France générosités

Mémento sur la mise en pratique du Règlement Général sur la Protection des Données personnelles

POUR LES ORGANISATIONS FAISANT APPEL À LA GÉNÉROSITÉ DU PUBLIC

Avertissement

Ce document constitue une aide à la mise en place des mesures de protection des données personnelles. Il ne s'impose pas aux organismes qui conservent la liberté de choix de politique interne.

La responsabilité de France générosités ne pourra pas être engagée en cas de contrôle par la CNIL. Par ailleurs, ce document n'a pas le caractère de code de conduite au sens de l'article 55 du RGPD, il n'est donc pas opposable à la CNIL.

France générosités

Sommaire

Vocation

Ce document découle des travaux menés au sein du groupe du travail “protection des données personnelles” de France générosités qui a été créé en octobre 2015. Il poursuit un double objectif :

- Aider chacun des organismes membres de France générosités à définir une politique de protection des données
- Accompagner chacun des organismes membres de France générosités dans une démarche de conformité au regard du cadre règlementaire français et européen. En particulier au regard du Règlement Européen dit Règlement Général sur la Protection des Données Personnelles (RGPD) adopté le 27 avril 2016, entré en vigueur le 25 mai 2018 et de la loi n° 2018-43 du 20 juin 2018 et de son décret d’application n° 2018-687 du 3 août 2018 qui ont modifié la loi Informatique et Libertés et son décret d’application
- Mettre en avant les caractéristiques des organismes faisant appel à la générosité du public et interpréter les règles de la protection des données à la lumière des spécificités du secteur caritatif

Ce document qui identifie un certain nombre de bonnes pratiques pourra constituer un point de départ pour les organismes faisant appel à la générosité du public dans leur mise en conformité avec les exigences du RGPD puisqu’il analyse les principales questions découlant des opérations de fundraising qui peuvent être menées. Il s’agit d’une première version qui sera par la suite nourrie de la pratique de chaque organisme.

Il faut toutefois souligner que le RGPD a vocation à s’appliquer dans de nombreux autres domaines qui ne sont pas étudiés dans le cadre du présent document (données des salariés, données des bénévoles, etc.).

Remerciements

Nous tenons à remercier les membres de France générosités qui ont nommé des personnes et mobilisé des ressources afin de participer à la réalisation de ce document.

Nous désirons également remercier l'ensemble des membres de France générosités qui ont su alimenter, par leurs observations et recommandations, les réflexions menées au sein du groupe de travail mis en place par France générosités.

Plus particulièrement, nous adressons tous nos remerciements à l'attention de ceux et celles qui ont participé à la préparation et la rédaction de ce mémento dans le cadre du groupe de travail.

Le groupe de travail se compose à la date de publication de ce guide de :

- **Laura Jennifer ANGULO QUINTANA**, Juriste, Action contre la Faim
- **Virginie BALLIF**, Juriste, Fondation de France
- **Xavier BERTIN**, Contrôle interne et relation donateurs, Fondation Arc
- **Anne-Lise BLANC**, Juriste, La SPA
- **Sandrine BLANCHARD**, Coordinatrice fédérale du fundraising, Handicap International
- **Vanessa BOUGEARD**, Chargée de marketing, Institut Curie
- **Emilie COLLENOT**, Juriste Secours Catholique
- **Blandine CONTAMIN-PAVLOVIC**, Juriste – CIL, Médecins du Monde
- **Typhaine DELEMER**, Risk and quality manager, AFM Telethon
- **Sophie EA**, Auditrice interne – CIL, UNICEF France
- **Frédérique FONTAINE**, Juriste, Institut Curie
- **Christine GOUDAL**, Responsable marketing, Institut Pasteur
- **Serge HATCHWELL**, Auditeur interne, AIDES
- **Liliane HOFFMANN**, Responsable Unité Études et Conseils, Secours Catholique
- **Caroline JOGUET**, Juriste, AIDES
- **Ann Sophie de JOTEMPS**, Responsable juridique et fiscal, France générosités
- **Didier KAMINER**, Bénévole, Secours Catholique
- **Pierre MICHAUT**, Chargé de projets Système d'Information – Logistique, Solidarités International
- **Sylvie MORIN-MIOT**, Directrice adjointe de la collecte de fonds privés, Médecins Sans Frontières
- **Laurence MORTIER**, Directrice Marketing et Collecte Grand Public, Handicap International
- **Céline PETIT**, Juriste, Institut Curie
- **Farid TAI**, Ancien Responsable juridique et fiscal, France générosités
- **Emilie TRAN**, Responsable juridique – CIL, Action contre la Faim
- **Igor VERSTEEG**, Chargé de conformité RGPD, Secours Catholique
- **Marion WIGISHOFF**, Chargée de mission, Fondation de France

Définitions - notions fondamentales

- **Accountability** : obligation pour un organisme responsable de traitement de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer à l'autorité de contrôle qu'il se conforme à ses obligations en matière de protection des données personnelles.
- **Comité européen de la protection des données (CEPD)** : a été institué par le RGPD, son rôle principal est de contribuer à l'application cohérente du Règlement général sur la protection des données. Il conseille la Commission européenne, en particulier sur le niveau de protection offert par les pays tiers ou les organisations internationales, et promeut la coopération entre les autorités nationales de surveillance. Il émet également des lignes directrices, des recommandations et des déclarations sur les meilleures pratiques. Il a vocation à prendre la suite du G29.
- **Délégué à la Protection des Données (DPD) ou Data Protection Officer (DPO)** : personne en charge de la protection des données personnelles et du respect de la réglementation relatives à ces données au sein d'une organisation. Fonction rendue obligatoire, dans certains cas, par le RGPD, il documente les traitements de données personnelles et veille à la réalisation des analyses de risques et des études d'impacts. Il est l'interlocuteur privilégié en cas de violation de données personnelles. Le DPD a vocation à remplacer le CIL (Correspondant Informatique et Libertés) dans le cadre du RGPD.
- **Donnée à caractère personnel** : toute information relative à une personne physique permettant de l'identifier directement ou indirectement. Par exemple, nom, numéro de téléphone, date de naissance, montant du don, adresse IP, adresse email, coordonnées bancaires, numéro de sécurité sociale, etc.
- **Donnée sensible** : information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle, les données génétiques, données relatives aux infractions pénales, aux condamnations, etc., les données biométriques, les données comportant des appréciations sur les difficultés sociales des personnes. En principe, la collecte et le traitement de ces données sont interdits. Cependant, dans la mesure où la finalité du traitement l'exige (la collecte de ces données est absolument nécessaire à l'organisme), ne sont pas soumis à cette interdiction les traitements pour lesquels la personne concernée a donné son consentement express. Ne sont pas non plus soumis à cette interdiction les traitements sont effectués dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées.
- **Finalité** : objectif principal des traitements pour lesquels les données personnelles sont collectées. (Exemples de finalité : gestion des donateurs, gestion des testateurs, etc.).
- **Privacy by Design (le respect de la vie privée dès la conception)** : démarche consistant à prendre des mesures visant la protection des droits des personnes dès la phase de conception d'un produit ou d'un service.
- **Privacy by default (le respect de la vie privée par défaut)** : démarche promue par le RGPD, liée au principe de responsabilisation des entreprises, qui correspond à la garantie par défaut d'un niveau maximal de protection des données.
- **Profilage** : toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant sa situation économique, sa santé, ses préférences ou centres d'intérêt, sa fiabilité ou son comportement, sa localisation et ses déplacements.
- **Registre** : document comportant la liste des traitements mis en œuvre. Les éléments que doit comporter ce document sont : le nom et les coordonnées des différents acteurs ; les finalités du traitement ; la description des catégories de personnes concernées ; la description des catégories de données ; la description des catégories de destinataires ; le transfert de données personnelles ; la description des mesures de sécurité adoptées ; les délais prévus pour l'effacement des différentes catégories de données.

- **Responsable de traitement (RT)** : personne ou organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel, et qui est tenue de s'assurer que le traitement est effectué conformément aux dispositions légales et règlementaires. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal. Le respect de la protection des données, ainsi que la gestion du droit à consultation, rectification et suppression desdites données ou encore la documentation du registre des traitements relèvent donc de la responsabilité du responsable du traitement et, le cas échéant, du sous-traitant.
- **Sous-traitant (ST)** : personne physique ou morale, service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Le respect de la protection des données relève donc de la responsabilité du responsable du traitement et, le cas échéant, du sous-traitant.
- **Traitement de données à caractère personnel** : toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé, en numérique ou sur papier, (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, etc.).
- **Violation des données** : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel, ou l'accès non autorisé à de telles données.

Sigles - abréviations

- **CNIL** : Commission Nationale de l'Informatique et des Libertés
- **DPD** : Délégué à la protection des données
- **DPO** : Data protection officer
- **AIPD** : Analyse d'impact sur la vie privée
- **PIA** : Privacy impact assessment
- **CEPD** : Comité européen de protection des données
- **LIL** : Loi informatique et libertés
- **RGPD** : Règlement général relatif à la protection des données
- **RT** : Responsable du traitement
- **ST** : Sous-traitant

Qu'est-ce que le RGPD ?

Le règlement général relatif à la protection des données est un règlement européen qui est entré en application en France le 25 mai 2018. Il a pour but de renforcer les droits et libertés des personnes en leur assurant une meilleure protection dans la façon dont leurs données personnelles sont utilisées par les organisations (consolidation des obligations d'information, restrictions en termes de recueil de consentement, nouveau droit à la portabilité des données, à l'effacement, etc.).

QUELLES SONT LES NOUVEAUTÉS DU RGPD ?

- Renforcement des droits et libertés des personnes
- Responsabilité autonome de l'organisme et coresponsabilité du sous-traitant
- Obligations renforcées en termes de sécurité
- Obligations renforcées de notification des violations de données, à la CNIL voire aux personnes concernées
- Privacy by design / by default : respect de la vie privée dès la conception d'un traitement / « minimisation des données »
- Renforcement des sanctions : des amendes administratives variant 10 millions à 20 millions d'euros selon la durée, la nature et la gravité de la violation. Peuvent également être prévues des sanctions pénales
- Désignation d'un DPD élargie et obligatoire dans certains cas
- Obligations du responsable de traitement en remplacement des formalités déclaratives auprès de la CNIL :
  - identifier les risques associés aux opérations de traitement et prendre les mesures nécessaires à leur prévention
  - cartographier ou faire un inventaire des traitements de données personnelles ; établir un registre des traitements sur la base de cet inventaire
  - évaluer les pratiques et mettre en place des procédures : notification des violations de données, gestion des réclamations et des plaintes, gestion des demandes de modifications des données, archivage et conservation des données
  - maintenir une documentation assurant la traçabilité des mesures

Partie 1
Les grandes étapes pour organiser la mise en conformité

Étape n°1
Mettre en place des actions générales pour documenter la conformité

- Établir une liste de traitements de données
- Tenir un registre des traitements (Article 30)

1. Cartographier les traitements de données personnelles

Dans le cadre du RGPD, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du RGPD sur leur activité et de répondre à ses exigences, **les organismes doivent au préalable recenser précisément :**

- les différents traitements de données personnelles ;
- les catégories de données personnelles traitées ;
- les finalités poursuivies par les opérations de traitements de données ;
- les acteurs (internes ou externes) qui traitent ces données, notamment les prestataires et sous-traitants ;
- les flux, en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union Européenne ou des pays ayant un niveau de protection adéquat.

La liste des traitements de données devra être établie par finalité principale (et non par outil ou applicatif utilisé).

