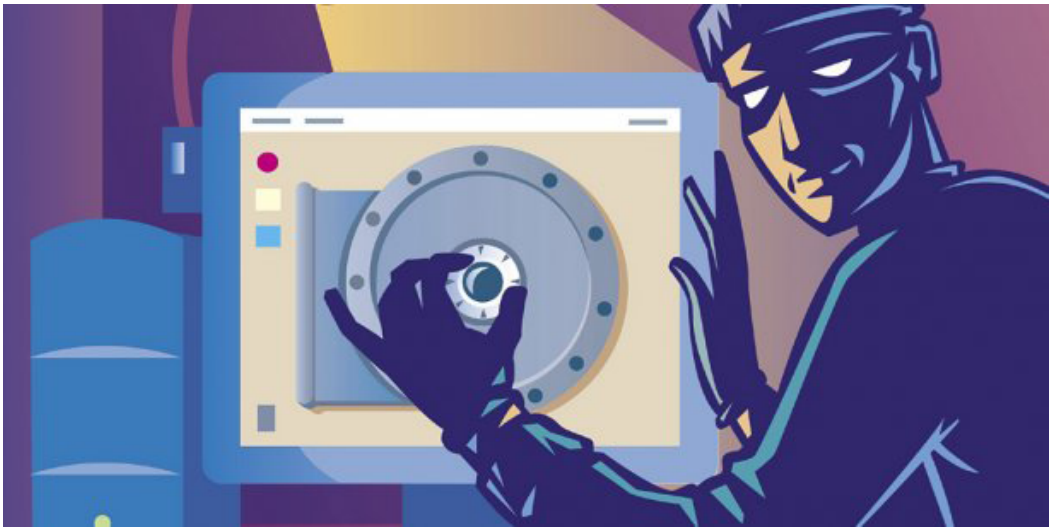
Imbrikation
réussissez !

L'OBSERVATOIRE IMBRIKATION

Scrute pour vous les nouveaux horizons

N° 13 - 21 septembre 2017



LA PROTECTION DES DONNEES

Dans 8 mois entrera en vigueur le Règlement Général sur la Protection des Données (RGPD) en Europe. Quels changements pour les entreprises ? Comment s'y préparer ? Quels acteurs sont présents sur le marché de la cybersécurité ?

Pourquoi ?

Les techniques de récolte, la quantité et les utilisations faites des données personnelles ont fortement évolué ces dernières années, rendant la législation actuelle obsolète. C'est la raison pour laquelle un nouveau règlement sera applicable à partir du 25 mai 2018 : le RGPD (Règlement Général sur la Protection des Données). Il concerne les données personnelles qui permettent d'identifier directement ou indirectement des personnes. Ce règlement vise à simplifier et harmoniser le traitement des données, et renforcer la sécurité des personnes.

Concrètement, le RGPD ça change quoi ?

Concernant la protection des personnes

- **Consentement explicite** : ceux qui traitent les données devront fournir la preuve explicite du consentement des personnes concernées.
- **Données protégées dès la conception et sécurisées par défaut** : les entreprises seront responsables de la sécurité des données stockées (privacy by design). Le cryptage des données est la norme minimale.
- **Droit à la portabilité des données** : Chaque individu devra être en mesure de récupérer les données le concernant dans un format facilement lisible. Il pourra les transmettre, les modifier ou les supprimer.
- **Protection des enfants** : Le consentement des enfants devra être obtenu dans des termes compréhensibles selon son âge. Les parents peuvent devoir donner leur accord. Une fois majeur, l'enfant peut demander la suppression de toutes les données récoltées durant son enfance.
- **Possibilité d'effectuer des actions collectives** : les associations pourront faire des recours collectifs contre les entreprises ne respectant pas la loi. Toute personne ayant subi un dommage matériel ou moral pourra obtenir des réparations.
- **Informations si vol de données** : En cas de faille de sécurité, les entreprises devront informer les autorités et les personnes concernées.

Nouveaux outils et obligations

- Tenue d'un registre des traitements effectués.
- Etudes d'impact pour les traitements à risques (données sensibles).
- Désignation d'un DPO (Délégué à la Protection des Données) pour les entreprises du secteur public, ou qui traitent de grandes quantités de données, ou de façon systématique, ou des données sensibles. Il est chargé de s'assurer de la bonne application de la loi, de vérifier les études d'impact et d'être le point de contact avec les autorités de contrôle.

Les principes

Une nouvelle logique. Alors qu'aujourd'hui la CNIL (Commission Nationale Informatique et Libertés) doit démontrer les manquements des entreprises, demain, les entreprises devront prouver qu'elles agissent en conformité avec la loi.

Un nouveau champ d'application. Le RGPD est un règlement européen : il devra être appliqué en l'état dans tous les pays de l'Union européenne. Il concernera toutes les entreprises de l'UE, mais aussi les entreprises à l'étranger utilisant des données de citoyens européens.

De nouvelles sanctions. Des sanctions financières allant jusqu'à 4% du chiffre d'affaires mondial annuel de l'entreprise ou 20 millions d'euros pourront être appliquées.

