Formation

RGPD et nouvelle loi Informatique et Libertés

Règlement européen sur la protection des données personnelles

Bernard LAUR

Ce séminaire vous propose une synthèse des différents volets de mise en œuvre du RGPD et de la nouvelle loi Informatique & Libertés. Il fait également le point sur les premiers retours d'expérience et l'évolution des offres des fournisseurs et sous-traitants. Il est destiné aux responsables métiers, juridiques, informatiques, CIL et futurs DPO qui veulent apprécier dans leur globalité les différents paramètres de la mise en conformité.

Du 25 au 26 février 2019
De 8h à 17h
Inscription au 71 53 08

Mise en conformité de l'entreprise et impact sur le système d'Information

Le 25 Mai 2018, le règlement européen de protection des données personnelles complété par une nouvelle loi Informatique et Libertés entre en vigueur. Il est à application directe et immédiate dans les pays de l'Union pour toute entreprise dans le monde qui collecte, stocke et traite des données personnelles de citoyens européens dont l'utilisation peut directement ou indirectement permettre de les identifier.
Le RGPD renforce le droit des personnes et change le rapport avec l'autorité de contrôle pour passer d'un régime déclaratif à une logique de responsabilisation et de justification de la protection des données personnelles (accountability) par les entreprises elles-mêmes. Il est par ailleurs basé sur des principes de co-responsabilité des sous-traitants et de «Privacy by design».
Outre ses volets juridiques, règlementaires et organisationnels, le RGPD implique une évolution lourde du système d'information, la mise en œuvre d'outils logiciels (consentement, pseudonymisation) et de processus de sécurité adaptés (chiffrement, détection de violations). Pour certaines entreprises, il constitue l'un des plus grands chantiers informatiques de ces dernières années.
Au-delà de l'obligation de mise en conformité, le RGPD apparait comme une opportunité majeure d'avantage concurrentiel et de renforcement des liens de confiance de l'entreprise avec ses clients et collaborateurs.

Avantages de cette formation

- Meilleurs experts francophones
- Participation au premier réseau francophone de DSI
- Meilleurs conférenciers francophones et internationaux du management d'entreprise et des SI
- Nombreux cas concrets et illustrations
- Mise à disposition du support de formation en version électronique
- Pédagogie repensée : interactions, vidéos, enquêtes en ligne, exercices...

A qui s'adresse cette formation ?

- DSI et responsables informatiques
- Responsables des études, de l'exploitation et des services utilisateurs
- Directeurs Financiers et contrôleurs de gestion
- Métiers et maîtrises d'ouvrages SI
- Directions générales
- Consultants et auditeurs

Votre contact : Anne RENAUD – email : anne.renaud@axians.com – Tél 71 53 08

>>>

❶ Contexte d'évolution du cadre règlementaire

UN CADRE RÈGLEMENTAIRE UNIFIÉ

- Trois objectifs : renforcer le droit des personnes, responsabiliser les acteurs, crédibiliser la régulation
- De quelles données d'entreprise parle-t-on ?
- RGPD : Obligation ou opportunité? Les raisons de se conformer au RGPD : quels sont les risques ?
- Le coût de la mise en conformité.
- Place de la directive Police-Justice, de la future directive e-Privacy. Evolution de la « règlementation cookies » et du Privacy Shield.
- Rôle de la Cnil, de l'Anssi, du G29.
- Différents contextes existants : Patriot Act, PCI-DSS, CADA, LRN, HDS, etc.

UN CHAMP D'APPLICATION ÉTENDU

- Homogénéisation des droits et rôles dans l'UE : Guichet unique, coopération entre autorités de contrôle via le CEPD (Comité européen de protection des données)
- Renforcement des droits des personnes.
- Approche globale et nouveaux outils : registre, étude d'impact, privacy by design, violations.
- Responsabilisation forte de l'entreprise (accountability) et des sous-traitants.
- Sanctions importantes.

❷ Synthèse des textes et concepts fondamentaux

Analyse et synthèse du RGPD, de la nouvelle loi Informatique et Libertés et des différents règlements connexes afin de dégager tous les concepts à prendre en compte.

