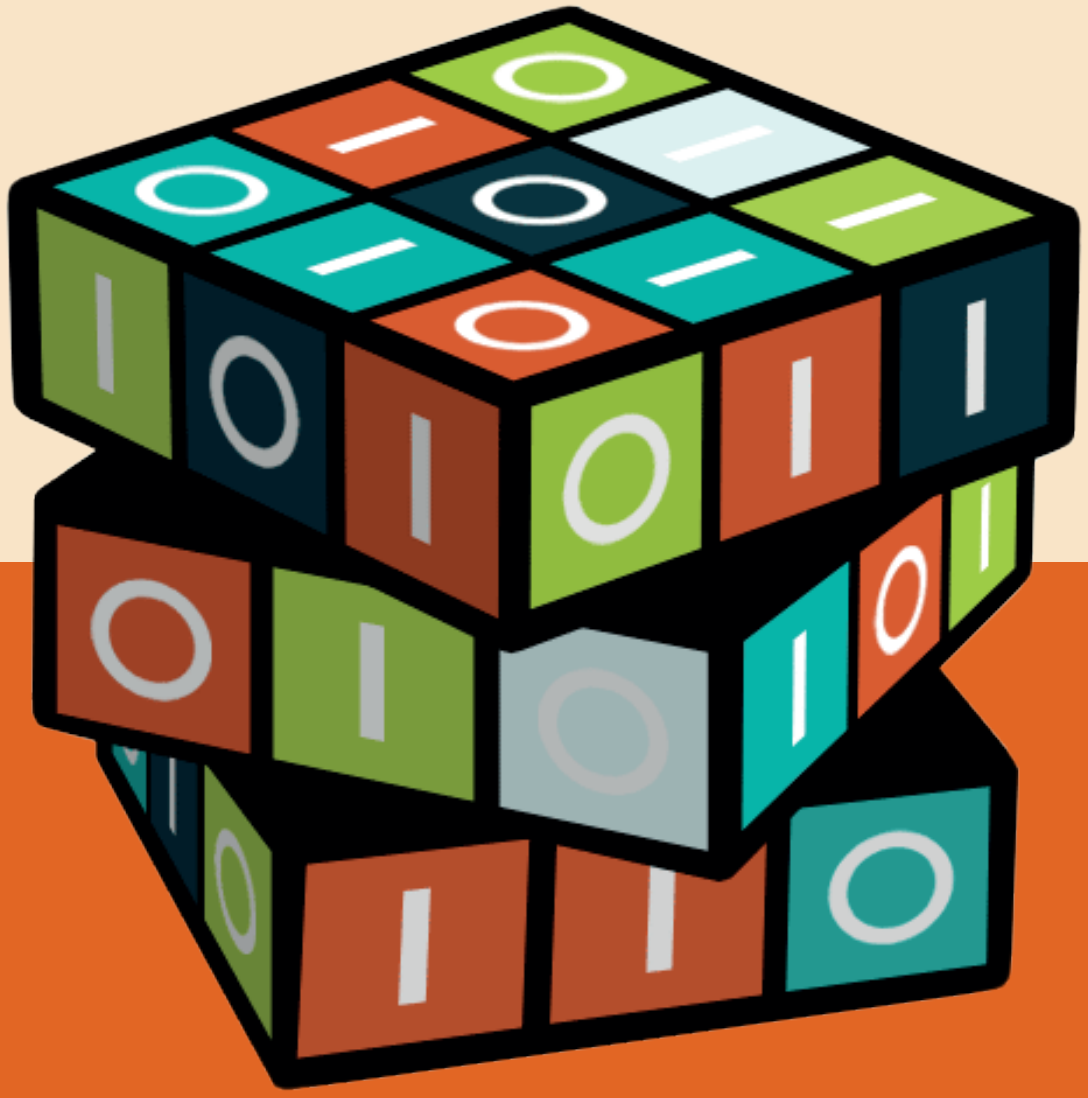
GDPR COMPLIANT

Le guide pratique



Umanis BEYOND DATA

LEXING ALAIN BENSOUSSAN AVOCATS

Segeco

IBM

ILS ONT PARTICIPÉ À CET E-BOOK

Nous tenions à remercier tous ceux qui ont apporté
leurs témoignages et leurs expertises sur ce sujet.

Luc ALLOIN, Associé Segeco Directeur Général Securymind
Alain BENSOUSSAN, Avocat à la Cour
Thierry BRUN, GDPR Ambassador, IBM
Benoît DESPRÉS, Directeur de la Maîtrise d'Ouvrage Finances et Risques, IBP
Charley DUPRÉ, DPO et Juriste, Volkswagen
Jean Philippe GAULIER, RSSI, Orange
Denis GENEST, Associé Segeco
Denis SKALSKI, Directeur Practice Data, Umanis
Stéphane TOURNADRE, Directeur Sécurité et Audit SI, Laboratoires Servier

SOMMAIRE

© Umanis 2018

PRÉFACE
par Alain Bensoussan, Avocat à la Cour

Le 25 mai 2018, le réveil risque d'être douloureux pour les entreprises qui n'auront pas pris pleinement la mesure du Règlement européen sur la protection des données.
Si cette réforme du droit des données personnelles vise à encourager l'innovation au sein du marché unique du numérique, elle vise surtout à garantir un niveau élevé de protection des citoyens.

Alors que la donnée est perçue comme un actif clé de l'entreprise, il n'en va pas de même pour le citoyen, la notion de donnée personnelle ramenant à celles de vie privée, de confidentialité et de libre circulation des informations personnelles.

Depuis la loi Informatique et Libertés du 6 janvier 1978, les principes de licéité de la collecte de données personnelles sont posés : proportionnalité des données collectées par rapport à la finalité du traitement, loyauté de la collecte, droit d'opposition des personnes concernées, interdiction de principe de la collecte de données sensibles. Avec l'arrivée du RGPD (ou GDPR en anglais, pour General Data Protection Regulation), le droit des personnes se trouve renforcé, rendant dans certains cas le consentement obligatoire. C'est la grande bascule opérée par le Règlement : passer d'une responsabilité a posteriori du Responsable de traitement, à une responsabilité a priori.

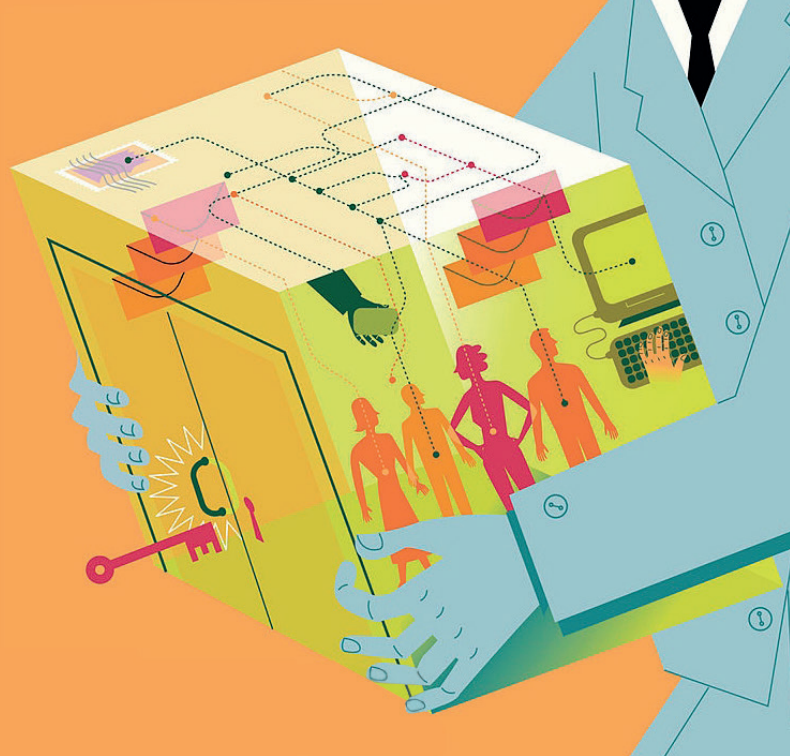
En effet, à partir du 25 mai 2018, chaque organisme devra édicter une politique de protection des données personnelles sur-mesure selon le traitement auquel il procède et surtout documenter celle-ci.