Exemple

Vous trouverez ci-après des exemples de finalité principale qui peuvent être établis au sein d'un organisme faisant appel à la générosité du public :

Gestion et sollicitation du donateur | Gestion de la relation avec les potentiels testateurs | Gestion de la relation avec les testateurs déclarés | Gestion des fournisseurs | Gestion et suivi du processus de création et de vie des fondations sous égide | Gestion et suivi du processus de traitement des libéralités | Gestion et suivi du processus de traitement des biens immobiliers

La liste donnée en exemple ci-dessus est à établir au cas par cas en fonction de chaque organisme.

2. Mettre en place un registre et documenter les procédures

Le RGPD prévoit que chaque organisme doit tenir un registre des traitements effectués sous sa responsabilité (Article 30). Ce registre comporte une liste d'informations très élargie. La cartographie doit vous permettre d'établir ensuite un registre plus précis.

Il est recommandé d'utiliser le modèle de registre mis en ligne par la CNIL dont la fiche ci-après s'inspire (cf. Annexe 1 Modèle de registre CNIL).

MODÈLE DE FICHE À PORTER AU REGISTRE		
Traitement n°1	**Gestion et sollicitation des donateurs**	
Nom et adresse du responsable du traitement	Association [•] 118 Rue [•] - 75000 Paris	
Date de mise en œuvre	20/10/2018	
Finalité principale	Gestion de la relation donateur	
Détail des finalités du traitement	• Information des donateurs • Actualisation du profil des donateurs • Prospection caritative • Edition de reçus fiscaux	
Service chargé de la mise en œuvre	Service communication et développement	
Fonction de la personne ou du service auprès duquel s'exerce le droit d'accès	Chargée de communication et développement	
Catégories de personnes concernées par le traitement	L'ensemble des donateurs	
Données traitées	**Catégories de données**	**Détails des données traitées**
	Données d'identification	• Nom et prénom • Adresse postale • Adresse électronique • Numéro de téléphone
	Autres	Date et montant du don
Catégories de destinataires	**Catégories de destinataires**	**Données concernées**
	Les agents habilités de l'association pour les stricts besoins de l'accomplissement de leurs missions	Toutes
Durée de conservation	L'association conserve les données à caractère personnel traitées à l'occasion de la réalisation d'un don pendant la durée nécessaire à la gestion de la relation donateur (à préciser selon les modalités spécifiques propres à chaque organisme / fiche pratique N°2).	
Mise à jour (date et objet)	Néant	

3. Établir une procédure de détection des violations des données personnelles

Dans le cadre du RGPD, l'organisme doit :

- établir une procédure de détection des violations de données personnelles et la réponse à un tel incident (transmission interne en urgence et à l'autorité de contrôle dans les 72 heures) ;
- définir contractuellement des exigences en termes de protection des données avec les sous-traitants informatiques (prestataires ou fournisseurs) et notamment les obligations de notification de faille de sécurité pouvant impacter les données personnelles (cf, annexe IV, modèle de contrat avec un sous-traitant ayant à gérer des données personnelles) ;
- effectuer régulièrement des contrôles ou audits de sécurité des sous-traitants informatiques (vérification des clauses de sécurité, audit technique de sécurité, tests d'intrusion, etc.) ;
- notifier à la CNIL toute violation de données personnelles (RGPD, art. 33).

Je réunis les infos et préviens immédiatement le DPD → Le DPD analyse l'impact → Le DPD notifie à la CNIL dans les 72 heures si l'impact est significatif → Les personnes concernées sont informées, en cas de risques résiduels élevés, en accord avec la CNIL

Étape n°2
Justifier les responsabilités internes en matière de protection des données

- Désignation d'un délégué à la protection des données (Article 37)
- Tenue de procédures écrites et d'organigrammes
- Processus internes / distribution des rôles
- Responsabilités des départements / services

1. Déterminer si l'organisme est dans l'obligation de désigner un Délégué à la Protection des Données (DPD)

Dans le cadre du RGPD, le DPD a vocation à être le véritable « chef d'orchestre » de la protection des données. Il exerce une mission d'information, de conseil et de contrôle interne. La mise en place d'un DPD s'inscrit dans la logique de responsabilisation (accountability) notamment par un changement de culture interne et la mobilisation des compétences internes ou externes (services support, services opérationnels, prestataires).

La désignation d'un DPD est obligatoire dans les trois situations suivantes :

- pour une autorité publique ou un organisme public ;
- pour un organisme dont l'activité de base l'amène à réaliser des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernée ;
- pour un organisme dont l'activité de base l'amène à traiter à grande échelle des données sensibles (origine raciale, opinion politique, etc.) ou relatives à des condamnations pénales et à des infractions.

La cartographie des traitements et le registre établis dans le cadre de la 1re étape permettent de déterminer si votre organisme est dans l'une de ces trois situations. Dans tous les cas, il est recommandé de documenter l'analyse effectuée pour déterminer si un DPD doit ou non être nommé.

Exemple

Pour une association d'intérêt général qui fait appel la générosité du public, outre le cas de traitement de données sensibles, il faut analyser si son activité de base l'amène à réaliser un suivi régulier et systématique à grande échelle des personnes concernées :

- la collecte de dons et le traitement afférent constituent son activité de base,
- ce traitement implique un suivi régulier et systématique des donateurs,
- le traitement de données est « à grande échelle » lorsqu'un certain nombre de critères sont réunis (cf. G29, lignes directrices du 13/12/2016 endossées par le CEPD : nombre d'individus concernés, volume de données et/ou les différentes catégories de données traitées, la durée, la permanence du traitement, l'étendue géographique du traitement).

2. Désigner un pilote de la protection des données

Si votre organisme n'est pas formellement dans l'obligation de désigner un DPD et décide de ne pas désigner de DPD, il reste toutefois fortement recommandé de désigner, à minima, une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au RGPD. Ce pilote constituera un atout majeur pour comprendre et respecter les obligations du RGPD, dialoguer avec l'autorité de contrôle et réduire les risques de contentieux.

Si votre organisme décide de désigner un DPD, celui-ci occupera un positionnement particulier au sein de l'organisation. En effet, il rapporte au niveau le plus élevé du RT, pouvant accéder aux instances décisionnaires : conseil d'administration, direction générale, etc. Il doit avoir accès aux données personnelles et à leurs traitements. Il apprécie concrètement les conditions dans lesquelles les traitements sont mis en œuvre. Il est informé et consulté sur tous les sujets ayant trait à la conformité de l'organisme au RGPD.

FOCUS : QUELLE RESPONSABILITÉ DU DPD EN CAS DE MANQUEMENT OU DE NON-CONFORMITÉ AU RGPD ?

Le DPD a un rôle de conseil, d'alerte, de coordination au sein de la structure et est l'interlocuteur des autorités de contrôle. En cas de poursuites administratives ou pénales envers l'organisme, c'est le représentant légal de la structure qui sera poursuivi et non le DPD.

Pour rappel, les sanctions encourues par le représentant légal des organismes peuvent être administratives (jusqu'à 20 millions d'euros) et/ou pénales. Le dispositif de délégation de pouvoirs n'est pas envisageable à l'égard du DPD.

Étape n°3
Gérer les traitements à risque

- Identifier les traitements de données personnelles à risques
- Conduire les analyses d'impact sur la protection des données lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (Article 35)

1. Évaluer si une étude d'impact sur la vie privée est nécessaire

Une analyse d'impact est un outil destiné à analyser un traitement de données personnelles dans une démarche de *« privacy by design »*. L'EIVP n'est pas obligatoire pour l'ensemble des traitements, mais uniquement pour les traitements présentant « un risque élevé pour les droits et libertés des personnes physiques ».

Le RGPD donne quelques exemples (Article 35 §3) pour lesquels la réalisation d'une étude d'impact est obligatoire, à savoir :

- l'évaluation systématique et approfondie d'aspects personnels, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative,
- les traitements à grande échelle de données sensibles (données de santé, opinions politiques, orientation sexuelle, etc.),
- le traitement à grande échelle de données relatives à des condamnations pénales et à des infractions,
- la surveillance systématique à grande échelle d'une zone accessible au public (notamment la vidéosurveillance).

La cartographie des traitements et le registre établis dans le cadre de la 1re étape permettent de déterminer si votre organisme est dans l'une de ces situations.

La liste mentionnée plus haut n'est pas exhaustive et le G29[1] avait retenu dix critères permettant de déterminer si un traitement est susceptible de présenter des risques élevés pour les droits et libertés des personnes physiques (cf. tableau ci-dessous). Ces critères peuvent être utilement repris.

Le G29 incitait d'ailleurs à la réalisation d'EIVP même dans les cas où il existait des doutes sur son caractère obligatoire, en raison de l'efficacité de cet outil pour démontrer la conformité.

G29 / Critères de détermination des situations à risques élevés

Plus il y a de critères remplis, plus les risques sont potentiellement élevés.

Si au moins deux des critères listés ci-après sont réunis, une étude d'impact s'impose.

Critère n°1 : évaluation ou scoring des caractéristiques d'une personne concernant sa performance au travail, sa situation économique, sa santé, ses préférences personnelles ou ses centres d'intérêts, sa fiabilité ou son comportement, sa localisation ou ses déplacements.

Critère n°2 : décisions automatisées produisant des effets juridiques ou affectant la personne de manière significative de façon similaire. (ex. : risques d'exclusion de la personne)

Critère n°3 : surveillance systématique d'une zone accessible au public.

Critère n°4 : sensibilité des données i.e. catégories particulières de données, données relatives à des infractions ou à des condamnations, données de communications électroniques, données de localisation, données financières, données utilisées à des fins personnelles par la personne concernée (ex. messagerie, application de suivi d'activité ou « life logging ») et dont la divulgation pourrait être perçue comme intrusive.

Critère n°5 : grande échelle (En fonction du nombre de personnes concernées, du volume et de la variété des données, de la portée géographique, du caractère permanent ou récurrent).

Critère n°6 : combinaison ou comparaison de fichiers issus de traitements de finalité différente et/ou mis en œuvre par des RT différents et sans que la personne s'y attende.

Critère n°7 : personnes vulnérables (mineurs, personnes âgées).

Critères n°8 : technologie ou solution innovante (ex. : une application internet qui aurait un impact significatif sur la vie quotidienne et la vie privée de la personne.).

Critère n°9 : transferts de données hors de l'Union Européenne.

1 Pour rappel, le G29 a été remplacé par le Comité européen de protection des données (CEPD), cf Définitions.

Critère n°10 : si le traitement empêche la personne d'exercer ses droits ou d'utiliser un service ou de bénéficier d'un contrat. (ex. : traitement par lequel une banque détecte dans ses bases de données, les personnes susceptibles de bénéficier ou de se voir refuser un prêt.).

FOCUS : PROFILAGE/SCORING ?

L'Article 22 du RGPD précise que « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire ».

Pour une association d'intérêt général qui fait appel à la générosité du public, il faut notamment analyser si son activité l'amène à réunir les conditions cumulatives suivantes : (1) la prise de décisions automatiques (2) produisant des effets juridiques à l'égard d'une personne physique, (3) sur la base d'un profilage (cf Définitions – Notions fondamentales ci-dessus).

Précision : s'il est courant au sein des organismes faisant appel à la générosité du public d'utiliser les techniques de profilage afin de cibler les destinataires d'une campagne d'appel aux dons (la structure réalise un scoring en attribuant des notes sur certains domaines ou elle choisit certains critères comme le montant de don, l'âge, ou le statut professionnel), ces techniques ne sont pas assimilables à du profilage « produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire » au sens de l'Article 22 (Réunion de travail avec la CNIL, 18 juillet 2018).