- Autorité de contrôle : nouveaux rôles, contrôle, certifications, réclamations.
- CEPD : place du Comité Européen de Protection des données. Contrôle de cohérence.
- Code de conduite et certification : importance majeure à venir.
- Communication, formation et information : Sensibilisation des clients, formation des collaborateurs.
- Consentement : manifester une volonté et « notariser » le consentement ?
- Co-responsabilité : quelle responsabilité des sous-traitants ?
- Données personnelles et sensibles: quelles informations identifient directement ou indirectement une personne ?
- Différenciation données personnelles / sensibles.
- Données transfrontalières : Transferts au sein de l'UE/hors UE, pays hors règlementation. Cas des US.
- DPO : Profil, rôle, missions du DPO.
- Droit à la portabilité des données : Différences avec le droit d'accès.
- Droit d'accès, consultation, modification, effacement, oubli
- Délais et procédure de validation. Quelles données conserver ?
- e-Privacy : Impacts sur les communications et gestion « centralisée » des cookies.
- Loi Informatique & Libertés : principaux apports : mineurs, pouvoirs de la CNIL, autorisations préalables, etc.
- Minimisation des données, Finalité : Les «données strictement nécessaires à la finalité poursuivie».
- Police-Justice : Quel impact sur la détention de données personnelles ?
- Privacy by design : Protection des données dès la conception des applications, sites Web et autres systèmes IT.
- Les travaux de référence (Ann Kavoukian - Ontario). Les 7 principes fondamentaux.
- Privacy by default : Garantie apportée par les mesures intégrées nativement dans le service.
- Responsable de traitement : Qui est responsable de traitement (RT)?. Place du DPO
- Traitement : définir un traitement et sa « licéité ».
- Violation de données : Comment déclarer aux autorités dans les 72 heures et informer les personnes concernées ?

❸ Grandes étapes de mise en conformité

Une analyse globale et exhaustive des traitements et données personnelles existantes, des conditions de conformité et de sécurité, débouchant sur un plan à moyen/long terme de mise en conformité.

ETAT DES LIEUX ET ANALYSE PRÉALABLE

- Nommer un DPO, créer une task force, informer
- Analyser l'environnement juridique propre à l'entreprise.
- Cartographier les données personnelles, définir niveaux de confidentialité et délais de conservation.
- Cartographier traitements et processus (y compris non automatisés), consentements et droits. Procéder à une étude d'impact si nécessaire. Création du registre.
- Inventaire des transferts et de la sous-traitance dans et hors UE.
- Identifier les écarts à partir d'une grille de conformité.

PLAN D'ACTION

- Plan d'action sur la base de l'état des lieux : informatique, organisation, processus.
- Répartition des tâches entre les parties (DPO, Métiers, DSI, RSSI, RT). Le DPO, MOA transverse en charge de la gestion des exigences.
- Comment gérer les «nouveaux» consentements, les droits des personnes, l'information préalable ?
- "Privacy by design" et "by default" : les exigences pour garantir l'intégrité des données et assurer un haut niveau de protection dès la conception (Privacy by design) et par défaut (Privacy by default).
- Mise à niveau de l'infrastructure de sécurité SI et de la gestion des risques (cas de violation de données). Etre ISO 27001 ?
- Elaboration de règles d'entreprise contraignantes (BCR) et clauses contractuelles type. Intégration du Privacy Shield.
- Sensibiliser, informer et former.

MAINTIEN DE LA CONFORMITÉ SUR LE LONG TERME

- Systématiser la « Protection by default », planifier l'audit périodique de compliance.

❹ Les mesures d'«accountability»

Au plan pratique, les premières mesures à prendre pour démontrer la démarche de conformité RGPD de l'entreprise.

NOMINATION DU DPO (DATA PROTECTION OFFICER)

- Est-il obligatoire ? Rôle des CIL ?
- A qui reporte-t-il ? Partager un DPO ?
- Lignes directrices du G29 (statut, missions).
- DPO, MOA « transverse » du RGPD.

