FELTEN & ASSOCIES

Avocats à la Cour

FELTEN & ASSOCIES

Avocats à la Cour

RGPD

Impact sur les associations: comment se conformer à ses obligations légales

CLAE Event – Luxembourg, le 12 novembre 2020

Anne Rosier
Senior Associate

Me Bernard FELTEN
Avocat à la Cour
Barreaux de Luxembourg et de Genève

PLAN

F&A

1. Avant-Propos
2. Le Règlement général sur la protection des données ou RGPD
3. Les notions de « donnée à caractère personnel », « personne concernée » et « traitement »
4. Le responsable du traitement des données au sein d'une association
5. La mise en conformité – exceptions?
6. Incidences pratiques sur:

- La tenue d'une base de données
- Les échanges et partages de contacts
- L'envoi de courriers postaux et courriels électroniques y compris à caractère publicitaire
- La conservation et la diffusion de photos
- La gestion du site internet
- Le traitement et la conservation d'informations sensibles
- La conservation et l'archivage des données

7. Conclusion – Doit-on craindre le RGPD? Risques réels encourus d'une non conformité

1. Avant-Propos

SITUATION ACTUELLE

- 25/05/2018: le « RGPD » (Règlement Général pour la Protection des Données), un règlement européen en matière de protection des données à caractère personnel, entre en vigueur et oblige toutes les organisations à se mettre en conformité
- Avant le RGPD, la loi luxembourgeoise modifiée du 2 août 2002 aujourd'hui abrogée a accompagné les organisations les obligeant à recourir au système très lourd des formalités préalables de notifications et autorisations pour pouvoir traiter de données à caractère personnel.
- Le RGPD a mis fin à ce système très lourd des formalités préalables (sauf exceptions) en obligeant les organisations à se conformer au règlement de manière proactive en se dotant de mesures organisationnelles et techniques appropriées en accord avec le RGPD.
- La « CNPD », (Commission Nationale pour la Protection des Données), l'autorité nationale en matière de protection des données, suit une approche positive d'accompagnement des organisations et encore plus des associations pour qui elle a même mis en ligne un « guide à l'attention du monde associatif » (www.cnpd.lu).
- Nous allons voir comment et par quels moyens suffisants, une association peut s'assurer d'être en conformité avec le RGPD sans s'exposer à de possibles sanctions futures lors d'un contrôle, d'une violation ou d'une plainte à son encontre.

2. Le RGPD

DEFINITION

- Il s'agit du **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**.
- Il est disponible à la lecture sur le site législatif de l'Union européenne (www.eur-lex.europa.eu) dans toutes les langues de l'UE.
- Il est applicable à TOUTES les associations.
- Toute association doit être en mesure de prouver la mise en œuvre de toutes les mesures organisationnelles et techniques pour assurer la mise en conformité de son organisation à ce règlement.

3. Notions essentielles

NOTIONS DE DONNÉE À CARACTÈRE PERSONNEL, DE PERSONNE CONCERNÉE ET DE TRAITEMENT

- A. Notion de donnée à caractère personnel (ou donnée personnelle)

1. Constitue une donnée à caractère personnel toute information concernant une personne **physique identifiée** directement ou **identifiable** indirectement:

- Il peut s'agir d'un nom, prénom, adresse email nominative : nous identifions directement la personne;
- Il peut s'agir d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'un enregistrement vocal, d'un numéro de sécurité sociale, etc., : la personne peut être identifiée non pas directement mais en faisant une recherche ou par le biais d'un croisement de plusieurs données et ce, sans même devoir disposer nécessairement des nom et prénom de la personne.

2. Certaines données sont en plus dites **sensibles** car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés : une opinion religieuse, politique, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des données philosophiques.

Ces données sensibles ont un cadre légal particulier, qui **interdit** toute collecte préalable sans un consentement écrit, clair et explicite de la personne concernée par exemple (ou en se fondant sur une autre base juridique comme une obligation légale) et elles peuvent parfois requérir pour leur traitement une validation par la CNPD.

3. Notions essentielles (2)

NOTION DE DONNÉE A CARACTÈRE PERSONNEL (SUITE)

Les données personnelles traitées par une association peuvent être assimilées, mais non limitées, aux **catégories** suivantes :

- données d'identification (nom, prénom, adresse, date et lieu de naissance, âge, nationalité, situation de famille, etc.)
- données professionnelles (fonction, adresse e-mail etc.)
- données financières (coordonnées bancaires, niveau de revenus, etc.)
- données administratives (matricule national, un diplôme, etc.)
- données concernant la santé (handicap, allergies, etc.)
- données biométriques (poids, photo, etc.)
- données de localisation
- une adresse IP (Internet Protocol) d'un PC, d'un modem
- données judiciaires (extrait de casier judiciaire p.ex.)

Les données peuvent être **collectées** par le biais d'un formulaire standardisé (forme la plus sûre et la plus complète permettant de ne pas collecter de données non nécessaires et de plus un tel formulaire est complété par la personne concernée), sous format papier ou électronique ou encore par le biais d'e-mails, par téléphone (ou application mobile) ou au cours d'un entretien physique.

3. Notions essentielles (3)

NOTION DE DONNÉE A CARACTÈRE PERSONNEL (SUITE)

L'association peut collecter/recevoir les données personnelles à **diverses occasions** :

- adhésion à l'association
- une inscription à un événement
- par le biais d'un don
- abonnement à une newsletter
- engagement comme bénévole
- candidat à un emploi de collaborateur
- lors d'une relation professionnelle
- ....

