Resilient Shield Consulting

Solutions innovantes pour clients exigeants

OFFRE DE CONSEIL

Méthode d'implémentation de la Réglementation Générale pour la Protection des Données

Version 1.0 – Octobre 2016

Table des matières

1. RÉSUMÉ

Toutes les entreprises européennes ont l'obligation de se mettre en conformité avec le Réglement Général sur la Protection des Données (RGPD). Celui-ci sera applicable dès le 25 mai 2018 et entrainera des sanctions financières très lourdes en cas d'infraction.
Les systèmes d'information traitant les données personnelles vont devoir répondre à des spécifications qui renforcent significativement le contrôle des citoyens européens sur les données qui les concernent.
Le personnel devra être formé. Les rôles et responsabilités sur la protection des données devront être distribués de façon appropriée et une nouvelle fonction sera parfois nécessaire : le Délégué à la Protection des Données (Data Protection Officer – DPO). Les systèmes d'information existant et les futurs systèmes devront répondre à des exigeances fondamentales liées à la protection des données tels que : l'approbation explicite sur le traitement de leurs données par les citoyens, le droit à l'oubli, la sécurité des données par défaut et dès la conception, …
Resilient Shield Consulting s'est inspiré des systèmes de management relatifs à la sécurité des systèmes d'information, à la qualité et à la continuité d'activités. Le système de management de la protection des données ainsi créé doit être simple, pragmatique et évolutif. Il tient compte de l'existant et l'améliore pour le rendre conforme à la réglementation. L'ensemble des dispositions de protection des données est maintenu avec un effort optimum au sein de l'Organisation.

2. DE QUOI S'AGIT- IL ?

Le ¨Parlement Européen et le Conseil de l'Union européenne ont adopté un Réglement Général sur la Protection des Données (RGPD) en avril 2016. Il sera applicable dès le 25 mai 2018 pour toutes les entreprises européennes et pour celles qui traitent des données d'organisation européennes.

Cette réforme a pour objectif de renforcer le contrôle des citoyens européens sur leurs données personnelles tout en simplifiant la réglementation pour les entreprises.

Les améliorations apportées par le nouveau cadre réglementaire sont nombreuses et nécessiteront un effort conséquent de la part des organisations concernées :

- Harmonisation des réglementations,
- Applicabilité extraterritoriale des dispositions,
- Evaluation d'impact des activités ayant des conséquences sur la protection des données,
- Obligation d'obtenir un consentement non ambigu sur le traitement par le propriétaire des données,
- Application correcte du droit à l'oubli du citoyen,
- Mise en œuvre de principes de sécurité par défaut et de protection des données dès la conception,
- Droit à la portabilité des données personnelles,
- Capacité à se prémunir de tout profilage ou traitement inaproprié appliqué à ses données,
- Nomination d'un Délégué à la Protection des Données (Data Protection Officer) pour certaines organisations,

- Etc...

Qu'est ce qu'une donnée personnelle ?
Les données personnelles permettent d'identifier directement ou indirectement une personne physique. Elles sont soumises à une réglementation juridique précise.
Exemples : Nom, numéro de téléphone, empreinte digitale, photographie,..

En savoir plus : « RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 » disponible sur http://eur-lex.europa.eu.

3. POURQUOI DOIT- ON IMPLÉMENTER LA RGPD ?

Toutes les entreprises européennes et celles qui traitent des données d'organisation européennes ont l'obligation de tenir compte de la réglementation RGPD et de rendre leurs activités conformes à ses dispositions.
Des sanctions financières pouvant s'élever à 4% du chiffre d'affaire annuel ou 20 millions d'euros sont prévues en cas de violation du règlement RGPD.

Au delà de la sanction financière, la RGPD impose un alignement des dispositions de sécurité sur tout le cycle de vie des données personnelles. Les exigeances des clients et des partenaires de toute organisation font de cet alignement une nécessité absolue pour l'avenir.

