Les associations face au Règlement Général de Protection des Données (GDPR)

Dominique Counasse

Liège – 3 mai 2018

1 – QU'EST-CE QUE LE RGPD ?

- C'est le règlement général pour la protection des données
- Règlement 2016/679 du Parlement européen et du Conseil
- adopté le 27 avril 2016,
- entrant en vigueur le 25 mai 2018,
- d'application immédiate sans nécessité d'une transcription en droit belge,
- précisant et élargissant les principes déjà énoncés par une directive précédente transposée en droit belge par la loi du 8/12/92.
- Des Guidelines établies par le Working Party 29 (futur Comité européen de la protection des données).
- Une loi belge en préparation pour préciser les mesures de portée nationale (infractions pénales, mesures de protection complémentaires, autorité de contrôle,…).

2 – QUE VISE LE RGPD ?

- Un **traitement**
- de **données personnelles,**
- dont certaines – les **données sensibles** – doivent être particulièrement protégées,
- données se rapportant à des personnes (les **personnes concernées**) dont il importe de sauvegarder les intérêts,
- traitement effectué par un **responsable du traitement**
- qui peut déléguer ce traitement à un **sous-traitant**
- ou qui peut transmettre les données en question à un **destinataire,**
- étant entendu que tout **transfert de données hors EEE** est sévèrement contrôlé et limité.

3 – QUELS PRINCIPES ÉNONCE-T-IL ?

Les données personnelles doivent être

- **traitées de manière légale, transparente et que leur utilisation soit facile à comprendre pour la personne concernée,**
- **pertinentes et limitées à l'objectif poursuivi,**
- **collectées dans un but déterminé, explicite et légal,**
- **exactes et tenues à jour,**
- **conservées uniquement durant le délai nécessaire au traitement poursuivi,**
- **et traitées en prenant des mesures de sécurité informatique adéquates.**

4 – QUEL TYPE DE TRAITEMENT EST VISÉ ?

- **Traitement de données à caractère personnel.**
- **Automatisé en tout ou en partie.**
- **Non automatisé de données contenues ou appelées à figurer dans un fichier (ensemble structuré de données centralisé ou non et accessible selon des critères déterminés).**

➔ **Applicable**

- **à des données structurées (figurant dans des champs informatiques),**
- **à des données non structurées (mails, documents scannés, …).**

5 – UNE ASSOCIATION EFFECTUE-T-ELLE UN TRAITEMENT DE DONNÉES ?

La définition du traitement de données est fort large :

Opération ou ensemble d'opérations appliquées à des données personnelles ou à un ensemble de données personnelles telles que

Collecte,
Enregistrement,
Conservation,
Extraction,
Consultation,
Utilisation,
Communication par transmission,
Diffusion,
Interconnexion,
Modification,
Effacement ou destruction.

➔ La réponse est Oui

5 – UN CLUB EFFECTUE-T- IL UN TRAITEMENT DE DONNÉES ?

La définition du traitement de données est fort large :

Opération ou ensemble d'opérations appliquées à des données personnelles ou à un ensemble de données personnelles telles que

- **Collecte,**
- **Enregistrement,**
- **Conservation,**
- **Extraction,**
- **Consultation,**
- **Utilisation,**
- **Communication par transmission,**
- **Diffusion,**
- **Interconnexion,**
- **Modification,**
- **Effacement ou destruction.**

➔ **La réponse est Oui**

6 – QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

- Toute information concernant une personne physique identifiée ou identifiable vivante.
- Données d'identification: Nom, NISS, adresse postale, numéro de compte bancaire, adresse mail, adresse IP, …
- Données professionnelles et privées associées à cet identifiant.
- Données sensibles :
  - données génétiques ou biométriques,
  - données relatives à la santé,
  - à l'origine raciale ou ethnique,
  - aux opinions politiques, aux convictions philosophiques ou religieuses, à l'appartenance syndicale,
  - à la vie ou à l'orientation sexuelle.

7 – UNE ASSOCIATION TRAITE-T-ELLE DES DONNÉES PERSONNELLES ?

Généralement toute affiliation à une association implique la collecte et l'utilisation de données telles que

- **les coordonnées d'une personne (nom, prénom, adresse),**
- **son numéro de compte bancaire (domiciliation bancaire),**
- **son adresse mail (pour permettre la communication),**
- **des informations concernant sa famille (si on les affilie également et parfois avec des tarifs réduits).**

➔ **La réponse est Oui**

7 – UN CLUB TRAITE-T- IL DES DONNÉES PERSONNELLES ?

Généralement toute affiliation à un club implique la collecte et l'utilisation de données telles que

- **les coordonnées d'une personne (nom, prénom, adresse),**
- **son numéro de compte bancaire (domiciliation bancaire),**
- **son adresse mail (pour permettre la communication),**
- **des informations concernant sa famille (si on les affilie également et parfois avec des tarifs réduits).**

➔ **La réponse est Oui**

9 – UN CERTIFICAT D'APTITUDE AU SPORT EST-IL UNE DONNÉE DE SANTÉ ?