Les traitements de ces données aident l'association à réaliser **ses objectifs/missions** :

- traiter l'inscription à un événement
- gérer la logistique d'un événement
- traiter un don selon les exigences légales en lien avec celui-ci

3. Notions essentielles (4)

NOTION DE DONNÉE A CARACTÈRE PERSONNEL (SUITE)

- fournir des informations demandées
- assurer la qualité des services proposés
- mener des campagnes d'information ou de collecte de dons
- gestion du personnel ou des bénévoles
- ....

3. Notions essentielles (5)

NOTIONS DE PERSONNE CONCERNÉE ET DE TRAITEMENT

B. La « personne concernée »

- La personne concernée est toute personne physique identifiée ou identifiable. Il peut s'agir des membres/adhérents, donateurs, fournisseurs, collaborateurs, administrateurs, bénévoles,...).

C. Le(s) « traitement(s) de données personnelles »

- Le traitement est une opération ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé, informatisé ou non: il peut s'agir de collecte, enregistrement, modification, diffusion, effacement ou destruction de données personnelles.

4. Le responsable du traitement des données

LE RESPONSABLE DU TRAITEMENT DES DONNÉES AU SEIN DE L'ASSOCIATION

Le responsable du traitement est la personne physique (ou morale), qui, seule ou conjointement, détermine au sein de l'association les finalités et moyens des traitements de données à caractère personnel à savoir :

- quels besoins justifient une collecte de données personnelles,
- quel est l'objectif/objectifs visés,
- comment les traiter,
- comment les protéger,
- comment les conserver,
- comment assurer leur effacement

Le RGPD vise **3 situations dans lesquelles la désignation d'un DPO est obligatoire** :

- le traitement de données personnelles est mis en œuvre par une **autorité publique ou un organisme public**;

- l'entité concernée a pour activités de base la mise en œuvre de traitement de données qui, du fait de leur nature, de leur portée et/ou de leur finalité, exigent un **suivi régulier et systématique à grande échelle d'individus** ;

- l'entité concernée a pour activités de base la mise en œuvre de **traitement à grande échelle de catégories particulières de données** (données de santé, relatives aux opinions philosophique, religieuses, etc.) ou de données relatives à des condamnations pénales ou des infractions.

=> Si l'un de ces trois critères est rempli, votre association a l'obligation de désigner un DPO.

Même s'il n'y a pas besoin d'un *Data Protection Officer* (« DPO ») au sens du RGPD, il y aura toujours une responsabilité de conformité à respecter au sein de votre association; celle-ci est le plus souvent endossée par la direction/fondateur de l'association ensemble avec les éventuels collaborateurs quand il s'agit d'une petite association.

Possible recours à un expert externe.

Aucun agrément par la CNPD.

LE RESPONSABLE DU TRAITEMENT DES DONNÉES AU SEIN DE L'ASSOCIATION (SUITE)

SANCTIONS ET AMENDES ADMINISTRATIVES

- Les violations par le responsable de traitement de ses obligations peuvent faire l'objet d'amendes pouvant s'élever jusqu'à **20'000'000 d'euros** ou, dans le cas d'une entreprise, jusqu'à **4% du chiffre d'affaires annuel mondial** total de l'exercice précédent, le montant le plus élevé étant retenu.

- Les amendes qui se veulent dissuasives sont évidemment proportionnées au cas d'espèce. Le RGPD prévoit qu'il doit être tenu compte de **circonstances aggravantes ou atténuantes** pour décider s'il y a lieu d'imposer une amende administrative et pour en fixer le montant.

- Ces circonstances concernent plus particulièrement la nature, la gravité et la durée de la violation, si la violation a été commise délibérément ou par négligence, si des mesures ont été pris pour atténuer le dommage subi par les personnes concernées, le degré de responsabilité du responsable de traitement compte tenu des mesures techniques et organisationnelles mises en œuvre, le degré de coopération du responsable de traitement avec la CNPD, les catégories de données personnelles concernées par la violation, ou la manière dont la CNPD a eu connaissance de la violation.

- Outre les amendes, la CNPD dispose de tout un arsenal coercitif :

  avertissements,

  rappels à l'ordre,

  injonction au responsable de traitement de se conformer au RGPD, ou de communiquer à une personne concernée une violation de données,

  limitation temporaire ou définitive, y compris une interdiction de traitement,

  ordonner la rectification ou l'effacement de données personnelles ou la limitation du traitement.

- Toute décision de la CNPD qui sanctionnerait un responsable de traitement est susceptible de recours devant le tribunal administratif qui statue comme juge du fond.

5. La mise en conformité

LA MISE EN CONFORMITÉ – EXCEPTIONS ?

Toute association, quelle que soit son activité, sa taille, les données personnelles traitées DOIT se mettre en conformité avec le RGPD.

Il n'y a pas d'exceptions dans l'approche globale – bémol: le principe de la proportionnalité des moyens à mettre en œuvre s'applique à votre association; les moyens dépendront de vos activités, de vos ressources financières et humaines, du nombre de vos membres, de la taille de votre association, etc.