Désormais, c'est aux entreprises qu'incombe la responsabilité de la manipulation des informations, depuis la localisation des données sensibles sur le réseau jusqu'à la gestion des accès, le stockage et la sécurité. Les entreprises doivent, dès à présent, se préparer à être en mesure de rapporter la preuve de la conformité des traitements de données aux principes posés par le RGPD. Elles devront édicter, sur mesure, une politique de sécurité, de gouvernance et de gestion des données sous peine de sanctions très lourdes : des amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel de l'entreprise sanctionnée.

Les organisations devront également se plier à de nouvelles exigences : droit à l'oubli et à la portabilité des données, consentements éclairés et explicites, notifications aux personnes et aux autorités en cas de failles de sécurité affectant leurs données, nomination d'un Data Privacy Officer, mise en place d'études d'impacts (PIA) systématiques pour les traitements sensibles.

Mais sa mise en application devrait aussi et surtout avoir un effet positif puisqu'il renforce les obligations de sécurité des entreprises, donnant ainsi à leurs clients l'assurance d'un niveau de protection accru pour le traitement de leurs données personnelles. Il permet ce faisant d'accroître également la confiance

© Umanis 2018



de ses partenaires et collaborateurs, et de renforcer sa position concurrentielle.

Le RGPD est donc une bonne nouvelle, puisqu'il renforce l'Europe et promeut l'intérêt général des citoyens de l'UE. Mais dans les faits, la mise en conformité requiert un effort combiné de tous les départements concernés par la gestion de données personnelles sous toutes ses formes (finance, IT, juridique, sécurité, marketing, RH..).

L'heure est donc venue pour les entreprises de mettre en place un véritable programme de protection de la vie privée reposant sur le droit fondamental et inaliénable que constitue, pour chaque citoyen, la protection de sa vie privée et de ses données personnelles.

© Umanis 2018

L'ABÉCÉDAIRE GDPR

Une donnée personnelle

Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement par référence à un identifiant tel que le nom, un numéro d'identification, une donnée de localisation, un identifiant en ligne, une adresse IP, etc.

Un traitement

C'est une opération ou un ensemble d'opérations effectuées sur des données à caractère personnel quel que soit le procédé, automatisé ou non. Un traitement est notamment constitué de la collecte, l'enregistrement, l'extraction, l'organisation, le stockage, la modification, la consultation, l'utilisation, la diffusion, l'effacement ou la destruction, etc.

Une donnée sensible

Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci. Par principe, la collecte et le traitement de ces données sont interdits.

La définition du risque selon la CNIL

Un risque est un scénario qui combine une situation crainte (atteinte de la sécurité des traitements et ses conséquences) avec toutes les possibilités qu'elle survienne (menaces sur les supports des traitements). On estime son niveau en termes de gravité (ampleur et nombre des impacts) et de vraisemblance (possibilité/probabilité qu'il se réalise). Pour la CNIL, gérer les risques est un moyen efficace de protéger *« libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel »* (article premier de la Directive 95/46/CE).

Le GDPR

Le General Data Protection Regulation (GDPR), est un règlement européen (2016/679) adopté en avril 2016 et qui sera applicable le 25 mai 2018. Ce texte à effet direct, c'est à dire qu'il n'y a pas besoin de loi nationale pour le transposer, a pour objectif l'amélioration de la protection et de la confidentialité des informations personnelles identifiables.

DPIA

L'application du nouveau règlement européen RGPD impose, en partie, la réalisation d'une analyse d'impact relative à la protection des données appelée DPIA pour Data Protection Impact Assessment). Cette démarche, repose sur une analyse de risques sécurité orientée uniquement sur les risques visant les données personnelles et leurs impacts sur les droits et libertés des personnes concernées par ces données.

PAR QUELS CHANTIERS DÉMARRER ?

« Notre objectif premier est d'établir au plus vite une cartographie des données qui sera un prérequis pour savoir où nous allons précisément. A partir de là, nous pourrons prioriser les actions et régler au plus vite les aspects les plus sensibles et confidentiels, ainsi que démarrer un vrai travail de pédagogie auprès des équipes opérationnelles. » explique Charley Dupré, Juriste chez Volkswagen. Nomination d'un DPO, révision du registre des traitements, droit à l'oubli, etc. les changements en interne sont nombreux et non négligeables !

☑ 1. TENIR UN REGISTRE DES TRAITEMENTS

Il contient, entre autres, le nom et les coordonnées du responsable du traitement, les finalités dudit traitement (relation commerciale, gestion RH…), les catégories de personnes concernées (clients, salariés, candidats) et la finalité du traitement (démarchage commercial, analyse statistique, etc.).

☑ 2. IDENTIFIER LE PÉRIMÈTRE DES DONNÉES

Toute entreprise dispose de données à caractère personnel et les capacités de collecte et de traitement élargissent le champ des activités potentiellement concernées (clients, prospects, patients, locataires, etc.). Le système d'information de l'entreprise se retrouve ainsi très largement impacté. Identifier le périmètre des données permet de réaliser une liste de tous les traitements qui touchent (ou pourraient toucher aux données personnelles) de façon à disposer d'une vision d'ensemble et de les transférer vers un autre opérateur ou fournisseur.

☑ 3. GARANTIR LE DROIT DES PERSONNES

Ce règlement renforce le droit des personnes physiques en interdisant tout traitement des données sans le consentement de celles-ci. Le droit à l'oubli oblige le Responsable du Traitement à garantir aux individus qui lui en feront la demande que leurs données seront bien supprimées dans le délai fixé. Le règlement instaure un droit à la portabilité. Il s'agit de la possibilité d'obtenir ses propres données personnelles le concernant, dans un format lisible et structuré.

© Umanis 2018

4. REVOIR LES CONTRATS FOURNISSEURS

Un principe nouveau apparaît : la coresponsabilité entre responsable de traitement et sous-traitant. Celle-ci doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs. Le responsable du traitement doit s'engager sur la voie de la conformité notamment en insérant des clauses contractuelles telle qu'une clause de « rendez-vous » - fixant les réunions d'étapes d'ici à mai 2018 – ou une clause d'audit, voire des pénalités financières en cas de manquement aux engagements qualité (SLA).

5. ÉDICTER UNE CHARTE DE BONNES PRATIQUES

Une charte permet de communiquer aux employés les bonnes pratiques à appliquer ainsi que les sanctions encourues en cas de non-respect de la loi. Par exemple, un salarié ne peut accéder ou supprimer des informations ne relevant pas de sa fonction ou enregistrer des données sur un support externe sans accord de sa hiérarchie. Il doit aussi respecter les règles de sécurité définies par le service informatique.