Il est rédigé par un médecin ➔ il constitue bien une donnée relative à la santé physique d'une personne !

IL FAUT DONC ÊTRE EXTRÊMEMENT ATTENTIF

- **à son contenu : mentionne-t-il uniquement l'aptitude à la pratique d'un sport en particulier ou de tout sport en général ? Fait-il état d'une pathologie handicapante ?**
- **à son mode de transmission (pli fermé ou non)**
- **à son destinataire, à savoir celui qui en demande la production et qui le conserve (l'association pour protéger sa responsabilité éventuelle ou l'assureur pour voir s'il va assurer ou non l'affilié)**

CAR LES RESPONSABILITES ET LES SECURITES VARIENT EN CONSEQUENCE

10 – QUELLES PERSONNES SONT PROTÉGÉES PAR LE RGPD ?

- Personnes physiques vivantes.
- Avec une protection particulière pour les enfants (personnes âgées de moins de 16 ans avec une possibilité pour les Etats membres de porter cet âge à 13 ans).
- Pas les personnes morales.
- Mais bien leurs représentants.
- Pas les personnes physiques décédées.

11 – QUELLES SONT LES PERSONNES DONT UNE FEDERATION, UN CLUB POSSÈDE LES DONNÉES ?

On peut les classer en différentes catégories :

- **adhérents, membres,**
- **Sympathisants et donateurs,**
- **bénéficiaires d'une intervention,**
- **membres du personnel et représentants légaux de l'association**
- **fournisseurs,**
  - **personnes physiques,**
  - **représentants des personnes morales,**
- **intervenants divers (avocats, …),**

étant entendu que le type de données possédées varie en fonction de leurs catégories.

12 – QUELS SONT LES ACTEURS VISÉS PAR LE RGPD ?

L'article 4 du RGPD indique

- **Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui seul ou conjointement avec d'autres,** détermine les finalités et les moyens du traitement**.**
- **Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel** pour le compte du responsable du traitement**.**
- **Destinataire : la personne physique ou morale, l'autorité publique, le service ou un autre organisme** qui reçoit communication de données à caractère personnel, **qu'il s'agisse ou non d'un tiers (ce dernier étant placé sous l'autorité directe du responsable du traitement ou du sous-traitant).**

13 – EN PRATIQUE QUE FAIT LE RESPONSABLE DU TRAITEMENT ?

Il détermine les finalités (le pourquoi ?) et les moyens du traitement (le comment ?).

- **Il choisit les données à traiter et le type de traitement à appliquer.**
- **Il définit le mode de conservation des données et la durée de celle-ci.**
- **Il est garant de leur sécurité et définit donc les mesures applicables.**
- **Il choisit librement ses sous-traitants.**
- **Il doit en principe établir un registre de traitement des données.**

S'il fait cela de concert avec une autre personne physique ou morale on parlera alors de responsables conjoints.

14 – EN PRATIQUE QUE FAIT LE SOUS-TRAITANT ?

Il agit pour le compte du responsable du traitement.

- **Il ne peut traiter que les données prévues par le responsable et uniquement dans le cadre strictement prévu par ce dernier.**
- **Il doit appliquer les modes de conservation et la durée de conservation choisis par le responsable.**
- **Il doit mettre en œuvre les mesures de sécurité choisies par le responsable.**
- **Il doit faire agréer ses propres sous-traitants par le responsable.**
- **Il doit établir un registre des catégories de traitement effectuées pour le compte du responsable.**

15 – QUEL EST LE RÔLE D'UNE ASSOCIATION ?

Soit l'association traite les données pour son propre compte :

- **données des membres adhérents, des sympathisants donateurs,**
- **données de son personnel, de ses représentants légaux,**
- **données de ses fournisseurs,**
- **données collectées pour la réalisation de son objet social.**

➔Elle est alors le responsable du traitement

Soit l'association traite des données pour le compte de tiers :

- **parce qu'elle joue le rôle d'une centrale d'achats en vue de faire bénéficier ses membres de tarifs préférentiels,**
- **parce qu'elle collecte des données pour un assureur,**
- **parce qu'elle collecte des données pour une administration.**

➔ Elle est alors un sous-traitant

19 – COMMENT SE CONFORMER AU RGPD ?

Il faut

- **identifier les données traitées,**
- **définir la base juridique de leur traitement / consentement**
- **respecter les droits des personnes concernées,**
- **mettre en œuvre des mesures techniques et organisationnelles adéquates pour assurer la sécurité des données,**
- **prévenir l'autorité de contrôle en cas de violation de données à caractère personnel (Data breach).**

22 – QUELLE EST LA BASE JURIDIQUE DU TRAITEMENT DE DONNÉES ?