Afin de passer en revue, de manière plus pratique, la documentation et le fil conducteur à suivre, votre association doit se familiariser (et bien évidemment appliquer !) les six grands principes du RGPD suivants:

- I. Licéité (base juridique sur laquelle on se fonde pour justifier le traitement des données), loyauté et transparence appliquées à vos pratiques de collectes de données
- II. Limitation des finalités
- III. Limitation des données personnelles collectées
- IV. Données exactes et complètes
- V. Limitation de la conservation des données personnelles
- VI. Intégrité et confidentialité

5. La mise en conformité (2)

I. LICÉITÉ, LOYAUTÉ ET TRANSPARENCE

Votre association doit collecter des données personnelles qui soient légitimes par rapport à l'objectif recherché mais elle doit aussi baser le(s) traitement(s) qu'elle en fait sur l'une des bases juridiques énoncées dans le RGPD (= notion de licéité du traitement) :

- **consentement de la personne concernée**
- traitement nécessaire à l'exécution d'un contrat
- traitement nécessaire au respect d'une obligation légale
- traitement nécessaire à la sauvegarde des intérêts vitaux
- traitement nécessaire à l'exécution d'une mission d'intérêt public
- traitement nécessaire aux fins des intérêts légitimes de l'association

Le consentement doit être donné par un acte positif clair par lequel la personne concernée (adhérent/membre, donateur, bénévole) manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données personnelles la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale (cette dernière est à éviter autant que possible car comment prouver un consentement oral en cas de problème).

5. La mise en conformité (3)

I. LICÉITÉ, LOYAUTÉ ET TRANSPARENCE (SUITE)

Ce consentement **doit** pouvoir être retiré aussi simplement qu'il a été donné.

Pour chaque adhérent/membre, vous devriez prévoir un mécanisme de recueil de consentement « *opt-in* », « *opt-out* » sur un formulaire de contact/adhésion en précisant les principales caractéristiques du traitement (son objet, sa finalité, sa durée) et évidemment consigner et conserver la preuve du consentement dans un fichier d'adhérents ou sur un autre support.

! Le RGPD interdit que les cases soient cochées par défaut de manière informatisée.

Exemple : le membre de l'association doit pouvoir cocher une case pour recevoir la newsletter et devrait pouvoir par ailleurs refuser toute opération marketing en ne cochant pas une case à cet effet.

Pour toutes les activités suivantes d'une association, un consentement explicite, clair du membre est requis :

- Inscription à une newsletter
- Annuaire des membres avec indication d'événements familiaux privés comme une naissance, mariage
- Coordonnées des membres sur site web de l'association
- Partage des données personnelles avec une autre association ou organisation pour un événement commun
- Appels aux donc avec noms des donateurs personnes physiques

5. La mise en conformité (4)

I. LICÉITÉ, LOYAUTÉ ET TRANSPARENCE (SUITE)

Dans le cas d'une association, une autre base juridique justifiant le traitement de données pourrait être la nécessité liée à **l'exécution d'un contrat** :

on vise plutôt ici le cas du salarié de l'association sous contrat de travail: en vertu de son contrat de travail, il doit y avoir traitement de ses données d'un point-de-vue gestion du personnel : dans ce cas, la légitimité sera l'exécution du contrat et non le consentement du salarié voire également pour certains traitements le **respect d'une obligation légale** (se conformer à des dispositions du code du travail, sécurité sociale).

Il peut y avoir comme autre base juridique permise, la **défense des intérêts légitimes** de l'association (sous réserve de respecter les libertés et droits fondamentaux de la personne concernée).

- Exemple : pour une association sportive, la publication des résultats des compétitions avec les noms prénoms des joueurs ou partage de données avec une Fédération.

Une dernière base juridique pourrait être **l'intérêt public** (bien commun, intérêt général) d'une autorité publique.

5. La mise en conformité (5)

II. LIMITATION DES FINALITES

Votre association ne peut collecter de données personnelles que pour des **objectifs** licites mais également **spécifiques**, **clairement exprimés** et **précisés** dans la politique de protection des données.

- Exemple : vous ne pouvez envoyer à des marques ou magasins de vêtements sportifs la liste de vos membres (si association sportive ou association nature) pour marketing par ces marques ou magasins même s'ils sont sponsors de vos événements à moins d'avoir prévu un consentement exprès (*opt in* /*opt out*) de vos membres sur vos formulaires/espace d'adhésion de vos membres sur votre site.

- Exemple : si une commune ou autre organisation gouvernementale exige, dans le cadre d'une demande de subvention, d'obtenir le registre de vos membres, vous devez refuser ! Vous pouvez leur indiquer le nombre des adhérents sans dévoiler leurs coordonnées personnelles ; les comptes de votre association devraient constituer un élément plus approprié.

- Exemple : un membre d'une association pourrait exiger la communication de la liste des autres membres (si les statuts de l'association le prévoient), à condition que cette demande de communication ait un lien direct avec l'activité de l'association. Par exemple, dans le cas du renouvellement du bureau d'une association, un candidat pourrait demander la liste des membres pour mener sa campagne et s'engager ensuite à la détruire.

5. La mise en conformité (6)

III. LIMITATION DES DONNÉES PERSONNELLES COLLECTÉES & IV. DONNÉES EXACTES ET COMPLÈTES

Limitation des données personnelles collectées

- Votre association ne doit collecter que les données personnelles **nécessaires** et **essentielles** à la réalisation de ses objectifs.
- Pour chacune des données personnelles collectées, posez-vous la question de son utilité et de son besoin pour la réalisation de l'objet de votre association.

Selon la méthode utilisée pour la collecte des données, votre association doit veiller à saisir des données exactes et complètes.

Les personnes concernées ont le droit de vous demander à ce que les données inexactes ou incomplètes soient modifiées voire supprimées.