Pour information, avant l'entrée en vigueur du RGPD, le G29 avait déjà admis dans ces lignes directrices du 3 octobre 2017, revues le 6 février 2018, que dans de nombreux cas, la publicité ciblée en ligne, bien que donnant lieu à une décision entièrement automatisée basée sur le profilage (qui se traduit par le fait d'exposer telle personne à telle publicité plutôt qu'à une autre), n'était pas assortie d'effets affectant les personnes de manière significative.

En conclusion, l'un des points majeurs de discussion réside dans la condition relative aux effets juridiques produits par la décision automatisée ou qui affecte de manière similaire et significative la personne concernée (Article 22). L'appréciation de cette condition doit se faire notamment au regard des éléments suivants :

- le degré d'intrusion du processus de profilage,
- les attentes et souhaits des personnes concernées,
- la manière dont l'annonce est diffusée, ou,
- la vulnérabilité des personnes concernées.

2. Réaliser les études d'impact sur la vie privée

Si l'organisme identifie des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées il doit mener, pour chacun de ces traitements, une EIVP avant la collecte de données et la mise en œuvre du traitement.

L'EIVP permet de :

- bâtir un traitement de données personnelles respectueux de la vie privée,
- apprécier les impacts sur la vie privée des personnes concernées,
- démontrer que les principes fondamentaux du RGPD sont respectés.

Dans une démarche d'accompagnement de la mise en conformité au RGPD, la CNIL met à disposition un logiciel d'analyse d'impact accompagné de différents guides (cf. Annexes 2 et 3). Cet outil ergonomique, disponible en français et en anglais, déroule l'intégralité de la méthode de réalisation d'une EIVP développée par la CNIL.

S'il n'est pas possible de réduire les risques liés au traitement par des mesures appropriées, une consultation de la CNIL est alors obligatoire avant de mettre en œuvre le traitement.

Contenu d'une EIVP

L'étude comprend une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité du traitement, une appréciation des risques sur les droits et libertés des personnes concernées, les mesures envisagées pour traiter ces risques et se conformer au règlement. Elle se déroule en quatre étapes :

1. **Étude du contexte** : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux.
2. **Étude des mesures** : identifier les mesures existantes ou prévues pour respecter les exigences légales et traiter les risques sur la vie privée
3. **Étude des risques** : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée.
4. **Validation** : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

Étape n°4
Justifier de la licéité et de la loyauté du traitement

- S'assurer que seules les données strictement nécessaires à la poursuite de la finalité des traitements sont collectées et traitées
- Identifier la base juridique sur laquelle se fonde le traitement : consentement de la personne, intérêt légitime, contrat, obligation légale, etc.
- Réviser les mentions d'information afin qu'elles soient conformes aux exigences du RGPD (Articles 12, 13 et 14)
- Établir les modalités d'exercice des droits des personnes concernées : droit d'accès, droit de rectification, droit à la portabilité, droit d'opposition, etc. (Articles 15 à 21).

Le RGPD renforce les principes préexistants pour qu'un traitement soit considéré comme légal : finalité, pertinence, loyauté, transparence, durée limitée, sécurité et droits des personnes.

1. Vérifier la base juridique sur laquelle est fondé le traitement (Consentement/Opt-in/Opt-out)

Il convient d'identifier la base juridique de chaque traitement de données personnelles au regard des six motifs suivants (Article 6) :

- le respect d'une obligation légale,
- l'intérêt légitime du responsable de traitement,
- le consentement libre et éclairé,
- l'exécution d'un contrat,
- la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique,
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

En principe, seuls les trois premiers motifs cités ci-dessus ont vocation à s'appliquer dans le cadre des relations de l'organisme faisant appel à la générosité du public avec la personne concernée (donateur, testateurs, etc.).

Un exemple de respect d'une obligation légale : l'émission de reçus fiscaux

Le RGPD prévoit que le traitement de données est licite lorsqu'il est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis (Article 6 b). Ce motif s'applique notamment dans le cadre de l'émission de reçus fiscaux.

En effet, si les organismes d'intérêt général peuvent émettre des reçus fiscaux permettant aux donateurs de déduire 66 ou 75% du montant de leurs dons de leurs impôts, il faut toutefois souligner que l'article L. 14 A du Livre des Procédures Fiscales institue une procédure spécifique de contrôle de la délivrance des reçus fiscaux permettant d'obtenir les réductions d'impôts prévues aux articles 200 (impôt sur le revenu), 238 bis (impôt sur les sociétés) et 978 (impôt sur la fortune immobilière) du Code général des impôts.

Depuis le 1er janvier 2018, l'administration fiscale peut contrôler sur place, dans les locaux de l'organisme que les montants portés sur les reçus correspondent bien aux dons et versements effectués. Les organismes devant alors présenter à l'administration fiscale « les documents et pièces de toute nature » permettant de justifier des dons effectués. Le délai de conservation de ces pièces justificatives a été fixé à 6 années pour l'ensemble des dons et versements effectués.

Un exemple d'intérêt légitime : la prospection caritative

Il est important de souligner que le RGPD ne revient pas sur les pratiques actuelles relatives à l'opt-in et l'opt-out dans le cadre des opérations de prospection, et notamment la distinction entre prospection commerciale et prospection caritative.

En effet, le RGDP prévoit spécifiquement que le traitement de données est licite lorsqu'il *« est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers »* et précise que *« le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime. »* (Considérant 47).

La règle actuelle qui distingue prospection commerciale et prospection caritative reste donc en vigueur.

L'envoi de sollicitations commerciales (Article L.34-5 du Code des postes et des communications électroniques) par voie électronique (mail, sms, mms) suppose bien que les personnes aient explicitement donné leur accord pour être démarchées, au moment de la collecte de leurs coordonnées. Le recueil du consentement doit alors s'exprimer par un

moyen simple comme par exemple une case à cocher à côté de laquelle il est indiqué que la personne est d'accord pour recevoir des opérations de prospection commerciale (opt-in).

Le recueil préalable du consentement n'est pas nécessaire, par exception, lorsque la prospection n'est pas de nature commerciale, ce qui est notamment le cas pour les prospections caritatives menées par les organismes faisant appel à la générosité du public. Dans ce cas, la personne doit simplement, au moment de la collecte des données être informée que ses données seront utilisées à des fins de prospection et être en mesure de s'opposer à cette utilisation de manière simple et gratuite par le biais d'un mail, d'un SMS, d'un courrier par voie postale ou encore par un appel téléphonique. Cela peut également se faire par le biais d'une case à cocher proposée directement sur le formulaire de recueil des données personnelles à côté de laquelle il est indiqué que la personne ne souhaite pas recevoir de la prospection caritative (opt out).

De même, pour la prospection par voie postale, le principe reste celui de l'information préalable et du droit d'opposition. L'envoi de sollicitations par voie postale est donc possible à condition que la personne soit, au moment de la collecte de ses coordonnées, informée de leur utilisation à des fins de prospection et en mesure de s'opposer à cette utilisation de manière simple et gratuite (cf ci-dessus).

En tout état de cause, l'existence d'un intérêt légitime du RT doit être mise en balance avec les intérêts et droits fondamentaux de la personne concernée, car ces derniers peuvent prévaloir sur l'intérêt du RT lorsque des données sont traitées dans des circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur.

Le consentement libre et éclairé en pratique

Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée. La personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

La personne doit être en mesure de refuser ou de retirer son consentement sans subir de préjudice. Enfin, la personne concernée doit avoir une information claire et complète des caractéristiques et modalités du traitement et les documents regroupant plusieurs informations ou questions doivent faire apparaitre distinctement la demande de consentement et ce à quoi elle renvoie (ex. : distinguer les conditions générales d'utilisation et le consentement à un traitement de données personnelles).

Dans un formulaire en ligne, le recueil du consentement pourra se matérialiser, par exemple, par une case à cocher non cochée par défaut (opt-in) ou une confirmation après validation de l'email envoyé.

Le consentement préalable de la personne concernée est notamment requis en cas de collecte de données sensibles (santé, orientation sexuelle, convictions religieuses, etc.) ou de réutilisation des données à d'autres finalités, ou d'utilisation de cookies pour certaines finalités.

Le RT doit être en mesure de prouver que la personne concernée a effectivement consenti à l'opération de traitement (consentement tracé et archivé).

2. Réviser les mentions d'information

Cette étape revient à justifier d'une procédure d'information aux personnes concernées par un traitement de données personnelles les concernant, notamment sur les modalités d'exercice de leurs droits d'accès, de rectification, d'effacement et de limitation du traitement (Article 12 et suivants).

De nouvelles mentions devenant obligatoires avec le RGPD il est nécessaire de réactualiser les mentions d'information figurant sur l'ensemble des supports (bulletins d'adhésion, newsletters, mailings, sites internet, etc.) afin qu'elles soient concises, accessibles, concrètes et compréhensibles (recours à des éléments visuels, icônes ou illustrations si nécessaire).

Contenu des mentions d'information lorsque les données sont collectées directement auprès de la personne concernée (Article 13)

Lors d'une collecte directe auprès d'une personne, les informations suivantes sont à fournir :

a) L'identité et les coordonnées du RT et, le cas échéant, du représentant du RT

b) Le cas échéant, les coordonnées du DPD

c) Les finalités du traitement (prospection caritative, prospection commerciale, etc.)

d) Les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent

e) L'existence d'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale

f) La durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée

g) L'existence et les modalités d'exercice des droits de la personne concernée

h) Le droit pour la personne de se rétracter ou de retirer son consentement au traitement de données sensibles si existant

i) Le droit d'introduire une réclamation auprès d'une autorité de contrôle

j) L'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22

k) Si le RT a l'intention d'effectuer un traitement ultérieur des données à caractère personnel ayant une finalité autre que celle pour laquelle les données ont été collectées

Exemples

Exemples de mentions d'information conforme aux exigences de l'Article 13 (sous réserve de l'interprétation de la CNIL) :

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par [identité et coordonnées du RT] qui dispose d'un délégué à la protection des données : [coordonnées du DPD].

Elles sont destinées à la Direction des relations donateurs et aux tiers mandatés par [identité du RT] à des fins de gestion interne, pour répondre à vos demandes ou faire appel à votre générosité.

Ces données peuvent faire l'objet d'un transfert à des tiers au sein de l'Union Européenne. [A ajouter si votre organisme est concerné : Dans le cadre d'un transfert vers un pays hors Union Européenne, des règles assurant la protection et la sécurité de ces données ont été mises en place. Le détail de ces règles et des informations relatives au transfert est disponible sur simple demande adressée à ...].

Elles sont conservées pendant la durée strictement nécessaire à la réalisation des finalités précitées [À PRÉCISER].

Conformément à la loi « informatique et libertés » et à la règlementation européenne, vous pouvez vous opposer à l'utilisation de vos données à caractère personnel. Vous pouvez également introduire une réclamation auprès de la CNIL.

Vous bénéficiez d'un droit d'accès à vos données pour leur rectification, limitation, portabilité ou effacement, en contactant : [Coordonnées de la personne chargée de cette tâche par le RT].

Ces données peuvent faire l'objet d'un échange avec certains organismes du secteur caritatif. Si vous ne le souhaitez pas, vous pouvez vous y opposer en cochant la case ci-contre : [OPT OUT].

3. Réviser les modalités d'exercice des droits des personnes concernées

Le RGPD précise les droits existants et en crée de nouveaux. Ainsi, la personne dont les données sont traitées dispose des droits suivants :

Droit d'accès (Article 15) : droit d'obtenir la confirmation que les données sont traitées ou non, et si oui, l'accès à ces données.

