JOURNÉE MONDIALE DE LA PROTECTION DES DONNÉES PERSONNELLES : INFORMEZ-VOUS ET PRENEZ VOS DONNÉES EN MAIN !

La **journée mondiale de la protection des données personnelles** se tient le **jeudi 28 janvier**. Il s'agit d'une initiative du Conseil de l'Europe relayée par la Commission européenne. Son but est de sensibiliser les citoyens européens sur l'importance de la protection de leurs données personnelles et du respect de leurs libertés et droits fondamentaux.

Cet évènement est ainsi l'occasion de faire un bilan des réalisations 2020 et de présenter les grands chantiers prévus en 2021 en matière de protection des données personnelles. Décryptage de **Luc HOBON,** Data Protection Officer (DPO) pour Total Marketing France et ses filiales.

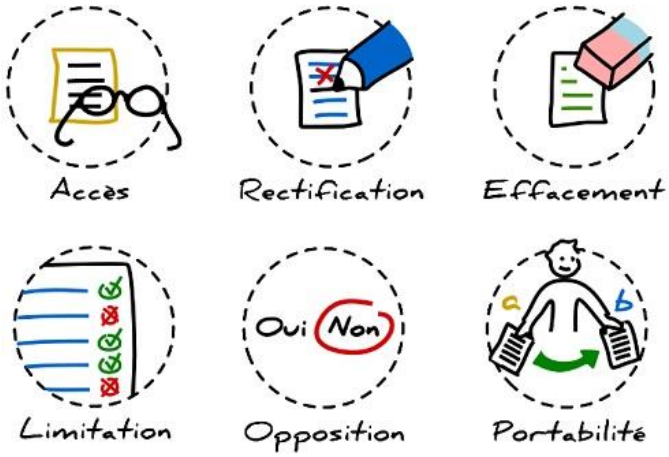
Lire l'article RGPD paru dans *L'aparté* en décembre 2019

Luc HOBON,
DPO de Total Marketing France et ses filiales

LES PRINCIPALES RÉALISATIONS EN 2020

1. Gestion des demandes d'exercice des droits des personnes concernées

Les personnes concernées par des traitements de données personnelles disposent de droits leur permettant de garder la maîtrise des informations les concernant : droit d'accès, de rectification, d'effacement, d'opposition, à la limitation, à la portabilité des données.



Quel est l'enjeu majeur ?

Les personnes concernées doivent être informées de leurs droits et disposer d'un point de contact pour exercer leurs droits.
Vous disposez seulement d'un délai d'un mois pour répondre aux demandes.
Vous devez également apporter la preuve à tout moment que vous avez effectivement bien répondu et réalisé les actions adéquates (rectification, effacement, ...).
Comment répondre ? Est-il possible de rejeter une demande tout en respectant le RGPD ?
Existe-t-il des modèles de courrier de réponse ? Comment tracer les échanges ?

Pour plus d'informations, consultez la **procédure CR FR GOUV PDP 001** sur le site NORMA

2. Gestion des incidents de sécurité et des violations de données personnelles

Un incident de sécurité est un évènement qui altère la sécurité d'un traitement avec l'apparition d'un impact potentiel.

Une violation de données personnelles est un incident de sécurité qui entraîne (de manière accidentelle ou illicite) la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles (transmises, conservées ou traitées d'une autre manière), ou l'accès non autorisé à de telles données.

Quel est l'enjeu majeur ?
Vous disposez seulement de 72 heures pour notifier à la CNIL une violation de données personnelles qui est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Comment évaluer ce risque ? Quelles ressources pouvez-vous mobiliser ? Comment tracer toutes les décisions prises ? Comment notifier la violation à la CNIL et aux personnes concernées ?

Pour plus d'informations, consultez la **procédure CR FR GOUV PDP 002** sur le site NORMA

3. Accueil de l'autorité de contrôle CNIL

La CNIL peut réaliser à tout moment des contrôles sur tous les sites web en ligne, les applications smartphone, les réseaux sociaux, etc.

La CNIL peut également à tout moment réaliser un contrôle inopiné dans les locaux de l'entreprise. Les agents de la CNIL viennent à l'improviste avec des questions précises liées à des plaintes reçues des prospects, clients, partenaires ou collaborateurs.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Quel est l'enjeu majeur ?
Vous devez démontrer que vous respectez bien les principes de la protection de données personnelles.
Par exemple, vous devez fournir les éléments suivants : By Design 3P de vos applications ou outils, votre registre des activités de traitement, les statistiques des demandes d'exercice de droits, …

Qui accueille les agents de la CNIL ? Quelles ressources pouvez-vous mobiliser ? Qui doit répondre directement aux agents ? Comment tracer les échanges ? Qui signe le procès-verbal ?

Pour plus d'informations, consultez la **procédure CR FR GOUV PDP 003** sur le site NORMA

FAIT MARQUANT 2020

Un exemple de réalisation concrète : une AIPD pour le contrôle d'accès biométrique du dépôt de Gennevilliers

Pour la première fois sur le périmètre de TMF, une analyse d'impact relative à la protection des données (AIPD) a été réalisée pour le contrôle d'accès biométrique du dépôt de Gennevilliers.

Quel est l'enjeu majeur ?