5. La mise en conformité (7)

V. LIMITATION DE LA CONSERVATION DES DONNÉES VI. INTÉGRITÉ ET CONFIDENTIALITÉ

Limitation de la conservation des données personnelles

- Votre association doit supprimer les données personnelles lorsqu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées.
- Exemple: si un membre démissionne ou est radié, ses données doivent être effacées (sauf s'il accepte de façon claire que certaines de ses données soient conservées, par exemple, ses coordonnées dans l'annuaire des anciens).

Intégrité et confidentialité

- Votre association doit traiter les données personnelles collectées de façon à garantir leur sécurité contre toute traitement non autorisé ou illicite (fuite, vol des données, cyber attaque de votre fichier adhérents), perte, destruction ou dégâts d'origine accidentelle et ce, au moyen de mesures organisationnelles et techniques appropriées.
- Par mesures techniques sont visées principalement la sécurité informatique et la conservation des données personnelles.
- Comme vu précédemment, l'association se dote de mesures organisationnelles et techniques proportionnelles à la taille, aux ressources humaines et financières, à l'activité de votre association ainsi qu'aux données personnelles collectées.

5. La mise en conformité (8)

DOCUMENTATION DE BASE A METTRE EN PLACE - INVENTAIRE

A. Un inventaire des données et des traitements

- Avant toute chose, votre association doit faire un **inventaire** de toutes les données personnelles ainsi que des traitements et leurs objectifs.
- Assurez-vous de faire cet inventaire sur un **support écrit** (idéalement sous la forme d'un tableau modulable) qui pourra ensuite vous servir de **registre** des traitements.
- Tout au long de la vie de votre association, au vu de son évolution, de l'évolution éventuelle des outils utilisés, vous pourrez adapter et enrichir ce registre des traitements de données.

5. La mise en conformité (9)

DOCUMENTATION DE BASE A METTRE EN PLACE (SUITE) – LE REGISTRE DES TRAITEMENTS

B. Un registre des traitements

Le **registre** doit reprendre les activités de l'association avec, pour chacune d'elles :

- les coordonnées du responsable traitement/sous-traitant éventuel (p.e un fournisseur IT, imprimeur)
- le(s) traitement(s)
- la/les catégorie(s) des données collectées, exploitées, conservées, partagées
- l'objectif/les objectifs poursuivi(s) (la/les finalités)
- la légitimité :
  - i) vous basez-vous sur le consentement requis ou non de la personne concernée ? (consentement pour envoi de newsletter, de demande de don, prise de photos lors d'un événement, etc .)
  - ii) ou le traitement effectué est-il nécessaire à l'exécution d'un contrat ? (contrat de travail d'un collaborateur par exemple, vous avez des obligations RH en matière de gestion de paie par exemple)
  - iii) ou pouvez-vous justifier que ce traitement protège et nourrit les intérêts légitimes de l'association ? (par exemple des photos d'événements culturels sur votre site web)
  - iv) ou est-ce que le traitement visé est une obligatoire pour remplir une obligation légale ? (par exemple traitement d'un don en vertu d'une règle fiscale)
- Informations des personnes concernées
- destinataires des données (l'association, les autres membres, un fournisseur, un partenaire, un sous-traitant informatique, un fournisseur de cloud, etc.)
- la durée de conservation de ces données
- le cas échéant les transferts de données vers un pays tiers (par rapport à l'UE) ou à une organisation internationale (si par exemple vous êtes une antenne locale)
- les mesures de sécurité organisationnelles et techniques

5. La mise en conformité (10)

DOCUMENTATION DE BASE A METTRE EN PLACE (SUITE) – LE REGISTRE (SUITE)

Le RGPD indique que la tenue d'un registre ne serait pas obligatoire pour votre association SI les conditions **CUMULATIVES** suivantes sont réunies :

- Moins de 250 employés ! (condition toujours remplie)
- Aucun risque pour les droits et libertés des personnes concernées
- Traitement **occasionnel** (non répétitif)
- Aucun traitement de données sensibles ou de données relatives à des condamnations pénales et infractions sous article 10 du RGPD (majoritairement le cas)

Toutes les associations ou presque doivent établir un tel registre car, pour les traitements de données qui ont un caractère **répétitif** (sont visées par exemple la mise à jour de la liste des membres, la gestion des cotisations, l'actualisation du site internet, etc.), la tenue d'un tel registre est **obligatoire**.

De plus, comme vu précédemment, la tenue d'un tel registre est un élément clé de votre mise en conformité et vous permet de gérer au mieux au fil de l'eau votre conformité.

Vous trouverez plein d'exemples de registres sur le Net.

5. La mise en conformité (11)

DOCUMENTATION DE BASE A METTRE EN PLACE (SUITE) – LA POLITIQUE DE PROTECTION DES DONNÉES

C. Politique de protection des données

Il vous faut également rédiger une politique de protection des données(ou charte vie privée ou politique de confidentialité, peu importe son appellation) que vous mettrez à disposition de toutes les personnes concernées en la faisant figurer de manière claire sur votre site ou dont vous enverrez un exemplaire avec tout formulaire à remplir, selon le choix de votre association.

Cette politique devra reprendre les points suivants :

- 1. l'engagement de l'association à respecter la vie privée eu égard au RGPD
- 2. ses valeurs et sa gestion des données personnelles
- 3. une clause d'acception générale de la politique: exemple :

  « En acceptant la présente politique, en utilisant nos services, en s'enregistrant à un événement de l'association ou en nous fournissant d'une quelconque autre manière vos données à caractère personnel, vous reconnaissez et accepter les termes de la présente politique ainsi que les traitements et transferts de données à caractère personnel qui seront réalisés conformément à la présente politique. »

  Vous pourrez également insérer dans le formulaire de contact/adhésion/inscription à un événement des cases à cocher (« opt-in ») pour des points particuliers comme l'adhésion à l'envoi d'une newsletter par exemple ou encore autorisation pour figurer sur un annuaire des membres).

