Une image contenant texte

Description générée automatiquement

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l’Union européenne est entré en application le 25 mai 2018. L’adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

L’association <NOM> a décidé de se mettre en conformité au RGPD.

ETUDE D’IMPACT SUR LA VIE PRIVEE

Règlement Général sur la Protection des Données

Intègr’Action Conseil

ljaunaux@integraction.fr

06 18 55 76 13

# Informations préliminaires

Ce document a été créé à l’usage exclusif des association fraternelles ; il est sous copyright. Vous pouvez le modifier, le compléter mais en aucun cas lui ôter sa page de garde ni la page de présentation d’Intègr’Action Conseil.

Ce document est essentiel, il doit faire partie des documents légaux que la CNIL peut vous demander en tant qu’association victime d’une fuite de données.

Il a d’abord été rédigé à l’usage des loges de la Grande Loge Franco-Maltaise (https://www.gl-fm.org) et est utilisable par toute association fraternelle qui souhaite avoir une étude de risques, même si elle dépend d’une fédération (GL, GO…)

Ce document vient en complément du registre des traitements mis à disposition des associations fraternelles. Il doit être adapté en fonction des traitements identifiés dans le registre.

Gardez en mémoire, et c’est de loin le plus important, que tout ceci est fait pour protéger les Frères et Sœurs de toute fuite de données. La plupart du temps vous appliquez déjà les mesures élémentaires de protection des données sans en avoir rédigé les principes.

C’est désormais chose faite.

# Etude d’impact sur la vie privée de <ASSOCIATION>.

## Table des matières

[Informations préliminaires 1](#_Toc99210954)

[Etude d’impact sur la vie privée de <ASSOCIATION>. 2](#_Toc99210955)

[Table des matières 2](#_Toc99210956)

[Intègr’Action Conseil 4](#_Toc99210957)

[Avants propos 5](#_Toc99210958)

[1- Périmètre du PIA 5](#_Toc99210959)

[1.1 Contexte et traitement concerné 5](#_Toc99210960)

[1.2 Description du traitement 6](#_Toc99210961)

[Pour la gestion des candidatures 6](#_Toc99210962)

[Pour la gestion des comptes-rendus 6](#_Toc99210963)

[Pour la gestion des membres 7](#_Toc99210964)

[Pour la gestion des cotisations 7](#_Toc99210965)

[Pour la gestion du tronc hospitalier 7](#_Toc99210966)

[Pour la gestion des publications 7](#_Toc99210967)

[1.3 Référentiels 8](#_Toc99210968)

[1.4 Données, processus et support 8](#_Toc99210969)

[Données, destinataires et durées de conservation 8](#_Toc99210970)

[1.5 Description des processus et supports 12](#_Toc99210971)

[Cartographie du système d’information 12](#_Toc99210972)

[Flux Gestion des candidatures 13](#_Toc99210973)

[Flux Gestion des comptes-rendus 14](#_Toc99210974)

[Flux Gestion des membres 14](#_Toc99210975)

[Flux Gestion des cotisations 14](#_Toc99210976)

[Flux Gestion du tronc hospitalier 14](#_Toc99210977)

[Flux Gestion des publications. 15](#_Toc99210978)

[2- Dispositif de Conformité et Principes Fondamentaux 15](#_Toc99210979)

[2.1 Les mesures de nature juridique 15](#_Toc99210980)

[2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées 16](#_Toc99210981)

[Concernant la gestion des candidatures 16](#_Toc99210982)

[Concernant la gestion des comptes-rendus 17](#_Toc99210983)

[Concernant la gestion des membres 18](#_Toc99210984)

[Concernant la gestion des cotisations 20](#_Toc99210985)

[Concernant la gestion du tronc hospitalier 21](#_Toc99210986)

[Concernant la gestion des publications 22](#_Toc99210987)

[3- Les atteintes potentielles à la vie privée 23](#_Toc99210988)

[3.1 Les vulnérabilités identifiées 23](#_Toc99210989)

[3.2 Les événements redoutés – Identification des risques 23](#_Toc99210990)

[3.3 Les menaces sur la vie privée 24](#_Toc99210991)

[3.4 Etude des risques sur la vie privée 24](#_Toc99210992)

[Tableau des risques selon la criticité et la vraisemblance. 24](#_Toc99210993)

[4- Validation du PIA 25](#_Toc99210994)

