RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

STEERING
LEGAL

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) : OFFRE DE MISE EN CONFORMITÉ

Le règlement UE 2016/679 relatif à la protection des données est directement applicable à l'ensemble des Etats membres le 25 mai 2018. Le RGPD (règlement général sur la protection des données) est une réglementation européenne obligatoire qui refond et renforce les droits et la protection des données à caractère personnel des personnes physiques. Cette nouvelle législation concerne tous les acteurs (personnes publiques, entreprises privées quelles que soient leur taille, les associations, les professions libérales, les artisans, etc.)

Cette nouvelle réglementation change la philosophie de la protection des données personnelles. Auparavant, une simple déclaration à la CNIL suffisait pour être en conformité avec la réglementation; à partir du 25 mai prochain, chaque « responsable de traitement » (qui est en premier le dirigeant sauf cas de délégation dûment organisée) devra être en mesure de justifier, à tout moment, qu'il est en règle au regard des prescriptions du RGPD, le non-respect de celles-ci étant passible de sanctions.

LE RGPD REPOSE SUR **QUATRE PRINCIPES CARDINAUX**

1. **Le principe de finalité.** Les données à caractère personnel ne peuvent être recueillies et traitées que pour une finalité déterminée, explicite et légitime, correspondant aux objectifs poursuivis par le « *responsable du traitement* ».

2. **Le principe de proportionnalité.** Seules les informations adéquates, pertinentes et nécessaires à la finalité du traitement peuvent faire l'objet d'un traitement de données à caractère personnel.

3. **Le principe d'une durée de conservation limitée des données.** Une durée de conservation doit être établie en fonction de la finalité de chaque fichier qui ne peut être conservé indéfiniment.

4. **Les principes de sécurité et de confidentialité.** Les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leur mission.

Ces grands principes doivent s'appliquer à n'importe quel traitement de données permettant l'identification d'une personne physique (fichiers d'adhérents, clients, fournisseurs, vidéosurveillance, géolocalisation, identification biométrique, etc.) quel que soit le support de stockage (logiciel métier, fichier informatique et physique, etc.)

C'est dans ce nouveau cadre technique et réglementaire complexe que le cabinet d'avocats STEERING LEGAL vous propose au besoin en partenariat avec la société de conseil et d'ingénierie informatique ILYEUM, une solution intégrée répondant à vos problématiques.

Cette offre unique, qui intègre à la fois l'audit informatique de votre système de gestion des données et l'audit juridique du traitement actuel de ces dernières, impose le respect de plusieurs étapes afin d'aboutir à une gestion des données personnelles conforme au RGPD.

1 CADRER ET PLANIFIER

ACTIONS

- Réunion de lancement avec les principaux acteurs concernés par le traitement des données et les systèmes d'information
- Estimation du nombre et de la nature des traitements hébergés

OBJECTIFS

- Valider le périmètre de la mission
- Préciser le nombre de jours et le calendrier de la mission

LIVRABLES

- Comptes rendu de la réunion de lancement
- Planning prévisionnel de la mission

2 CONNAITRE ET CARTOGRAPHIER LES DONNÉES HÉBERGÉES

ACTIONS

- Conduite d'entretiens avec les principaux responsables métiers
- Recensement et classification des traitements de données à caractère personnel par l'intermédiaire d'outils informatiques

OBJECTIFS

- Identifier les traitements hébergés et déterminer ceux qui contiennent des données personnelles
- Vérifier que les données collectées ne sont pas excessives regard de la finalité du traitement
- Vérifier qu'il y a une base légale au traitement de données personnelles
- Respecter le principe de minimisation (i.e. collecte des seules données pertinentes et strictement nécessaires à la finalité du traitement)
- Procéder à la tenue du registre des traitements
- Définir une politique de durée de conservation
- Informer les personnes concernées sur le traitement de leurs données personnelles

LIVRABLES

- Comptes rendus d'entretien
- Cartographie des traitements de données à caractère personnel
- Création d'un registre des activités de traitement

3 IDENTIFIER ET CONTRÔLER LES SOUS TRAITANTS (FOURNISSEURS ET PRESTATAIRES)

ACTIONS

- Liste les contrats conclus avec des personnes qui traitent des données à caractère personnel pour le compte du client

OBJECTIFS

- Identifier les différents sous-traitants
- Vérifier la conformité des sous-traitants et les mesures mises en place dans les contrats de sous-traitance
- Conclure un avenant aux contrats de sous-traitance si nécessaire

LIVRABLES

- Vade-mecum sur la passation des contrats de sous-traitance au regard du RGPD comprenant un clausier-type et des recommandations

4 ANALYSER LES ÉCARTS ET PRENDRE LES MESURES CORRECTIVES

ACTIONS

- Mesure des écarts par rapport aux exigences du RGPD
- Identification des risques et des actions correctives

OBJECTIFS

- Avoir un diagnostic précis de la conformité des traitements opérés par rapport aux RGPD
- Enclencher une démarche corrective pour mettre fin aux non-conformités

LIVRABLES

- Rapport de diagnostic des écarts aux RGPD

5 DÉTERMINER UN PLAN D'ACTIONS

ACTIONS

- Identification et confirmation des risques de non-conformité ou RGPD
- Assistance à la validation du plan d'actions

OBJECTIFS

- Établir un plan d'actions comportant une priorisation des risques, une allocation des moyens pour mettre en œuvre les mesures correctives et un délai de réalisation

LIVRABLES

- Rapport comprenant l'analyse du plan d'actions et la documentation, juridique et technique

6 ASSURER LA CONTINUITÉ DU RESPECT DU RGPD, LA DÉSIGNATION D'UN DPO

ACTIONS

- Désignation d'un DPO interne (un membre du personnel du responsable du traitement) ou externe (sur la base d'un contrat de services conclu avec un prestataire).