- 4. Le responsable du traitement

  L'association est en principe le responsable du traitement. Vous ajouterez les coordonnées de contact ou vous renverrez à la rubrique contact de votre site internet. Vous pouvez indiquer une adresse email générique ou nominative.

5. La mise en conformité (12)

DOCUMENTATION DE BASE A METTRE EN PLACE – LA POLITIQUE DE PROTECTION DES DONNÉES (SUITE)

- 5. Les catégories de données personnelles collectées
- 6. Utilisation ou non de cookies : en fonction de l'existence ou non de ces cookies, vous indiquerez alors l'existence d'un pop-up lors de la visite du site de l'association
- 7. Les finalités du traitement
- 8. La base juridique ou licéité du traitement
- **9. Les droits des personnes concernées**
- 10. La durée de conservation des données
- 11. La possibilité d'une réclamation auprès de la CNPD en indiquant clairement les coordonnées de celle-ci
- 12. La sécurité – mesures organisationnelles et techniques
- 13. La communication éventuelle des données à des tiers
- 14. Le transfert éventuel des données vers des pays tiers par rapport à l'Espace Economique Européen
- 15. Mise à jour de la politique
- 16. Mesures en cas d'incident ou de violation des données

DOCUMENTATION DE BASE A METTRE EN PLACE – LA POLITIQUE DE PROTECTION DES DONNÉES (SUITE)

Arrêtons-nous quelques instant sur le point 9 relatif aux droits des personnes concernées.

Le RGPD met l'accent sur les droits de la personne concernée; votre association doit permettre à toute personne concernée de pouvoir faire valoir ses différents droits sur ses données personnelles auprès de votre association.

Vous devez reprendre ces droits dans votre politique de protection des données et en expliquer le contenu :

- **Droit d'accès** permet de demander quelles données personnelles sont détenues par l'association et demander une communication de celles-ci afin d'en vérifier le contenu.
- **Droit de rectification** permet de demander la rectification des informations inexactes ou incomplètes.
- **Droit à l'effacement** (« droit à l'oubli ») permet de demander à l'association l'effacement des données personnelles.
- **Droit à retirer le consentement** : le retrait ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait – ce retrait peut se faire par « *opt-out* » par exemple en prévoyant une case à décocher sur l'espace personnel de connexion/adhésion du membre.

5. La mise en conformité (14)

DOCUMENTATION DE BASE A METTRE EN PLACE – LA POLITIQUE DE PROTECTION DES DONNÉES(SUITE)

- **Droit à la limitation du traitement** permet de demander à l'association de geler temporairement l'utilisation de certaines données.
- **Droit d'opposition** permet à tout moment de s'opposer à ce que l'association utilise certaines des données personnelles.
- **Droit de soumettre une plainte** à la CNPD en cas d'insatisfaction – l'association doit indiquer les coordonnées de celle-ci.
- [**Droit à la portabilité** : dans le cadre d'une association pas applicable car permet de récupérer les données fournies sous un format lisible et transférable facilement vers une autre organisation – sans objet et disproportionné.
- **Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage** – pas applicable à un environnement associatif – il s'agit de collecter et d'analyser vos activités sur le site de l'association ou via des sites partenaires pour permettre de construire des profils pour mieux cerner la personnalité ou les comportements des personnes concernées et pouvant entraîner des décisions automatiques à partir de ce profilage sans l'intervention d'un humain.]

5. La mise en conformité (15)

DOCUMENTATION DE BASE A METTRE EN PLACE – REDACTION DE PROCEDURES

Votre association doit se doter d'une ou plusieurs procédures pour assurer sa conformité au RGPD. Ici encore le principe de proportionnalité doit s'appliquer au regard une fois encore de la taille, des activités, des ressources en personnel, de la présence ou non de bénévoles, etc.

Exemples: procédure sur le recrutement des bénévoles, procédure sur le recrutement de personnel, procédure sur les mesures de sécurité des outils et accès informatiques,...

Il appartient à l'association de revoir à intervalles réguliers sa politique et ses procédures pour qu'elles reflètent à tout moment la réalité des activités, des finalités et des traitements, de l'organisation interne.

6. INCIDENCES PRATIQUES

TENUE D'UNE BASE DE DONNÉES

ATTENTION : les principes qui suivent peuvent également s'appliquer à d'autres cas pratiques que nous examinerons par la suite.

- Vous ne devez saisir dans la base et ne traiter que les données personnelles strictement nécessaires à la poursuite de la finalité.
- Vous devez sécuriser cette base de données contre les pertes ainsi que contre les attaques externes et le vol de données.
- Vous devez pouvoir en authentifier les utilisateurs (si évidemment plusieurs personnes y ont accès) - Avec une mise en place par exemple d'une gestion efficace des droits d'accès avec un traçage éventuel si envisageable et une gestion des incidents liés à des accès non autorisés, – toujours au regard de l'application du principe de proportionnalité par rapport à l'association !
- Vous devez également sécuriser les postes de travail et l'informatique mobile, sécuriser le ou les serveurs, sécuriser votre site web.
- Vous devez assurer la sauvegarde et la continuité de votre base (back-up).
- Vous devez disposer d'un outil de conservation et d'archivage des données.
- Vous devez pouvoir encadrer éventuellement la maintenance et la destruction des données si vous ne le faites pas vous-même.
- Vous devez sécuriser les partages avec d'autres fournisseurs et partenaires.
- Vous devez gérer la sous-traitance IT, le choix d'un cloud, etc.
- Vous devez protéger l'accès physique à vos bureaux.

