

# Formation audit et conformité RGPD EU-GDPR des entreprises

**Durée : 2 jours ou 3 jours.** Les 2 premiers jours sont transversaux entre l'informatique, le juridique et le marketing. Une 3<sup>ème</sup> journée (optionnelle) d'approfondissement du savoir-faire est recommandée pour les projets « sensibles » en matière de protection des données.

Journées de 07 h 00.

## OBJECTIFS :

- Découvrir les contraintes et les opportunités du règlement pour les protections des données
- S'appropriier les méthodologies d'audit et de mise en conformité au RGPD EU-GDPR
- Etre nommé comme DPO ou mieux choisir son délégué à la protection des données
- Renforcer la protection des données personnelles pour éviter les amendes administratives

**LE FORMATEUR :** PIERRE ELEMENTO – [contact@pierre-elemento.com](mailto:contact@pierre-elemento.com)

Plus de de 30 thématiques enseignées autour du digital : conformité RGPD / EU-GDPR, cloud computing, transformation digitale, communication web, webmarketing, réseaux sociaux, référencement naturel, Google adwords, Web analytics, e-réputation, e-commerce, social selling, growth hacking, RP 2.0...

**6 ENTREPRISES CLASSÉES AU CAC40 ET 5 AGENCES DE COMMUNICATION FORMÉES SUR LA PÉRIODE 2016/2017/2018.** Au total, le formateur Pierre Elemento a formé plus 500 étudiants, professionnels et décideurs au cours des 3 dernières années.  
**En savoir plus :** <http://pierre-elemento.com/>

## PROGRAMME ET PLAN DE FORMATION

### Jour 1 :

#### **Ch1. Introduction à la conformité RGPD / EU-GDPR**

- Les amendes et l'obligation légale des entreprises de mise en conformité au RGPD
- Les risques juridiques de co-responsabilité des sous-traitants et des fournisseurs
- L'obligation des maîtres d'ouvrage de choisir des prestataires « EU-GDPR compliant »
- L'atout des maîtres d'œuvre conformes RGPD pour remporter les propositions commerciales et les appels d'offre

#### **Ch2. Faire de la publicité et se promouvoir en conformité avec le RGPD**

- Le consentement avant le profiling, le retargeting et les cookies third-party
- La préconisation du double opt-in pour l'e-mailing et les newsletters
- La prospection commerciale en conformité stricte avec le RGPD
- La suppression ou le recyclage des données publicitaires collectées avant le RGPD
- Les méthodes de stockage des preuves de conformité
- La charte de protection des données personnelles à rédiger sur les sites web

#### **Ch3. L'obligation de rectification, suppression et portabilité des données**

- La minimisation obligatoire de la durée de vie des données
- Le droit à la rectification et à l'oubli
- Quelques exemples de réussite en matière de portabilité des données

- Mieux décider entre l'automatisation et la génération manuelle de la portabilité
- Quelques exemples de logiciels de référence non conformes au EU-GDPR

## **Jour 2 :**

### **Ch4. Collecter, traiter et stocker des données en conformité avec le RGPD**

- Comprendre les concepts de « security by default » et « security by design »
- Sécuriser et minimiser les formulaires de collecte d'informations personnelles
- Crypter les données sensibles dans les bases et échanges de données
- Fournir des données personnelles masquées aux sous-traitants
- Définir une politique cohérente et minimaliste d'accès aux données
- Le tracking obligatoire des accès aux données sensibles
- La sécurisation et l'authentification des postes de travail
- La sécurisation des cloud extranet et des partages de fichiers
- La vérification de la conformité RGPD des sous-traitants
- Les décharges de responsabilité à faire signer aux clients non conformes au RGPD

### **Ch5. Nommer un délégué à la protection des données (DPD ou DPO)**

- Les contraintes légales de nomination d'un DPO
- Les formations obligatoires et les certifications pour devenir DPO
- Le rôle du DPO interne ou externalisé
- Les mentions légales à afficher et les réunions de sensibilisation des équipes
- La contrainte légale de la tenue d'un registre d'accountability
- Les contrôles éventuels d'accountability par la CNIL
- La mise à disposition des clients de tout ou partie de l'accountability
- La collaboration au quotidien avec les informaticiens, les chefs de projets et les équipes des sous-traitants
- Les nouveaux outils de Data Protection Management System (DPMS)
- L'obligation d'études d'impact en prévention des fuites ou pertes de données
- L'obligation d'informer la CNIL en cas de piratage des données

### **Ch6. Travaux pratiques de consolidation des acquis**

## **Journée 3 (en option)**

### **Ch7. Audit des failles de sécurité d'un site web ou d'une application mobile**

- Url Rewriting
- Cookie Rewriting
- HTML Rewriting
- Md5 et Sh1 Rewriting
- Les failles Ajax et JSON
- L'injection SQL et NOSQL
- Les autres techniques pour identifier des failles de sécurités

### **Ch8. Travaux pratiques personnalisés autour du système d'information de sa propre entreprise**