UIMM Yonne
LA FABRIQUE DE L'AVENIR

MEDEF Yonne

RGPD

Règlement Général sur la Protection des Données

Xavier LECLERC

PDG DPMS / Président de l'UDPO

25 mai 2018

Agenda

Le RGPD/GDPR Sensibilisation au règlement
Les grands principes : mise en application, pénalités, accountability Les contraintes réglementaires : article 30 tenue d'un registre
Impacts sur les entreprises
La gouvernance du programme GDPR et les impacts sur les processus Les impacts sur le système d'information
DPO et certification
Le Délégué à la Protection des Données ou Data Protection Officer La certification
Questions / réponses

Le Groupe DPMS au service de votre CONFORMITE

2004 axil DPMS Group

Conseils
CIL externe
Revue de conformité
Audits

2008 PrivaCIL DPMS Group

Edition de logiciel

2012 anaxil DPMS Group

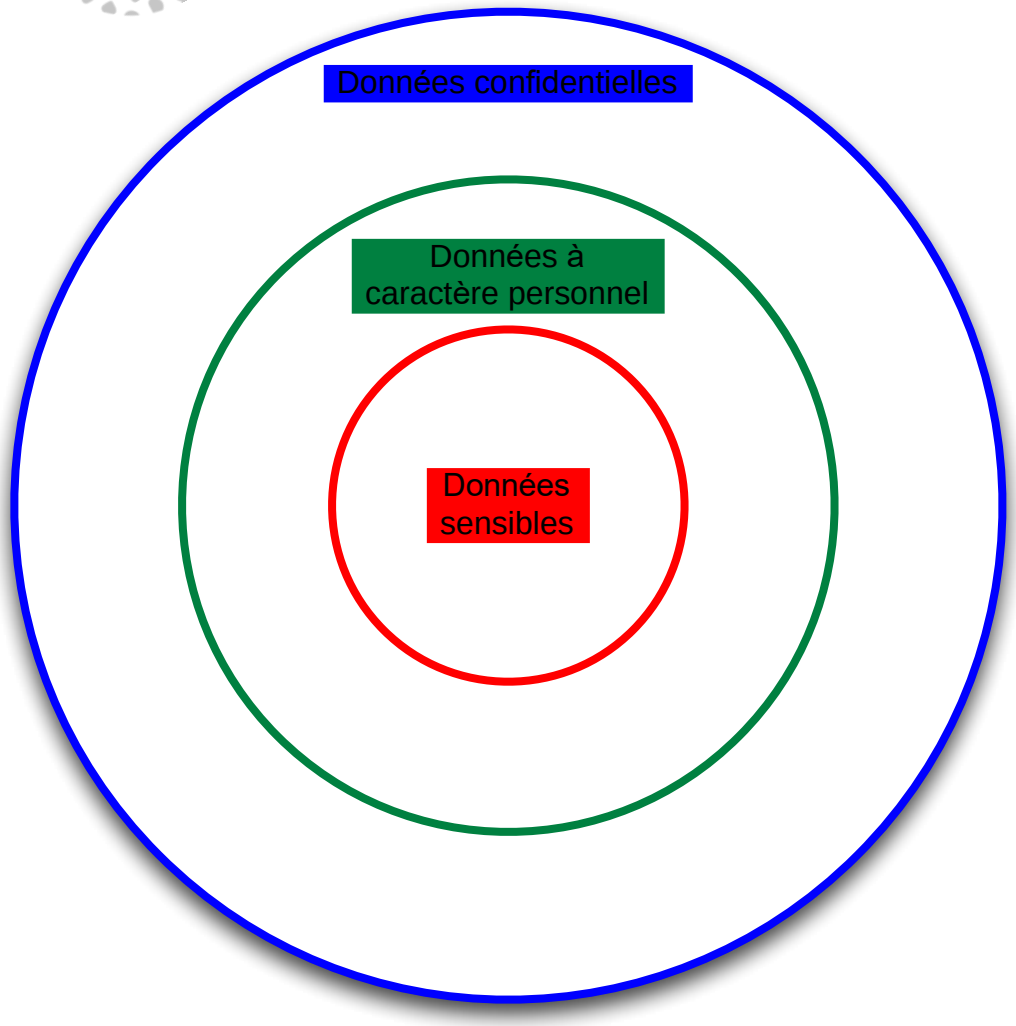
Formation labellisées CNIL
Mutualisation CIL
Qualifié Bureau Véritas certification (DPO et Référents RGDP)

