## Règlement général européen sur la protection des données (RGPD)

# Tout savoir sur les nouvelles en matière de protection des

*L'affaire Cambridge Analytica (utilisation indue des données personnelles de millions d'utilisateurs de Facebook) est venue nous le rappeler : la protection des données personnelles des citoyens est désormais un enjeu incontournable. C'est dans ce contexte qu'est entré en vigueur le 25 mai dernier le Règlement général européen sur la protection des données personnelles (RGPD).*
*Ce texte uniformise et modifie sensiblement les règles applicables dans les 28 pays membres de l'UE en matière de données personnelles, avec un double objectif : le renforcement des droits des citoyens et une responsabilisation accrue des entreprises manipulant des données personnelles.*

### À qui s'applique le RGPD ?

Qu'on se le dise, tout le monde (ou presque) est concerné par le RGPD ! En effet, le RGPD s'applique à tout organisme dès lors que (i) il met en œuvre un (des) traitement(s) de données personnelles sur le territoire de l'UE, (ii) il est établi sur le territoire de l'UE, ou (iii) les personnes concernées par le traitement sont des citoyens ou ressortissants européens.
Un traitement de données est défini comme toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel. À titre d'exemple, la collecte, la conservation, la consultation, l'utilisation, la mise à disposition, l'effacement ou la destruction, constituent un traitement de données à caractère personnel.
Une donnée à caractère personnel est toute information relative à une personne physique identifiée ou qui peut l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres : un nom, une adresse postale ou de courriel sont des données personnelles.

### Que change le RGPD pour les entreprises ?

Si le RGPD allège (voire supprime) les formalités déclaratives des entreprises opérant des traitements de données personnelles, il accroît considérablement leurs obligations. Au nombre de ces obligations (dont le non-respect est beaucoup plus durement sanctionné), figurent notamment :

# obligations données personnelles

**• La nomination d'un délégué à la protection des données personnelles**
(DPO pour "Data Protection Officer").
Cette nomination est obligatoire pour les organismes publics, les entreprises traitant des données sensibles à grande échelle, ainsi que les entreprises dont les principales activités impliquent de façon récurrente et systématique le traitement de grands volumes de données. Véritable "chef d'orchestre" de la conformité, le DPO est en charge de l'application et du déploiement en interne du RGPD.

**• L' "accountability"**
Désormais, toute entité traitant des données personnelles devra non seulement documenter l'ensemble de ses traitements, mais également être en mesure d'en attester la conformité au RGPD.

**• Le principe de "privacy by design"**
Selon ce principe, tout nouveau produit, service ou système exploitant des données personnelles, doit garantir dès sa conception le plus haut niveau possible de protection des données.

**• Le principe de "privacy by default"**
Selon ce principe, toute entreprise procédant à un traitement de données personnelles, doit garantir par défaut le plus haut niveau possible de protection des données afin d'assurer que seules seront traitées les données nécessaires à la finalité spécifique du traitement.

**• Un devoir d'information renforcé**
Toute personne dont les données personnelles font l'objet d'un traitement doit être clairement informée des finalités de ce traitement avant sa mise en œuvre et, le cas échéant, autoriser l'utilisation de ses données.

**• La notification des failles de sécurité**
Toute détection par une entreprise d'une faille en matière de sécurité (accès non autorisé, perte ou vol de données personnelles), doit être notifiée auprès de l'autorité de contrôle dans les 72 heures.

**• La responsabilité des prestataires et sous-traitants (Article 28)**
Toute société se voyant confier par le responsable d'un traitement de données à caractère personnel, la gestion de tout ou partie de ce traitement (hébergement, archivage, routage de courriels, etc.), assumera désormais une responsabilité directe.

## L'impact pour la FFT et les clubs

**Quelles sont les mesures adoptées par la FFT pour se mettre en conformité avec le RGPD ?**
Le travail de mise en conformité de la politique "données personnelles" de la FFT a été impulsé par le Correspondant Informatique et Libertés, avec la Direction des Systèmes d'Information et la Direction Expérience et Data Client. Ce travail a consisté, dans un premier temps, à la mise en conformité des traitements de données personnelles existants et, dans un second temps, à celle des traitements mis en œuvre après l'entrée en vigueur de la nouvelle réglementation.

Les traitements de données personnelles mis en œuvre au sein de chaque direction de la FFT ont été catégorisés selon leur importance. Les traitements identifiés comme ayant un impact business/opérationnel/juridique/image fort, ont fait l'objet d'une analyse poussée au moyen d'un outil d'autodiagnostic. À la suite de cette analyse, un plan de mise en conformité, portant notamment sur la sécurité et la confidentialité des données, a été établi pour ces traitements et est actuellement en cours d'application.
Pour les traitements de données personnelles mis en œuvre après l'entrée en vigueur du RGPD, un travail de sensibilisation est mené auprès de chaque direction.
En parallèle, des outils de conformité ont été établis et mis à disposition des directions : nouvelles mentions d'information, nouvelles clauses contractuelles de sous-traitance, mise à disposition d'un registre de recensement des activités de traitement de données, etc.

Par ailleurs, la FFT a procédé à la nomination d'un Délégué à la Protection des Données, qui a pris ses fonctions le 25 mai dernier.

**Et pour les clubs ?**
Parce qu'ils stockent les données personnelles de leurs adhérents et/ou de leurs salariés, les clubs sont concernés par le RGPD. Toutefois, consciente que l'application du RGPD doit tenir compte de la taille de certains organismes, la CNIL a édité en association avec Bpifrance un guide pratique adapté aux TPE/PME, ainsi qu'une méthodologie pour se préparer en 6 étapes. Ces documents sont disponibles sur le site Internet de la CNIL (www.cnil.fr).