OM Conseil
Donnez du sens à votre SI

Version 10042018

Kit GDPR pour les PME et les établissements publics

Préparez votre conformité au GDPR de manière concrète avec OM Conseil

Glossaire

DPD (Délégué à la Protection des Données) : Fonction au sein d'une organisation qui a la charge de veiller à la conformité réglementaire en matière de données de l'organisation. Le DPP a les mêmes fonctions que le Correspondant Informatique et Libertés (CIL), mais ses compétences juridiques sont plus poussées.

DPO (Data Protection Officer) : voir la définition du DPD.

PIA (Privacy Impact Assessment) : Préconisée par l'article 35 du règlement européen, l'analyse d'impact sur les données personnelles est un bon outil de responsabilisation pour les entreprises. Il permet à la fois de se conformer aux exigences du GDPR et de démontrer auprès des autorités de contrôle que des mesures appropriées ont été prises pour assurer la conformité.

CIL (Correspondant Informatique et Libertés) : fonction jusqu'alors située au coeur de la conformité Informatique et Libertés, le CIL veille à la sécurité juridique et informatique de son organisme. Le CIL a vocation à devenir le DPD dans le cadre du RGPD, applicable en mai 2018.

Contexte

Le nouveau Règlement européen sur la protection des données personnelles, communément appelé “**GDPR**”, “**RGPD**” ou encore règlement **(EU) 2016/679** du 27 avril 2016, se prépare en 6 étapes.

La réforme poursuit 3 objectifs :

1. **Renforcer les droits des personnes physiques**, notamment par la création d’un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
2. **Responsabiliser les acteurs traitant des données personnelles** (responsables de traitement et leurs sous-traitants) ;
3. **Crédibiliser la régulation grâce à une coopération renforcée entre les différentes autorités européennes de protection des données** (CNIL & consoeurs), qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux tout en faisant appliquer par les juges des sanctions renforcées.

Et ce n’est pas réservé qu’aux entreprises et organisations européennes mais à toute organisation qui traite des données personnelles de citoyens européens.

Définition d’une donnée à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Définition d'un Responsable de Traitement

Pour la CNIL : Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Pour nous, et concrètement sur le terrain, le Responsable de Traitement est la personne en charge d'un ou plusieurs processus de traitement de données à caractère personnel (chef de service, manager, directeur, etc.). C'est cette personne, généralement opérationnelle, ou proche des opérationnels, qui sera la mieux placée pour organiser la sécurité des données traitées. Cela n'enlève en rien la responsabilité juridique du représentant légal.

Définition d’un Sous-Traitant

Les sous-traitants sont les organismes qui traitent des données personnelles pour le compte d’un autre organisme, dans le cadre d’un service ou d’une prestation. Sont notamment concernés :

- Les prestataires de services informatiques (hébergement, maintenance, …)
- Les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique (ESN) ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données
- Les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients

Définition d’un traitement de donnée

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Les 6 étapes du plan d'actions de la CNIL

Etape 1 : **Désigner un pilote en charge de la gouvernance des données personnelles** de la structure. Le CIL, s'il est interne à la structure, peut assurer ce rôle.

Etape 2 : **Cartographier vos traitements de données personnelles**.

Etape 3 : **Prioriser les actions sur la base de la cartographie** réalisée à l'étape 2.

Etape 4 : **Gérer les risques en réalisant une étude d'impact (PIA)** pour chacun des risques détectés à l'étape 3. Un logiciel Open Source et gratuit est fourni par la CNIL.

Etape 5 : **Mettre en place des procédures organisationnelles et techniques qui garantissent la protection des données** à tout moment.