De quoi parle-t-on ? – Art.2 L

Information portant sur une personne physique :

- **Les données directement nominatives**
  - **nom/prénom, numéro de sécurité sociale, …**
- **Les données indirectement nominatives**
  - **numéro de téléphone, plaque d'immatriculation, numéro de CB, adresse IP, RFID, …**
- **Les données qui peuvent être rattachées à une donnée nominative**
  - **Achats, déplacements réels ou virtuels, communication, centres d'intérêt, segmentation, etc.**

Les données confidentielles ne sont pas toutes à caractère personnel mais toutes les données à caractère personnel sont confidentielles


Données confidentielles
Données à caractère personnel
Données sensibles

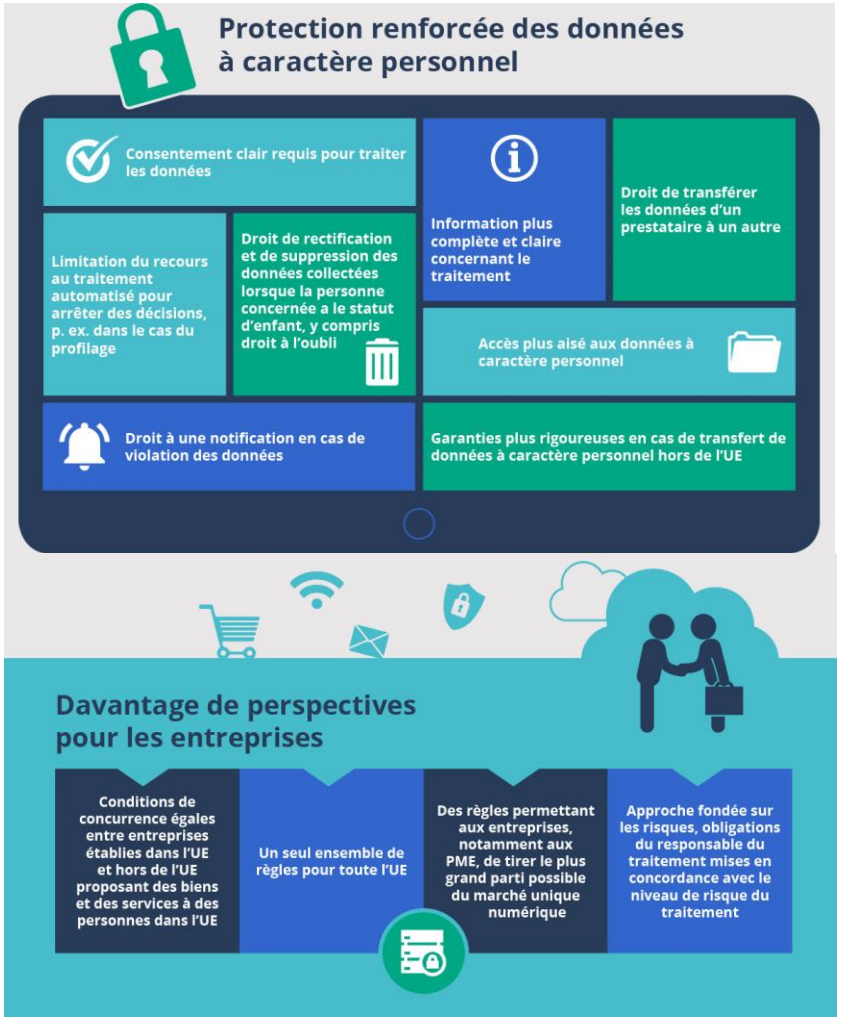
Lecture du cadre légal

- **Adoption de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- **Convention 108 du Conseil de l'Europe**
- **Directive européenne 95/46/CE du 24/10/1995**

