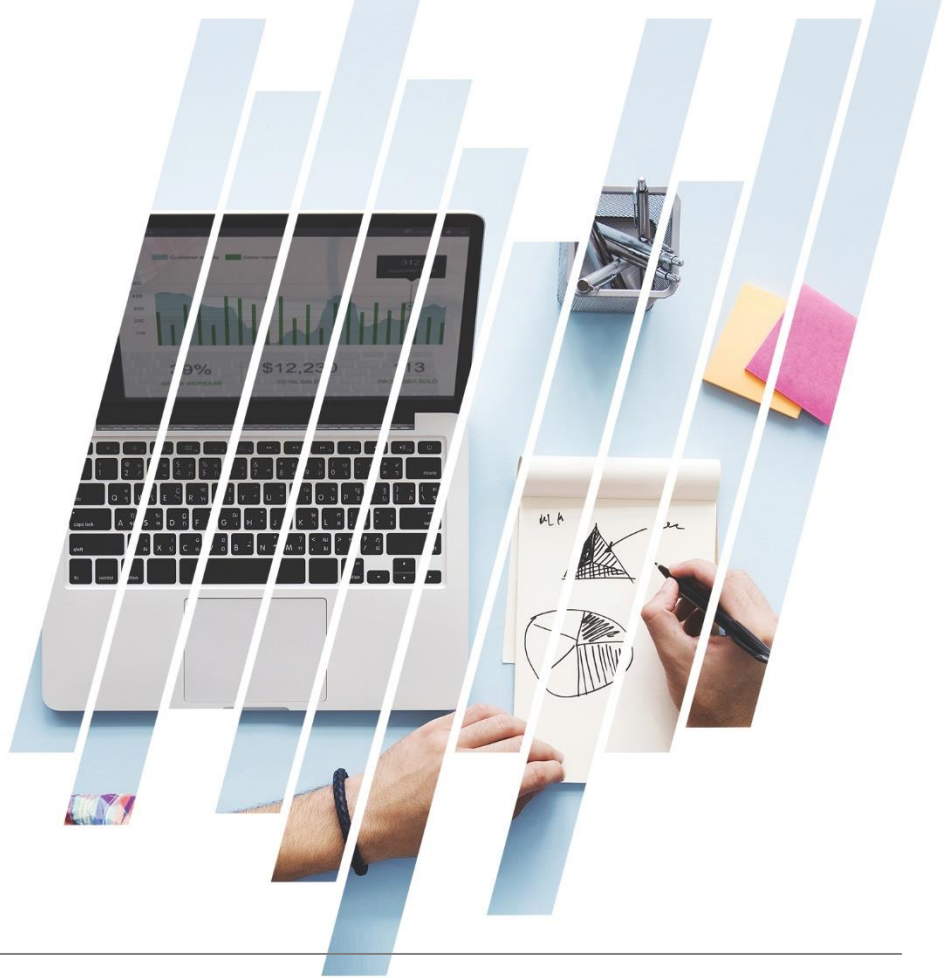
RGPD : le vrai du faux

Mercredi 18 mars 2020

Viviane GELLES
Avocat – DPO externe
Certification DPO AFNOR 2019

Jurisexpert
CABINET D'AVOCATS

RGPD : 2 ans déjà…



- **Vrai ou faux?**
- **J’ai besoin du consentement de la personne concernée pour traiter ses données à caractère personnel**

- **Vrai ou faux?**
- **J’ai besoin du consentement de la personne concernée pour traiter ses données à caractère personnel**
  - **Le choix d’une base légales différentes bases légales permettant de traiter les données**
  - **En fonction**
    - **Du traitement mis en œuvre**
    - **Des conditions requises par la base légale choisie**
    - **Des conséquences qui y sont attachées**
  - **Informer les personnes concernées sur la base légale retenue**
    - **Mentions d’information**
    - **Registre**

- **Vrai ou faux?**
- **En présence d’une faille de sécurité, je dois non seulement la notifier à la CNIL mais aussi informer les personnes concernées.**

