FONDATION PLURIEL

Conjuguons nos singuliers

CHARTE DE LA FONDATION PLURIEL EN FAVEUR DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Préambule

Les applications numériques connaissent un accroissement considérable et concernent aujourd'hui tous les aspects de notre vie quotidienne. Elles ouvrent des potentialités en termes de fichage, de stockage et d'usage de données à caractère personnel qui induisent des interrogations éthiques et nécessitent un encadrement juridique.

La France a déterminé un dispositif juridique de la protection numérique de la vie privée bien avant la révolution numérique des années 1990-2000, puisque c'est la loi ° 78-17 du 6 janvier 1978, dite « Loi Informatique et Libertés », qui règlemente l'utilisation des informations relatives aux personnes physiques.
La Fondation Pluriel est pleinement concernée par cette législation puisqu'elle assume la responsabilité de plus de 40 traitements automatisés de données à caractère personnelle[1] dans le cadre de ses activités.
Cette législation impose des obligations strictes pour le représentant la Fondation et ses employés quant à la collecte et à l'utilisation qui peuvent être faites des données personnelles, à leur durée de conservation, à leur sécurité, et donne des droits aux personnes concernées.

La protection des données des personnes physiques à l'égard des traitements informatiques constitue un droit fondamental pour l'Union européenne. Compte tenu de l'évolution des technologies, de l'intensification de la collecte et des échanges de données, celle-ci a décidé de renforcer et d'uniformiser les règles de protection ; un Règlement européen[2] a ainsi été adopté et s'impose à tous les Etats de l'Union depuis le 25 mai 2018. Celui-ci a été intégré dans la « Loi Informatique et Libertés » en 2018.

Cependant, la protection des données exige l'adoption de mesures techniques et organisationnelles par les organismes qui traitent les données. Cette gouvernance responsable implique notamment de prendre en considération la protection des données dès la conception des applications informatiques et de pouvoir vérifier régulièrement et prouver en permanence le respect des règles légales.

Consciente que la protection de la vie privée des usagers, des familles, des bénévoles et des salariés doit faire l'objet d'une vigilance particulière et constante, la Fondation Pluriel a donc souhaité édicter la présente charte. Elle s'inscrit dans le cadre des principes d'éthique et de transparence qui guident l'action de la Fondation.

[1] Art2 loi 78~1 7: Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée au qui peut être identifiée, directement au indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.
[2] Règlement n"2016/579 du Parlement et du Conseil du 27ovril2016 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.

Périmètre

Cette charte s'applique à l'ensemble du périmètre de la Fondation Pluriel.

Elle concerne également toute personne, physique ou morale, qui serait amenée à traiter des données à caractère personnel pour le compte de la Fondation.

Principes et objectifs

La présente charte établit une politique de gestion informatique des données à caractère personnel reposant sur cinq principes essentiels :

- Se conformer aux normes d'application facultatives et aux recommandations de la Commission Nationale de L'Informatique et des Libertés (CNIL) et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), tout en répondant aux besoins de l'Association (et notamment des usagers) ;
- Anticiper l'application des règles de protection des données lors de la conception de produits et services informatiques destinés à traiter des données personnelles ;
- Contrôler en permanence le respect des obligations légales et des engagements pris par la Fondation Pluriel pendant toute la durée de vie des traitements de données ;
- Assurer la plus grande transparence sur les traitements de données, à l'exception des informations dont la divulgation serait susceptible de compromettre leur sécurité ;
- Faciliter l'exercice des droits que la loi reconnaît aux personnes dont les données sont traitées.

Elle a pour ambition de permettre à la Fondation Pluriel de respecter les obligations du Règlement européen sur la protection des données personnelles adopté le 27 avril 2016.
La mise en œuvre de cette politique constitue un gage de confiance pour l'ensemble des parties prenantes (usagers, salariés, clients, partenaires...) et contribue à sécuriser l'action de la Fondation.

Diffusion

Cette charte est communiquée à la Commission Ethique mise en place par la Fondation et aux Instances Représentatives du Personnel.
Elle est diffusée auprès de toute personne extérieure concernée par les traitements de données à caractère personnel mis en œuvre par la Fondation Pluriel ou par toute personne ayant légitimement accès aux ressources informatiques qu'elles utilisent.
Elle fait l'objet d'une mise à disposition permanente sur le site Internet de la Fondation et sur son intranet.