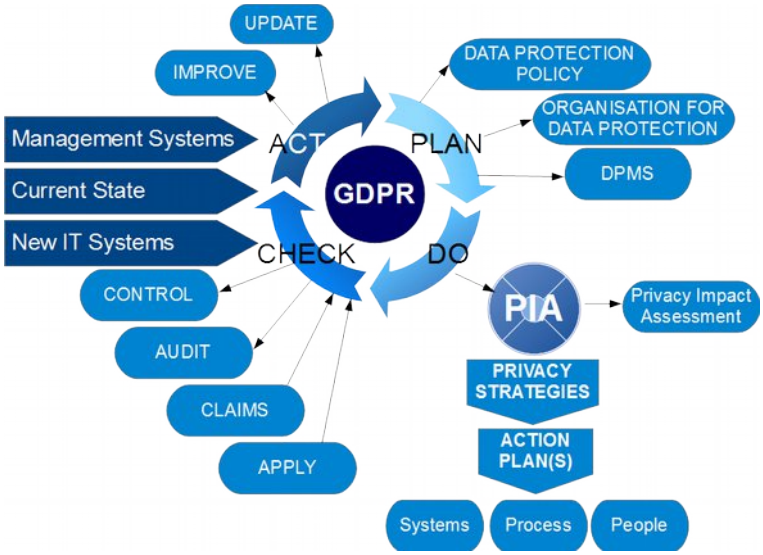
4. LA MÉTHODE DE RESILIENT SHIELD CONSULTING

HYPOTHÈSE DE CONSTRUCTION DE LA MÉTHODE

Resilient Shield a développé une méthodologie efficiente de mise en œuvre de la RGPD. Elle est basée sur un constat simple : la conformité à la **RGPD** nécessite de **mettre en œuvre un système de management de la protection des données** ou de faire **évoluer les systèmes existants**. Les dispositions de la réglementation constitutent le cahier des charges fonctionnel de ce système, autrement dit la feuille de route. Parmi les dispositifs existant que nous devrions faire évoluer, nous identifions le système de management de la qualité, le système de management de la sécurité et le système de management de la continuité. Ils doivent alors être conformes à la réglementation RGPD.
Le texte réglementaire montre de façon explicite combien l'ensemble de ces systèmes de management sont interdépendants. Une démarche cohérente produit donc un gain d'efficacité et d'optimisation des coûts.
La mise en place de principes d'amélioration continue est une autre nécessité liée à la GDPR. La complexité et l'évolutivité des systèmes d'information demandent des dispositions souples et sans cesse optimisées. L'ensemble des processus informatiques liés au traitement des données personnelles est impacté et touche chaque composante : systèmes d'information, procédures, personnel impliqué et sous-traitants.
En 2018, de nouvelles dispositions pour la protection des données personnelles verront le jour et elles devront se maintenir et s'améliorer au cours des années suivantes.

LA MÉTHODE DPMS (DATA PROTECTION MANAGEMENT SYSTEM)

Resilient Shield Consulting a donc développé une méthode originale totalement compatible avec la réglementation RGPD et avec les normes en vigueur en sécurité de l'information, qualité et continuité des activités.
Cette méthode prend en compte l'existant car beaucoup d'entreprises disposent d'une méthode plus ou moins élaborée de gestion et de protection des données personnelles.
Elle intégre également une approche cyclique d'amélioration continue comme les autres systèmes de management. Celle-ci est communément appelée PDCA (Plan – Do – Check – Act).



DPMS Methodology - © Resilient Shield Consulting 2016

Nous initions notre démarche par un état des lieux. Cette étape fondamentale permet de connaître les développements existants et connexes à la protection des données que l'Organisation a menés. Il apporte aussi une compréhension de l'univers des données de l'Organisation et une première classification des données personnelles selon les critères de la RGPD.
Notre méthodologie intégre évidemment le PIA (Privacy Impact Assessment) tel que demandé par la réglementation. Il peut être basé sur l'outil EBIOS comme le préconise la CNIL (Commission Nationale de l'Informatique et des Libertés) ou d'autres outils d'analyse des risques et des impacts compatibles avec les besoins.
Le rapport PIA sera alors la pierre angulaire pour la conception des stratégies de protection et de traitement des données personnelles : anonymisation, security by design, droit à l'oubli,etc...
Notre méthodologie concerne également la conception et le suivi des plans d'actions pour la protection des données. L'accompagnement est réalisé sur les aspects organisationnels, procéduraux, technologiques et réglementaires.
Comme tout système de management, votre DPMS devra être contrôlé, audité et amélioré. Les processus sous-traités devront faire éventuellement l'objet de solutions particulières pour assurer la bonne gestion des données personnelles placées sous leur contrôle. Nous intégrons toutes les dispositions nécessaires à une conformité constante de votre organisation avec la réglementation RGPD notamment l'enregistrement des preuves de traitement approprié des données.

Resilient Shield Consulting est en mesure d'accompagner ses clients sur tout le cycle de vie du DPMS. Elle peut contribuer à la création des différents livrables du projet, parmi lesquels nous trouvons :

- Rapport d'état des lieux intégrant un inventaire et une cartographie des données.
- Système de Management DPMS documenté avec les procédures associées (Organisation, audit, ..)
  Politique de protection des données personnelles
- Plan de projet RGPD
- Rapport PIA
- Rapport des stratégies de protection des données compatibles RGPD.
- Plan d'Action pour l'implémentation de la RGPD.
- Suivi des projets
- ...

5. LES BÉNÉFICES DE NOTRE OFFRE

- Notre équipe pluridisciplinaire maitrise toute la démarche de protection des données personnelles: **réglementation et droit, sécurité, continuité, reengineeering des processus, gestion de projet et qualité.**
- Nos ressources sont très **expérimentées** et ont mené des missions pertinentes dans de nombreux secteurs d'activités, dont le votre probablement.

- Nos méthodes de travail privilégient un haut niveau d'**innovation** et une **qualité** irréprochable de nos prestations. L'efficacité résultante de notre approche vous permet de maitriser les coûts sur tout le cycle de vie de votre système de management de la protection des données.
- Notre méthodologie est conforme à la réglementation de protection des données et sa modularité permet de s'adapter à votre périmètre d'action.
- Notre politique de prix est **compétitive** et adaptée à votre budget.

6. CONTACTEZ-NOUS

Resilient Shield
Consulting SAS

75 Boulevard Haussmann - 75008 Paris
eMail : contact@resilient-shield.com
Web:http://www.resilient-shield.com

Votre contact :
Stéphane Hesschentier
Tél : 07 86 16 50 17
s.hesschentier@resilient-shield.com

Crédits photos : Resilient Shield Consulting SAS, Pixabay