Si un traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes, le RGPD impose de réaliser une AIPD.
Il faut démontrer à la CNIL que toutes les précautions ont été prises dès la conception pour protéger au mieux les données personnelles.

4. Information / Sensibilisation / Formation

Nous devons démontrer à la CNIL que toutes les personnes qui manipulent des données personnelles ont été sensibilisées, informées ou formées à la protection des données personnelles : quelles sont les règles et bonnes pratiques, quels sont les risques et les conséquences en cas de manquement.

Lire l'article paru dans TOTEM mag (numéro de novembre 2020)

Présentation au Comité de direction Mobilités & Nouvelles Energies (MNE) et lors de 2 webinaires à destination de l'ensemble des collaborateurs de MNE
Pour visionner le replay, cliquez ici.

Formation réalisée auprès des assistantes de direction et information des correspondants Communication de TMF pour ajouter les mentions d'information RGPD à tous les questionnaires ou enquêtes quelque soit l'outil utilisé (Interview, Forms, ...)
Pour plus d'informations, consultez ce guide de bonnes pratiques.

Animation d'un atelier RGPD lors du Business Ethics Day du 10 décembre 2020
Pour visionner le replay, cliquez ici.

LES CHANTIERS PRÉVUS EN 2021...

- **S'assurer de la conformité RGPD dès la conception d'un projet : By Design 3P**
  Vous devez être capable de démontrer la conformité RGPD de toute application , tout outil, toute opération marketing, tout nouveau produit ou service qui utilise des données personnelles.
  Pour cela, il existe une méthologie du groupe Total qui doit être respectée et en particulier le By Design 3P qui permet de démontrer à la CNIL la prise en compte du Privacy By Design et du Privacy By Default (minimisation des données personnelles).

Pour plus d'informations, contactez le référent protection des données personnelles de votre entité : **votre Data Privacy Liaison (DPL)**

- **Mettre en conformité les sites web et les applications mobiles avant le 31 mars 2021**
  Les sites web sont la vitrine du groupe Total. Ils doivent être irréprochables. C'est une cible privilégiée pour détecter les non-conformités et alerter la CNIL.
  Il y a de nombreuses obligations à respecter : les mentions d'informations, les conditions générales d'utilisation (CGU), la charte de données personnelles et traceurs, le bandeau cookies et autres traceurs et pour finir la collecte du consentement.

  Vous devez appliquer au plus tard le 31 mars 2021 les nouvelles lignes directrices de la CNIL sur les cookies et autres traceurs.

  Pour plus d'informations, n'hésitez pas à visionner le webinaire « *La conformité des sites Internet au RGPD* » **en cliquant ici.**

- **Réaliser les analyses d'impact relative à la protection des données (AIPD)**

  - Vidéoprotection dans les stations-service (Direction Réseau)
  - Vidéosurveillance des dépôts (Direction Supply et Logistique France)
  - Angel Protect System : améliorer la sécurité des personnes intervenant lors des travaux (Direction HSEQ)
  - Désignation du conducteur à l'ANTAI en cas d'infraction routière *via* la plateforme TOTAL Mobility (Direction Mobilités et Nouvelles Energies)
  - Application GR Diplomatic qui permet aux diplomates de payer leur carburant sans accise avec une carte TOTAL (Direction MNE)

- **Définir le programme de contrôle des traitements pour TMF**
  Nous devons démontrer que nous avons un programme de contrôle cohérent qui permet de garantir la conformité RGPD de l'ensemble des activités de traitement.
  Il est important de détailler qui contrôle quoi, quand, comment et de conserver les preuves de ces contrôles.
  Les façons de faire sont multiples : un traitement de bout en bout, une application qui porte plusieurs traitements, une équipe ou un service ou une direction, une thématique (les sites web, les CRM, les outils de marketing automation, d'éditique, d'archivage, ...), etc.

... ET APRÈS

- **Maintenir la conformité**
  Toute nouveauté qui touche à une donnée personnelle nécessite une étude préalable (Privacy By Design) pour s'assurer de sa conformité RGPD. Selon les cas, il est indispensable de mettre à jour toute la documentation permettant de démontrer l'« accountability » de l'entreprise.

- **Réaliser les contrôles de conformité**
  Le programme de contrôle permet de savoir ce qu'il faut contrôler : quoi, quand et comment. Ensuite, il faut réaliser les contrôles, les documenter et bien sûr mener les actions correctives et préventives associées.

- **Réaliser des exercices**
  Pour être fin prêt, rien ne vaut la pratique. Il est important de réaliser régulièrement des exercices pour éprouver nos procédures et vérifier que toutes les personnes concernées savent ce qu'elles doivent faire.
  Par exemple :
  - Cyberattaque avec violation de données personnelles
  - Contrôle inopiné de la CNIL

Au-delà des obligations légales, le RGPD est une opportunité pour :

- Rationaliser les données que vous collectez,
- Optimiser vos traitements
- Renforcer la confiance avec vos prospects, clients, fournisseurs, partenaires, prestataires, salariés, candidats.

Les actions menées peuvent constituer un avantage concurrentiel et améliorer l'image de notre entreprise.

POUR PLUS D'INFORMATIONS :

consultez la page WAT de la branche MS :
Programme PDP - Protection des Données Personnelles et GDPR

consultez la page WAT de Total Marketing France sur la protection des données