Règles de protection des données

Cette charte décrit l'ensemble des mesures, règles et moyens mis en œuvre par la Fondation Pluriel pour appliquer les cinq principes précédemment énumérés. Véritable « code de conduite », elle détermine les rôles et les responsabilités de chacun des acteurs impliqués dans la mise en œuvre des traitements informatiques.

Responsabilité

Protection des données dès la conception et protection des données par défaut :

La Fondation Pluriel accomplit toutes les démarches requises par la loi « Informatique et libertés » et le « Règlement Général à la Protection des Données » préalablement à la mise en œuvre des traitements de données à caractère personnel, soit :

- S'assurer que le délégué à la protection des données est associé en temps utile à toutes les questions relatives à la protection des données personnelles ;
- Evaluer les risques de chaque traitement afin de mettre en œuvre les moyens techniques et organisationnels appropriés pour que le traitement soit assorti de mesures suffisantes pour garantir la protection des droits et libertés des personnes ;
- S'assurer avant de confier à un tiers une opération de traitement que celui-ci présente les garanties suffisantes demandées ;
- En cas de risque élevé pour les droits et les libertés des personnes physiques, réaliser une analyse d'impact

Ces engagements sont mis en œuvre dès lors que les outils informatiques portent sur des données réelles et non fictives, même lorsque les traitements sont mis en œuvre à titre expérimental.

Registres

Comme l'impose le Règlement Européen à la Protection des Données, la Fondation Pluriel tient à jour des registres répertoriant les traitements de données à caractère personnel en tant que responsable de traitement et en tant que sous-traitant.

En outre, ces registres comportent une description de chaque traitement :

- Le nom et l'adresse du responsable du traitement et de son représentant légal ;
- La fonction de la personne auprès de laquelle s'exerce le droit d'accès et de rectification ;
- L'existence ou non d'un sous-traitant ;
- Le service chargé de la mise en œuvre du traitement ;
- Les finalités et sous-finalités du traitement ;
- Son fondement juridique ;
- Sa date de mise en œuvre ;
- L'outil utilisé et sa description ;
- Les dates des mises à jour ;
- Une description des catégories de données traitées ;
- La durée de conservation de chaque type de données ;
- Les catégories de personnes dont les données sont traitées ;
- Les catégories de destinataires internes et les catégories de destinataires externes habilités à recevoir communication régulière des données ;
- En cas de transfert hors Union Européenne, la finalité du transfert, les catégories de personnes concernées, la nature des données transférées, les catégories de destinataires du transfert (prestataire, etc.), la nature des traitements opérés chez le destinataire, le pays d'établissement et la garantie permettant d'encadrer le transfert ;
- Les mesures prises pour assurer la sécurité des données ;

Aux termes de la loi, les registres sont communicables, si la Fondation Pluriel l'estime opportun, à toute personne qui en fait la demande. Soucieuse d'assurer la plus grande transparence sur son activité, la Fondation Pluriel a décidé de les mettre en permanence à la disposition de tous sur l'Intranet de l'association.

Pièces justificatives

Les documents attestant du respect des règles décrites dans la présente charte font l'objet d'une conservation centralisée et sécurisée et peuvent ainsi être immédiatement présentés à la CNIL en cas de contrôle.

Finalités de la collecte de données à caractère personnel :

La Fondation Pluriel détermine précisément les finalités pour lesquelles elle recueille des données à caractère personnel. Ces finalités sont légitimes et respectées pendant la durée de vie du traitement.

Les données recueillies ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

Les organismes destinataires des données sont informés des règles d'utilisation : une utilisation des données pour une finalité autre que celles prévues par une loi ou par la Fondation Pluriel n'est pas autorisée.

Transparence et licéité de la collecte

La Fondation Pluriel ne collecte pas de données à caractère personnel à l'insu des personnes concernées. De la même manière, la Fondation Pluriel ne collecte pas des données à caractère personnel lorsque les personnes concernées s'y opposent légitimement.