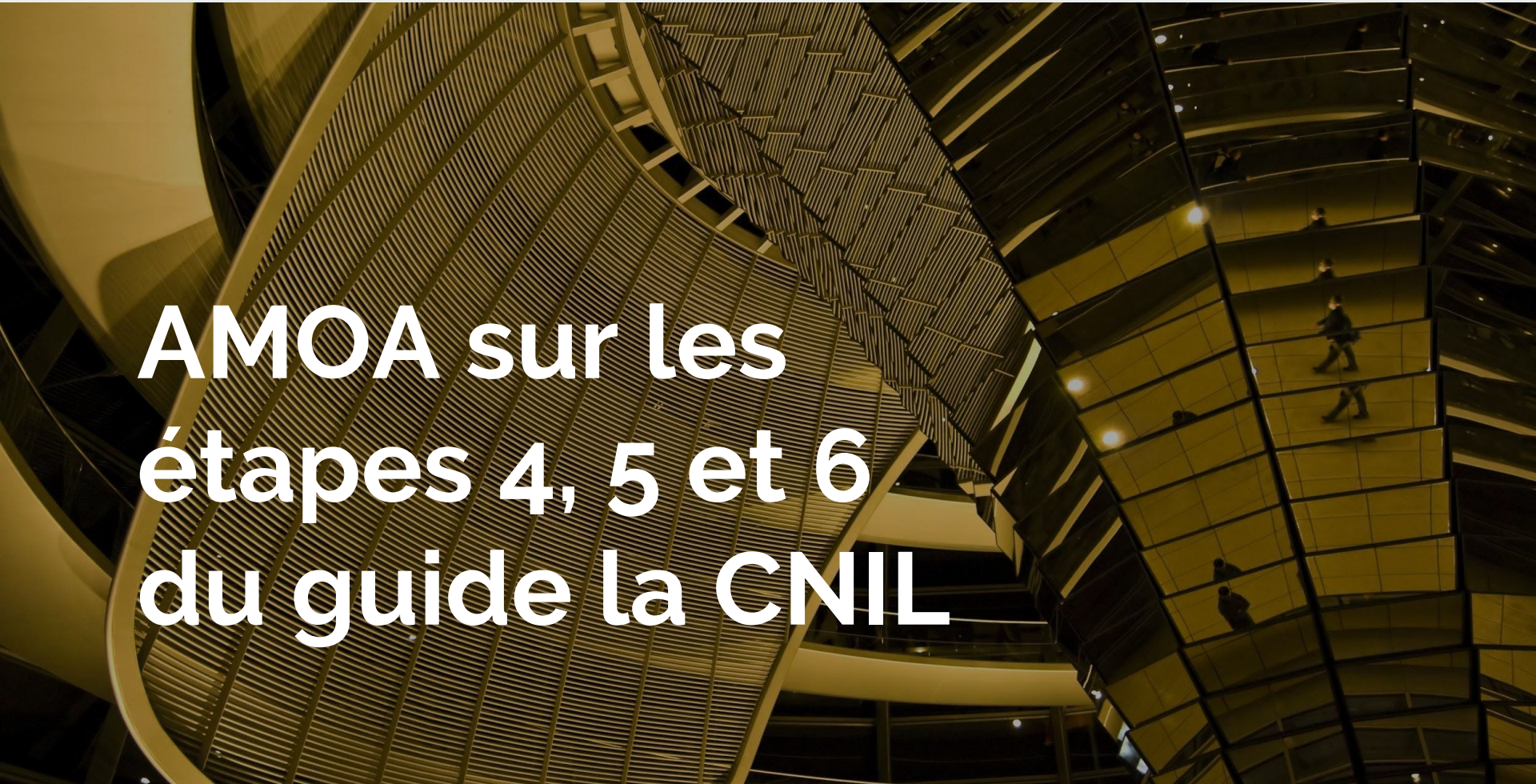
Etape 6 : **Finaliser la documentation de la conformité pour prouver la "bonne foi"** du propriétaire des traitements ainsi que l'engagement continu à appliquer la loi.

AMOA sur les étapes 2 et 3 du guide la CNIL

Le temps nécessaire pour l'assistance des équipes dans la cartographie des traitements de données à caractère personnel **est estimé à une demi-journée de réunion par service.**

Déroulement :

1. Réunion de lancement de deux heures avec l'ensemble des responsables des traitements.
2. Des échanges en face à face avec chacun des responsables de traitement.
3. Analyse des registres (tableaux de collecte préalablement remplis par les différents responsables de traitements).
4. Présentation des résultats par le Pilote aux cadres et à la Direction.
5. Réunion d'échange et brainstorming pour établir les actions à mener avec leur priorisation au regard des risques. Estimée à une voire deux demi-journées en fonction des disponibilités et du niveau d'engagement à co-développer des solutions par le collectif.



AMOA sur les étapes 4, 5 et 6 du guide la CNIL

Le temps nécessaire pour ces étapes est directement proportionnel à l'état de maturité de l'organisation et de son SI, par rapport à la sécurité à appliquer sur les traitements de données à caractère personnel.

Estimations de temps pour les missions d'AMOA des étapes 4, 5 et 6 :

Etape 4 - Gestion des risques avec étude d'impact sur la protection des données (PIA). Temps estimé à **1 jour pour 1 risque élevé sur 1 traitement de données**.

Etape 5 - Organisation des processus internes et du SI.

Etape 6 - Documentation de la conformité GDPR.

3 bénéfices d'une mise en conformité au GDPR

1. Le Privacy-by-Design améliore la sécurité globale des données de l'organisation
2. Le GDPR force à entrer dans une culture de la "data", qui prend alors sens et devient, plus encore qu'avant, un capital informationnel important
3. L'organisation des processus aide à mieux se structurer autours du cycle de vie de la data qui au final correspond souvent au cycle de vie du Client dans l'organisation. La vision à moyen terme et la raison d'être de l'organisation peuvent être enrichies par cette amélioration. L'Agilité peut se déployer plus facilement tout en supprimant les processus de gestion et les briques IT inutiles.