Droit de rectification (Article 16) : droit d'obtenir, dans les meilleurs délais, que les données inexactes soient rectifiées et que les données incomplètes soient complétées.

Droit à l'effacement (Article 17) : droit d'obtenir, dans les meilleurs délais, l'effacement de ses données lorsque la personne a retiré son consentement au traitement, lorsqu'elle s'y oppose, lorsque les données ne sont plus nécessaires au regard des finalités du traitement, lorsqu'elles ont fait l'objet d'un traitement illicite, ou lorsqu'elles doivent être effacées en vertu d'une obligation légale.

Droit à la limitation du traitement (Article 18) : droit d'obtenir la limitation du traitement notamment lorsque la personne conteste l'exactitude des données, lorsque leur traitement est illicite, ou lorsqu'elle en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice.

Droit à la portabilité (Article 20) : droit de recevoir les données dans un format structuré, couramment utilisé, lisible par machine, et de les transmettre à un autre responsable de traitement sans que le responsable du traitement initial y fasse obstacle, lorsque le traitement est fondé sur le consentement ou sur un contrat, et effectué à l'aide de procédés automatisés.

Droit d'opposition (Article 21) : droit de s'opposer à tout moment au traitement des données, sauf lorsque celui-ci est nécessaire à l'exécution d'une mission d'intérêt public ou aux

fins des intérêts légitimes du responsable du traitement. La personne peut également s'opposer au traitement fait à des fins de prospection.

L'organisme doit définir les modalités d'exercice des demandes d'accès et de rectification

Pour ce faire il faut prévoir une procédure qui explicite :

- la possibilité d'offrir sans frais aux personnes qui en font la demande un accès à leurs données, et à une demande de rectification,
- la possibilité de faire une demande d'accès et de rectification par voie électronique,
- les modalités de réponse aux demandes d'accès, de rectification et d'effacement dans des délais raisonnables,
- les motivations d'un refus à une demande d'accès, de rectification,
- les mesures raisonnables à prendre pour vérifier l'identité de la personne qui demande l'accès à ses données et notamment les précautions nécessaires aux demandes d'accès aux dossiers des légataires/legs concernant des informations sensibles et confidentielles.

L'organisme doit définir une procédure relative au droit à l'effacement et au droit à la limitation

Il faut pour ce faire prévoir une procédure qui permette :

- de répondre dans les meilleurs délais à la personne ayant introduit une demande d'effacement,
- d'exercer le droit à la limitation du traitement des données personnelles, notamment en permettant de répondre à la demande faite par une personne qui s'oppose à de futures sollicitations mais souhaite la conservation de ses données dans le cadre d'un autre traitement et pour une autre finalité tout en respectant les éventuelles obligations légales de l'organisme,
- de conserver les demandes de suppression ou d'effacement et les réponses faites à ces demandes dans le respect de l'obligation de traçabilité et de documentation imposée au RT,
- de définir des modèles de réponse aux demandes de suppression et d'effacement ou de limitation de traitement.

Exemple

Exemple de réponse aux demandes de suppression et d'effacement : nous ne pouvons effacer certaines de vos données personnelles nécessaires durant 6 ans pour les raisons fiscales en vertu de l'article L 14 A du Livre des Procédures fiscales, nous nous engageons à ne plus les utiliser à des fin de prospection caritative.

Étape n°5

Justifier des procédures d'accès aux données et autres mesures de sécurité

- Sensibiliser les utilisateurs des enjeux en matière de sécurité et de vie privée
- Reconnaitre ses utilisateurs pour pouvoir leur donner les accès nécessaires
- Gérer les habilitations : limiter aux seuls accès dont l'utilisateur a besoin
- Tracer les accès et gérer les incidents : journaliser les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité)
- Sécuriser les postes de travail : prévenir les accès frauduleux, l'exécution de virus ou la prise de contrôle à distance, notamment via Internet
- Sécuriser l'informatique mobile : anticiper l'atteinte à la sécurité des données consécutive au vol ou à la perte d'un équipement mobile
- Protéger le réseau informatique interne : autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place
- Sécuriser les serveurs : renforcer les mesures de sécurité appliquées aux serveurs
- Sécuriser les sites web : s'assurer que les bonnes pratiques minimales sont appliquées aux sites web
- Sauvegarder et prévoir la continuité d'activité : effectuer les sauvegardes régulières pour limiter l'impact d'une disparition non désirée de données
- Archiver de manière sécurisée : archiver les données qui ne sont plus utilisées au quotidien mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de contentieux
- Encadrer la maintenance et la destruction des données : garantir la sécurité des données à tout moment du cycle de vie des matériels et logiciels
- Gérer la sous-traitance : encadrer la sécurité des données avec les sous-traitants
- Sécuriser les échanges avec d'autres organismes : renforcer la sécurité de toute transmission de données à caractère personnel
- Protéger les locaux : renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux
- Encadrer les développements informatiques : intégrer sécurité et protection de la vie privée au plus tôt dans les projets
- Chiffrer, garantir l'intégrité ou signer : assurer l'intégrité, la confidentialité et l'authenticité d'une information.

1. Revoir les profils d'habilitation

Il faut limiter l'accès aux données personnelles aux seuls utilisateurs dûment habilités. L'habilitation tient compte de la qualité de l'utilisateur (salarié, bénévole) mais doit surtout prendre en considération sa fonction ou sa mission.

Les habilitations doivent être circonscrites aux bases ou aux catégories de données (prospects, donateurs, testateurs, etc.) dont se servent les utilisateurs.

L'organisme doit aussi s'assurer que l'accès aux bases intermédiaire ou d'archivage soit limité à un nombre restreint d'utilisateurs.

De plus, il est nécessaire de mettre en place des mesures de journalisation visant à l'enregistrement des actions de chaque utilisateur sur le système ou la base concernée pendant une durée définie.

L'accès donné doit être limité dans le temps. Les permissions d'accès des utilisateurs doivent prendre fin dès que leur habilitation ne se justifie plus au regard de leurs missions et/ou fonctions.

Enfin, il faut éviter les comptes et accès partagés par plusieurs personnes.

Exemple

Un salarié est spécifiquement en charge de la relation avec les testateurs. Celui-ci collecte des données personnelles sensibles, lesquelles sont rassemblées dans un logiciel regroupant également les données personnelles des donateurs et des prospects et sur lequel travaille toute une équipe. Le salarié qui s'occupe spécifiquement de la relation avec les testateurs doit être la seule personne habilitée à avoir accès aux données personnels des testateurs qui figurent en base.

2. Sensibiliser les utilisateurs sur le caractère confidentiel des données personnelles

L'élaboration d'une charte informatique à destination des utilisateurs permet de leur faire connaître les règles et consignes à respecter (confidentialité, changement des mots de passe, procédures d'enregistrement et de radiation des utilisateurs, mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès au traitement, etc.).

Il faut sensibiliser les utilisateurs via des formations internes ou externes.

Il est recommandé faire signer aux utilisateurs un engagement de confidentialité ou d'inclure une clause de confidentialité dans les contrats de travail.

3. Gérer les risques de manière proactive et préventive

L'organisme doit prendre des mesures visant les données stockées sur les serveurs et des mesures spécifiques concernant le transfert de ces données.

Il faut également mettre en place des mesures de détection des déplacements ou des copies de données non autorisées en déclenchant des alertes aux équipes en charge de la sécurité informatique.

Ainsi que mettre en place des mécanismes permettant d'isoler les environnements de production et de non production (test, recette).

Enfin, il est nécessaire de prendre des précautions concernant la segmentation réseau, pare-feu, anonymisation éventuelle des données personnelles en environnements de non production.

Étape n°6
Justifier des mesures concernant les sous-traitants

- Faire appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources)
- Identifier et responsabiliser l'ensemble des sous-traitants
- Réviser l'ensemble des contrats
- Exiger la communication par le prestataire de sa politique de sécurité des moyens d'information
- Le sous-traitant doit vous offrir des « garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (Article 28)
- Prendre et documenter les moyens (audits de sécurité, visites des installations, ect.) permettant d'assurer l'effectivité des garanties offertes par le sous-traitant en matière de protection des données
- Prévoir un contrat avec les sous-traitants qui définit notamment l'objet, la durée, la finalité du traitement et les obligations des parties

1. Identifier l'ensemble des sous-traitants

Une personne physique ou morale est un sous-traitant dès lors qu'il traite des données personnelles pour votre compte, sur instruction et sous votre autorité (Article 4 §7).

Cela concerne tous les acteurs impliqués dans le traitement des données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'UE et qu'ils agissent en qualité de RT ou de sous-traitant. Ces informations doivent figurer dans le registre de traitement.

2. Analyser et réviser les contrats

Il est nécessaire d'établir avec chaque sous-traitant un contrat précisant les obligations et responsabilités de chaque partie (un modèle proposé à l'annexe 4). Cela peut être fait aussi sous la forme d'avenant au contrat existant.

Lorsqu'un de ces sous-traitants fait lui-même appel à un autre sous-traitant, le sous-traitant de rang 1 devra également établir un contrat (ou avenant au contrat existant) avec ce dernier contenant les mêmes clauses en matière de protection des données personnelles.

>> Conseils pour régir le cadre contractuel des relations avec les sous-traitants :

Selon que le sous-traitant est établi dans un pays reconnu comme ayant un niveau de protection des données personnelles suffisant par l'UE ou non, les clauses à insérer et les formalités à effectuer sont différentes.

Le sous-traitant est établi dans un pays reconnu adéquat par l'UE :

Vérifier que les points suivants sont bien prévus dans les contrats :

- le sous-traitant ne traite que sur instruction du RT et prend toutes les mesures de sécurité requises,
- le sous-traitant ne sous-traite pas sans l'autorisation écrite du RT. L'autorisation peut être spécifique c'est-à-dire accordée pour un sous-traitant en particulier, ou, générale, c'est-à-dire que le sous-traitant doit informer le RT de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants,
- le sous-traitant de rang 1 doit soumettre son propre sous-traitant de rang 2 aux mêmes obligations que celles figurant dans le contrat signé avec le RT,
- le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles permettant d'assurer la conformité du traitement au RGPD,
- le sous-traitant met à disposition du RT toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre au RT de réaliser des audits,
- le sous-traitant tient un registre qui recense les traitements qu'il effectue pour le compte du RT,
- le sous-traitant est tenu d'une obligation d'assistance, d'alerte et de conseil :
  - il doit immédiatement informer le RT lorsque l'une de ses instructions lui parait illicite,
  - lorsqu'une personne souhaite exercer ses droits (accès, rectification, effacement, portabilité, opposition, ne pas faire l'objet d'une décision individuelle automatisée, y compris le profilage) il doit aider le RT à donner suite à cette demande,

  - il doit garantir le respect des obligations en matière de sécurité du traitement, de notification de violation de données et d'analyse d'impact relative à la protection des données.
- le sous-traitant doit garantir la sécurité des données qu'il traite :
  - ses employés doivent être soumis à une obligation de confidentialité,
  - il doit notifier au RT toute violation de données,
  - au terme de sa prestation et selon les instructions du RT, il doit renvoyer toutes les données et détruire les copies existantes sauf si une obligation légale lui impose de les conserver.
- le sous-traitant doit prendre en compte les principes de protection des données dès la conception de ses prestations :
  - le sous-traitant doit garantir que, par défaut, seules sont traitées les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personnes qui y a accès.
- le sous-traitant devra désigner un DPD suivant la réglementation.

