentielle. Vous devez connaître tous les téléphones, toutes les tablettes et tous les ordinateurs portables ou de bureau ayant accès aux données de la société.

- **Inventoriez les appareils autorisés et non autorisés (CSC 1)**
  Auditez tout appareil ayant accès aux données.
- **Inventoriez les logiciels autorisés et non autorisés (CSC 2)**
  Auditez toute application utilisée sur le réseau – permettant ou non d'accéder directement aux données de l'entreprise.
- **Protégez-vous contre les logiciels malveillants (CSC 8)**
  Vérifiez que tous les appareils sont protégés par un antivirus et anti-malware à jour. Assurez-vous que des scans et mises à jour régulières sont effectuées.

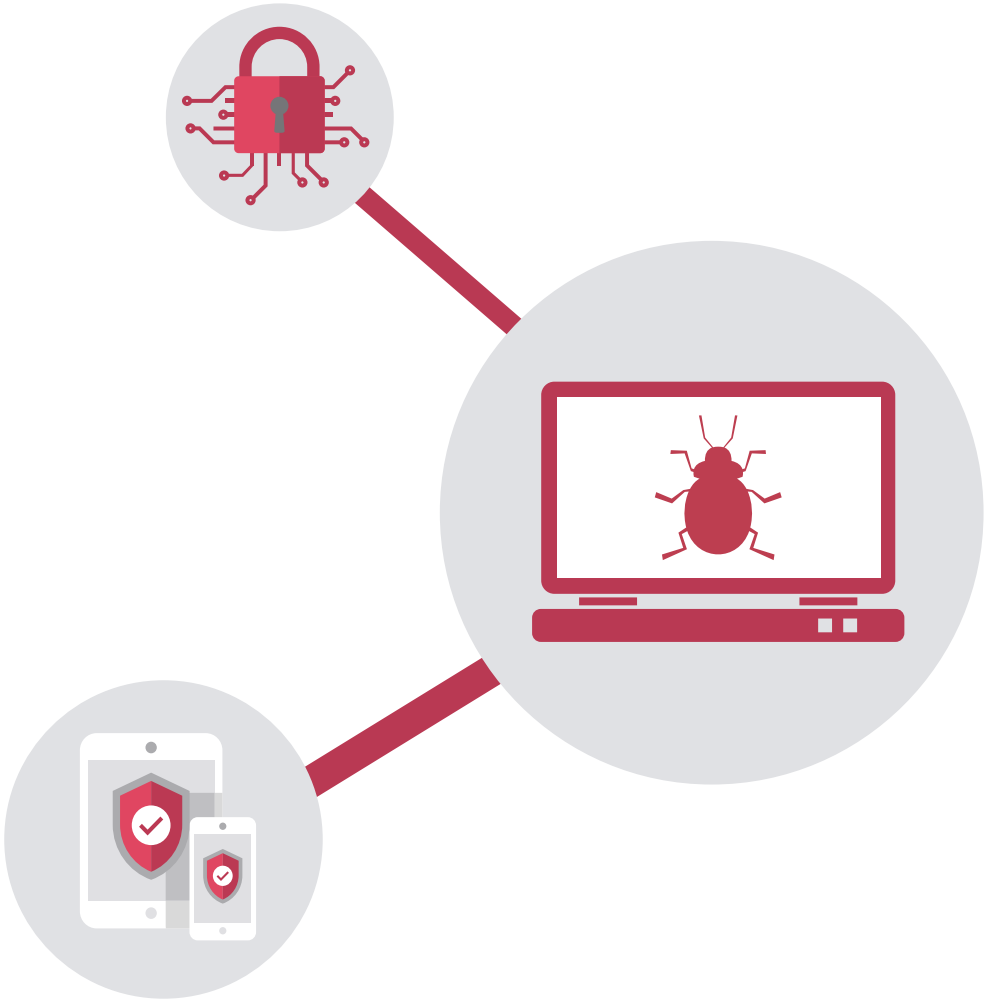
Sécurité des appareils

Les services informatiques doivent par ailleurs envisager les vérifications suivantes :

