ORDRE DES EXPERTS-COMPTABLES
Conseil Supérieur

GESTION DES DONNÉES PERSONNELLES

Comment se préparer au nouveau règlement européen RGPD ?

Les nouvelles obligations

- Le Règlement européen complète les obligations existantes dans la loi française de 1978 relatives à la gestion des données personnelles
  - La gestion des données personnelles s'impose aux entreprises clientes depuis plusieurs années … mais aussi aux experts-comptables !

Le RGPD

- **Règlement général sur la protection des données (RGPD)**
  - Il instaure un cadre commun de protection des données à l'échelle européenne
    - Contrairement à une directive, il est directement applicable dans tous les Etats membres
  - Champ d'application étendu
    - Si le responsable du traitement des données personnelles (RT) ou le sous-traitant (ST) est établi sur le territoire de l'Union européenne ou qu'ils mettent en œuvre des traitements de données visant à fournir des biens et des services aux résidents européens ou à les « cibler »

Le RGPD

- Objectifs du règlement européen
  - Renforcer les droits des individus
    - Information claire, intelligible et aisément accessible sur le traitement des données
    - **Nécessité de donner un consentement ou de pouvoir s'opposer au traitement de ses données personnelles**
    - **Charge de la preuve du consentement qui repose sur le responsable du traitement**
    - Droit à la portabilité des données personnelles
    - Possibilité de recours collectifs, droit à réparation des dommages matériel ou moral
  - Responsabiliser les entreprises
    - Fin des déclarations préalables auprès des autorités de contrôle sauf dans certains cas : par exemple, autorisations en matière de recherche en santé
    - **MAIS** de nouvelles **obligations** (tenue d'un registre des traitements, notification des failles de sécurité, délégué à la protection des données – DPO, études d'impact sur la vie privée)
    - et la nécessité **d'être en mesure de démontrer la conformité**

- **Date d'application du Règlement**
  - Le 25 mai 2018 dans tous les pays de l'Union européenne !
    - Les fichiers déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement
      - **Il est donc nécessaire de se préparer dès maintenant**

Comment se préparer dans les cabinets ?

- Il faut procéder par étapes pour être prêts le 25 mai 2018 !
  - Etape 1
    - Désigner une personne responsable
  - Etape 2
    - Faire une cartographie des traitements de données personnelles existants dans le cabinet
  - Etape 3
    - Arrêter un plan d'action
  - Etape 4
    - Gérer les risques
  - Etape 5
    - Organiser les processus internes
  - Etape 6
    - Documenter

Comment se préparer dans les cabinets ?

- **Etape 1 : Désigner une personne chargée de réaliser une cartographie des traitements de données personnelles**
  - Désignation d'une personne chargée de ces questions
  - Obligation de désigner un **Délégué à la protection des données personnelle DPO**
    - Pour les autorités et organismes publics (ministères, collectivités territoriales, établissements publics)
    - Pour les organismes **dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle** (compagnies d'assurance ou les banques pour leurs fichiers clients, opérateurs téléphoniques ou fournisseurs d'accès internet)
    - Pour les organismes dont les activités de base **les amènent à traiter à grande échelle des données dites "sensibles"** (données biométriques, génétiques, relatives à la santé, la vie sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale) ou **relatives à des condamnations pénales et infractions**
  - **Pas d'obligation pour la plupart des cabinets d'EC même si la CNIL** encourage cette désignation
    - Possibilité de désigner un DPO mutualisé ou externe

Comment se préparer dans les cabinets ?

- **Etape 2 : Faire une cartographie des traitements de données personnelles existants**
  - **Inventaire des traitements** de données personnelles mis en œuvre
    - **Afin d'évaluer les pratiques et identifier les risques** associés à ces opérations de traitement
    - Et arrêter **un plan d'action**
  - Outil incontournable à votre disposition
    - Le **registre** des traitements
      - **Modèles de registre sous Excel accessible sur le site de la CNIL**
      - Les modèles de déclaration CNIL peuvent également vous aider pour déterminer les finalités des traitements

Comment se préparer dans les cabinets ?

