DPO FORUM

DPO CIRCLE

Les différents chantiers à mettre en œuvre pour se conformer au GDPR

23 octobre 2018

Philippe MEULDERS

DPO Circle - Genval, le 23 Octobre 2018

1. Education et sensibilisation

Le plus grand défi !

L'enjeu derrière le GDPR :

- la sécurité de l'information (croissance exponentielle des cyber-attaques, envoi de DCP à des personnes non autorisées, …)
- Périmètre : Confidentialité, intégrité, disponibilité, résiliences des systèmes et services
- Données à caractère personnel v. Données confidentielles

Le GDPR, un coût indispensable

- Image de marque
- Valorisation boursière ou du capital, survie de l'organisation
- Sanctions

Autres bénéfices apportés parle GDPR :

- Ne plus saisir les mêmes DCP dans plusieurs applications,
- Réduire le coût d'archivage papier / électronique,
- Mieux maîtriser les processus métiers,
- Avoir des données à jour,
- mieux connaître ses sous-traitants, …

GDPRPRO.com

ICT CONTROL
Your Trusted Advisor

DPO CIRCLE

2. Registre de traitements et Gap analysis

Formation des intervenants

Des fiches exhaustives :

- RT / ST
- Finalités
- Personnes concernées (Data subjects)
- DCP traitées
- Systèmes IT (y inclus shadow IT, objets connectés, DB & serveurs sur lesquels les DCP sont hébergés)
- Destinataires internes et externes des DCP
- Canaux de communication et niveau de sécurité requis

GDPRPRO.com ICT CONTROL Your Trusted Advisor DPO CIRCLE

2. Registre de traitements et Gap analysis

Validation des fiches par les métiers

Minimiser le nombre de fiches (finalités)

Gap analysis juridique (licéité, etc.)

Gap analysis Sécurité IT

(forces/faiblesses)

Portefeuille de projets / chantiers priorisés

par niveau de risque

3. Gouvernance GDPR et procédures

Politique GDPR (acteurs et rôles) : CoDir, CRO, DPO, employés, externes, …

Revue de toutes les procédures / Modops

Procédure de gestion des droits des Data subjects

Procédure de gestion des violations de données

Data protection by Design (conception) & by default

Data Protection Impact Analysis (DPIA)

Sessions de sensibilisation à toute l'organisation

GDPRPRO.com ICT CONTROL Your Trusted Advisor DPO CIRCLE

4. Chantiers juridiques

La partie émergée de l'Iceberg

Les contrats clients

Les contrats sous-traitants (Data processors)

Les contrats employés

Le Transfert de données hors EEE

Les termes et conditions diverses (site web publics et privés, emails, …)

Une Cyber-assurance

GDPRPRO.com

ICT CONTROL Your Trusted Advisor

DPO CIRCLE

5. Chantiers IT

Recommandations du Gap analysis IT

Possibilité d'exercer les droits des data subjects pour toute application / système IT

Extraction, suppression, anonymisation des données via scripts dans les DB

Nouvelles releases et interfaces utilisateurs

Mettre en œuvre la protection dès la conception et par défaut pour tout nouveau projet

BCP / DRP

6. Suppression des données

Un des chantiers le plus vaste

Tableau récapitulatif de la « durée légale de rétention des données » pour tous les traitements et DCP

Voir en pratique comment supprimer les données dans tous les systèmes, applications, répertoires (shadow IT) + les supports papiers

Validation et lancement des opérations de suppression

Instructions formelles aux sous-traitants

7. Mesures de sécurité de l'information

Description des mesures de sécurité en place

Mettre en œuvre les recommandations du Gap analysis Sécurité IT

Décrire l'encryption, pseudonymisation en place et planifier de nouveaux objectifs

Audits internes et des sous-traitants, Pen tests, SOC (Security Operating Center - détection)

Minimisation et contrôles des accès applicatifs, répertoires, DB et systèmes (utilisateurs et comptes à hauts privilèges)

DPIA

Plan de gestion et de communication de crise (cyber-attaque, panne IT conséquente, …)

8. Violation de données

3 cas :

- « pas » de risque ou risque résiduel faible : registre des incidents
- Risque pour le data subject : Registre + Notification à l'Autorité de contrôle
- Risque important pour le DS : R + N + Notifiation au DS

En tant que Data Controller (Responsable de traitement)

(évaluation du risque + 72h)

En tant que Data Processor (Sous-traitant)

9. Documenter la mise en conformité

Renversement de la charge de la preuve en cas de contrôle par l'Autorité de contrôle

Stocker toutes les évidences de mise en œuvre du GDPR (formations GDPR, audits, registres, DPIA, Analyses DP by design / default, mesures organisationnels et de sécurité mis en place et planifiés, encadrement des transferts de DCP hors EEE, information des personnes, les Politiques et procédures, les contrats etc.)

Mise à jour du registre de traitement

Registre de violation de DCP à jour

Registre de gestion et suivi de l'exercice des droits des Data subjects à jour

GDPRPRO.com

ICT CONTROL
Your Trusted Advisor

DPO CIRCLE

DPO and GDPR professionals

Association belge des professionnels du RGPD.

Rejoignez gratuitement les membres et participer aux différentes réunions et tables rondes sur différents sujets relatifs à la protection des données.

DPOCIRCLE.EU

Experience sharing, advocacy and development of toolbox, Up to two round table meeting in a month

Conferences with the involvement of Data Protection authorities (Belgian ADP, EU EDPS) and Secretary of state

Annual Conference in Genval 2018

300 members

Solvay Brussels School
Economics & Management

European Program in Data Protection
Next edition starting on March 22

Solvay.edu/gdpr

coms.solvay.edu/gdpr-modules-alumni-2018

Solvay Executive Education

Solvay Brussels School
Executive Education

DPO CIRCLE

IT MANAGEMENT Academy

Extended Education for DPO professionals

DPO and GDPR implementation professionals require extended knowledge and practice. We are delighted to give access to our **Alumni of the Program in European Data Protection** to extended education that both created and sustained the reputation of **Sol School** in domains like **Digital Transformation**, **Technology Implementation**, **Security, Risk Management, Compliance and Auditing**, and much more.

Benefit from our spec

S1 – Information Security Management	G1 – The CIO Foundation	M1 – Applications Build and Management	B1 – Enterprise Strategy and Architecture	A Po
S2 – IT Security Practices	G2 – IT Governance Workshop	M2 – IT Services and Run Management	B2 – Business Transformation	A2 – Soft Skills for IT professionals
S3 – Cybersecurity Workshop	G3 – IT Risk and Legal concerns	M3 – IT Sourcing Management	B3 – Digital Agility and Innovation	A3 – Building Expert Opinion

PROGRAMME IN EUROPEAN DATA PROTECTION

Leading to certified DPO

Solvay Brussels School
Economics & Management


GDPRPRO
DPOASASERVICE
gdprpro.com

MERCI POUR VOTRE PRESENCE

Questions?