Le sous-traitant est établi dans un pays non reconnu adéquat par l'UE :

- Vérifier si le sous-traitant est établi au sein de l'UE et dans la négative si son pays d'établissement offre un niveau de protection des données personnelles suffisant pour l'UE (https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde).
- Si le pays d'établissement du sous-traitant n'est pas reconnu comme adéquat par l'UE, les transferts de données personnelles transitant vers ce pays nécessitent d'être encadrées par des clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne, un code de conduite approuvé (comportant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées), un mécanisme de certification approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées), un arrangement administratif ou un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques (convention internationale, ...)

Obligation de notification de toute violation des données :

Le sous-traitant doit notifier au RT, dans les meilleurs délais, afin que le Client puisse en informer la CNIL dans les 72 heures de la connaissance de la violation des données en précisant :

- la nature de la violation,
- le nombre approximatif de personnes concernées,
- les mesures prises pour y remédier,
- nom et coordonnées du DPO ou d'un autre point de contact
- les conséquences de la violation,
- les mesures prises pour y remédier ou atténuer les conséquences.

Une fois cette notification effectuée, deux options se présentent :

1. soit le RT notifie cette violation à la CNIL (Article 33) et communique à la personne concernée la violation (Article 34),
2. soit le sous-traitant effectue lui-même, pour le compte du RT, cette notification à la CNIL et le cas échéant, aux personnes concernées, dans les conditions définies dans le contrat.

>> Conseils méthodologiques :

- Privilégier les contrats avec des sous-traitants établis dans des pays reconnus adéquats par l'UE.
- Discuter avec le sous-traitant des clauses contractuelles que celui-ci propose dans le cadre de son obligation d'assistance et de conseil.
- Selon le type de contrat et son niveau de complexité technique, consulter les directions concernées au sein de la structure. Par exemple, dans le cadre d'un contrat impliquant des prestations informatiques, soumettre la partie relative aux mesures de sécurité techniques et organisationnelles à la direction informatique.
- Vérifier par où transitent précisément les données personnelles en demandant au sous-traitant un schéma informatique.

Étape n°7
Limiter les durées de conservation

- Définir une durée de conservation en fonction de la finalité de chaque traitement de données personnelles (Article 5§1)
- « Les données à caractère personnel devraient être adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées. Cela exige, notamment, de **garantir que la durée de conservation des données soit limitée au strict minimum.** » (Considérant 39)
- « Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, **des délais devraient être fixés par le responsable du traitement pour leur effacement ou pour un examen périodique.** »
- Définir des règles d'archivage et de suppression des données

1. Définir une durée de conservation en base active

Le RGPD n'apporte pas de bouleversement majeur concernant la question de la durée de conservation et l'archivage des données.

Les données à caractère personnel doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte. La durée de conservation sera donc différente en fonction des finalités poursuivies et de la nature des données.

Une fois que l'objectif poursuivi par la collecte des données a été atteint, il n'y a plus lieu de conserver les données et elles doivent être supprimées par le RT.

Exemple

À l'occasion d'un don ponctuel sur internet, les coordonnées de la carte bancaire du donateur ne peuvent être conservées que le temps nécessaire à la réalisation de l'opération de paiement.

2. Définir les règles d'archivage

À l'issue de leur conservation en base active, certaines données peuvent faire l'objet d'un archivage lorsqu'elles présentent encore un intérêt. L'archivage peut notamment être nécessaire pour satisfaire à une obligation à la charge de la structure ou se prémunir contre un éventuel contentieux.

Il s'agit alors d'un archivage intermédiaire qui constitue une étape intermédiaire avant la suppression.

L'archivage doit être sélectif. Le RT doit veiller à archiver uniquement les données utiles au respect de l'obligation prévue ou pour faire valoir un droit en justice. Il est donc obligatoire d'opérer un tri parmi la totalité des données collectées pour ne garder que les seules données indispensables.

L'archivage doit également être limité dans le temps. Les données nécessaires pour répondre à une obligation légale ou réglementaire peuvent ainsi être archivées le temps nécessaire à l'accomplissement de l'obligation en cause. Celles-ci doivent toutefois être supprimées lorsque le motif justifiant leur archivage n'a plus raison d'être.

Exemple

Depuis le 1er janvier 2018 et s'agissant des dons et versements effectués à compter du 1er janvier 2017, l'administration peut contrôler sur place que les montants portés sur les reçus fiscaux délivrés par les organismes faisant appel à la générosité du public correspondent bien aux fonds reçus. Dans le cadre d'un tel contrôle l'ensemble des documents mentionnés à l'article L. 102 E du Livre des Procédures Fiscales, jusqu'à six ans en arrière, doit être présenté à l'administration.

Ainsi, même lorsque le donateur n'est plus en base active, certaines données doivent être gardées en archivage intermédiaire pour un temps limité afin que l'organisme soit en mesure de satisfaire à un contrôle de l'administration fiscale sur la régularité des montants portés sur les reçus fiscaux.

L'organisme devra toutefois opérer un tri pour ne conserver que les données personnelles indispensables à l'émission des reçus fiscaux. De plus, il ne pourra se baser sur ce fondement pour conserver les données au-delà de six années.

Seules les données présentant un intérêt historique, scientifique ou statistique peuvent être conservées sans limitation de durée. Dans ce cas, on parle **d'archivage définitif.** En tout état de cause, il est obligatoire de sélectionner les seules données pouvant relever de cette exception.

Il appartient à chaque organisme de :

- délimiter les étapes du cycle de vie pour chaque donnée ou traitement et de les formaliser par des procédures internes,
- définir de manière concrète les modalités de passage d'une donnée personnelle de la base active à un archivage intermédiaire et, à partir de quel moment elle sera effacée.

Mode d'archivage

Le choix du mode d'archivage intermédiaire est laissé à l'appréciation du RT. Les données peuvent ainsi être archivées :

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (ex : le service du contentieux) ou
- dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

S'agissant des archives définitives (c'est- à-dire les seules données présentant un intérêt historique, scientifique ou statistique), il est recommandé de les conserver sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter.

Précision : les durées de conservation des données personnelles relèvent de politiques internes qui peuvent être très différentes d'une organisation à une autre. En pratique, ces différences trouvent leur justification au regard des spécificités propres à chaque cause et à chaque organisation qui fait appel à la générosité du public, voire même au sein d'une même organisation au regard des spécificités des projets financés par les donateurs.

Partie 2
Fiches pratiques

Fiche n°1
Traitement de données de testateurs et testateurs potentiels : quel est le raisonnement à suivre ?

Quelle est la finalité du traitement ?

Pour rappel : la collecte de données personnelles doit répondre à des finalités précises (article 5 du RGPD).

Il faut distinguer les testateurs et les potentiels testateurs :

- Les finalités du traitement de données **de testateurs** peuvent être **la gestion des relations testateurs et le suivi du traitement des legs**, avec comme sous-finalités :
  - Fidéliser les testateurs ;
  - Encaisser les legs au décès des testateurs ;
  - Assurer la traçabilité du traitement des legs ;
  - Gérer les charges privées ;
  - Mesurer et analyser les legs reçus à des fins statistiques.
- La finalité du traitement de données de **testateurs potentiels** peut être la **prospection** caritative.

Quelle est la base juridique du traitement ?

Pour rappel : 6 bases juridiques sont prévues (article 6 du RGPD) :

- **Le respect d'une obligation légale ;**
- **L'intérêt légitime du responsable de traitement ;**
- **Le consentement libre et éclairé ;**
- **L'exécution d'un contrat ;**
- **La sauvegarde des intérêts vitaux de la personne concernée** ou d'une autre personne physique ;
- **L'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique.

Dans le cas de collecte des données personnelles des testateurs, deux bases juridiques peuvent être retenues pour justifier leur traitement :

- l'intérêt légitime en matière de prospection de testateurs potentiels. De plus, le traitement de données des testateurs à des fins de fidélisation peut être considéré comme étant réalisé pour répondre à un intérêt légitime des OSBL. Le legs étant une ressource hypothétique, il est en effet nécessaire que ces organismes poursuivent leur relation de confiance avec les testateurs. De la même manière, le suivi du processus de traitement des legs et leur analyse statique répondent à un intérêt légitime des OSBL,
- le consentement préalable en cas de collecte de données sensibles (santé, orientation sexuelle, convictions religieuses, etc.) ou de réutilisation des données pour d'autres finalités que la gestion de la relation testateur ou potentiel testateur.
  Dans ce cas, outre les mentions d'informations sur l'utilisation des données, la personne doit donner son consentement par une démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée.
  Le RT doit être en mesure de prouver que la personne concernée a effectivement consenti à l'opération de traitement (consentement tracé et archivé).

NB : *il est possible d'envoyer une newsletter ou une invitation à un événement à des testateurs et potentiels testateurs qui ont donnés leur consentement mais également à ceux qui ne l'ont pas donné dans le cadre de la gestion des relations testateurs/potentiels testateurs ou dans le cadre de campagnes de prospection et de fidélisation. Penser à indiquer dans la newsletter ou sur l'invitation que la personne peut demander à ne plus en recevoir de manière simple et gratuite (cf, Etape n° 4).*

Quelles sont les données fréquemment collectées et traitées ?

Pour rappel : les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) (article 5 c) RGPD).

D'une manière générale, il s'agit de données d'identification des testateurs et potentiels testateurs :

- Nom ;
- Prénom ;
- Civilité ;
- Date et lieu de naissance ;
- Date de décès ;
- Adresse postale ;
- Adresse électronique ;
- Numéro de téléphone.

D'autres données peuvent être collectées et traitées notamment des données d'identification et de vie professionnelle des tiers liés aux legs tels que les notaires, les huissiers, les commissaires-priseurs, les créanciers, la famille et les salariés des testateurs décédés.

Des informations d'ordre économique et financier des testateurs décédés peuvent également être collectées en particulier la valeur de leurs biens.

Enfin, les organisations peuvent être amenées à recueillir des données « sensibles » relatives aux testateurs et potentiels testateurs (informations confessionnelles, médicales, familiales).

Quelle est la durée de conservation des données personnelles ?

Pour rappel : la durée de conservation des données ne doit en principe pas excéder celle nécessaire au regard des finalités pour lesquelles elles sont traitées (article 5 du RGPD).

Il faut distinguer les testateurs et les testateurs potentiels :

- Dans le cas des testateurs déclarés, les données sont conservées jusqu'à **l'exécution du testament** ou jusqu'au changement d'avis de la personne concernée.
- Dans le cas des testateurs potentiels, la durée de conservation est déterminée en fonction de la politique de chaque organisation. Étant précisé que celle-ci doit pouvoir la justifier au regard de ses spécificités propres. À titre indicatif, une durée de conservation des données de 108 mois (soit 9 ans) à compter du dernier intérêt exprimé (demande de brochure ou autres) est préconisée comme *« pertinente et proportionnée au vu de la réglementation relative à la protection des données personnelles et des contraintes inhérentes au secteur caritatif »* par la CNIL (cf, séance plénière du 20 septembre 2018).

Par la suite, soit les données sont conservées suite à l'accord donné par la personne au moyen d'un opt in. Soit les données sont conservées en archivage intermédiaire pour se prémunir contre un éventuel contentieux notamment une action en réduction exercée par les héritiers réservataires ou une interprétation de testament. Afin de fixer une durée en archivage intermédiaire, il est possible de s'aligner sur la durée de prescription en matière de succession.

Quels sont les destinataires des données personnelles ?

Pour rappel : il s'agit des personnes qui ont accès aux données et seules doivent avoir accès aux informations les personnes dûment habilitées par le responsable du traitement.

Les destinataires des données sont donc les personnes qui ont accès aux données collectées.