6. NOMMER UN DPO

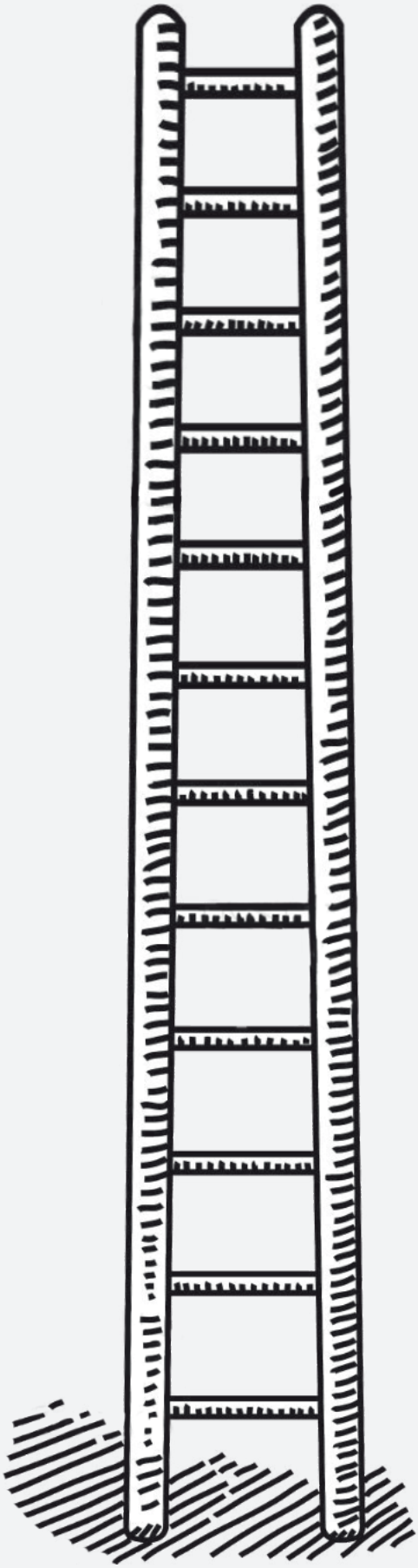
Le DPO, le délégué à la protection des données, est le « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. La désignation d'un délégué est obligatoire pour les autorités ou les organismes publics, les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

7. SE PRÉPARER À LA FUITE DES DONNÉES

En cas de fuite des données, il devient obligatoire de notifier la CNIL si possible dans les 72 heures après en avoir pris connaissance. Les personnes concernées doivent également être averties quand la fuite présente un risque élevé pour leurs droits et libertés (vol de mots de passe ou de numéros de cartes bancaires). En amont, une procédure de management des risques doit être mise en place pour détecter, signaler et investiguer en cas de violation des données que vous traitez.

« Un programme GDPR est avant tout une démarche opérationnelle de mise en conformité dans laquelle les outils sont des accélérateurs et ont la capacité d'industrialiser les activités. Cette démarche s'organise autour de chantiers métiers de conformité juridique se traduisant par une conformité du SI » détaille Thierry Brun, GDPR Ambassador chez IBM.

LES ÉTAPES DE MISE EN CONFORMITÉ CNIL



01

DÉSIGNER UN PILOTE

Délégué à la protection des données avec pour missions d'informer, conseiller et contrôler

02

CARTOGRAPHIER

Recenser de manière précise tous les traitements relatifs aux données personnelles, tenir le registre des traitements et réaliser un GAP analysis

03

PRIORISER

Identifier les actions à mener et les prioriser par rapport aux risques encourus

04

GÉRER LES RISQUES

Mener une analyse d'impact sur la protection des données (PIA) concernées par des traitements à risques élevés

05

ORGANISER LES PROCESSUS INTERNES

Mettre en place l'organisation nécessaire à la prise en compte de la protection des données

06

DOCUMENTER

ÉXECUTION DU PLAN DE MISE EN CONFORMITÉ

© Umanis 2018

QUI FAIT QUOI ?

Direction Générale et de l'Organisation

- Met en place une organisation intégrant les Responsables fonctionnels de Traitement et le DPO
- Valide des procédures de Gouvernance (procédure en cas de violation, demandes de personnes physiques, processus associés au Privacy By Design ou Privacy By Default)
- Avertit l'autorité de contrôle sous 72h en cas de violation et les personnes physiques concernées sous 1 mois

Service juridique

- Révise les contrats et les mentions légales
- Aménage de nouvelles mentions dans les contrats
- Organise une gestion contractuelle des relations avec les « sous-traitants » et « co-responsables » (centres de services, call centers, etc.)

DPO

DSI (>70 % des actions de mise en conformité)

- Met en place des actions d'évolution du SI et d'optimisation de la connaissance sur les DCP et traitements associés (cartographie détaillée des données structurées et non structurées)
- Elabore des outils : anonymisation et pseudonymisation, gestion des droits des personnes physiques et tenues de la base des consentements, prévention des brèches, etc...
- Organise l'évolution des processus, notamment lors de la conception en appliquant le principe du Privacy By Design

RSSI

- Aménage le PSSI et met en place les outils de protection adaptés à la protection des DCP
- Met en œuvre les actions associées à la Sécurité (informatique, intellectuelle et physique)

PME, DAVANTAGE PÉNALISÉES ?

Gare à l'argument des PME en danger à cause de l'application du GDPR ! Au contraire, plus il existe de services, de filiales, de départements, plus le travail de sensibilisation des acteurs, et de vérification sera lourd. Moins l'entreprise est de taille importante, plus elle gagne en flexibilité pour réaliser les changements GDPR. Exception faite des PME qui manipulent un grand nombre de DCP. Plus leur nombre est élevé, plus l'effort sera important.

© Umanis 2018

GDPR ; Y-A-T-IL UN PILOTE DANS L'AVION ?

Dès mai 2018, nombre d'entreprises devront se doter d'un DPO (Data Protection Officer), délégué à la protection des données en français. Zoom sur son profil, ses responsabilités et son champ d'action.

Qu'il s'agisse par exemple du projet de lancement d'un objet connecté qui exploite les comportements ou la localisation, d'un outil de gestion de la relation client (CRM) ou encore d'une campagne e-marketing utilisant des outils de profilage, ... le DPO s'associe à l'ensemble des stratégies de développement.

« Le DPO est garant de la confiance que doivent pouvoir avoir les clients, les salariés, dans l'intégrité et la sécurisation des données qu'ils confient à l'entreprise. Personne clé au cœur de la stratégie digitale de l'entreprise, il est un tiers de confiance, tout comme les Commissaires Aux Comptes le sont pour les données comptables et financières des organisations. »
Denis Genest, Associé Segeco.

Coordinateur, le DPO dispose de multiples missions : informer le responsable de traitement ou le sous-traitant, ainsi que leurs employés, contrôler le respect du règlement, conseiller l'organisme sur la réalisation d'une analyse d'impact, vérifier l'exécution et coopérer avec l'autorité de contrôle. Le poste de délégué est à la frontière du droit avec les aspects IT, le marketing, en incluant les relations client, business, CRM.

« Il s'agit de sortir de sa zone de confort et de prendre contact avec les opérationnels. Être à la fois didactique et accessible pour faire comprendre les enjeux et inciter ses collaborateurs à se tourner vers le DPO dès que des données personnelles sont en jeu. S'il n'est pas assez visible et reconnu au sein de l'entreprise, le DPO ne dispose pas suffisamment de marge de manœuvre » explique Charley Dupré de Volkswagen.
« Le DPO est à considérer comme le "commissaire aux comptes" du GDPR. Il a le même rôle et positionnement que le CAC que nous connaissons bien pour informer, conseiller, vérifier, auditer les éléments comptables d'une entreprise. » ajoute Denis Skalski, Directeur Conseil chez Umanis.