  (date limite de transposition : 23/10/1998)
- **Loi 2004-801 du 6 août 2004 modifiant la loi du 6 janvier 1978**
- **Circulaire du 12 mars 1993 (secteur public)**
- **Décret d'application N°2005-1309 du 20 octobre 2005**
- **Délibération n°2006-147 du 23 05 2006 (règlement intérieur CNIL)**
- **Décret d'application N° 2007-451 du 25 mars 2007**
- **Loi 2009-526 du 12 mai 2009**
- **Proposition de la Commission des Lois du Sénat du 24/02/10 (Détraigne – Escoffier), votée le 23 mars 2010**
- **Lois organiques et ordinaires relatives au défenseur des droits du 29 mars 2011**
- **Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, applicable au 25 mai 2018**
- **Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique**

Le RGPD et le quotidien des organismes et des CIL/DPO

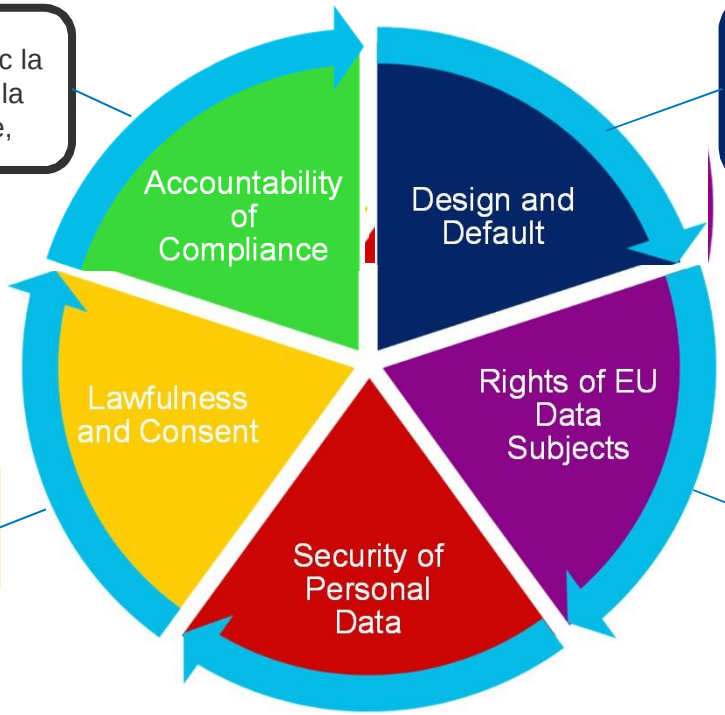
Le Règlement Européen



Source : Conseil de l'union européenne

Vision du règlement

Obligation de démontrer la conformité des traitements avec la réglementation du RGPD sur la protection des DCP : registre, documentation



Les RT et ST doivent prendre les mesures techniques et organisationnelles pour démonter la conformité avec les règles du RGPD

Licéité du traitement uniquement si consentement explicite, obligation légale, à la demande des autorités avec réquisition et en cas d'intérêt légitime

Obligation de répondre aux demandes liées aux droits des européens Accès, Rectification, Portabilité, …

Obligation de mettre toutes les mesures de sécurité nécessaire pour protéger les données, notamment dans le cas des failles

Les besoins nés de la réglementation

Conformité :

Les organismes doivent être en conformité avec la loi Informatique et Libertés.
Etre en conformité, c'est s'assurer de minimiser les risques en maximisant la relation de confiance.

Nommer un DPO (Data Protection Officer ou Délégué à la Protection des Données) :

Avec le RGPD, la nomination d'un DPO est obligatoire pour tout organisme public, et pour tous les organismes traitant des données sensibles ou mettant en œuvre un traitement de profilage / segmentation comportementale.

Analyse de risques, analyse d'impacts :

Apprendre à aborder les risques liés à la protection des Données à caractère personnel et en analyser les impact sur l'activité de l'entreprise : réputation, confiance, finances…

Gouvernance et accountability :

L'Accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données : **tenir le registre des traitements (article 30)**.

Se préparer pour le règlement européen :

Le 25 mai 2018, c'est demain. L'émergence du Règlement Européen va nécessiter la continuité des lois en vigueur tout en se préparant à la transformation vers les nouvelles normes et règles.

Les Risques

Les impacts d'un manquement au respect des textes de loi I&L peuvent mettre en danger :

- La réputation de l'entreprise auprès de ses clients et de ses fournisseurs,
- La stabilité sociale et sociétale,
- Le positionnement de l'entreprise.