En chiffres

D'après une étude menée par Umanis, toutes les entreprises interrogées pensent que le RGPD aura un impact au niveau technologique. Seulement 31% pensent qu'elles seront prêtes à temps, tandis que 23% pensent que cela est impossible.

Les étapes pour se préparer

1. **Désigner un pilote** qui se chargera de la mise en conformité, ou nommer un DPO (Délégué) si besoin. Les entreprises pour qui le DPO n'est pas obligatoire peuvent partager un même DPO.
2. **Cartographier les traitements de données personnelles** (informatisées ou non).
3. **Prioriser les actions** à mener pour entrer en conformité : travaux informatiques...
4. **Gérer les risques.** Si vous avez identifié des traitements de données personnelles à risques, vous devez pour chacun d'eux réaliser une analyse d'impact.
5. **Organiser les processus internes** : être capable de répondre aux demandes des particuliers souhaitant accéder à leurs données, établir un protocole en cas de faille de sécurité, ...
6. **Documenter la conformité** : regrouper la documentation

La cybersécurité et ses applications

Avec le RGPD, les entreprises devront s'assurer que les données personnelles qu'elles stockent sont bien protégées. En France, plus de 52% des entreprises ont déjà vécu une tentative d'attaques visant le réseau informatique. Le marché de la cybersécurité est très porteur : +7,9% de croissance entre 2015 et 2016. Il représentait 81,6 milliards de dollars en 2016 au niveau mondial. En France, il est estimé à plus de 1,2 millard d'euros pour 2020.
Sur ce marché, on retrouve les grands groupes qui proposent des solutions globales comme Orange, Atos, Capgemini, IBM, Airbus, Thales... De nombreuses entreprises plus jeunes arrivent sur le marché avec des offres plus distinctes :

Mails

91% des cyber-attaques démarrent avec un email. La sécurisation des emails est donc un marché porteur. VadeSecure a développé un filtre pour bloquer les messages dangereux.
Pour protéger les données sensibles envoyées dans des messages électroniques, Idecsi propose une solution similaire et un service d'audit pour vérifier le niveau de securité en place. LockEmail propose un cryptage des emails. Les destinataires détiennent une clé spécifique unique leur permettant de lire le contenu.

Sécurisation du Cloud

La société Tanker crypte les données avant qu'elles ne soient placées dans des espaces de stockage en ligne comme Dropbox. Oodrive et Coreye en revanche proposent des espaces de stockage sécurisés.

Authenticité des documents

De nombreuses entreprises sont présentes sur ce marché : Advanced Track & Trace propose des solutions de traçabilité des documents pour prévenir la falsification (badges d'accès, contrats, billets de banque, billetterie...). AriadNext contrôle l'authenticité des documents, y insère des cachets électroniques (2D Doc)... Woleet et KeeeX s'appuient sur la blockchain pour horodater et signer des documents en toute sécurité. Seald permet de suivre ses documents même après envoi et de savoir qui les lit à quel endroit, et s'il est renvoyé à d'autres personnes.

Détection de menaces

Des entreprises comme CybelAngel et Leakwatch se sont spécialisées dans la détection de menaces : elles détectent les contrefaçons et surveillent la fuite et la vente d'informations confidentielles sur le dark web.

Sécurisation du réseau et des mobiles

Pour les salariés équipés de téléphones et manipulant des données confidentielles, il existe des solutions pour chiffrer entièrement le terminal, comme celles d'Ercom. Il existe des logiciels pour surveiller et protéger le réseau informatique des entreprises comme Quarkslab, Cyberwatch, Tehtris... ITrust propose des audits et des formations.

Gestion des accès

Un salarié au cours de sa journée peut être confronté à plusieurs mots de passe différents à entrer. Cela peut être un frein à la productivité, ou un risque de sécurité si les mots de passe sont enregistrés. Avencis propose un code unique débloquant l'accès aux applications et sites tandis que TrustDesigner utilise l'identification biométrique pour dévérouiller des sessions de travail numériques, ou des accès physiques. Inwebo combine les deux en fonction des usages. Il est possible d'enregistrer ses mots de passe en ligne dans des applications comme Dashlane ou Lastpass. BrainwareGRC et ISdecisions proposent de gérer les droits d'accès aux fichiers et de prévenir les violations de droits.

Détection et réparation de failles

Les plateformes de Bug Bounty - qui proposent des récompenses en échange d'identification de failles - se développent. Les sociétés peuvent exposer leurs problèmes et proposer des récompenses sur des sites comme Yeswehack, ou Yogosha. Elles font alors appel à des experts externes. L'entreprise TrustInSoft utilise un programme capable de détecter des failles dans le code des sites, des logiciels et des applications.

Les limites

Technicité : Les dirigeants des entreprises sont souvent démunis face à la cybersécurité et ont des difficultés à prendre des décisions.

Investissement : La protection de ses données et de son réseau informatique représente un coût important.

Si vous avez des questions, ou si vous êtes intéressé par d'autres sujets, écrivez-nous : imbk-partenaires@imbrikation.fr

Imbrikation réussissez !

Imbrikation SAS
7 rue Alexander Fleming
49066 Angers Cedex
02 41 20 28 89