L'opérateur a opté pour une désignation en interne, un choix qui revient à l'entreprise qui pourra aussi bien nommer un DPO externe.
« Dans notre cas, le DPO est rattaché à la compliance, c'est une juriste de formation. » explique Stéphane Tournadre, Directeur Sécurité et Audit SI des laboratoires Servier.

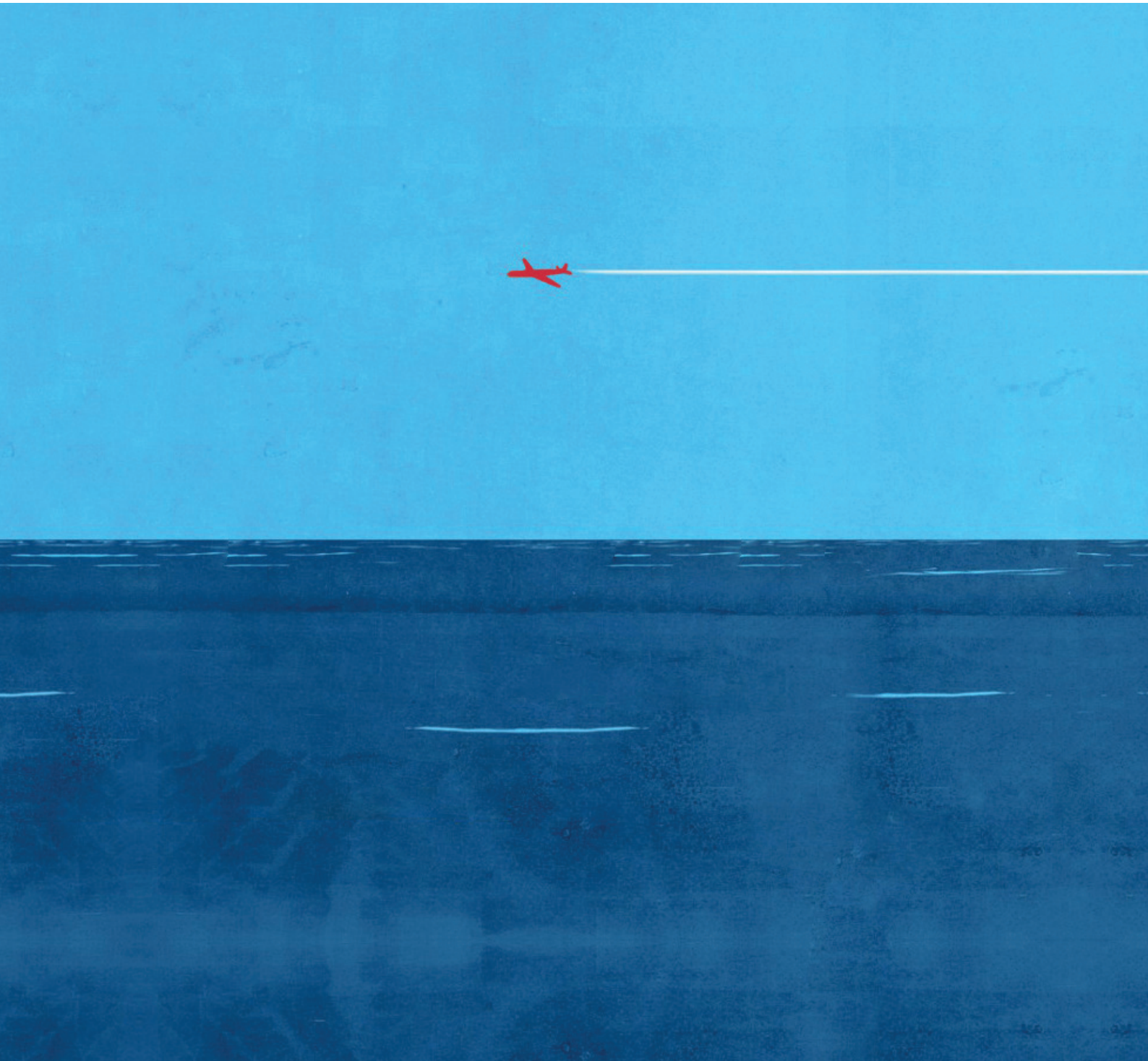
POUR QUI LE DPO EST-IL OBLIGATOIRE ?

- **Les entreprises dont les activités de base les amènent à réaliser des traitements de suivi régulier et systématique des personnes à grande échelle,**
- **Les entreprises dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions,**
- **Les autorités ou les organismes publics.**

© Umanis 2018

Le DPO traduit dans le GDPR le chapitre sur l'accountability qui va définir la façon dont l'entreprise répondra aux exigences réglementaires.
« Nous avions un CIL et deux juristes. Désormais, un DPO, deux juristes et un ingénieur sécurité contrôlent la mise en œuvre effective des bonnes pratiques » précise Stéphane Tournadre.

C'est un nouveau métier qui voit le jour avec la création de plusieurs milliers de postes de DPO.
Leurs responsabilités ? Piloter les travaux de mise en conformité, réaliser des audits internes, fédérer les Responsables de Traitement mais aussi appliquer les procédures de mises en place entre l'entreprise et la CNIL en cas de violation.



DPO, QUELLES COMPÉTENCES POUR LE PILOTE DU GDPR ?

01
MAÎTRISE
le cadre juridique

02
CONNAÎT L'ACTIVITÉ
organisation, systèmes d'information, sécurité, rôle des données et leur valorisation dans l'activité de l'entreprise

03
AGIT EN TOUTE INDÉPENDANCE
sans conflit d'intérêt

04
COMMUNIQUE
au niveau le plus élevé de l'organisme

05
CONTRÔLE
le respect du règlement et la législation nationale en matière de protection des données

06
COOPÈRE
avec l'autorité de contrôle, la CNIL

© Umanis 2018

SÉCURITÉ DES DONNÉES, TOUS RESPONSABLES !

Avec le GDPR, l'heure de la responsabilisation a sonné ! Face au développement de l'externalisation de services entiers et du cloud, le règlement européen partage la responsabilité entre le Responsable de Traitement, dit contrôleur, et ses sous-traitants, les processeurs. Reste à définir clairement les limites de cette double co-responsabilité.

« L'apport de ce règlement est que le Data Processeur devient totalement exposé à ses manquements en cas de défaut. Ce n'est plus uniquement la responsabilité du Responsable de Traitement » avertit Jean-Philippe Gaulier de Orange.

Luc Alloin, Associé Segeco, Directeur Général de SecuryMind ajoute que ***« la sécurité des données, dont est responsable chaque responsable de traitement, devra être construite avec les services internes, mais également avec ses sous-traitants. Plus que jamais elle devra être outillée, auditée et sa robustesse régulièrement testée. »***

En effet, la sécurité des données personnelles devra être assurée par le Responsable de Traitement mais aussi par le sous-traitant. Leur objectif commun est ainsi d'assurer la confidentialité, l'intégrité, la disponibilité et surtout la notion nouvelle de ***« résilience des systèmes et des services de traitement des données ».***

Les exigences du nouveau règlement ont une influence directe sur les futurs contrats conclus avec les prestataires. Jusqu'ici les sous-traitants avaient une responsabilité contractuelle vis-à-vis du Responsable du Traitement sous réserve d'un contrat écrit entre les deux parties.

À partir du 25 mai 2018, même en l'absence d'un contrat signé, les sous-traitants seront désormais partiellement responsables des traitements de données qu'ils mettent en œuvre pour le compte d'une entreprise tierce. Ils pourront donc être audités voire sanctionnés en cas de non-respect du GDPR.