Panorama des risques :

	Risques CNIL	Risques Judicaires	Risques Economiques	Risques Sociaux
Matérialisation	Mises en demeure, injonction, fermeture des sites.	Inopposabilité des preuves.	Un fichier clients / usagers / administrés non déclaré à la CNIL n'a aucune valeur financière ni juridique.	Le licenciement d'un salarié sur la base d'un traitement non déclaré n'a pas de valeur.
Sanctions	Administratives.	Pénales, civiles, 5 ans de prison	Nullité des transactions.	Nullité des licenciements.
Coûts	Amendes Jusqu'à 3.000.000 € 2018 : 2 ou 4% du CA groupe ou 10 - 20 M€ (le plus haut montant étant retenu)	300.000 €	Pertes sèches de la valeur de la vente. Pertes de contrats pour non respect de la règlementation	Coûts des procédures et un minimum de 6 mois de salaire.

Les phases méthodologiques

Orientations
Choix

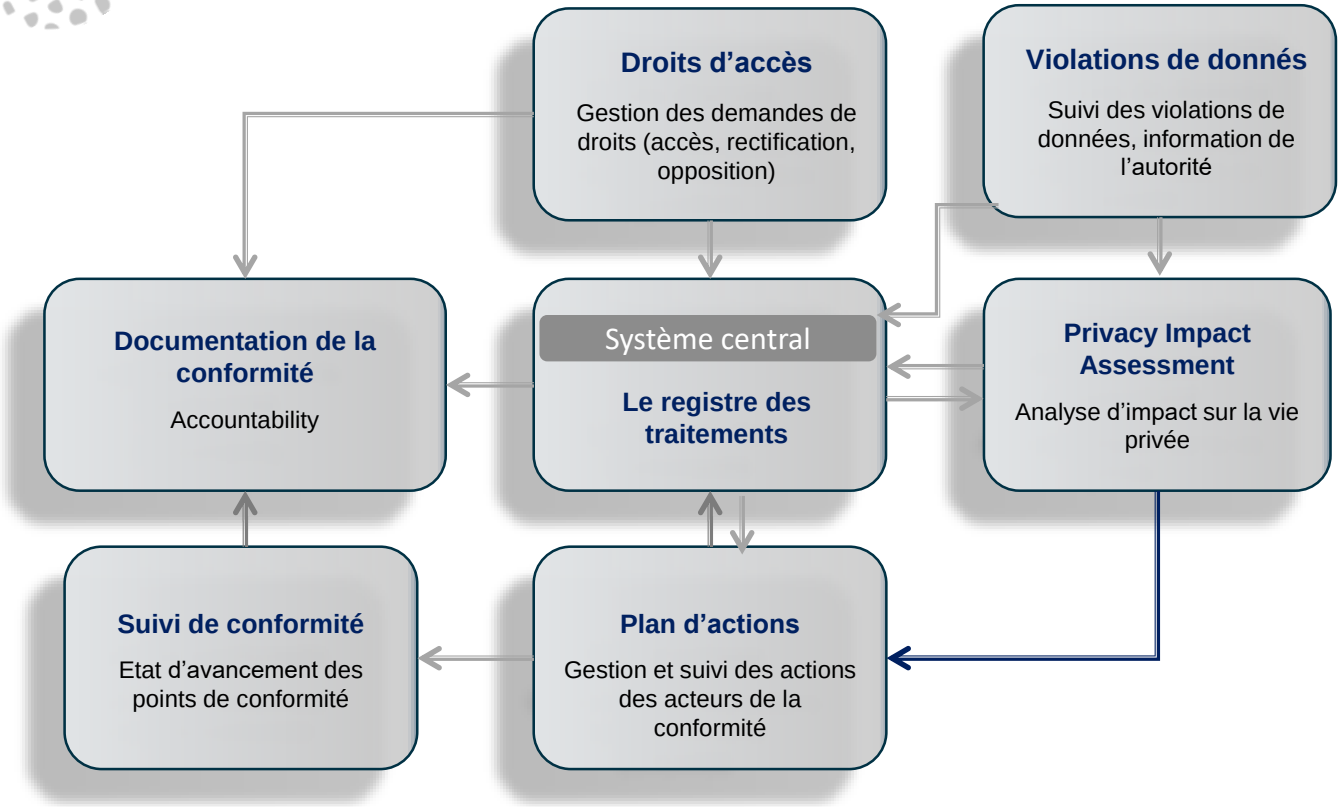
1 Maturité GDPR → 2 État des lieux GDPR → 3 → 4 5 Trajectoire GDPR 6 → Maintien de GDPR