La Fondation Pluriel indique aux personnes auprès desquelles elle recueille leurs données à caractère personnel :

- L'entité responsable du traitement et ses coordonnées ;
- Les finalités poursuivies par le traitement auquel les données sont destinées ;
- La base juridique du traitement ;
- Le caractère obligatoire ou facultatif des réponses et les conséquences éventuelles, à leur égard, d'un défaut de réponse ;
- Les destinataires des données ;
- La durée de conservation des données ;
- Les droits d'accès, de rectification, à limitation, à portabilité et d'opposition que les personnes concernées tiennent des dispositions légales, les fonctions et coordonnées de la personne auprès de laquelle ils s'exercent ;
- Le cas échéant, les transferts de données à caractère personnel à destination d'un Etat non membre de l'Union européenne ;
- La possibilité d'introduire une réclamation auprès d'une autorité de contrôle.

Limitation de la collecte des données à caractère personnel

La Fondation Pluriel se limite au recueil des seules données à caractère personnel autorisées par les textes et nécessaires à l'atteinte des finalités énoncées.

En application de ce principe de « minimisation » des données, elle contrôle régulièrement les enregistrements de données, s'assure que les dispositifs informatiques ne permettent pas d'enregistrer des données non autorisées et sensibilise son personnel pour que seules des données objectives, neutres et factuelles soient enregistrées.

Elle veille particulièrement à ce qu'aucun enregistrement de données sensibles (santé, opinions...) ne soit fait à l'insu des personnes concernées, sauf disposition législative spécifique.

Limitation de la conservation des données à caractère personnel

La Fondation Pluriel veille à la mise à jour des données à caractère personnel qu'elle traite tout en respectant les finalités visées.

Les durées de conservation n'excèdent pas celles nécessaires à l'atteinte des finalités visées et respectent les normes réglementaires applicables.

La Fondation Pluriel privilégie les effacements automatiques des données personnelles ou s'assure de leur anonymisation selon les modalités prescrites par la CNIL.

Elle sensibilise ses salariés afin qu'aucune extraction de données ne soit conservée au-delà de la durée nécessaire et suffisante.

Sécurité physique et logique des données à caractère personnel

La Fondation Pluriel détermine et met en œuvre les moyens nécessaires à la protection des systèmes de traitement de données à caractère personnel pour éviter toute intrusion malveillante et prévenir toute perte, altération ou divulgation de données à des personnes non autorisées.

Ainsi le Schéma Directeur Informatique, révisé tous les cinq ans précise les 8 axes de sécurité informatique mis en œuvre à la Fondation Pluriel. Une vérification quotidienne du fonctionnement des mesures de sécurité est consignée dans le rapport d'exploitation établi par le service informatique. Une journalisation des accès aux bases de données les plus sensibles est assurée. Des audits sur les modifications des droits d'accès sont régulièrement réalisés et consignés.

La Fondation Pluriel détermine et met en œuvre des mesures permettant de garantir la confidentialité des données, notamment par des actions de sensibilisation des salariés et des recommandations de bonnes pratiques quant à l'utilisation de leurs postes de travail informatique.

La Fondation Pluriel exige de ses prestataires de services informatiques qu'ils présentent des garanties suffisantes pour assurer la sécurité et la confidentialité des données à caractère personnel. A cette fin elle inscrit systématiquement les prescriptions requises dans les pièces des marchés de fourniture de produits et services informatiques.

Elle s'assure que les prestataires de services informatiques prennent toute disposition pour empêcher la divulgation ou l'altération des données, n'assurent pas d'opération de télémaintenance sans un contrôle de la Fondation Pluriel, et restituent les données en fin de contrat.

Droits d'accès, de rectification, de limitation ou d'opposition

La Fondation Pluriel veille à informer toute personne qui en fait la demande de l'existence de données à caractère personnel qui la concernent, de l'usage qui en est fait et de ses droits de rectification, de limitation ou d'opposition.

Une procédure est mise en place afin que la mention des droits des personnes soit systématiquement prévue lors de la conception des formulaires de collectes de données (sur support papier ou en ligne).

La Fondation Pluriel met en œuvre les moyens nécessaires pour garantir et faciliter l'exercice des droits des personnes dont les données sont traitées :

- Une procédure de gestion des réclamations et demandes relatives à l'exercice des droits des personnes détermine notamment les modalités d'exercice, la chaîne de traitement et les délais de communication. Celle-ci est consultable sur l'intranet de la Fondation Pluriel ;
- La Fondation Pluriel donne suite à toute demande d'accès, de rectification, de limitation ou d'opposition dans un délai d'un mois à compter de la vérification de l'identité du demandeur et de la réalité de ses droits. Au besoin, ce délai peut être prolongé d'une durée équivalente, compte tenu de la complexité de la demande et du nombre de données sollicitées. La Fondation Pluriel informe alors la personne concernée de cette prolongation et des motifs du report. Conformément à la loi, la Fondation Pluriel peut cependant s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique ;
- La transmission des données demandées est faite de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simple ;
- Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il

en soit autrement. Lorsque la communication des informations se fait sur un autre support elle s'effectue sans frais pour le demandeur ;

- La Fondation Pluriel prend toute mesure pour rectifier ou supprimer les informations erronées et en fournir la preuve aux personnes concernées ;
- Toutes les demandes et les suites qui leurs sont réservées sont répertoriées dans un registre tenu à la disposition de la CNIL.