« Sur l'aspect de co-responsabilité, l'un des risques est que dans la mesure où chacun est responsable, il peut y avoir la tentation de ne pas définir cette responsabilité et que chacun pense que c'est de la responsabilité de l'autre. Ce risque doit être cadré. » fait remarquer Charley Dupré de Volkswagen.

Par ailleurs, le GDPR impose des obligations plus strictes aux responsables de données.
Ils devront conserver des registres de toutes les activités de traitement effectuées sous leur responsabilité, y compris toutes les informations susceptibles de démontrer leur conformité.

Globalement, ce dispositif permettra de traiter plus efficacement la circulation de données complexes faisant intervenir différents acteurs, avec plusieurs niveaux de prestation. Le tout, en renforçant les relations contrôleur-processeur pour un meilleur encadrement des données collectées.

© Umanis 2018

QUELLES SONT LES NOUVELLES OBLIGATIONS DES SOUS-TRAITANTS ?

- ☑ Tenir un registre des traitements
- ☑ En cas de violation de sécurité, mettre en œuvre les procédures et mesures de sécurité
- ☑ Contester les instructions du Responsable de Traitement si elles sont contraires à la loi
- ☑ Assister le Responsable de Traitement en cas de demande d'accès, d'effacement, de portabilité, etc…

GDPR ; QUELS IMPACTS SUR L'IOT & LE BIG DATA ?

L'ensemble des objets connectés se trouve véritablement exposé aux piratages et sa multiplication laisse donc craindre une réelle explosion des cybermenaces. Ceci est d'autant plus vrai que les hackers devraient y avoir un intérêt avec la possibilité de voler des données de plus en plus confidentielles.

« Avec le GDPR, nous devenons maîtres du calendrier. Il y aura moins de travail administratif et en plus cette procédure sera valable sur l'ensemble des pays de l'UE. Il s'agit d'un gain de temps par exemple dans le domaine de la santé connectée » explique Stéphane Tournadre des Laboratoires Servier.

Avec l'avènement de l'Internet des objets (IoT), d'importants volumes de données sur les préférences et les comportements clients sont générés. Le risque sur la confidentialité s'accentue et la nouvelle réglementation vient lutter contre ce phénomène.

De l'autre côté de l'Atlantique, le fabricant de télévisions Vizio s'est récemment vu infliger une amende de 2,2 millions de dollars par l'autorité américaine de protection des consommateurs.
La raison ? Avoir espionné ses clients pendant plus de deux ans sans leur consentement. Une surveillance qui avait pour but de partager ces données avec des sociétés de marketing tierces.

LG et Samsung ont également été accusés d'espionner leurs utilisateurs en 2013 et 2015. D'ailleurs, dans sa charte de confidentialité, Samsung prévient désormais ses clients : ***« Sachez que si vos paroles contiennent des informations personnelles ou sensibles, elles seront incluses dans les données capturées et transmises à une partie tierce ».***

Si l'amende infligée paraît significative ; dans l'hypothèse où Vizio vendrait ses téléviseurs en Europe d'ici l'entrée en vigueur du GDPR en mai 2018, l'entreprise s'exposerait cette fois à une amende supérieure à 292 millions de dollars !

Tout comme les télévisions, les voitures connectées, ayant une adresse IP, font partie de l'Internet des objets. L'accès à un numéro de carte bleue et à l'identité des conducteurs après un achat est possible en collectant les données d'une voiture connectée. On peut ainsi en déduire où la personne concernée vit, travaille, et sa façon de conduire.

« Dans le secteur de l'automobile, les véhicules connectés et autonomes vont être une problématique phare que ce soit en termes de sécurité ou de données personnelles. Avec les pénalités qu'il peut y avoir, le sujet rentrera en ligne de compte et ne sera plus secondaire. En ce qui concerne l'autopartage, si à terme des véhicules autonomes sont en location, il y aura aussi des problématiques en ce qui concerne la géolocalisation et les données personnelles. » conclut Charley Dupré de Volkswagen.

Bien que l'objet connecté soit considéré comme un produit dès qu'il est explicitement associé à son utilisateur ; il devient émetteur et porteur de données personnelles.

© Umanis 2018

BIG DATA, MACHINE ARRIÈRE TOUTE !

Tout traitement des données personnelles doit être en phase avec les raisons pour lesquelles elles ont été collectées et cela va à l'encontre du fondement même des projets de deep learning ou de big data au sens large, où il s'agit de collecter et de stocker un maximum de données (maximisation de la collecte par défaut). Les données ont été agrégées en volume dans des datalakes sans intégrer les contraintes règlementaires.
La question est aujourd'hui de s'assurer de l'auditabilité des processus sans avoir à les repenser.

Certes, le GDPR contraint la collecte, les usages et l'exploitation des données personnelles par les entreprises mais n'oublions pas, que 90% des données actuelles ont été produites ces deux dernières années. Nous n'en sommes qu'au début du phénomène sous l'effet de l'IoT et de l'intelligence artificielle.

Le GDPR est finalement une formidable occasion pour accélérer la transformation digitale des entreprises car on sait aujourd'hui que le succès est dans la collecte, l'exploitation et la transformation intelligente de la data.

Il est en effet nécessaire de connaître les données dont on dispose (et leur qualité) pour vous lancer dans le Big Data dont les nouveaux usages concernent pour beaucoup l'analyse prédictive et prescriptive sur de très grands volumes.

Par ailleurs, la nouvelle génération d'outils de Data Preparation, Data Discovery, Dataviz et Data Science vous ouvre ce nouveau champ des possibles.

« Les demandes d'archivage sont mises en exergue par le GDPR. Pour l'instant, la réaction habituelle est de tout garder, ce qui représente un risque. Certaines données ont vocation à être supprimées à l'issue d'un certain temps. » explique Denis Skalski, Directeur Conseil chez Umanis.

© Umanis 2018


12
3

GOUVERNANCE DES DONNÉES ; LA RÉPONSE AU PRINCIPE D'ACCOUNTABILITY

Mai 2018 annonce une logique de responsabilisation qui prend le pas sur la logique déclarative qui prévalait jusqu'à présent.

L'accountability n'est pas une révolution. Depuis la loi informatique et liberté de 1978, les organisations ont l'obligation de se conformer au principe de protection des données. Quelle est la nouveauté du règlement ? l'obligation de rapporter la preuve de la conformité, de la documenter à des fins de démonstration.

L'entreprise pourra être sanctionnée sur ce seul manquement en cas de fuite de données ou non. Cela nécessite une analyse au cas par cas des traitements selon la nature de la portée, du contexte et de la finalité du traitement. Le tout, au regard des risques pour les droits et libertés des personnes. Avec l'accountability, nous devenons *« "adultes" et responsables. Il nous revient de faire nous-mêmes ces contrôles »* tranche Stéphane Tournadre des laboratoires Servier. Il s'agit d'adapter les mesures selon les besoins : pseudonymisation, cryptage des DCP, confidentialité, disponibilité, accès, procédures de test pour évaluer l'efficacité des mesures.

PREMIER PAS : LE REGISTE DE TRAITEMENT

« Le registre sera l'outil de démonstration de la conformité et le tableau de bord du DPO à échéance mai 2018. Pour répondre à cette obligation, nous répertorions 4 exigences fonctionnelles proches du registre : l'analyse de risques (PIA), la formalisation du plan d'actions et le suivi de la conformité, la documentation de la conformité, la gestion des demandes de droits des personnes. C'est ainsi que la notion de "registre étendu" incluant ces 4 fonctions en sus du registre, apparaît sur le marché. » explique Thierry Brun, GDPR Ambassador chez IBM.