6. INCIDENCES PRATIQUES (2)

LES ÉCHANGES ET PARTAGES DE CONTACTS

- Vous pourriez devoir confier un fichier contenant des données personnelles de vos membres à un fournisseur externe pour la prestation de certains services :

  Exemple: à un imprimeur qui, en plus de produire un ou plusieurs documents, pourrait se voir confier la gestion du mailing sur base du fichier partagé.

- Votre association reste responsable de s'assurer que les données partagées seront traitées en conformité avec le RGPD en ce compris leur conservation ou destruction.
- Il vous appartient donc de choisir avec soin vos sous-traitants, choisissez-les en Europe par préférence et précisez les devoirs et obligations sous le RGPD dans un contrat écrit.
- Il existe des modèles de clause ou de contrat sur le Net ou sur le site des autorités nationales en charge. Les reprendre, c'est vous protéger.
- Concernant le fichier comme tel, il doit respecter également les principes vu ci-avant pour la tenue de la base des données .

6. INCIDENCES PRATIQUES (3)

ENVOI DE COURRIERS POSTAUX ET COURRIELS ÉLECTRONIQUES Y COMPRIS À CARACTÈRE PUBLICITAIRE

Il faut considérer les données collectées **avant** le 25 mai 2018 (pour rappel date d'entrée en vigueur du RGPD) et **après** cette date (nouveaux adhérents, membres ou donateurs).

- Si votre association envoyait déjà des newsletters, des appels aux dons avant l'entrée en vigueur du RGPD, vous ne devez pas demander de la part de vos membres/adhérents existants avant le 25 mai 2018 un consentement express.
- Depuis le 25 mai 2018, vous devez veiller à indiquer clairement les traitements effectués par votre association en lien avec l'exigence d'un consentement positif. Par le biais d'un formulaire papier ou plus facile, par le biais d'un formulaire de contact en ligne sur lequel vous auriez ajouté une case à cocher pour un consentement positif « *opt-in* » exprès de la part de vos membres/adhérents.
- Le plus aisé est de prévoir autant de cases à cocher qu'il n'y a de traitements envisagés (une case pour l'envoi d'une newsletter, une case pour la mention du nom de l'adhérent dans un annuaire, une case pour recevoir les invitations aux événements de l'association voire d'associations partenaires, une case pour l'envoi automatique de matériel pour un appel aux dons, etc.).
- Par ailleurs, vous devez permettre que l'adhérent/membre puisse à tout moment se désinscrire de toute newsletter, site, envoi de courrier sans difficulté et accéder à sa volonté de voir ses données effacées le cas échéant.
- **! La seule exception** à cette obligation de prévoir un consentement positif concerne l'envoi d'un **courrier toutes boîtes**.
- En fonction du nombre d'adhérents/membres et des moyens financiers de votre association, il est plus facile de tenir un fichier de ceux-ci à jour en ligne et de vous assurer de la collecte de leur consentement exprès tel que décrit ci-avant.

6. INCIDENCES PRATIQUES (SUITE)

LA CONSERVATION ET LA DIFFUSION DE PHOTOS

Le RGPD considère qu'une photographie d'une personne est une donnée personnelle.

Vous faites face à deux droits :

- le droit à l'image (visé dans la loi luxembourgeoise du 11 août 1982 sur le respect à la vie privée) pour lequel un consentement tacite/présumé pour une prise de vue dans un lieu privatif est suffisant **SI** les photos sont prises au vu et au su des participants. La diffusion ultérieure des photos est également permise.
- le droit à la protection des données personnelles qui requiert en principe un consentement explicite sauf si vous pouvez vous baser sur une autre légitimation que le consentement comme par exemple la poursuite « d'intérêts légitimes » de l'association:

Exemple : un événement culturel, une manifestation sportive avec un article dans un média ou encore une publication de photos d'un événement sur le site web de l'association (avec accès de connexion réservé ou non aux membres).

6. INCIDENCES PRATIQUES (SUITE)

LA CONSERVATION ET LA DIFFUSION DE PHOTOS (SUITE)

- Avant de prendre une photo ou une vidéo d'une personne, vous devez lui demander son autorisation. Attention son acquiescement pour être prise en photo ne veut pas dire qu'elle consent automatiquement à la diffusion ultérieure de celle-ci. Il y a donc 2 consentements distincts à rechercher dans ce cas: son accord pour la prise de vue et son accord sur la diffusion.
- Assurez-vous de toujours avertir les participants (adhérents ou non) à un événement que vous allez prendre des photos et que vous allez éventuellement utiliser les photos.
- Vous pouvez recueillir le consentement des participants en mettant à disposition une liste de présence avec une case à cocher pour la publication ultérieure ou le faire lors de l'inscription à l'événement, en ligne.
- S'il s'agit de mineurs, ce sont aux représentants légaux à donner leur consentement préalable.
- La jurisprudence différencie entre les **photos ciblées** et **les photos non-ciblées**. Les photos ciblées sont celles dans lesquelles une personne est le sujet principal, en y figurant seul, en y étant mise en avant ou en y prenant une pose. Le fait de prendre la pose face à un objectif induit un consentement implicite par contre ne sous-tend pas un consentement sur sa diffusion.
- Les photos non-ciblées reflètent l'ambiance générale sans avoir une ou plusieurs personnes en tant que sujet principal. Il suffit lors d'événements publics d'en informer les personnes concernées (manifestations sportives, spectacles culturels, marchés de Noël, etc.) par exemple par le biais des conditions générales de l'événement (sur le site web de l'association, sur le formulaire d'inscription à l'événement, sur un billet d'entrée ou par un affichage approprié, visible, incontournable sur place le jour de l'événement.