Gestion des violations de données

Un dispositif de détection des violations éventuelles de données[3] est mis en œuvre afin que des mesures de remédiation soient aussitôt élaborées, appliquées et contrôlées.

En cas de risque au regard de la vie privée des personnes concernées, la Fondation Pluriel informe la CNIL dans un délai maximal de 72 heures après leur détection. Si cela a des conséquences sur la sécurité des soins et la disponibilité, l'intégrité et/ou confidentialité des données de santé, l'incident est à signaler à l'Agence Régionale de Santé. Lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés, les personnes dont les données personnelles auraient été interceptées sont informées.

Accès aux données - Transfert de données

Dans le cas où la Fondation Pluriel a recours à des prestataires de service pour la collecte, le traitement et l'hébergement des données, ils sont notamment choisis pour les garanties de sécurité suffisantes qu'ils offrent. Un contrat écrit comportant les clauses obligatoires imposées par le « Règlement Européen à la Protection des données » est établi entre la Fondation Pluriel et les prestataires.

Les destinataires des données sont mentionnés sur les formulaires de collecte des données. Ils sont informés que l'usage qu'ils font des données doit être conforme à la finalité du traitement mis en œuvre par la Fondation Pluriel.

- La Fondation Pluriel peut avoir l'obligation de transmettre des données à caractère personnel à des autorités habilitées par la loi, notamment si elle en est tenue par réquisition judiciaire. Dans ces cas, une vérification de l'identité du demandeur et du fondement légal de la demande est réalisée selon une procédure formalisée. La Fondation Pluriel veille notamment à ce que -sauf disposition législative spécifique- la transmission ne porte pas sur l'ensemble d'une base de données mais uniquement sur la personne visée par la réquisition et pour une période limitée.
  La Fondation Pluriel s'engage à ne pas transférer les données en dehors de l'Union Européenne vers des pays dont la CNIL considère qu'ils n'offrent pas un niveau suffisant de protection des données.

Dans le cas où La Fondation Pluriel souhaite recourir au « cloud computing » qui peut conduire à un transfert des données vers l'étranger :

- Elle détermine les données pouvant être hébergées dans le « cloud computing » en fonction de leur sensibilité ou de réglementations spécifiques (sur les données de santé par exemple) ;
- Elle identifie le type de service et le mode de déploiement les plus adaptés à ses besoins ;
- Elle définit ses propres exigences de sécurité technique et juridique au regard notamment de risques potentiels (défaillance du prestataire par ex.), et choisit le prestataire en fonction des garanties offertes ;
- Elle demande une formalisation des règles de sécurité et de confidentialité des données dans le cohtrat de prestation de services en se fondant sur les clauses contractuelles type édictées par le « Règlement Européen à la Protection des données ».

[3] : on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l 'objet d'un traitement

Moyens dévolus à la protection des données

Délégué à la Protection des Données

Conformément aux dispositions du « Règlement Européen à la Protection des données », la Fondation Pluriel a désigné un Délégué à la Protection des Données désigné sous le nom de « Délégué à la Protection des Données » (DPO), après notification à la CNIL et information des représentants du personnel.