En parallèle de la mise en place du registre de traitements, plusieurs actions doivent voir le jour notamment un inventaire des traitements, une répartition des rôles et des responsabilités ainsi que la sensibilisation des équipes et du DPO au principe d'accountability.

© Umanis 2018

PSEUDONYMISATION & ANONYMISATION ; EN ROUTE VERS LE ZÉRO RISQUE !

La pseudonymisation des données au-delà d'améliorer la sécurité, permet leur utilisation de manière plus libre. L'occasion de collecter sans prendre de risque auprès des personnes concernées. Mais alors, quelles données rendre anonymes ?

Lorsque les données à caractère personnel sont effectivement anonymisées, il ne s'agit alors plus de données dites personnelles. Résultat, elles ne sont pas assujetties au règlement sur la protection des données et leur utilisation devient plus souple. La question qui en découle est quelles techniques utiliser pour sécuriser correctement ?

« Il va s'agir de mettre en œuvre, une organisation, des outillages et des processus internes nous permettant de mieux maîtriser nos données à caractère personnel. Il s'agira de déterminer quels moyens techniques utiliser pour anonymiser telle ou telle donnée par exemple. » **ajoute Benoit Després d'IBP.**

Il existe actuellement deux techniques d'anonymisation. La randomisation consiste soit à modifier les données afin d'éliminer les liens qui pourraient être établis entre celles-ci et l'individu, soit de permuter les données entre les individus afin de rendre le lien entre les deux moins susceptibles d'être réalisé.

La seconde technique, la généralisation, réduit les données pour inclure des informations qui ne sont pas aussi précises, ce qui limite le risque d'identification d'un individu.
Quant à la pseudonymisation, cette technique remplace toutes les caractéristiques d'identification des données par un pseudonyme ou, en d'autres termes, une valeur qui n'autorise pas la personne concernée à être identifiée directement. Considérée comme une mesure réduisant la liaison dans un ensemble de données, la pseudonymisation est la méthode préconisée dans le règlement GDPR.

Le groupe Orange dispose déjà d'une usine d'anonymisation en interne. ***« Le principe est simple : il s'agit de prendre un jeu de données hors production (jeux de test, dev, BI), le passer dans l'usine en lui appliquant des règles mathématiques qui permettent la perte de l'identification et utiliser le jeu qui en ressort. Même si ce jeu venait à être publié aucun recoupement ne pourra être fait. La clé d'anonymisation peut être conservée on parle alors de pseudonymisation. »*** assure Jean-Philippe Gaulier du groupe Orange.

« À quel endroit et par qui est créée la donnée, comment est-elle supprimée ou rendue anonyme ? Une bonne structuration du SI implique que ces opérations ne soient effectuées qu'une fois, en un point et sous la responsabilité d'un rôle utilisateur unique. »

Arnaud Escoffier, Manager de la Gouvernance de la Donnée chez Umanis.

© Umanis 2018

Cette technique de pseudonymisation est déjà appliquée dans le monde bancaire et notamment pour les moyens de paiement (règlementation PCIS) pour sécuriser les numéros de cartes bancaires.

À noter que la mise en place d'un système d'anonymisation requière des efforts de conception et une concertation efficace avec les opérationnels. Il revient à chaque entreprise de définir au cas par cas quelles données sécuriser, et quelles méthodes et outils choisir.

« C'est une forme d'investissement très rentable pour les entreprises. Elles auront à l'esprit qu'en anonymisant suffisamment les données appropriées, elles pourront garder une pertinence en terme d'analyse d'information, tout en diminuant le risque de fuite de données à quasiment zéro » soutient Charley Dupré de Volkswagen.

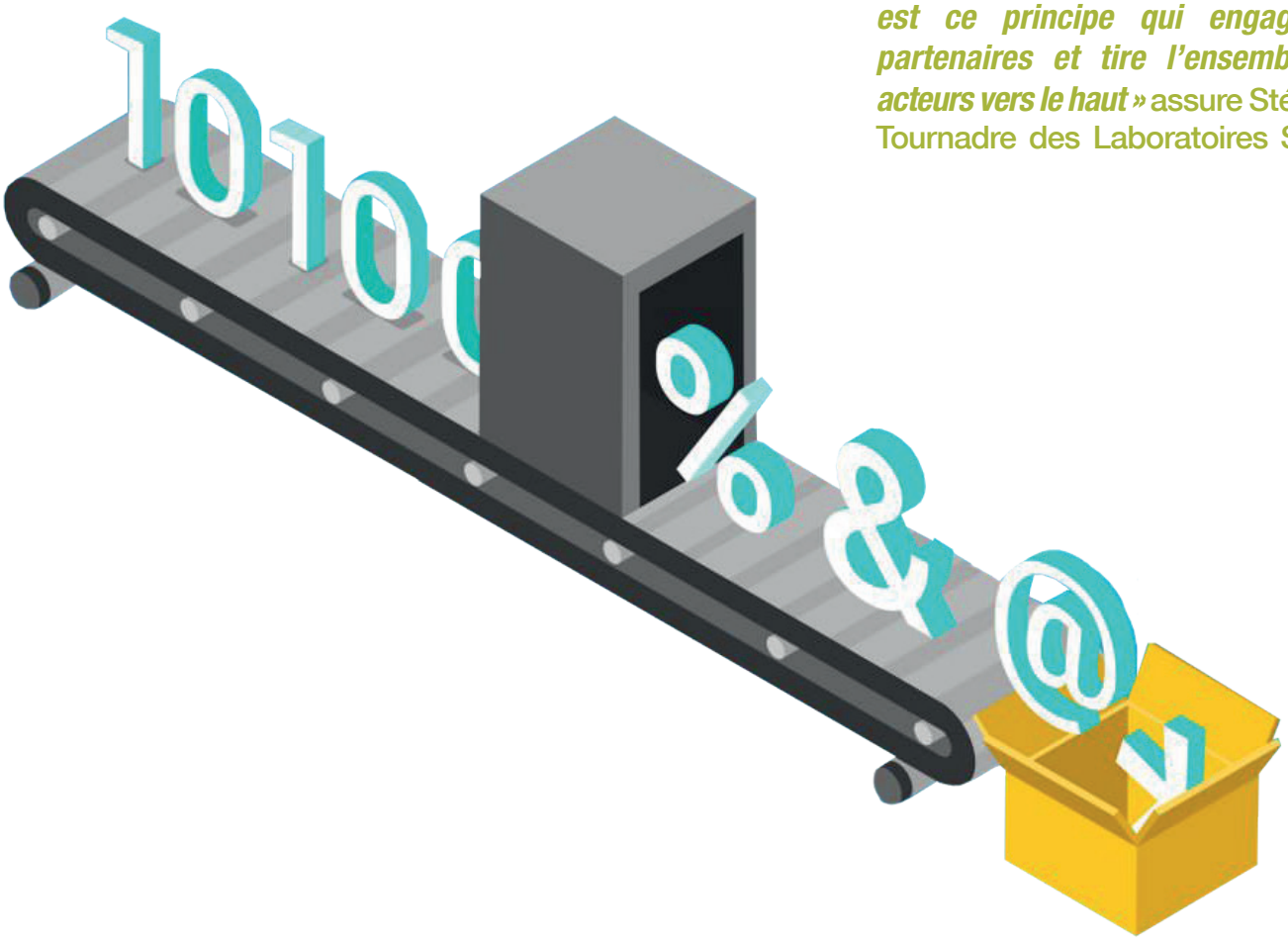
VALORISER SES DONNÉES C'EST TRANSFORMER SA CONFORMITÉ EN OPPORTUNITÉ !