Concernant les testateurs et potentiels testateurs, il s'agira habituellement des services ou des personnes en charge des relations testateurs, des services libéralités ou encore des services marketing et communication.

De plus, des tiers mandatés pour réaliser les finalités précitées peuvent avoir accès aux données (sous-traitants). Ici, il est important de vérifier s'il existe un transfert de données hors de l'Union européenne et de l'encadrer avec des clauses spécifiques.

Quels sont les droits des testateurs et testateurs potentiels ?

Les testateurs et testateurs potentiels disposent de différents droits :

- Droit à l'information ;
- Droit d'accès aux données ;
- Droit de rectification des données ;
- Droit d'effacement des données ;
- Droit à la portabilité des données ;
- Droit à la limitation du traitement ;
- Droit d'opposition au traitement ;
- Droit d'introduire une réclamation auprès de la CNIL.

Attention : en fonction de la base juridique du traitement, certains droits ne peuvent être exercés. Par exemple, lorsque la base juridique du traitement est l'intérêt légitime, les personnes concernées ne peuvent exercer leur droit à la portabilité des données.

Concernant le droit à l'information, celui-ci se concrétise dans les mentions d'informations présentes lors de chaque collecte de données personnelles.

Exemple

Exemple de mention pour les testateurs :

Xxx [nom du responsable de traitement] collecte et traite de manière informatisée les informations que vous lui transmettez afin d'assurer la gestion des relations testateurs et le suivi du processus de traitement des legs.

La collecte et le traitement de ces données à caractère personnel se justifient par les intérêts légitimes de xxx [nom du responsable de traitement] de fidéliser les testateurs, d'encaisser les legs au décès de ces derniers, d'en assurer la traçabilité, de gérer les charges privées et de mesurer les legs reçus à des fins statistiques.

Ces données sont destinées à notre service xxx [destinataire] ainsi qu'à des tiers mandatés [à ajouter si votre organisme est concerné] et sont conservées uniquement pour la durée strictement nécessaire à la réalisation des finalités précitées.

Ces données peuvent faire l'objet d'un transfert à des tiers au sein de l'union européenne [à ajouter si votre organisme est concerné].

Conformément à la loi « informatique et libertés », vous pouvez vous opposer à l'utilisation de vos données ou introduire une réclamation auprès de la cnil. Vous bénéficiez d'un droit d'accès à vos données pour les rectifier, les mettre à jour, les limiter ou les supprimer ainsi que d'un droit à la portabilité de vos données.

Pour exercer ces droits, merci de contacter xxx au : [coordonnées de la personne chargée de cette tâche par le rt].

N'hésitez pas à contacter notre délégué à la protection des données pour toute question concernant le respect de vos données personnelles à : [coordonnées du dpo].

Quelles sont les mesures de sécurité à mettre en place ?

Pour rappel, la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (article 32 du RGPD)

Plusieurs mesures de sécurité **de base** sont à prévoir :

- Contrôler l'accès aux données des utilisateurs.
- Mesures de traçabilité de l'accès aux données.
- Mesures de protection des logiciels utilisés.
- Sauvegarde des données.
- Chiffrement des données.
- Contrôler la sous-traitance.

Cette liste est non exhaustive et la mise en place de toutes les mesures précitées n'est pas imposée. **Le niveau de sécurité doit simplement être adapté aux risques soulevés par le traitement.** Dans ce sens, la CNIL précise les « bonnes questions à se poser » :

1. Quels pourraient être les impacts sur les personnes concernées en cas :
   - d'accès illégitime ?
   - de modification non désirée ?
   - de disparition ?
2. Est-ce grave ?
3. Comment chacun de ces scénarios pourrait-il arriver ?
4. Est-ce vraisemblable ?
5. Quelles mesures (de prévention, de protection, de détection, de réaction...) devrait-on prévoir pour réduire ces risques à un niveau acceptable ?

Ainsi, pour les données sensibles des testateurs et testateurs potentiels, il sera opportun de restreindre au maximum l'accès à ces données et de les chiffrer.

France générosités

Fiche n°2

Traitement de données de donateurs potentiels et potentiels donateurs/prospects : quel est le raisonnement à suivre ?

Quelle est la finalité du traitement ?

Pour rappel : la collecte de données personnelles doit répondre à des finalités précises (article 5 du RGPD).

La finalité du traitement des données personnelles de donateurs par une organisation faisant appel à la générosité du public a pour finalité **la gestion des relations donateurs**, avec comme sous-finalités possibles de :

- Adresser aux donateurs les reçus fiscaux correspondant au don qu'ils ont effectué
- Inviter les donateurs à des évènements ;
- Informer les donateurs (ex. : sur les projets qu'ils ont contribués à financer) ;
- Solliciter les donateurs pour effectuer de nouveaux dons ;
- Etc.

La finalité du traitement des données personnelles de potentiels donateurs par un organisme faisant appel à la générosité du public peut avoir pour finalité **la prospection caritative.**

Quelle est la base juridique du traitement ?

Pour rappel, 6 bases juridiques sont prévues (article 6 du RGPD) :

- **Le respect d'une obligation légale,**
- **L'intérêt légitime du responsable de traitement,**
- **Le consentement libre et éclairé,**
- **L'exécution d'un contrat,**
- **La sauvegarde des intérêts vitaux de la personne concernée** ou d'une autre personne physique,
- **L'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique.

Dans le cas de collecte des données personnelles des donateurs, trois bases juridiques peuvent être retenues pour justifier leur traitement :

- **L'intérêt légitime** en matière de prospection caritative menée par les organismes faisant appel à la générosité du public.
- **Le respect d'une obligation légale** pour l'édition des reçus fiscaux par les organismes d'intérêt général.

Cette base est retenue quand le donateur a effectivement effectué un don : depuis le 1er janvier 2018, l'administration fiscale peut contrôler sur place, dans les locaux de l'organisme, que les montants portés sur les reçus correspondent bien aux dons et versements effectués. Les organismes devant alors présenter à l'administration fiscale « les documents et pièces de toute nature » permettant de justifier des dons effectués au cours des six dernières années (pour les dons effectués à partir du 1er janvier 2017).

- **Le consentement préalable** en cas de réutilisation des données pour d'autres finalités que la gestion de la relation donateur ou potentiel donateur.
  Dans ce cas, outre les mentions d'informations sur l'utilisation des données, la personne doit donner son consentement par une démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée.
  Le RT doit être en mesure de prouver que la personne concernée a effectivement consenti à l'opération de traitement (consentement tracé et archivé).

***NB :** il est possible d'envoyer une newsletter ou une invitation à un événement à des donateurs et potentiels donateurs qui ont donnés leur consentement mais également à ceux qui ne l'ont pas donné dans le cadre de la gestion des relations donateurs ou potentiels donateurs ou dans le cadre de campagnes de prospection et de fidélisation. Penser à indiquer dans la newsletter ou sur l'invitation que la personne peut demander à ne plus en recevoir de manière simple et gratuite (cf. étape n° 4).*

Exemple

Pour l'envoi d'une newsletter :

☐ J'accepte que [association] m'adresse sa newsletter. Je pourrai me désinscrire à tout moment par un simple clic.

OU

Clic de validation sur un lien qui sera envoyé par email à l'adresse électronique communiquée, en confirmation de l'abonnement.

ET

Dans chaque email envoyé par la suite, un lien de désabonnement doit être systématiquement intégré, permettant à la personne de retirer son consentement à tout moment de façon simple et gratuite, sans subir de préjudice (opt-out).

Quelles sont les données personnelles fréquemment collectées ?

Pour rappel, les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) (Article 5 c) RGPD).

Dans le cadre de la gestion des relations donateurs et prospects, une association est généralement amenée à conserver :

- les données d'identification de la personne (nom et prénom, adresse postale, adresse électronique, numéro de téléphone),
- les données de connexion, si l'association dispose d'un espace donateur en ligne,
- les données d'ordre financier (date et montant du don, données bancaires).

Quelle est la durée de conservation des données personnelles ?

Pour rappel, la durée de conservation des données ne doit en principe pas excéder celle nécessaire au regard des finalités pour lesquelles elles sont traitées (Article 5 du RGPD).

La durée de conservation des données des donateurs en base active est déterminée en fonction de la politique de chaque organisation et limitée à celle nécessaire à la gestion de la relation donateur. Etant précisé que celle-ci doit pouvoir la justifier au regard de ses spécificités propres. À titre indicatif, une durée de conservation de 72 mois (soit 6 ans) à compter du dernier don ou dernier consentement est préconisée comme *« pertinente et proportionnée au vu de la réglementation relative à la protection des données personnelles et des contraintes inhérentes au secteur caritatif » par la CNIL* (cf, séance plénière du 20 septembre 2018).

Par la suite, soit les données sont conservées en archivage intermédiaire pour satisfaire à une obligation ou se prémunir contre un éventuel contentieux. Soit les données sont conservées suite à l'accord donné par la personne au moyen d'un opt-in.

Si un autre traitement séparé a été adjoint, alors la durée dépend de la finalité du traitement.

Exemple

Pour l'envoi d'une newsletter : les données sont conservées jusqu'à la désinscription de l'abonné donateur (potentiel), possible à tout moment et devant être proposée lors de l'envoi de chaque email ou courrier.

Quels sont les destinataires des données personnelles ?

Pour rappel : il s'agit des personnes qui ont accès aux données et seules doivent avoir accès aux informations les personnes dûment habilitées par le responsable du traitement.

Il s'agit des agents habilités par l'association, pour les stricts besoins de l'accomplissement de leurs missions, qui ont accès aux données.

Concrètement, pour les données des donateurs :

- en interne : il s'agit habituellement des services ou des personnes en charge de la gestion de la relation donateurs, des services libéralités ou encore des services marketing et communication,
- en externe : il peut s'agir de tiers missionnés pour réaliser les finalités précitées (sous-traitants). Par exemple, l'émission des reçus fiscaux peut faire l'objet d'une sous-traitance.

Quels sont les droits des donateurs et prospects ?

Quand leurs données sont collectées, les donateurs disposent de différents droits que l'association doit respecter :

- Droit à **l'information**
- Droit **d'accès** aux données
- Droit de **rectification** des données
- Droit **d'effacement** des données
- Droit à la **portabilité** des données lorsque le traitement est fondé sur le consentement ou sur un contrat
- Droit à la **limitation** du traitement
- Droit **d'opposition** au traitement
- Droit d'introduire une **réclamation** auprès de la CNIL

L'association doit assurer l'effectivité de ces droits et définir les modalités de leur exercice par les donateurs.

Attention : en fonction de la base juridique du traitement, certains droits ne peuvent être exercés. Par exemple, lorsque la base juridique du traitement est l'intérêt légitime, les personnes concernées ne peuvent exercer leur droit à la portabilité des données.

Concernant le droit à l'information, celui-ci se concrétise dans les mentions d'informations présentes lors de chaque collecte de données personnelles.

Exemple

Exemple de mentions d'informations pour les donateurs

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par [identité et coordonnées de l'association RT].

Elles sont destinées à la Direction des relations donateurs [et autres Directions le cas échéant] et aux tiers mandatés par [identité du RT] à des fins de gestion interne, pour répondre à vos demandes ou faire appel à votre générosité.

Elles sont conservées pendant la durée strictement nécessaire à la réalisation des finalités précitées.

Ces données peuvent faire l'objet d'un transfert à des tiers au sein de l'Union Européenne. [A ajouter si votre organisme est concerné : Dans le cadre d'un transfert vers un pays hors Union Européenne, des règles assurant la protection et la sécurité de ces données ont été mises en place. Le détail de ces règles et des informations relatives au transfert est disponible sur simple demande adressée à...]