Organisation	Chantiers GDPR	Outils accélérateurs GDPR
Gouvenance	Cartographier les traitements de données	▪ Registre de traitement & Cartographie
	Gouvernance : DPO & communauté	▪ Registre étendu aux plan d'actions
	Sensibilisation et formation	▪ E-learning / Serious game / Présentiel
	Protection des données personnelles	▪ Cartographie, effacement, anonymisation, chiffrement
	Mise en oeuvre des PIA	▪ Registre étendu au PIA
	Gestion du consentement	▪ Collecte et exposition des consentements
	Droit des personnes	▪ Registre étendu aux droits des personnes
	Transfert des données	▪ Registre de traitement
	Failles de sécurité	▪ Sécurité opérationnelle et incidents

Gestion projet RGPD

- Revue initiale de conformité (registre, plan d'actions)
- Accountability : bilan annuel, rapports, documentation
- Sensibilisation
- Audit
- Organisation
  - Référents RGPD
  - Comité projet (DJ, DSI, DRH…)
- Outil de pilotage (ex : Privacil – DPMS)

RGPD – Le registre étendu



Principales Évolutions RGPD

En résumé

- La responsabilisation, Article 24
- Le registre, Article 30
- L'EIVP Article 35 et L'AIVP Article 36
- Les notifications des failles de sécurité
- La co-responsabilisation
- Les sanctions
- Nouveaux droits : portabilité, oubli…
- Privacy by design

Le contexte

Renforcement des contrôles et des sanctions :

Renforcement des contrôles par la CNIL.
Renforcement des sanctions financières : 4% du chiffre d'affaire global groupe (**jusqu'à 20 M€**).
Continuité des sanctions pénales : 300.000 € / 5 ans de prison.

Le CIL devient DPO ? :

CIL vs DPO :

CIL	Tenir le registre des traitements	Etablir son bilan annuel	Traiter les demandes et les reclamations	Garantir la conformité des traitements	Alerter le responsable des traitements sur les non conformités
DPO	Gérer la documentation (dont le registre de l'organisme)	Accountability Rapports d'activité	Réaliser les Etudes d'Impact Vie Privée et traiter l'exercice des droits	Controler la conformité des traitements	S'assurer de la Privacy by design / default Notifier les failles de sécurité à la CNIL

Types de CIL / DPO

- Pour les grandes entreprises : DPO interne, essentiel et stratégique voir obligatoire
- Pour les PME ou le secteur public, la mutualisation ou l'externalisation est la seule solution : n'ont pas la bonne personne en interne, temps plein, n'ont pas le budget …
- Beaucoup de petites structures vont peiner à être conformes.

Types de CIL / DPO

- Concept du « CIL / DPO mutualisé »

- Première fois en France en 2006 : CIL mutualisé pour la profession notariale : offices et instances (3000).

- En 2011, les procédures métiers mises en place par Xavier Leclerc (revue initiale, bilan, audit) sont homologuées par la CNIL (unique à ce jour)

Professionnalisation = Certification

- Permettre aux entreprises de distinguer le bon grain de l'ivraie

- Permettre aux CIL en place de devenir DPO

- Art. 37.5 : *le Délégué est désigné sur la base de ses qualités professionnelles et de ses connaissances spécialisées du droit et des pratiques en matière de protection des données…*

- Art. 38 du RGPD : *le RT et le ST aident le délégué…en lui permettant d'entretenir ses connaissances spécialisées*

Professionnalisation = Certification

➢Partenariat Bureau Veritas certification et l'Union des DPO (UDPO) – exemple suivi de l'Italie

UNION DES DPO

➢ Certification par BVC des
- DPO
- Référents RGPD

Qualification Formation DPO
BUREAU VERITAS Certification

➢ Délivrance par l'UDPO d'une carte professionnelle aux adhérents certifiés

Professionnalisation = Certification

➢Formation par un organisme qualifié par BVC (ANAXIL est le premier en France : 6 jours / 48h)

➢ + Expérience minimum de 2 ans pour les DPO selon niveau d'études

➢ + Réussir à l'examen de certification (centre d'examen = UDPO)