MAINTENANCE DU REGISTRE

- Inventaire des traitements. Formalisme. Informations à fournir.
- Quels outils logiciels d'aide (ActeCIL, PrivaCIL, DPO, etc)?

RÉALISATION D'ANALYSE D'IMPACT (PIA – PROTECTION IMPACT ASSESSMENT)

- Quels traitements y sont soumis ?
- La méthodologie eBios. Finalité du traitement, proportionnalité aux objectifs, risques supportés, mesures de protection, etc. L'alternative ISO 27018.
- Comparaison à une grille de conformité. Les logiciels d'aide (Nymity, Avepoint, etc)? L'outil PIA de la CNIL.
- Dans quel cas consulter l'autorité ?

ACCOUNTABILITY

- Que faut-il documenter ?
- Révision des documents commerciaux (CGV, CGU), contrats, etc.

❺ Impacts sur le Système d'Information

La mise en conformité RGPD de l'entreprise a un impact majeur sur le SI, sa stratégie, son organisation, qu'il faut planifier et budgéter.

GOUVERNANCE DES DONNÉES

- Inventaire et cartographie des données. Les outils (Compliance Guardian, Carto-SI, Control Point, CA, etc)
- Nouvelles règles de gestion (sauvegarde, archivage) et de protection (Chiffrement, intégrité, signature) fonction de la sensibilité / conservation et de la hiérarchie de stockage.
- Impact sur le Big Data, l'IoT, l'IA, la Blockchain? Vers une restriction du patrimoine informationnel ?

SÉCURITÉ DU SI

- Adéquation de l'infrastructure de sécurité et du SMSI : 5 niveaux et 15 points de contrôle.
- Quelle politique de gestion des profils à privilèges ?

SÉCURITÉ DES DONNÉES

- Sécurisation des données personnelles aux niveaux PC/mobile, accès, stockage, PRA, Cloud, etc.
- La «pseudonymisation». Pour quels types de données ? Les pseudonymes sont-ils des données personnelles ?
- Anonymisation par randomisation ou généralisation, masquage de zones.
- Outils de pseudonymisation/anonymisation (Lamane, Solix, IBM, Oracle, Informatica, etc), de chiffrement (Safenet, Sophos, etc) et les CASB-Cloud Access Security Broker (SkyHigh, CipherCloud, etc)

ADMINISTRATION DES RISQUES

Détecter une violation, la diffusion « extérieure » de données .
Mise en place de DLP (Data Leak Prevention). L'offre (Symantec, Forcepoint, etc). Suivi de e-réputation.
Gestion de la crise « violation des données ».

APPLICATIONS ET PROGICIELS

- Gérer et notariser les consentements, les droits (modification, effacement, oubli). Nouveaux outils de CIAM-Consumer Identity and Access Mangement (Gigya, Celebrus, etc). L'accès aux archivages.
- API et services de transfert de données (Onecub).
- De « nouveaux » progiciels (CRM, marketing, service desk, etc).

PRIVACY BY DESIGN / BY DEFAULT

- Intégrer dès la conception les exigences du DPO, du RSSI.
- Impacts au niveau cahier des charges, programmation, revue de code, tests, mise en production. Apports des méthodes agiles et de Devops. Anonymisation des jeux de tests.
- Les bonnes pratiques et méthodes (Secure SDLC, OWAPS)

« SHADOW IT »

- Gérer les projets gouvernés par les métiers, la dispersion des données.

LES OFFRES DES SOUS-TRAITANTS ET FOURNISSEURS

- Impact du « Privacy by design » sur les progiciels, le Cloud. Qui doit fournir le PIA ?
- Clauses de conformité dans les contrats (ISO, SOC, CISPE)?
- Comment les GAFAM ont (déjà) intégré le RGPD.

L'IMPACT DU RGPD SUR LES SECTEURS ET LES MÉTIERS

- Marketing, DRH, commercial. Données de santé.
- e-Commerce, Programmatique.