- Contenu du **registre** des traitements
  - Questions à se poser pour chaque traitement
    - Qui ?
      - Indiquer dans le registre le nom et les coordonnées du RT (et de son représentant légal) et du délégué à la protection des données le cas échéant
      - Identifiez les responsables des services opérationnels traitant les données au sein de votre cabinet
      - Etablissez la liste des ST
    - Quoi ?
      - Identifiez les catégories de données traitées
      - Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (données relatives à la santé par exemple)
    - Pourquoi ?
      - Indiquez la ou les finalités pour lesquelles les données sont collectées ou traitées (traitement technique du dossier, gestion RH…)

Comment se préparer dans les cabinets ?

- **Le registre des traitements**
  - Où ?
    - Déterminez le pays où les données sont hébergées
    - Indiquez vers quels pays les données sont éventuellement transférées
  - Jusqu'à quand ?
    - Indiquer la durée de conservation pour chaque catégorie de données
  - Comment ?
    - Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

Comment se préparer dans les cabinets ?

- **Etape 3 : arrêter un plan d'action**
  - Déterminer les actions à mettre en œuvre pour respecter les nouvelles règles du RGPD
  - Points incontournables à vérifier
    - Avoir la certitude que seules les données strictement nécessaires à la poursuite de l'objectif du traitement sont collectées et traitées
    - Identifier la base juridique sur laquelle se fonde le traitement
      - Par exemple : intérêt légitime, contrat, obligation légale, consentement de la personne lorsqu'il est nécessaire
    - Revoir les mentions d'information afin qu'elles soient conformes aux exigences du RGPD
    - Vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités
      - Vérifier les clauses contractuelles rappelant les obligations du ST en matière de sécurité, de confidentialité et de protection des données personnelles traitées
        - » Modèles de clauses sur le site de la CNIL
    - Revoir les modalités d'exercice des droits des personnes concernées
      - Droit d'accès, de rectification, droit à la portabilité, retrait du consentement etc.
    - Vérifier les mesures de sécurité mises en place

Comment se préparer dans les cabinets ?

- **Vigilance particulière pour les traitements**
  - Portant sur des **données sensibles** (santé, concernant des mineurs)
  - Ayant pour objet ou pour effet
    - La surveillance systématique à grande échelle d'une zone accessible au public (vidéo surveillance)
    - L'évaluation systématique et approfondie d'aspects personnels permettant la prise de décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative (profilage)
  - Transférant des données hors de l'Union européenne

Comment se préparer dans les cabinets ?

- Etape 4 : gérer les risques
  - Si identification de traitements de données personnelles susceptibles d'engendrer **des risques élevés pour les droits et libertés des personnes concernées**
    - Notamment les traitements de données sensibles et les traitements reposant sur le profilage
  - Réalisation obligatoire d'une étude d'impact sur la protection des données (PIA)
  - Consultation de l'autorité de protection des données avant de mettre en œuvre ce traitement qui pourra s'y opposer
- Que contient une étude d'impact sur la protection des données (PIA) ?
  - Une description du traitement et de ses finalités
  - Une évaluation de la nécessité et de la proportionnalité du traitement
  - Une appréciation des risques sur les droits et libertés des personnes concernées
  - Les mesures envisagées pour traiter ces risques et se conformer au RGPD
- Modèles et guides pour réaliser une PIA sur le site de la CNIL

Comment se préparer dans les cabinets ?

- **Etape 5 : organiser les processus internes**
  - Mise en place de procédures internes pour assurer la protection des données tout au long du traitement
    - Procédure à mettre en place en cas de faille de sécurité, de demandes de rectification ou d'accès, de demande de modification des données collectées, de changement de prestataire
    - Mise en place des procédures prévues dans le RGPD
      - Audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes, etc.
  - Etablissement d'une politique de protection des données personnelles dans le cabinet

Comment se préparer dans les cabinets ?

- **Etape 6 : Documenter**
  - Nécessité de prouver la conformité au RGPD en cas de contrôle
  - Nécessité de constituer et regrouper la documentation nécessaire
    - Les procédures et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu
  - **Lien avec la NPMQ norme professionnelle de maîtrise de la qualité et le manuel existant dans les cabinets !**