Conformément à la loi « informatique et libertés » et à la règlementation européenne, vous pouvez vous opposer à l'utilisation de vos données à caractère personnel. Vous bénéficiez également d'un droit d'accès à vos données pour leur rectification, limitation, portabilité ou effacement, en contactant : [Coordonnées de la personne chargée de cette tâche par le RT].

Vous pouvez également écrire à notre Délégué à la protection des données à [coordonnées de la personne chargée de cette tâche par le RT] ou introduire une réclamation auprès de la CNIL.

Quelles sont les mesures de sécurité à mettre en place ?

Pour rappel, la protection des données personnelles nécessite de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (Article 32 du RGPD)

Concrètement, pour sécuriser ses bases de données des donateurs, l'association définit les moyens appropriés, par exemple :

- Un contrôle d'accès aux données par les utilisateurs (ex : identifiant et mot de passe unique, etc.)
- Des mesures de traçabilité (ex : journalisation des accès des utilisateurs, etc.)
- Des mesures de protection des logiciels (ex : antivirus, mises à jour et correctifs de sécurité, tests, etc.)
- Des sauvegardes des données (ex : sauvegarde chaque nuit et stockage dans un data center sécurisé, etc.)
- Le chiffrement des données (ex : site accessible en https, utilisation de TLS, etc.)
- Le contrôle des sous-traitants (ex : mise à jour des documents contractuels, possibilités d'audits, etc.)

Cette liste est non exhaustive et la mise en place de toutes les mesures précitées n'est pas imposée. **Le niveau de sécurité doit simplement être adapté aux risques soulevés par le traitement.** Dans ce sens, la CNIL précise les « bonnes questions à se poser » :

2. Quels pourraient être les impacts sur les personnes concernées en cas :
   - d'accès illégitime ?
   - de modification non désirée ?
   - de disparition ?
6. Est-ce grave ?
7. Comment chacun de ces scénarios pourrait-il arriver ?
8. Est-ce vraisemblable ?
9. Quelles mesures (de prévention, de protection, de détection, de réaction...) devrait-on prévoir pour réduire ces risques à un niveau acceptable ?

Annexe 1
Modèle de registre CNIL

Exemple de registre

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.

Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme **en tant que responsable de traitement.** Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévue par le RGPD.

Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la règlementation.

Composition du document

1. **Une première page du registre recense les informations communes à toutes vos activités de traitement.**

- Les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne)
- Les coordonnées du délégué à la protection des données (DPO) si vous en disposez
- La liste des activités de votre organisme impliquant le traitement de données personnelles.

2. **Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.**

Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.

Registre des activités de traitement de [Nom de l'organisme]

Coordonnées du responsable de l'organisme (responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)	Ex. : nom et prénom du responsable légal Adresse CP Ville Téléphone Adresse de messagerie
Nom et coordonnées du délégué à la protection des données (si vous avez désigné un DPO)	Ex. : nom et prénom du DPO Société (si DPO externe) Adresse CP Ville Téléphone Adresse de messagerie

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

ACTIVITÉS	DÉSIGNATION DES ACTIVITÉS (EXEMPLES)
Activité 1	Gestion de la paie
Activité 2	Gestion des prospects
Activité 3	Gestion des fournisseurs
Activité 4	Vente en ligne
Activité 5	Sécurisation des locaux
Activité 6	
Activité 7	
Activité 8	
Activité 9	

Vous devrez créer et tenir à jour une fiche de registre par activité. Le modèle de fiche de registre est disponible sur la page suivante.

Fiche de registre de l'activité 1

(Reprise de l'activité 1 de la liste des activités)

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	
Nom du logiciel ou de l'application (si pertinent)	

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

.....

.....

.....

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. .....

2. .....

3. .....

4. .....

Catégories de données collectées

Listez les différentes données traitées

☐ État-civil, identité, données d'identification, images (nom, prénom, adresse, photographie, date et lieu de naissance, etc.)

.....

☐ Vie personnelle (habitudes de vie, situation familiale, etc.)

.....

☐ Vie professionnelle (CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)

.....

☐ Informations d'ordre économique et financier (revenus, situation financière, données bancaires, etc.)

.....

☐ Données de connexion (adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

.....

☐ Données de localisation (déplacements, données GPS, GSM, ...)

.....

☐ Internet (cookies, traceurs, données de navigation, mesures d'audience, ...)

.....

☐ Autres catégories de données (précisez) :

.....

.....

.....

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? : .....

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

_____ jours _____ mois _____ ans Autre durée : _____

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

.....

.....

.....

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.

1. .....

2. .....

3. .....

4. .....

Organismes externes

Exemples : filiales, partenaires, etc.

1. .....

2. .....

3. .....

4. .....

Sous-traitants

Exemples : hébergeurs, prestataires et maintenance informatiques, etc.

1. .....

2. .....

3. .....

4. .....

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays : .....

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs. Décrivez les mesures :

.....

.....

☐ Mesures de traçabilité. Précisez la nature des traces (exemple : journalisation des accès des utilisateurs), les données enregistrées (exemple : identifiant, date et heure de connexion, etc.) et leur durée de conservation :

.....

.....

☐ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.). Décrivez les mesures :

.....

.....

☐ Sauvegarde des données. Décrivez les modalités :

.....

.....

☐ Chiffrement des données. Décrivez les mesures (exemple : site accessible en https, utilisation de TLS, etc.) :

.....

.....

☐ Contrôle des sous-traitants. Décrivez les modalités :

.....

.....

☐ Autres mesures :

.....

.....

.....

.....

Annexe 2
Analyse d'impact relative à la protection des données : la méthode

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

Annexe 3
Analyse d'impact relative à la protection des données : les modèles

https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf

Annexe 4
Modèle d'avenant au contrat sous-traitant

Avenant au contrat de licence d'applications hébergées et prestations de services N° _____

ENTRE

La société XXX, [forme juridique et déclaration à préciser], dont le siège social est situé au XXX, immatriculée au RCS de XXX sous le numéro XXX, représentée par XXX en qualité de XXX, dûment habilité aux fins des présentes :

Ci-après dénommée « XXX» ou le « Prestataire ».

D'une part

L'association/la Fondation ABCD, [forme juridique et déclaration à préciser], dont le siège est XXX, représentée par XXX, en qualité de XXX, dûment habilitée aux fins des présentes,

Ci-après dénommée « ABCD » ou le « Client ».

D'autre part

Le Prestataire et le Client sont ci-après dénommés ensemble les « Parties » et individuellement et indifféremment une « Partie ».

LES PARTIES ONT PRÉALABLEMENT EXPOSÉ CE QUI SUIT

Les parties ont conclu le [à préciser] un contrat de licence d'applications hébergées et de prestations de services n° [à préciser] (ci-après le « Contrat »).

Dans le cadre de ce Contrat, le Prestataire concède au Client un droit d'utilisation des Progiciels XXX et YYY et est amené à traiter pour le compte du Client des données à caractère personnel des contacts du Client.

Les Parties souhaitent modifier et préciser le Contrat afin de prendre en compte les modifications de la règlementation relative à la protection des données à caractère personnel, et notamment le 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 (ci-après le « Règlement »).

LES PARTIES SONT CONVENUES DE CE QUI SUIT.

ARTICLE 1. OBJET

L'objet du présent avenant (« l'Avenant ») est de compléter le Contrat en ce qui concerne les données à caractère personnel pour prendre en compte l'entrée en application du Règlement.

À l'exception des modifications introduites par l'Avenant, le Contrat reste inchangé et s'applique dans toutes ses stipulations.

ARTICLE 2. DESCRIPTION DES TRAITEMENTS

Le Prestataire est autorisé à traiter pour le compte du Client les données à caractère personnel nécessaires pour fournir au Client les Prestations objet du Contrat.

Les catégories de données à caractère personnel concernées, les finalités des traitements, la nature des traitements, les durées de conservation des données à caractère personnel sont définies en Annexe I.

Compte tenu des Prestations réalisées pour le Client, il est expressément convenu entre les Parties que, au sens du Règlement, le Client est responsable de traitement et le Prestataire est sous-traitant.

ARTICLE 3. OBLIGATIONS DU PRESTATAIRE VIS-A-VIS DU CLIENT

Le Prestataire s'engage à :

1. apporter conseil et assistance au Client dans le cadre de la mise en œuvre des obligations incombant à ce dernier au titre du règlement ;

2. traiter les données uniquement dans le cadre des Prestations et pour la ou les seule(s) finalité(s) définies en Annexe II ;

3. ne pas utiliser les données à d'autres fins que la stricte exécution du Contrat ;

4. traiter les données conformément aux finalités et aux instructions documentées du Client figurant en Annexe I. Si le Prestataire considère qu'une instruction constitue une violation du Règlement ou de toute autre disposition du droit national relatif à la protection des données, il en informe immédiatement le Client ;

5. notifier annuellement au Client la liste des données à caractère personnel dont la durée de conservation telle que définie à l'Annexe I est arrivée à expiration et requérir les instructions du Client quant à la purge de ces données ;

6. garantir la confidentialité des données à caractère personnel traitées dans le cadre du Contrat ;

7. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du Contrat :
   - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
   - reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

8. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut ;

9. mettre en œuvre les mesures techniques et organisationnelles appropriées afin de protéger les données personnelles communiquées par le Client, de manière permanente et documentée, contre la destruction accidentelle ou l'altération, la diffusion ou l'accès non autorisé.

ARTICLE 4. SOUS-TRAITANCE

Le Prestataire est autorisé par le Client à sous-traiter une partie des Prestations mettant en œuvre un traitement de données à caractère personnel aux sociétés suivantes :

- Dénomination sociale, Adresse, Siret, etc.

pour mener les activités de traitement suivantes :

- Préciser les activités sous traitées
- Préciser la date du contrat de prestation

Tout recours à d'autres sous-traitants par le Prestataire devra recueillir l'autorisation écrite, préalable et spécifique du Client.

Nonobstant cette autorisation de sous-traitance, le Prestataire reste pleinement responsable devant le Client de l'exécution de l'ensemble des obligations découlant du Contrat.

Le Prestataire s'engage par ailleurs à répercuter à ses sous-traitants les obligations contractuelles et opérationnelles lui incombant.

Il appartient au Prestataire de s'assurer :

- que ses sous-traitants présentent les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du Règlement, et,
- de la contractualisation avec ses sous-traitants, incluant notamment les obligations de confidentialité et de sécurité des données.

Le Prestataire se porte fort à l'égard du Client du respect des obligations en matière de protection des données par ses sous-traitants et dégage le Prestataire de toute responsabilité en cas de non-respect de leurs obligations par ses sous-traitants.

Le Prestataire s'oblige à répertorier et identifier les transferts de données à caractère personnel et la chaîne de sous-traitance dans son ensemble dans le cadre d'un schéma qui détaille les flux de données et permet d'avoir une visibilité complète sur les cas de sous-traitants de second rang (cf, exemple de schéma Annexe III).

ARTICLE 5. TRANSFERT DE DONNEES DANS UN PAYS TIERS AU SENS DU PRESENT REGLEMENT

Tout transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale devra faire l'objet d'un avenant distinct qui devra respecter les garanties prévues au chapitre 5, aux articles 44 à 50 du Règlement.

ARTICLE 6. RESPONSABILITES DU CLIENT

Le Client est seul responsable de l'utilisation par ses préposés :

- des Progiciels et des Services et garantit leur utilisation conformément à la règlementation, notamment relative aux données à caractère personnel, et aux modes d'emploi communiqués par le Prestataire et/ou aux formations assurées au Client ;
- des informations de connexion (notamment liens, identifiants nécessaires, mise à disposition de web services) aux Progiciels et Services et de leur respect de la confidentialité de ces informations.