6. INCIDENCES PRATIQUES

LA CONSERVATION ET LA DIFFUSION DE PHOTOS (SUITE)

Conseils :

- Si vous n'avez pas recueilli le consentement explicite pour la publication, évitez la publication ou alors floutez le visage de la personne.
- Si vous prenez des photos de l'ambiance générale, vous n'avez pas besoin de recueillir un consentement explicite ni sur la prise de vue ni sur la diffusion ultérieure mais si la photo est ciblée sur la personne, veuillez à recueillir son consentement pour la prise de vue(sauf si la personne prend la pose et se sait photographiée (consentement tacite)) et pour la diffusion.
- S'il s'agit d'un enfant, il faut absolument obtenir un accord si possible écrit des parents/tuteurs lors de l'événement au plus tard.

6. INCIDENCES PRATIQUES

GESTION DU SITE INTERNET DE L'ASSOCIATION

- La politique de protection des données doit y être facilement accessible.
- Les coordonnées de contact de l'association doivent l'être également.
- Si vous renvoyez sur votre site à lien accédant à un annuaire des membres de l'association, ou que vous reprenez la liste des membres fondateurs ou des donateurs particuliers, vous devez avoir recueilli leur agrément préalable.
- Si vous mettez un formulaire de contact/d'adhésion en ligne, vous devez appliquer toutes les mesures de sécurité énoncées plus haut en renvoyant bien entendu à la politique de protection des données et en recherchant le consentement exprès de l'utilisateur/membre/futur adhérent.
- Concernant la gestion du site, vu que l'association est responsable de sa conformité des mesures techniques mises en place, elle doit veiller à sécuriser ce site contre toute cyber attaque, vol de données accessibles en se rapprochant éventuellement d'un des très nombreux prestataires disponibles sur la Place du Luxembourg pour la conception ou un audit.

6. INCIDENCES PRATIQUES

LE TRAITEMENT ET LA CONSERVATION D'INFORMATIONS SENSIBLES

- Certaines données personnelles sont en plus dites **sensibles** quand elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés : une opinion religieuse, politique, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des données philosophiques.
- Si vous deviez, au sein de votre association, traiter de données sensibles, vous devriez prendre en considération les risques liés aux droits et libertés des personnes physiques (respect de la vie privée mais aussi respect de la liberté d'expression, de la liberté de pensée, de conscience et de religion, interdiction de discrimination et droit à la liberté de mouvement.
- **PRINCIPE: interdiction de de collecter et d'utiliser des données personnelles sensibles.**
- Exceptions: vous en avez le droit uniquement dans les cas prévus par le RGPD ((10 exceptions existent) :

  - la personne concernée a donné son consentement écrit, clair et spécifique au traitement de ses données.

  - le traitement est effectué, dans le cadre de vos activités légitimes et moyennant les garanties de sécurité appropriées, par votre **association qui poursuit** une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres ou aux personnes entretenant avec vous des contacts réguliers en lien avec vos finalités et que les données à caractère personnel ne soient pas communiquées en dehors de votre association sans le consentement des personnes concernées.

6. INCIDENCES PRATIQUES

LE TRAITEMENT ET LA CONSERVATION D'INFORMATIONS SENSIBLES (SUITE)

- le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

- le traitement porte sur des **données à caractère personnel qui sont manifestement rendues publiques par la personne concernée.**

- le traitement est nécessaire aux fins de l'exécution des obligations en **matière de droit du travail, de la sécurité sociale et de la protection sociale**.

- le traitement est indispensable dans un cadre médical .

- D'un point de vue juridique, il faut être très rigoureux dans l'appréciation de ces conditions et faire attention au consentement explicite des personnes qui doit vraiment être justifié par un écrit dont il est nécessaire de conserver la trace ensuite.
- Si vous avez cerné votre exception, il sera ensuite important de la documenter – pour pouvoir démontrer que le RGPD est bien respecté.
- Si vous opérez le traitement de données sensibles, il est indispensable de sensibiliser vos collaborateurs car les risques de contentieux autant que de sanctions sont réels.
- Il est également nécessaire que vous preniez des mesures techniques supplémentaires pour protéger ces données personnelles sensibles. Cela passe notamment par une pseudonymisation des données ou par leur chiffrement fortement recommandés.