OBJECTIFS

- Suivi de la mise en œuvre du plan d'actions sur la durée avec l'ensemble des personnes concernées.
- informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- contrôler le respect du règlement et du droit national en matière de protection des données ;
- conseiller sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution ;
- coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.
- s'informer sur le contenu des nouvelles obligations, sensibiliser les décideurs sur l'impact de ces nouvelles règles, piloter la conformité en continu

LIVRABLES

- Formation du DPO interne ou mise en place d'un contrat d'externalisation de la fonction DPO avec STEERING LEGAL
- Mise à jour de la documentation juridique et contractuelle de l'entreprise pour la rendre conforme aux dispositions du RGPD vis-à-vis des personnes concernées par un traitement des données personnelles (salariés, fournisseurs, clients, etc.)

NOTRE ÉQUIPE

STEERING LEGAL

Composés d'avocats internationaux français, le cabinet STEERING LEGAL vous accompagne dans tous les domaines du droit des affaires. A l'aide d'équipes pluridisciplinaires, polyglottes et expérimentées, nous sommes en mesure de vous proposer un très haut niveau de compétence à un coût particulièrement compétitif.

Le cabinet STEERING LEGAL a mis en place une cellule dédiée à la mise en conformité au RGDP pilotée par **Maîtres Frédéric Raimbault et Sébastien Fleury, avocats associés**. Ils y assurent (i) l'information de nos clients et du public en publiant dans des revues et journaux (*Les Echos*, *la Gazette*, *etc.*) et (ii) le pilotage des dossiers et des équipes en lien avec les différents bureaux de STEERING LEGAL en France ou à l'étranger. Ils dispensent ainsi un service complet, adapté et réactif.

Nos équipes géreront votre dossier avec une double exigence de **réactivité** et de **disponibilité**.

STEERING LEGAL entend mettre tout en œuvre pour vous assister en toutes circonstances, afin de vous apporter la réponse la plus adaptée, dans un souci de pragmatisme et de réactivité. La compétence et l'expérience de nos équipes nous permettent de conjuguer fiabilité et célérité dans nos réponses, dans l'intérêt de nos clients.

CONTACTS

Me Frédéric RAIMBAULT
STEERING LEGAL
1 rue de Buffon
49100 Angers, France

fraimbault@steeringlegal.com
Tél. : + 33 (0)2 41 77 15 36
Mob. : + 33 (0)6 11 82 28 91

Me Sébastien FLEURY
STEERING LEGAL
20, rue Fortuny
75017 Paris, France

sfleury@steeringlegal.com
Tél. : +33 (0)1 45 05 15 65
Mob. : +33 (0)6 22 42 53 35

NOTRE ÉQUIPE

SOCIÉTÉ ILYEUM

Fondée en 2010, ILYEUM est une société de conseil et d'ingénierie informatique, spécialisée dans :

- Le conseil IT
- L'assistance à maitrise d'ouvrage stratégique
- Le pilotage de projets
- La conception de systèmes décisionnels
- Le développement d'applications business, notamment les portails d'entreprises

ILYEUM, qui emploie une équipe d'environ 100 consultants experts, intervient dans 4 domaines de compétences clés :

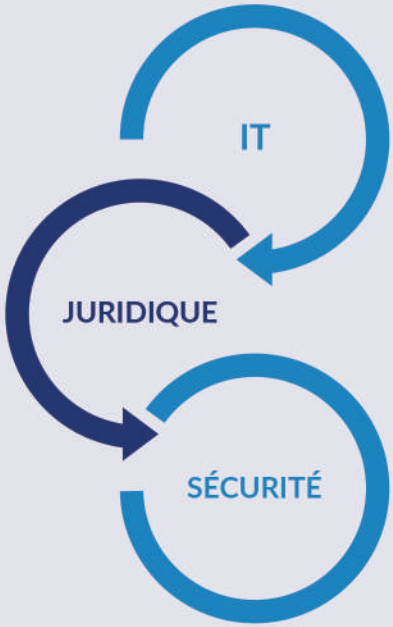
- Développement d'applicatifs sur mesure dans les domaines Java J2EE, Microsoft .Net et SharePoint, PHP ainsi que sur les technologies front-end les plus récentes (*react.js*, *AngularJS*…)
- EAI (*WebMethod et Tibco*)
- Business Intelligence (*BO*, *Datastage*, *Cognos*, *Qlikview*, *MS BI*, *SAS*, *Jaspersoft*…)
- Infrastructure et Solution y compris support opérationnel

CONTACTS

M. Mohammed CHOUITER
ILYEUM SAS
10, rue Chateaudun
75009 Paris
France

mchouiter@ilyeum.com
Tél. : +33 (0)1 83 81 96 00

STEERING LEGAL



ILYEUM