➢ = Certification par BVC

BUREAU VERITAS
Certification

QUALIFICATION CERTIFICATE

ANAXIL
1198 avenue du Dr. Maurice Donat
06 250 Mougins - France

Bureau Veritas Certification France certify that the company mentioned above meets the requirements for DPO certification according to the following standards:

Standard

DPO SCHEME
FOR THE CERTIFICATION OF PERSONS
Version : 26/06/2017

in compliance with CEPAS SCH73 procedure

Scope

TRAINING COURSE QUALIFICATION

FORMATION REGLEMENT EUROPEEN
SUR LA PROTECTION DES DONNEES (RGPD)
FORMATION DPO

Certification cycle start date: **13 July 2017**

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: **12 July 2020**

Original certification date: **13 July 2017**

Certificate No : **FR038288– VERSION 1**
File No : **7064024**

Date: 31 August 2017

Jacques Matillon – Managing Director

Certification body address: 66 Prescot Street, London E1 8HG, United Kingdom.
Local office: Bureau Veritas Certification France : 60 avenue du Général de Gaulle 92046 Paris la Défense

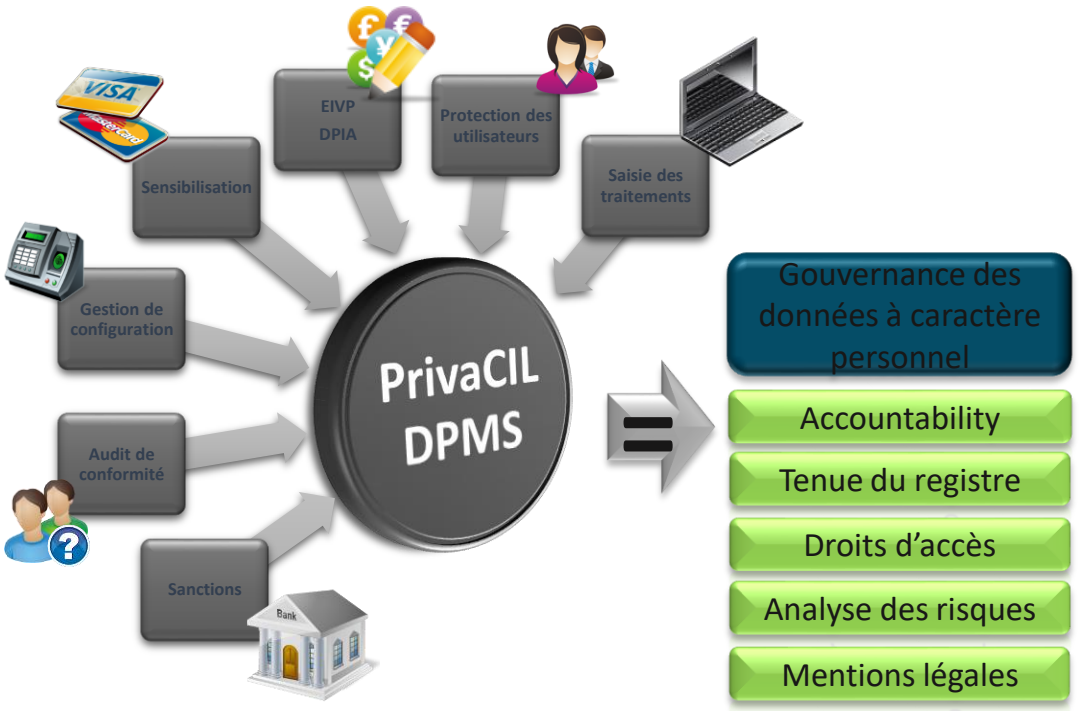
Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: +33 (0) 1 41 97 00 60

PrivaCIL-DPMS : Gestion de la conformité

Une solution adaptée

Dans le cadre du RGPD/GDPR, une **solution logicielle** vous donnera la possibilité de vous préparer efficacement pour le 25 mai 2018.

La multitude de nouveautés et le temps qu'elles demandent, oblige à se munir d'un outil efficace, source de solution et de gain de temps. Puissante, modulable et évolutive.



Merci pour votre attention !

Xavier LECLERC – PDG DPMS / Président de l'UDPO
xavier.leclerc@dpms.eu • Tel : + 33 (0)6 61 30 25 92

www.dpms.eu

www.udpo.fr