Le GDPR, avec sa logique de transparence et de responsabilité a une incidence majeure sur les activités de l'entreprise, sur sa culture et sur les échanges qu'elle entretient avec ses clients, fournisseurs ou partenaires. À long terme, la réglementation permettra de développer un avantage concurrentiel pérenne et éthique.

L'utilisation de données collectées par les entreprises est directement liée à la relation de confiance entretenue entre l'entreprise et ses clients. Si le règlement européen sur la protection des données définit les responsabilités des entreprises, il s'agit avant tout d'une question de confiance qui s'instaure entre le client et l'entreprise.

Il y a fort à parier qu'en faisant l'effort de repenser la façon de gérer les données, la connaissance client, tant recherchée par les entreprises aujourd'hui, s'en trouvera dès lors améliorée.

« Le système se sécurise davantage. Précédemment, si notre sous-traitant perdait les données, nous restions responsables. La force du règlement est ce principe qui engage nos partenaires et tire l'ensemble des acteurs vers le haut » assure Stéphane Tournadre des Laboratoires Servier.



© Umanis 2018

Une relation gagnant/gagnant entre ceux qui produisent les données, les entreprises qui les exploitent et leurs clients qui en sont à la fois la source et la cible se concrétise.
« Dans notre secteur d'activité, la protection des données personnelles est un impératif fort. C'est propre à notre ADN. Avec cette nouvelle règlementation, nous sommes dans la continuité. Ce n'est pas une révolution mais une évolution. » explique Benoit Després, Directeur de la Maîtrise d'Ouvrage Finances et Risques chez Informatique Banque Populaire (IBP). ***« Le secret bancaire est d'ailleurs bien plus contraignant sur certains aspects et depuis longtemps »*** précise ce dernier.

« Dans le secteur de la santé, la protection des données personnelles fait depuis longtemps l'objet d'une vigilance particulière. La capacité à garantir aux patients que les informations contenues dans leurs dossiers sont inaccessibles, sauf à ses traitants, donnera un avantage décisif. C'est la clé de voute du développement de la e-santé » Pascal Woitier, Associé Crysal Protection Sociale.

Si on se place du point de vue du consommateur, les avantages sont concrets avec un gain de confiance considérable notamment par rapport aux scandales de fuite de données de ces dernières années. C'est plus engageant de savoir de manière transparente l'usage qui va être fait des données et l'éventuelle conservation par des tiers.

« Il s'agit aussi pour les entreprises de structurer leurs données afin d'éviter une collecte trop boulimique, de se forcer à poser la question au préalable sur la pertinence des données. Cette réforme sera bénéfique à la fois pour les entreprises et pour les particuliers. » conclut Charley Dupré de Volkswagen.

© Umanis 2018

GDPR, MATURITÉ DES ENTREPRISES EN FRANCE

Règlement général sur la protection des données

LES ENTREPRISES SONT LOIN D'ÊTRE PRÊTES

67% sont encore en veille technologique

1/2 ignore les problématiques induites par la mise en conformité

1/3 n'a aucune idée des impacts du GDPR au niveau IT

1/4 est à la recherche d'une démarche outillée

UN RÉVEIL TARDIF

0% des entreprises interrogées pense que le GDPR n'aura pas d'impact au niveau technologique et considère que ce n'est pas un sujet prioritaire

36% des entreprises pensent que l'impact IT va être considérable car elles sont loin de pouvoir répondre aux exigences à venir

1/3 a anticipé certains chantiers et pense subir un impact modéré au niveau IT

ÉTAT D'AVANCEMENT DES ENTREPRISES À DATE

1. Étude en cours par la DSI/RSSI
2. Prise en main par le juridique
3. Sensibilisation de l'organisation

77% pensent qu'il faut aborder le sujet du GDPR et de la sécurité des données dès aujourd'hui

23% ont désigné une entité de pilotage dédiée

70% n'ont pas nommé de DPO

PLAN ORSEC TOP 5 CHANTIERS PRIORITAIRES

1. Sécurisation des données et des traitements
2. Mise en place du "Privacy by design" et gestion du droit à l'oubli
3. Priorisation des actions à mener pour être en conformité
4. Maîtrise des risques (cyberattaques, vol de données, etc)
5. Cartographie des traitements de données personnelles

LES CHANTIERS LES MOINS SENSIBLES À COURT TERME

1. Définition d'un référentiel de données à caractère personnel et mise en place d'une gouvernance
2. évaluation des écarts entre l'existant et la réglementation à venir
3. Analyse des risques

Seuls **7%** des entreprises considèrent que la désignation d'un pilote GDPR (CIL, DPO) est une priorité

77% des répondants perçoivent le GDPR comme une formidable opportunité pour créer de la valeur à partir de leurs données

MAI 2018, COMPLIANT READY ?

31% Conforme à temps

46% Aucune idée

23% Impossible

2/3 des entreprises ne seront, à priori pas prête à horizon 2018

*78 répondants / 5 à 7 « GDPR compliant ? Impacts à court terme au niveau IT » / 27 avril 2017

Umanis BEYOND DATA

À moins d'un an de l'entrée en vigueur, les entreprises ont pris conscience que cela va au-delà des simples aspects juridiques et organisationnels car les données personnelles sont un actif stratégique précieux … mais particulièrement vulnérable. La donnée et son exploitation sont en effet au cœur de la transformation digitale des entreprises aujourd'hui.

À date, aucun outil ou solution IT ne sort du lot. Les entreprises n'en sont pas encore à ce stade de leur réflexion. Seul IBM ressort avec… 5% des répondants ! Il faut préciser que c'est le seul éditeur qui propose un catalogue d'outils qui couvre tous les chantiers IT impactés.

LES ENTREPRISES FRANÇAISES COMMENCENT JUSTE À APPRÉHENDER L'ÉTENDUE DES DÉFIS TECHNOLOGIQUES À RELEVER POUR CONTINUER À FAIRE DU BUSINESS AUTOUR DE LA DONNÉE TOUT EN PRÉSERVANT LA CONFIANCE, ESSENTIELLE DANS CETTE NOUVELLE ÉCONOMIE NUMÉRIQUE.

UMANIS, NOTRE OFFRE GDPR

Le GDPR, c'est un ensemble de chantiers transverses qui impactent votre organisation, les processus métiers, la sécurité et bien entendu vos applications et vos systèmes IT. Par où commencer ? Comment parer à l'urgence et répondre rapidement et l'essentiel ? Quelle trajectoire adopter pour être en conformité ? Quelle gouvernance des données ? Quel référentiel pour les données sensibles à caractère personnel ? Quelle démarche outillée et quelle solution technologique choisir ? Umanis, c'est une approche globale « Data Centric » allant du conseil à la mise en œuvre en passant par la cartographie des processus de l'entreprise, la maîtrise du cycle de vie des données, la mise en place d'une méthode "multi-dimensionnelle" ou encore l'utilisation d'accélérateurs techniques pour s'assurer du « Privacy by Design ».

Notre offre intègre l'ensemble des axes fondamentaux du GDPR : licéité, droits des personnes, sécurité, sensibilisation, accountability, gestion des risques, gestion des sous-traitants et Privacy by Design. Ces axes sont supports de l'analyse des traitements sur les plan business, IT, juridique et organisationnel.

1. Lancement

L'objectif est de sensibiliser et de sécuriser. À l'issue du lancement, un planning est dressé et une étude organisée. En parallèle, la formation et la communication sont mises en place et une segmentation des traitements développée.