En particulier, le Prestataire ne saurait être tenu responsable de toute utilisation illégale ou non conforme par le Client et ses préposés des Progiciels et des Services et notamment en cas de :

- détournement des champs de bases des données ;
- mention de qualificatifs interdits par la règlementation ;
- extraction de contenus des bases de données du Client ;
- création de profils utilisateurs.

ARTICLE 7. INFORMATION - ASSISTANCE DU CLIENT

Le prestataire s'engage à apporter conseil et assistance au Client dans le cadre de la mise en œuvre des obligations incombant à ce dernier au titre du règlement.

À ce titre :

- le Prestataire établit et tient à jour le registre des activités de traitement prévu par l'article 30 du Règlement. Il tient à la disposition du Client la copie de ce registre correspondant aux traitements réalisés pour le compte du Client ;
- le Prestataire apporte conseil et assistance au Client dans le cadre de la mise en œuvre des obligations incombant à ce dernier au titre du Règlement. En particulier, le Prestataire aide le Client pour la réalisation d'analyses d'impact relatives à la protection des données et la consultation préalable de l'autorité de contrôle

A compléter selon les éléments propres à chaque prestataire selon son organisation et prestations proposées

ARTICLE 8. MESURES DE SÉCURITÉ DU TRAITEMENT

Le Prestataire s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque qui figurent à l'Annexe IV au titre de l'article 32 du Règlement.

ARTICLE 9. DROIT D'INFORMATION ET EXERCICE DES DROITS DES PERSONNES

Il appartient au Client de fournir, au moment de la collecte des données, l'information aux personnes concernées par les opérations de traitement au titre des articles 13 ou 14 du Règlement, étant entendu que la formulation et le format de l'information destinée aux personnes demeurent de la seule responsabilité du Client.

Dans la mesure du possible, le Prestataire doit aider le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Il s'agit notamment du droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, à la portabilité des données.

Lorsque les personnes concernées exercent auprès du Prestataire des demandes d'exercice de leurs droits, le Prestataire doit adresser ces demandes, dès réception par courrier électronique à

[préciser coordonnées responsable Client en charge de la réception de la notification]

ARTICLE 10. NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL

Le Prestataire notifie au Client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Cette notification est accompagnée de toute documentation utile afin de permettre au Client

- de s'assurer que toutes les mesures nécessaires ont été prises pour mettre fin à la violation et minimiser ses effets ;
- de notifier la violation en question à la CNIL, conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance ;
- de communiquer, si nécessaire, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais (cf, article 34).

Le Prestataire adresse cette notification à :

[préciser coordonnées responsable Client en charge de la réception de la notification]

Elle est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et contient au moins, dans la mesure où il en a connaissance :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le Prestataire propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

ARTICLE 11. PRESTATAIRES TIERS

Dans le cadre de ses activités, le Client fait également appel à d'autres prestataires amenés à accéder aux données à caractère personnel des contacts du Client figurant dans la base de données objet des Prestations et hébergée par le Prestataire.

La liste et l'identification de ces autres prestataires (dénomination sociale, adresse, coordonnées de contact) et les missions de ces prestataires pour le compte du Client sont détaillées en Annexe II. Tout ajout ou toute modification de la liste de ces prestataires tiers fera l'objet d'une modification de l'Annexe II de l'Avenant.

Le Prestataire transmet au Client les informations de connexion à la base de données hébergée par le Prestataire.

Le Client fait seul son affaire et est seul responsable de :

- la transmission de ces informations de connexion (notamment liens, identifiants nécessaires, mise à disposition de web services) à ces tiers et est seul responsable de cette transmission ;
- la contractualisation avec ces prestataires tiers, incluant notamment les obligations de confidentialité et de sécurité des données.

Le Client se porte fort à l'égard du Prestataire du respect de ces obligations par ces prestataires tiers et dégage le Prestataire de toute responsabilité en cas de non-respect de leurs obligations par ces prestataires tiers.

ARTICLE 12. FOURNISSEURS DE SOLUTIONS

Le Client est informé que le Prestataire fournit les Prestations objet du Contrat avec les solutions suivantes :

- XXX
- YYY

et que les fournisseurs de ces solutions peuvent pour les seuls besoins de la maintenance desdites solutions, avoir accès aux données du Client.

Les contrats du Prestataire avec les fournisseurs de ces solutions garantissent la confidentialité des données du Client.

ARTICLE 13. AUDIT

Le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris les inspections, par le Client ou un autre auditeur qu'elle a mandaté, et contribuer à cet audit.

Les opérations d'audit sont à la charge exclusive du Client qui ne pourra réclamer de défraiement au Prestataire sauf audit exceptionnel diligenté à la suite de défaillances dans les obligations du Prestataire concernant la mise en œuvre des Prestations ou en cas de suspicion d'un manquement grave aux obligations et si cette suspicion s'avère fondée à la suite des opérations d'audit.

ARTICLE 14. SORT DES DONNÉES

Au terme du contrat, le Prestataire, selon les instructions du Client, s'engage à :

- détruire toutes les données à caractère personnel ou les renvoyer au Client ;
- détruire toutes les copies existantes sauf obligation légale de les conserver. Une fois détruites, le Prestataire doit justifier par écrit de la destruction.

ARTICLE 15. ENTREE EN VIGUEUR

L'Avenant prend effet rétroactivement le 25 mai 2018 pour la même durée que le Contrat.

ARTICLE 16. DIVERS

L'Avenant est composé du présent document et de ses 4 annexes.

Fait à _____ le _____ en deux exemplaires originaux, chacune des Parties reconnaissant, par sa signature, avoir reçu le sien.

Pour le Prestataire :

Nom :

Qualité :

Signature :

Pour le Client :

Nom :

Qualité :

Signature :

Annexe 1 (avenant)
Finalités des traitements

Description des traitements faisant l'objet de la sous-traitance

Catégories de données	Finalités	Nature du traitement	Durée de conservation	

Annexe 2 (avenant)
Prestataires tiers intervenant en liaison avec le prestataire

Prestataire tiers n° 1

Dénomination sociale .....

.....

Adresse .....

.....

Coordonnées de contact .....

Missions pour le compte du Client .....

.....

.....

Prestataire tiers n° 1

Dénomination sociale .....

.....

Adresse .....

.....

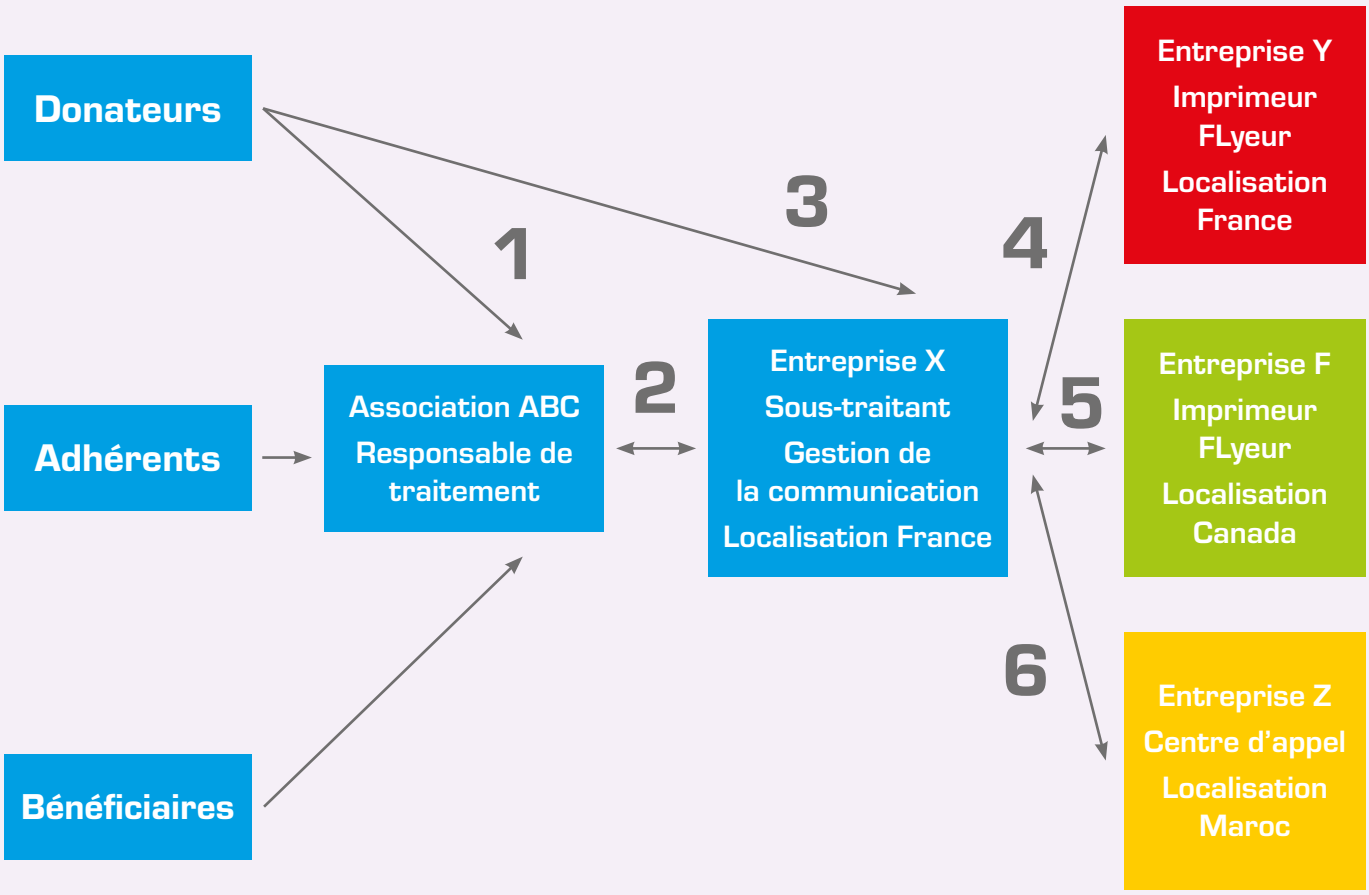
Coordonnées de contact .....

Missions pour le compte du Client .....

.....

.....

Annexe 3 (avenant)
Exemple de schéma de flux de données personnelles – chaine sous traitance



Transferts France

Transferts hors U.E. Adéquat

Transferts U.E. Non Adéquat

Flux de données

1 Identité, adresse, don, ...
2 Nom, Prénom, adresse, numéro tél, adresse mail, ...
3 Informations concernant le donateur,...
4 Nom, prénom, adresse, don, ...
5 Nom, Prénom, numéro tél, don, ...
6 Nom, Prénom, adresse, adresse mail, don, ...

Annexe 4 (avenant)
Mesures de sécurité du traitement

Cette annexe présente, de façon détaillée, les dispositifs de sécurité informatique mis en place par le Prestataire (Règlement, Article 32).

Hébergement

- Descriptif du centre d'hébergement principal
- Descriptif du centre d'hébergement de secours

Sécurité des infrastructures

- Sécurité logique
- Sécurité des accès réseaux
- Sécurité des postes de travail
- Sécurité des transferts de flux

Sécurité organisationnelle

- Confidentialité

Supervision

Solutions de secours

- Continuité de service
- Procédure de sauvegarde
- Archivage et destruction des données


France
générosités

94/96 boulevard Magenta – 75010 Paris
Tél. 01 53 36 35 49 – Fax 01 45 96 41 96
info@francegenerosites.org

www.francegenerosites.org

France générosités