- **Mettez en place une authentification multifactorielle**
  Vérifiez que chaque appareil est sécurisé. Idéalement, utiliser l'authentification biométrique en plus des mots de passe (voir page 14 : « Appareils de protection en amont »).
- **Assurez l'accès à distance**
  Vérifiez l'accès à distance aux appareils pour récupérer ou effacer les données personnelles, mettre en quarantaine des processus ou y mettre fin, et fermer et verrouiller l'appareil en cas de perte ou de vol (voir page 14 : « Détection et réponse »).
- **Informez chaque employé des protocoles et procédures de sécurité**
  Assurez-vous que chaque employé est sensibilisé et connaît ses responsabilités en matière de cybersécurité, y compris le signalement d'une activité suspecte.
- **Organisez des formations actives à la cybersécurité**
  Créez des ateliers, des séminaires, organisez des exercices de protection contre l'hameçonnage – assurez-vous que chacun sache comment éviter les erreurs courantes et rester conforme au GDPR.
- **Réduisez au maximum l'utilisation d'appareils/applis personnels**
  Découragez l'utilisation d'appareils et d'applis personnels pour le travail. La mise en place d'une politique de CYOD complète vous sera utile.

Mettre en œuvre un cadre de sécurité comme celui-ci devrait vous aider à garder le contrôle sur tous les appareils de votre société, protéger les données et faciliter l'application de la portabilité des données et du droit à l'oubli.

Pour en savoir plus sur l'approche de la sécurité multi-niveaux de HP, lisez notre livre blanc La sécurité commence aux points d'extrémité.



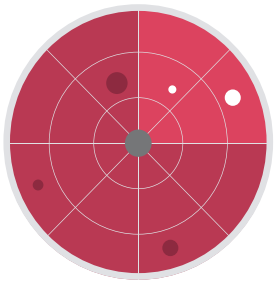
Pourquoi chaque employé doit être cybersensibilisé

La négligence des collaborateurs occasionne davantage de fuites de données que les attaques cybercriminelles[8]. Sécuriser chaque appareil signifie aussi sécuriser son utilisateur.

- En 2014, plus de 235 GO de données ont été dérobées à Sony Pictures Entertainment suite à une cyberattaque d'ampleur, dite de phishing. Les employés de Sony ont en effet saisi leurs identifiants Apple dans un faux formulaire créé par les hackers, prétextant une fausse vérification.[9]
- En 2014, des photos de célébrités nues ont envahi Internet, après que Ryan Collins, un hacker de 36 ans, ait eu accès au iCloud de Jennifer Lawrence et ses alias par des emails de hameçonnage se faisant passer pour Apple.[10]
- En 2012, 68 millions de mots de passe Dropbox ont été piratés à cause d'un employé utilisant le même mot de passe pour les systèmes internes que pour son compte LinkedIn[11]
- Le Président Donald Trump utilisait jusqu'à récemment un téléphone Samsung Galaxy standard. Les experts ne se demandent plus s'il a été piraté, mais par combien de services secrets étrangers il l'a déjà été.[12]

[8]https://business.lesechos.fr/directions-numeriques/technologie/cybersecurite/0211237702835-la-negligence-des-collaborateurs-fait-des-cyber-degats-213551.php
[9]https://www.newstoprotect.axa/economie/cybersecurite-negligences-couts-entreprises
[10]http://www.numerama.com/magazine/30399-des-photos-de-femmes-celebres-nues-piratees-sur-icloud.html
[11]http://www.numerama.com/tech/191949-une-base-de-68-millions-de-comptes-dropbox-circule-chez-les-pirates.html
[12]http://www.fredzone.org/trump-utilise-toujours-son-galaxy-s3-nen-deplaise-aux-services-secrets-697

Détection et réponse

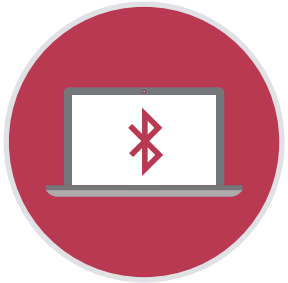


« Détection et réponse » est un cadre de cybersécurité admettant que la prévention totale est quasiment impossible

Ce qui compte, c'est prendre conscience de la faille (détection) et agir immédiatement (réponse).