2. Audit & Inventaire

Où sont les urgences et les foyers potentiel d'incendie ? Nécessairement, vous devez faire un état de maturité GDPR. Ensuite, la cartographie des processus et traitements est dressée, une étude de risque (PIA) et un design du plan d'actions outillés. Autant d'opérations menant au développement et à l'industrialisation.

3. Analyse & Consolidation

Il s'agit de rendre conforme le traitement en suivant le plan de mise en conformité développé par une liste des traitements sensibles assujettis EIVP, une étude d'impacts techniques, la mise en œuvre de la plateforme de GDPR & Data Management, et celle de solutions connexes (Digital, Quality…). L'analyse vise également à identifier les projets nécessitant le Privacy By Design.

4. Restitution

Un rapport d'étonnement intégrant le cahier de préconisations conclut nos opérations. Il s'agit ensuite de maintenir en condition permanente de conformité notamment par l'assistance, le coaching et la gestion de vie GDPR.

© Umanis 2018

NOS OUTILS

- Case Management (enrichissement) dont base documentaire
- Meta-data Management (data lineage)
- Master Data Management (maîtrise des données et nouveaux services / GDPR)
- Outils de chiffrement, pseudonymisation
- Outils de sécurité dont tracking des malveillances
- Outils de gestion des data (extractions, mise en quarantaine, suppressions, contrôles…)
- Cartographie données structurées et non structurées : Stored IQ + Iserver

À PROPOS D'UMANIS

Créé en 1990, Umanis est le leader français en data, digital et solutions métiers packagées. 2 700 passionnés de nouvelles technologies sont à votre service chez vous, dans nos agences ou depuis nos centres de services onshore et nearshore. Umanis accompagne ses clients sur la globalité de leurs projets informatiques (conseil, développement, intégration et infogérance) dans des domaines d'expérience qui font la différence par l'engagement, l'industrialisation et l'innovation. Reconnu pour son expertise technique comme fonctionnelle, Umanis est partenaire stratégique des plus grands éditeurs de logiciels du marché.

© Umanis 2018

MISE EN CONFORMITÉ ET SÉCURISATION DE LA RELATION CLIENTS ET SALARIÉS ?

Segeco vous éclaire

La prise en compte du règlement européen en 2018 va nécessiter des entreprises un effort certain afin de satisfaire les différentes exigences tout en profitant au mieux des opportunités historiques de développement dans l'exploitation des données.

Pour vous accompagner dans votre démarche de mise en conformité, Segeco, fort de ses métiers et de ses expertises sectorielles, vous propose un accompagnement de bout en bout et dans la durée. A titre illustratif, dans le domaine de la protection sociale et de l'assurance santé, nous nous appuyons sur les expertises métiers de Crysal, société de conseil du Groupe *SEGECO* dédiée au secteur de la protection sociale et disposant d'une expertise particulière dans la branche Santé. Le cabinet s'adresse aux acteurs des régimes complémentaires et obligatoires, ainsi qu'aux opérateurs de services gravitant dans cet écosystème (plateformes santé, concentrateurs techniques ou encore éditeurs). Nos consultants interviennent depuis la réflexion stratégique jusqu'aux transformations opérationnelles.

Le Groupe Segeco est né il y a plus de 40 ans en Auvergne dans l'exercice du métier d'Experts Comptables et de Commissaires aux Comptes. Issu de cette tradition de tiers de confiance sur la sincérité et l'intégrité des données financières, nous avons étoffé nos compétences pour répondre toujours mieux aux besoins de nos clients, jusqu'à couvrir tous les aspects de la maîtrise des risques, de la performance de l'entreprise et de la sécurisation des relations avec les tiers.

Notre double culture de tiers de confiance basée sur le respect de normes professionnelles strictes et d'entreprise de croissance régionale, ETI au service des ETI, nous a permis de développer des services d'expertise de proximité en Audit, Comptabilité, Droit, Conseil en organisation, Rapprochement d'Entreprises et Scurisation du patrimoine de données de nos clients PME, ETI et Grands Comptes.

La garantie de la sincérité et de l'intégrité des données est au cœur de tous nos métiers.
Nous le faisons en appliquant des méthodologies robustes adaptées au secteur d'activité de nos clients.

© Umanis 2018

SECURYMIND, filiale 100% du groupe *SEGECO*, diagnostique chaque problème de sûreté dans sa singularité : sûreté physique, sécurité informatique, ingénierie sociale, formations. Le cabinet accompagne les clients exigeants, privés et publics, dans la compréhension et la réduction de leur risque de sûreté.

Spécialisé dans la protection de l'information et des données en particulier en cybersécurité, le cabinet les questionne davantage et de façon fondamentale, sur la valeur des données traitées, les rapports des différents niveaux de responsabilités et sur la formalisation par les Directions Générales d'une véritable stratégie du digital au sein même de ses modèles de création de valeur.

Compte tenu des métiers du Groupe, des expertises des Femmes et des Hommes qui le composent, Segeco vous accompagne pour créer de la confiance et définir avec vous les stratégies adaptées d'organisation, de protection et de valorisation de vos données, dans le cadre nécessaire de la mise en conformité au Règlement européen et de développement de votre patrimoine digital.

© Umanis 2018

TECHNOLOGIES ?
IBM ; outiller votre démarche complète

Du point de vue de la mise en œuvre du GDPR, l'application de la réglementation se traduit, selon IBM éditeur de solutions, par cinq domaines de transformation : le principe d'« Accountability », le droit des citoyens, la gestion du consentement, la sécurité des données personnelles et celui de « Privacy by Design ».

Pour chacun de ces domaines nous avons identifié des fonctions essentielles dans la phase d'état des lieux (analyse d'écart) tout comme dans la phase de trajectoire de mise en conformité. Chacune de ses fonctions pourra ensuite être appuyée ou accélérée par la mise en œuvre d'une solution technologique.

PRIVACIL BY CASE MANAGER

Gouvernance, conduite du changement, processus

Inventaire de conformité - Registre de traitement & plan d'actions & PI - Conservation des données

STORED IQ & I. ANALYZER

Données personnelles : analyse des risques et processus de traitement

Cartographie des données personnelles	• Exploration données non structurées • Exploration données structurées
Cartographie des données & Effacement portabilité	• Anonymisation / Data Masking • Chiffrement des fichiers • Suppression / Mise en quarantaine • Restitution / Transfert / Rectification

GUARDIUM DP

Sécurité et Protection Opérationnelle

Sécurité Opérationnelle du Système d'Information - Protection opérationnelle des données - Contrôle activité des utilisateurs, habilitation - Gestion des incidents

Consentement

Gestion du consentement

Privacy by Design / Privacy by Default

Bases de données - Applications - Infrastructure / Mobiles

© Umanis 2018

NOS DIFFÉRENCIATEURS

- STDS (Short Term Design Solution) : méthode d'engagement rapide.
- La solution la plus complète, intégrée et augmentée des applications métiers notamment, partenaires.
- Une offre de services unique avec ses partenaires.
- Une souplesse contractuelle.

BÉNÉFICES CLIENTS

- Aligner l'organisation du projet de conformité SI GDPR avec tous les acteurs client.
- Maîtriser le temps de mise en œuvre (Intégration, technologie augmentée et verticaux métiers).
- Assurer la disponibilité des ressources technologiques sur le marché
- Contrôler les coûts sur la période de transformation du SI.de 153,3 M€.

© Umanis 2018

GDPR COMPLIANT

Le guide pratique

Cet ebook vous est offert par :

Umanis
BEYOND DATA

LEXING
ALAIN BENSOUSSAN AVOCATS

Segeco

IBM