- **Vrai ou faux?**
- **En présence d'une faille de sécurité, je dois non seulement la notifier à la CNIL mais aussi informer les personnes concernées.**
  - **Obligation de notification à la CNIL dans les meilleurs délais et, si possible, 72h après en avoir pris connaissance**
  - **Information des personnes concernées lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées**
    - En des termes simples et clairs
    - Nature de la violation
    - Nom et coordonnées du DPO
    - Conséquences probables de la violation
    - Mesures prises pour y remédier et en atténuer les conséquences négatives
  - **Sauf si**
    - **Les données étaient chiffrées**
    - **La communication exigerait des efforts disproportionnés (dans ce cas plutôt communication publique)**
    - **Mesures prises ultérieurement garantissant que le risque élevé n'est plus susceptible de se matérialiser**

- **Vrai ou faux?**
- **Si je ne suis pas en conformité au RGPD, je risque une amende de 20 millions d’euros.**

- **Vrai ou faux?**
- **Si je ne suis pas en conformité au RGPD, je risque une amende de 20 millions d'euros.**
  - **C'est le maximum encouru**
  - **Ca ne concerne « que » :**
    - **Le non respect des principes de base, y compris le consentement**
    - **Le non respect des droits des personnes concernées**
    - **Les transferts de données hors UE**
    - **(…)**
  - **Mais pas :**
    - **Privacy by design / by default**
    - **La contractualisation avec les sous-traitants**
    - **L'obligation de tenir un registre**
    - **Les failles de sécurité**
    - **AIPD**
    - **Obligation de nommer un DPO**
    - **(…)**

- **Vrai ou faux?**
- **La désignation d’un DPO me permet de garantir la conformité au RGPD.**

- **Vrai ou faux?**
- **La désignation d’un DPO me permet de garantir la conformité au RGPD.**
  - **La désignation n’est pas obligatoire pour tous**
    - **Autorités publiques**
    - **Traitement à grande échelle de données sensibles**
    - **Traitement exigeant un suivi systématique et régulier à grande échelle**
  - **Elle ne suffit pas à garantir la conformité**

- **Vrai ou faux?**
- **Je ne peux pas nommer nommer mon responsable informatique comme DPO**

- **Vrai ou faux?**
- **Je ne peux pas nommer nommer mon responsable informatique comme DPO**
  - Profil DPO
    - Connaissances juridiques et techniques
    - Positionnement hiérarchique
    - Conflit d'intérêts
      - Directeur général
      - DRH
      - Directeur informatique
      - (…)
      - S'ils participent à la détermination des finalités / moyens
    - Pas de transfert de responsabilité par délégation de pouvoir
    - Désignation en ligne
    - N'est pas un salarié protégé

- **Vrai ou faux?**
- **Je travaille en B2B uniquement, mais je suis quand même concernée par le RGPD**

- **Vrai ou faux?**
- **Je travaille en B2B uniquement, mais je suis quand même concernée par le RGPD**
  - Données personnelles : données identifiant directement ou indirectement une personne physique
  - Données des salariés des fournisseurs, prestataires, clients, partenaires…
  - Dénomination sociale correspondant aux nom et prénom de l'entrepreneur
  - Aménagement : prospection commerciale B2B
    - En B2C
      - Consentement ou P&S analogues
    - En B2B
      - Information de l'utilisation à des fins de prospection au moment de la collecte
      - Faculté d'opposition à tout moment
      - Identité de l'annonceur
      - Objet de la sollicitation en rapport avec la fonction occupée
      - Ces règles ne s'appliquent pas aux adresses professionnelles génériques

- **Vrai ou faux?**
- **J’ai mis mon site Internet en conformité avec les recommandations de la CNIL sur les cookies, mais je devrais à nouveau le faire évoluer prochainement.**

- **Vrai ou faux?**
- **J’ai mis mon site Internet en conformité avec les recommandations de la CNIL sur les cookies, mais je devrais à nouveau le faire évoluer prochainement.**
  - **Lignes directrices de la CNIL de juillet 2019**
  - **Projet de recommandation de la CNIL en janvier 2020, soumis à consultation publique**
    - **Concerne les univers logués / non logués**
    - **S’applique à tous traceurs sauf**
      - **Authentification, contenu d’un panier d’achat, personnalisation de l’interface, mesures d’audience, limitation de l’accès gratuit sur les sites payants, conservation du choix de l’internaute en terme de dépôt de traceurs…**
    - **Traceurs de l’éditeur / de sites tiers**
    - **Consentement éclairé (sur finalités, données, resp., destinataires…)**