Il existe des logiciels qui transforment tout appareil en détecteur en temps réel et permettent à l'administrateur de réagir, par exemple en éteignant les appareils, en mettant des fichiers en quarantaine ou en effaçant des données.

Privacy by design devices



Appareils de protection en amont

Les appareils HP sont un parfait exemple de protection en amont. Leurs fonctions de sécurité comprennent le premier BIOS auto-réparateur au monde, le verrouillage Bluetooth automatique (qui verrouille l'appareil lorsque vous vous éloignez) et des écrans de confidentialité intégrés.

Si ces fonctions en elles-mêmes ne garantissent pas la conformité au GDPR, elles y contribuent beaucoup.

Se préparer au GDPR

Les mesures concrètes à prendre

Le GDPR entrera en vigueur le 25 mai 2018. Il reste encore un peu de temps pour s'y préparer, mais comme vous pouvez vous en douter, il y a beaucoup à faire.

La première étape est de faire un **audit de la situation actuelle de vos données**. Déterminez où vos données sont stockées, où elles sont copiées et qui en a l'accès. Si vous utilisez des solutions Cloud, trouvez où leurs serveurs sont basés et s'ils sont conformes au GDPR. Même chose pour tout SaaS ou toute société partenaire avec laquelle vous travaillez et partagez vos données. Cela vous donnera une idée précise de l'étendue des modifications à apporter pour être à la norme.

Créez une politique de données sur mesure. Ajoutez-y des procédures et protocoles détaillés sur le lieu de stockage des données, qui en a l'accès et en fait des copies en-dehors de la société ou à l'étranger pour les multinationales. Ajoutez des procédures de récupération et d'effacement des données personnelles. Diffusez cette politique à tous les membres de la société, et organisez des sessions de formation en soulignant leur importance.

Personnalisez votre politique de sécurité. Créez un cadre de cybersécurité fonctionnant sur le principe Détection / Réponse au niveau des terminaux et revoyez au besoin votre politique d'appareils. Investissez dans de nouvelles technologies si nécessaire. Seuls 36 % des directeurs informatiques estiment suffisant leur budget pour assurer la sécurité des terminaux.[13] Les pénalités liées à la non-conformité GDPR peuvent être le déclencheur permettant d'être mieux entendus par la Direction.

[13]Ponemon 2016 State of the Endpoint Report

Se préparer au GDPR

Conformité GDPR

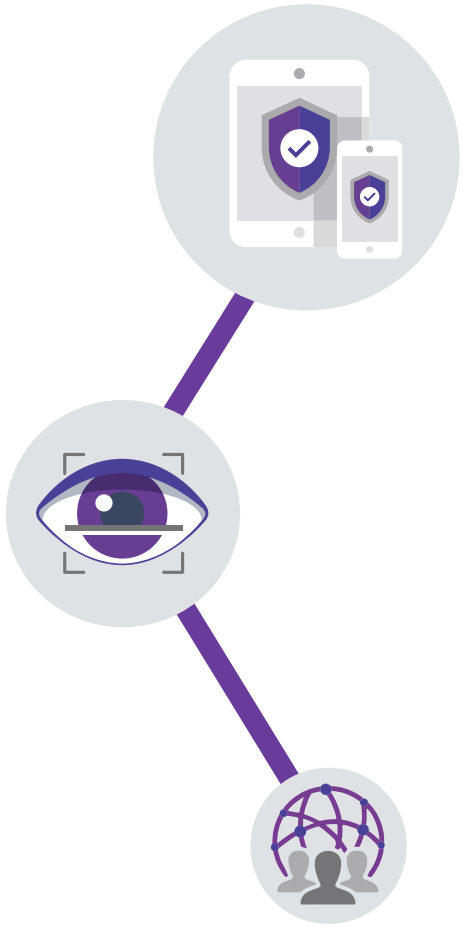
5 étapes fondamentales pour la conformité GDPR

1. Désignez au besoin une personne chargée des données, un responsable de la protection des données.
2. Effectuez un audit complet de vos données, y compris le caractère approprié ou non des fournisseurs de Cloud et de SaaS dans l'optique du GDPR.
3. Créez un nouveau cadre de gouvernance des données, y compris des procédures de portabilité des données et de droit à l'oubli.
4. Créez un nouveau cadre de cybersécurité, avec la mise en place d'une sécurité des terminaux multi-niveaux.
5. Communiquez les politiques et protocoles à toutes les personnes de votre société.