- Sa mission s'applique par conséquent à l'ensemble des traitements informatiques de données personnelles ;
- Elle s'exerce pour l'ensemble du périmètre de la Fondation Pluriel ;
- Le DPO exerce ses missions en toute indépendance avec respect de la confidentialité et ne reçoit aucune instruction pour l'exercice de sa mission ;
- Le DPO est rattaché à la Direction générale qu'il rencontre plusieurs fois par an ;
- Il est associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;
- Il est consulté, préalablement à leur mise en œuvre, sur l'ensemble des nouveaux traitements de données à caractère personnel ;
- Il établit et tient à jour des registres recensant de façon exhaustive les traitements de données à caractère personnel et les met à la disposition des personnes concernées ;
- Il informe et conseille les responsables des traitements ainsi que le personnel qui procèdent aux traitements sur les obligations qui leur incombent en vertu des lois et des règlements en vigueur en matière de protection des données ;
- Il veille au respect des obligations prévues par la loi et les règlements en vigueur en réalisant une analyse des traitements, en termes de finalité, de proportionnalité, de pertinence des données, de durée de conservation, de destinataires, d'encadrement des sous-traitants, d'information sur les droits des personnes et de transferts hors UE et informe le responsable de traitement s'il faut réaliser une analyse d'impact relative à la protection des données ;
- Il conseille sur la réalisation de l'analyse d'impact relative à la protection des données et vérifie l'exécution de celle-ci en termes de sécurité, de confidentialité et d'intégrité des traitements. Cette analyse détermine un niveau de criticité et les mesures à prendre pour réduire la gravité et/ou la probabilité des risques identifiés pour chaque traitement ;
- A cette fin, il peut faire toute recommandation utile au responsable de traitement, il établit un plan d'actions correctives et préventives qu'il présente à la Direction générale et consulte la CNIL lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
- Il pilote et documente la conformité, supervise les actions permettant de juger du degré de conformité de la Fondation Pluriel, de mettre en évidence les éventuelles non-conformité et de vérifier le respect du cadre légal ou de la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles ;
- Il veille à une sensibilisation des personnes qui traitent des données à caractère personnel par tous les moyens utiles ;
- Il reçoit et traite toutes les questions des personnes concernées relatives au traitement de leurs données à caractère personnel et à l'exercice de leurs droits ;
- Il informe la Direction générale des manquements constatés ;
- Il établit un bilan annuel de ses activités qu'il présente à la Direction Générale ;
- Le DPO coopère avec la CNIL et fait office de point de contact de celle-ci ;
- Pour l'exercice de ses missions le DPO dispose d'un soutien en termes de ressources financières et d'infrastructures et suit régulièrement des formations dispensées par la CNIL ou par d'autres organismes.

Référents à la Protection des Données :

Un réseau de personnes identifiées (nommément, par direction ou par service) assiste le DPO dans ses missions :

- Ces Référents à la Protection des Données sont sensibilisés aux problématiques et principes de protection des données ;
- Ils permettent d'améliorer la connaissance et la régularité des traitements relevant de la « loi informatique et Libertés » et du « règlement européen à la protection des données » ;
- Ils contribuent à la sensibilisation du personnel ;
- Ils assurent un rôle d'alerte du DPO en cas de constat d'un manquement à la loi et au règlement en vigueur.

Auditeurs internes

Afin de pouvoir vérifier la conformité des traitements de données les plus sensibles selon une périodicité biennale, une équipe d'auditeurs est affectée à cet examen :

- Les auditeurs font partie du personnel et justifient d'une formation à l'audit par un organisme extérieur qualifié ;
- Ils ont déjà réalisé au moins un exercice pratique d'audit, en présence d'un formateur/auditeur qualifié ;
- Leur qualification est maintenue via la conduite d'au moins un audit par an d'une part, la participation à la réunion annuelle des auditeurs internes d'autre part ;
- Pour la conduite de l'audit « Protection des données personnelles » ils bénéficient d'une formation préalable spécifique sur les principes de protection des données et les points de contrôles.

Procédures internes

Des procédures internes destinées à assurer le respect des règles de protection des données sont élaborées par le DPO en relation avec les services, signées par le directeur Général ou les responsables concernés, diffusées et mises à jour.

Elles concernent à ce jour :

- Les modalités de gestion des nouveaux traitements et de mise à jour des traitements existants ;
- Le contrôle de la mise en œuvre des mesures de protection des données personnelles et l'évaluation de l'efficacité des mesures de sécurité ;
- L'analyse de la conformité des nouveaux traitements ou des modifications des traitements existants afin de s'assurer de la protection des données par défaut et dès la conception ;
- Les analyses d'impact à la protection des données ;
- Le traitement des demandes d'exercices des droits des personnes ;
- La gestion des violations de données.

Validité et actualisation

La présente charte entre en vigueur le 1er mars 2022. Elle fera l'objet d'une actualisation en cas de besoin.

Le Directeur Général de la Fondation Pluriel

Franck AIGUBELLE