- **Consentement libre**
  - **Enregistrement du refus dans les mêmes conditions (durée notamment) que l'enregistrement de l'acceptation**
  - **Possibilité de ne pas faire de choix (croix de fermeture)**
  - **Ne pas utiliser de pratiques de design destinées à laisser penser que le consentement est obligatoire**

- **Consentement spécifique / personnalisé**
- **Durée recommandée de conservation : 6 mois**

- **Information en plusieurs niveaux : exemples**
- Finalité
  - « publicité personnalisée »
  - Puis détails : différentes opérations techniques telles que l'affichage de la publicité, le plafonnement de l'affichage (« capping publicitaire », consistant à ne pas présenter à un utilisateur une même publicité de manière trop répétitive), la lutte contre la fraude au clic (détection d'éditeurs prétendant réaliser une audience publicitaire supérieure à la réalité), la facturation de la prestation d'affichage, la mesure des cibles ayant plus d'appétences à la publicité pour mieux comprendre l'audience, etc
- Destinataires
  - Partenaires publicitaires
  - Liste à jour
  - Bouton « gestion des cookies » accessible sur chaque page permettant de regarder la liste actualisée facilement, retirer son consentement etc.

La preuve du consentement

- Enregistrement via le le traceur (pour navigateur web) ou via le paramètre utilisé pour stocker l'information du consentement dans le cas d'une application mobile
- Horodatage du consentement, du contexte dans lequel il a été recueilli (identification du site web ou de l'application mobile), type de mécanisme de recueil du consentement utilisé et des finalités auxquelles l'utilisateur a consenti
- Mise sous séquestre auprès d'un tiers du code informatique utilisé par l'organisme recueillant le consentement, pour les différentes versions de son site ou de son application mobile
- OU capture d'écran du rendu visuel affiché sur un terminal mobile ou bureau conservée pour chaque version du site ou de l'application
- OU audits réguliers des mécanismes de recueil du consentement mis en œuvre par les sites ou applications depuis lesquels il est recueilli

- **Vrai ou faux?**
- **La CNIL est clémente lors des premiers contrôles « post RGPD »**

- **Vrai ou faux?**
- **La CNIL est clémente lors des premiers contrôles « post RGPD »**
  - **10 sanctions publiques en 2019**
  - **Entre 20KE et 50 ME**
  - **Programme annuel de contrôle 2020**
    - **Données de santé**
    - **Traceurs**
    - **Géolocalisation**

- **Vrai ou faux?**
- **Le droit à l'oubli existait avant l'entrée en vigueur du RGPD**

- **Vrai ou faux?**
- **Le droit à l'oubli existait avant l'entrée en vigueur du RGPD**
  - **Loi République Numérique de 2016**
  - **Droit à l'oubli des mineurs**
    - **Réseaux sociaux, moteurs de recherche, plateformes d'échange…**
  - **Elargissement aux majeurs par le RGPD**
    - **Droit à l'effacement**
    - **Droit au déréférencement**

- **Vrai ou faux?**
- **Tout organisme traitant des données personnelles doit tenir un registre**

- **Vrai ou faux?**
- **Tout organisme traitant des données personnelles doit tenir un registre**
  - **Organisme employant moins de 250 salariés**
  - **Ne doivent tenir un registre que pour**
    - **les traitements non occasionnels**
    - **Ou comportant un risque pour les droits et libertés des personnes concernées (géolocalisation, videosurveillance…)**
    - **Ou portant sur des données sensibles**

- **Vrai ou faux?**
- **Le RGPD ne s’applique pas aux données anonymisées**

- **Vrai ou faux?**
- **Le RGPD ne s'applique pas aux données anonymisées**
  - **Anonymisation : procédé irreversible rendant impossible toute identification des personnes concernées**
    - **Impossible d'isoler tout ou partie des enregistrements se rapportant à un individu en particulier**
    - **Ne permet pas de rapprocher deux enregistrements concernant la même personne**
  - **Ne pas confondre avec la pseudonymisation**
    - **Remplacer données directement identifiantes par données indirectement identifiantes**
    - **Données pseudonymisées restent soumises au RGPD**

Merci de votre attention !

Viviane GELLES

Jurisexpert
CABINET D'AVOCATS