Sécuriser les terminaux

6 étapes essentielles pour sécuriser les terminaux

1. Vérifiez tous les appareils autorisés ou non autorisés accédant aux données personnelles.
2. Investissez dans de nouveaux appareils mieux sécurisés, le cas échéant.
3. Garantissez l'accès à distance et les droits à l'effacement pour les données de l'entreprise.
4. Mettez en place un scan régulier et une politique de mise à jour des logiciels de sécurité.
5. Mettez en place un logiciel de détection et de réponse en temps réel.
6. Formez vos employés à la cybersécurité.



Calendrier de sécurité des terminaux

Planning de base de sécurisation des terminaux avant le GDPR

2017

Mai

Désignez un chef de projet chargé de sécuriser les terminaux

Juin

Effectuez un audit des politiques de sécurité, pratiques et appareils actuelles

Juillet

Étudiez les besoins des appareils et les politiques pour la sécurité des terminaux (CYOD/BYOD etc.)

Août

Envisagez des solutions logicielles pour la détection et la réponse aux menaces de sécurité

Septembre

Créez un système d'accès hiérarchisé multi-niveaux pour les données de la société

Octobre

Créez un cloud public/privé pour autoriser un accès approprié aux données hors site

Novembre

Créez un programme de formation, y compris des exercices réguliers de protection contre l'hameçonnage

Décembre

Communiquez les nouvelles politiques de sécurité à toute la société

2018

Janvier

Mettez en place une nouvelle architecture de données sur cloud public/privé

Février

Mettez en place une nouvelle politique d'appareils

Mars

Mettez en place une solution logicielle Détection / Réponse

Avril

Formez vos utilisateurs à la sécurité, y compris aux politiques relatives au GDPR

Mai

Le GDPR entre en vigueur

Résumé

Le GDPR arrive bientôt

Avec un peu de chance, les pratiques de sécurité de votre société sont déjà en accord avec ce nouveau règlement, et si vous exercez dans plusieurs pays européens, vous avez peut-être déjà été confronté à certaines de ses mesures les plus restrictives.

Avec un peu de chance, les pratiques de sécurité de votre société sont déjà en accord avec ce nouveau règlement, et si vous exercez dans plusieurs pays européens, vous avez peut-être déjà été confronté à certaines de ses mesures les plus restrictives.

Les mesures de sécurité que nous recommandons de mettre en place afin d'être conforme au GDPR permettent de prévenir toute faille qui risquerait de coûter des sommes astronomiques à votre société. En 2016, le coût global des cyberattaques concernant les entreprises françaises s'élèvait à 1,8 milliard d'euros.[14]

De plus, de nombreuses mesures requises pour une sécurité vraiment renforcée permettront dans le même temps d'être conforme à d'autres aspects du GDPR. Restreindre l'accès aux données à certains utilisateurs, appareils et réseaux minimise le risque, mais facilite aussi le suivi des données personnelles, et donc la conformité à la portabilité des données et au droit à l'oubli, sans parler des transferts internationaux.

Cet eGuide n'est qu'un début. Chez HP, la sécurité a toujours été au cœur de nos préoccupations. Depuis des années, la protection en amont fait partie de notre politique. Et maintenant qu'elle n'est plus seulement souhaitable mais exigée, nous sommes bien placés pour vous aider à adopter la même approche.

Pour en savoir plus sur la sécurité des produits HP et vous aider à rester conforme au GDPR, consultez notre page dédiée sur le **site HP**.

[14]Rapport annuel 2016 Symantec - https://www.symantec.com/content/dam/symantec/fr/docs/reports/2016-norton-cyber-security-insights-comparisons-france-fr.pdf