6. INCIDENCES PRATIQUES

LA CONSERVATION ET L'ARCHIVAGE DES DONNÉES

- PRINCIPE: votre association ne peut conserver de données personnelles au-delà de la fin de leur traitement sauf certaines exceptions comme pour les données relatives à la gestion de son personnel.
- Exemple : si un membre résilie son adhésion, vous ne pouvez garder de données personnelles le concernant sauf à lui demander son consentement personnel par exemple pour qu'il continue à figurer dans un annuaire comme ancien membre ou si l'intérêt légitime de l'association prévaut (victoires passées, événements culturels, sportifs ou autres, etc.).
- Les délais d'archivage doivent s'évaluer au cas par cas: autre exemple: concernant les données d'un salarié de l'association, vous avez l'obligation de conserver ses données au-delà du traitement effectué: après son départ, 5 ans minimum voire 10 ans en vertu de certaines lois applicables.
- L'archivage pour des intérêts légitimes pourrait vous amener à conserver sur des durées bien plus longues les archives de toutes vos activités passées: photos d'événements passés, vidéos, newsletters.
- Comment pouvez-vous assurer la sécurité des données personnelles de votre personnel, adhérents, fournisseurs, partenaires) que vous conservez? Le volet sécurité est étroitement lié à celui de la conservation et de l'archivage.
- C'est un volet très personnel à chaque association en fonction de son réseau informatique, de ses ressources financières et de sa taille.
- Quels sont les supports qui abritent les données :

  supports matériels : serveur, ordinateur portable, disque dur

  logiciels : système d'exploitation, logiciel choisi

  canaux de communication : wifi, internet, cloud

  support papier: photocopie

- Un bon outil de conservation est un outil qui permet de ne pas altérer les données, de ne pas permettre leur modification de manière indue et de les protéger contre le vol, la perte.
- Vous devez également instaurer des réflexes au sein de votre structure comme par exemple mettre à jour votre antivirus de manière régulière, changer vos mots de passe pour éviter usurpation/intrusion, destruction malveillante. Vous devez également vous assurer de copies de back-up régulières, limiter la connexion de supports mobiles à l'indispensable (clé USB).

6. INCIDENCES PRATIQUES

QUE FAIRE EN CAS DE VIOLATION DES DONNÉES?

- Si votre association pense que son site internet ou sa base de données a été piratée ou si un collaborateur s'est fait voler son ordinateur, il faut notifier le fait à la CNPD dans les 72H qui suivent le moment du constat. Et si l'attaque ou la perte est susceptible d'entraîner un risque pour les droits et libertés des personnes dans la base des données, il faut en avertir la CNPD.
- Il vous faudra évaluer l'impact : quel type d'incident survenu, la nature, la sensitivité et le volume des données personnelles, la facilité d'identification des personnes, la sévérité des conséquences pour les personnes, le nombre des personnes concernées, les caractéristiques spéciales de ces personnes.
- Un incident ne déclenche pas automatiquement une sanction administrative car la CNPD prendra en compte les mesures techniques et organisationnelles mises en œuvre mais par contre la non-notification d'un incident est un critère aggravant ; la CNPD tiendra compte de la manière dont elle a été informée, par qui et comment.
- Il existe sur le site de la CNPD un formulaire de notification pour la violation des données à utiliser ainsi que les instructions à suivre.
- Il faudra documenter la violation en indiquant les faits, ses effets et les mesures prises pour y remédier et ce, de manière proactive et répertorier cette violation dans le registre des incidents à tenir par l'association. Ce registre doit être disponible en tous temps sur demande de la CNPD ;
- Si la violation notifiée ne comporte pas de risque pour les personnes concernées, il n'y aura pas d'autres démarches exigées comme une communication aux personnes concernées.

QUE FAIRE EN CAS DE VIOLATION DES DONNÉES?

Par contre, si la violation emporte un risque élevé en termes de risques pour les droits et libertés des personnes, vous devez communiquer la violation de leurs données aux personnes concernées en des termes clairs et simples en leur donnant la possibilité de se protéger (par exemple en leur demandant de changer de mot de passe, de prévenir les proches, de bloquer une carte bancaire ou d'avertir leur banque, etc.)

Conclusion :

- Si violation: voir le risque pour les droits et libertés des personnes: si le risque existe alors
  - si risque non élevé, juste faire une notification à la CNPD car toute violation doit être enregistrée mais pas besoin de communication aux personnes concernées
  - si risque élevé, notification à la CNPD + notification aux personnes concernées
- Si l'association sous-traite et que le sous-traitant traite des données personnelles à son tour, il doit bien évidemment notifier à l'association toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance.
- Une violation de données personnelles a des répercussions possibles sur la réputation de votre association, sur la vie privée de personnes qui vous ont accordé leur confiance voire un impact financier. Il vaut mieux prévenir que guérir et devoir faire face i) aux médias, ii) à une sanction éventuelle de la part de la CNPD voire iii) d'une action en justice à l'encontre de l'association et/ou de son responsable.

CONCLUSION

- Comme nous l'indiquions dans notre avant-propos, l'objectif de la CNPD est avant tout d'accompagner toute association dans sa mise en conformité.
- Nous vous invitons à consulter régulièrement le site luxembourgeois de la CNPD. Celle-ci a publié entre autres un guide pour le monde associatif auquel vous pouvez vous référer comme outil de base pour vous assurer de la conformité de votre association au RGPD.
- Vous avez l'obligation de vous doter de mesures organisationnelles et techniques. La protection des données personnelles et de la vie privée de vos membres, collaborateurs, bénévoles, fournisseurs ; partenaires doit constituer une priorité et un réflexe dans la conduite de vos activités.

F&A

QUESTIONS ?

F&A

MERCI POUR VOTRE ATTENTION !

CONTACTS

F&A

GENÈVE

Rue de la Cité, 27
CH-1204 Genève

Tel : (+41) 225 520 775
Fax : (+41) 225 520 776

www.feltenlawyers.com

LUXEMBOURG

Rue J.P. Brasseur, 2
L-1258 Luxembourg

Tel : (+352) 45 77 45-1
Fax : (+352) 45 75 05

www.feltenlawyers.com