JE DOIS OBTENIR LE CONSENTEMENT DE LA PERSONNE CONCERNÉE.

23 – COMMENT GÉRER LE CONSENTEMENT ?

- **Le consentement exige une action affirmative claire.**
- **Le silence, les cases pré-cochées ou l'absence de réaction ne constituent pas un consentement !**
- **Le consentement doit être vérifiable. Cela signifie qu'il faut conserver une preuve concernant la façon et le moment où le consentement a été donné.**
- **Les individus ont le droit de retirer leur consentement à tout moment.**
- **On n'est pas tenu d'obtenir un nouveau consentement des personnes concernées si celui donné auparavant répond déjà aux nouvelles exigences. On doit donc s'assurer que ce dernier réponde bien aux normes requises par la nouvelle législation.**

23 – COMMENT GÉRER LE CONSENTEMENT ?

En pratique

- **On doit veiller à ce que les personnes concernées reçoivent une explication claire du traitement auquel elles consentent ➔ nécessité d'imposer la lecture de la politique de confidentialité et de traitement (Policy) sur les sites Web.**
- **On doit veiller à ce que le mécanisme de consentement soit vraiment volontaire et « opt-in » ➔ case à cocher sur les sites Web et nécessité de détailler les consentements au cas où plusieurs finalités sont envisagées.**
- **On doit permettre aux personnes concernées de retirer leur consentement facilement.**

24 – QUELS SONT LES DROITS DES PERSONNES CONCERNÉES ?

- Droit à l'information
- Droit d'accès
- Droit de rectification
- Droit à la portabilité
- Droit à l'intervention humaine
- Droit à l'oubli
- Droit d'opposition

28 – COMMENT GÉRER LES DROIT D'OUBLI ET D'OPPOSITION ?

- **Droit à l'oubli**
  - La personne concernée peut demander d'être « oubliée » mais ce droit n'est pas absolu.
  - Obligation d'effacement si les données ne sont plus nécessaires, en cas de retrait du consentement qui constituait la base juridique du traitement, si le traitement cause des dommages aux personnes concernées, en cas de traitement illicite.
  - Pour s'opposer à l'effacement des données, il faut justifier d'une obligation légale (prescription), d'une mission d'intérêt public, d'une finalité de recherche scientifique ou historique, de la constatation, l'exercice ou la défense de droits en justice.

➔ **Problématique des Back-up et des DB démultipliées !**

- **Droit d'opposition**
  - La personne concernée peut s'opposer :
    - au direct marketing : lorsque l'on reçoit une demande d'opposition, on doit cesser de traiter immédiatement les données de la personne concernée sans exceptions,
    - au traitement sur la base des intérêts légitimes : lorsque l'on reçoit une opposition, on doit arrêter le traitement de ces données sauf s'il y a des exceptions légales ou à moins de prouver que l'intérêt légitime est à ce point impérieux qu'il contrecarre les droits des personnes concernées,
    - au traitement pour des recherches scientifiques/historiques dans certains cas.
    - On doit informer la personne concernée de son droit de s'opposer dès la première communication et dans la privacy notice.

29 – COMMENT GÉRER LES DONNÉES DES MINEURS ?

- Lorsque la base juridique du traitement repose uniquement sur le consentement de la personne concernée,
- en cas d'offre directe de services de la société de l'information,
- le consentement doit être donné ou autorisé par le titulaire de l'autorité parentale.
- Une fois majeur, l'enfant peut retirer son consentement et s'opposer au traitement.
- Pas de consentement nécessaire en cas de services de prévention ou de conseil.

35 – QUELLES SANCTIONS EN CAS DE NON RESPECT DU RGPD ?

- **Sanctions**
- 17 mesures possibles: classement sans suite, non-lieu, conciliation, avertissement, interdiction temporaire, astreinte, communication au parquet, publication de la décision, amende administrative, etc.
- Amende administrative: pouvant aller jusqu'à 10 ou 20,000,000 € !
- Recours possible: cour des marchés

- **Autorité de protection des données (ancienne CPVP)**
  - Médiateur de la protection des données: examen des plaintes
  - Service d'inspection: organe d'enquête; larges pouvoirs d'investigation (officiers de police judiciaire)
  - Mesures provisoires possibles (**suspension du traitement**…)
  - Chambre contentieuse

SITES INTERNET UTILES

- **CNIL**
  - https://www.cnil.fr/professionnel
- **BCSS**
  - **https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/general-data-protection-regulation**
- **CPVP**
  - **https://www.privacycommission.be/fr/reglement-general-sur-la-protection-des-donnees-0**
- **Article 29 Working party**
  - **http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083**
- **Portail européen**
  - **http://www.eugdpr.org/eugdpr.org.html**