Plusieurs accompagnements possibles

- Mission d'AMOA selon recommandations de la CNIL
- Accompagnement technique sur la sécurité des données à caractère personnel
- Accompagnement organisationnel sur les processus de traitement des données
- Accompagnement juridique pour refonte de vos contrats de sous-traitance et commerciaux

Les sources utiles pour avancer

Le RGPD et ses textes officiels

Se préparer en 6 étapes grâce aux excellentes fiches de la CNIL

Devenir Délégué à la Protection des Données (DPD / DPO)

L'analyse d'impact relative à la protection des données

Consultant et DPD externalisé

Enfin si vous préférez les courtes vidéos didactiques, voici notre préférée avec Cookie Connecté

Qui sommes-nous ?

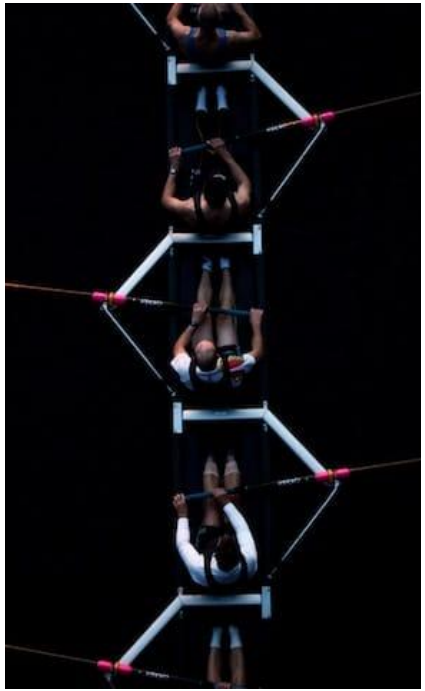
OM Conseil est une Entreprise de Services du Numérique basée à Saint-Quentin-en-Yvelines et créée en juillet 2003

Composée d'une vingtaine de collaborateurs assistés d'une cinquantaine de partenaires au niveau national (les Partners OMC n'interviennent qu'avec l'accord de nos Clients et en toute transparence).

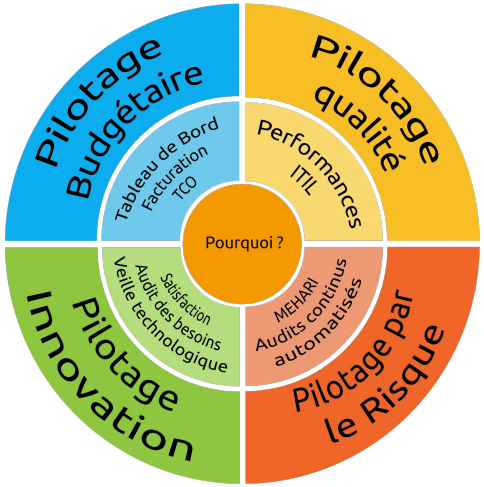
Plus d'infos juridiques et fiscales sur Societe.com

3 valeurs façonnent notre ADN depuis bientôt 15 ans, ces valeurs tiennent en une simple phrase :

Engagés et honnêtes, tout simplement !



Une méthode d'accompagnement sur le long terme



Pilotage informatique à 360°

En prenant en compte à la fois votre budget, la qualité, les risques et les dernières innovations technologiques,

Nous permettons d'augmenter le niveau de maturité du système d'informations tout en créant de la valeur.

Nous libérons ainsi les énergies qui permettent d'obtenir un plus grand engagement des collaborateurs pour, in fine, plus d'innovation et de réussite !

Nos autres domaines de compétences

- Etat des lieux, diagnostic et création de schémas directeurs pour vos Systèmes d'Informations
- Contrat de maintenance, de support, de conseil & d'accompagnement Informatique et Télécoms
- Solutions de messagerie et de travail collaboratif
- Lutte anti-intrusion, lutte antivirale et contrôle de qui fait quoi
- Re-déploiement de vos infrastructures existantes sur des clouds privés (OVH) ou publics (AWS, Microsoft Azure, ...)
- Déploiement et infogérance d'infrastructures hyperconvergées Nutanix
- Solutions de sauvegarde
- Solutions de Téléphonie sur IP (ToIP)

Et l'avenir, d'ici 2030 ?

Une approche innovante, depuis 15 ans déjà, qui prend en compte la durabilité et la résilience du SI ainsi que le bien-être des utilisateurs, dans une recherche permanente du juste prix et sans oublier la sécurité.

Plus d'infos sur notre vision à long terme.

OM Conseil
1 place Charles de Gaulle
78180 Montigny-le-Bretonneux

01 61 38 07 55

www.om-conseil.fr