[4.1 Formalisation des mesures de sécurité à déployer 26](#_Toc99210995)

[4.2 Préconisations de sécurisation 26](#_Toc99210996)

[5- Réagir en cas de violation des données personnelles 27](#_Toc99210997)

[5.1 Documenter la violation 27](#_Toc99210998)

[5.2 Délais 27](#_Toc99210999)

[5.3 Notifier à la CNIL 28](#_Toc99211000)

[5.4 Action de la CNIL 28](#_Toc99211001)

[5.5 Cadre Légal 28](#_Toc99211002)

[Révisions du Document 29](#_Toc99211003)

## Intègr’Action Conseil

Intègr’Action Conseil. est une Société fondée en octobre 2016. Malgré sa jeunesse apparente, Laurent Jaunaux - son fondateur - a exercé le métier de Consultant en Systèmes d’Informations pendant plus de 25 années à l’international. Il a travaillé pour des Sociétés de Conseil en Systèmes d’Informations (SSII) parmi les plus grosses :

* Corporate Business Solutions (Société basée en Allemagne)
* Wipro Technologies (Société Indienne - 158.000 employés)
* Tata Consultancy Services (Société Indienne - 488.000 employés)

En tant que Consultant et Manager, il a travaillé pour des grands comptes, concevant ou déployant leurs systèmes d’information ou les conseillant sur leurs politiques de sécurité des systèmes d’information. Parmi ces comptes nous trouvons :

* EADS
* Thales
* Shell
* OCDE
* Heidelberger Drückmaschinen
* …

Après plus de 25 années de Conseil, Laurent Jaunaux a souhaité créer sa propre entreprise afin de répondre aux besoins d’entreprises plus modestes, plus accessibles et à la taille plus humaine.

**Laurent Jaunaux est certifié ISO 27001**, « Lead Auditor » dans la mise en place de systèmes de management de la sécurité de l’information (cybersécurité). Il est également certifié EBIOS (méthode de gestion des risques de l’Agence Nationale de Sécurité des Systèmes d’Information), membre du réseau « cybermalveillance » de l’ANSSI et formateur enregistré comme tel auprès de la DIRRECT à Montpellier.

Intègr’Action Conseil. fournit les services suivants :

* Conseil en Sécurité de l’Information (Cybersécurité, RGPD, DPO…)
* Formation Professionnelle (Nouvelles Technologies, Confidentialité, Internet…). A ce titre Intègr’Action Conseil. possède un numéro de formateur.

Soucieuse du développement durable et consciente de sa responsabilité sociale, Intègr’Action Conseil est une entreprise qui s’engage au respect des normes ISO 26000.

## Avants propos

La CNIL a exposé aux différents acteurs de la sécurité des systèmes d’information la méthodologie requise pour rédiger une étude d’impact sur la vie privée, encore appelée PIA pour Privacy Impact Assessment.

Celle-ci repose sur 4 éléments :

1. Une étude du contexte
2. Une étude des principes fondamentaux
3. Une étude des risques liés à la sécurité des données
4. Une validation du PIA.

Le PIA que nous vous proposons repose sur cette méthodologie commune à l’ensemble des pays de l’Union Européenne.

Concernant l’étude de risques, la méthodologie que nous appliquons est proportionnelle à la taille de l’entreprise. Il s’agit d’une étude adaptée par Laurent Jaunaux sas sur la méthodologie COSO et guidée par un formulaire détaillant les points de contrôles.

Cette méthodologie d’audit est rapide à mettre en place et elle concerne les points suivants :

1. Développements et acquisitions
2. Gestion du changement
3. Sauvegardes et restaurations
4. Désastres
5. Continuité d'activité
6. Accès logiques
7. Accès physiques
8. Traitements et batchs
9. Direction et gouvernance
10. Contrats et prestataires

# 1- Périmètre du PIA

## 1.1 Contexte et traitement concerné

Une association fraternelle est généralement tournée vers le symbolisme, la philosophique, la spiritualité et elle aborde souvent des sujets d’actualité liés à des thématiques politiques ou religieuses.

Ces associations n’emploient généralement pas de salariés. Tous leurs membres sont des bénévoles.

L’aspect initiatique de l’association doit être retenu comme composante essentielle. Ses membres sont divisés en 3 grades – mot issu de la terminologie militaire – qui sont :

* Apprenti
* Compagnon
* Maître Maçon.

L’association fraternelle est déclarée association Loi 1901.

Pour le RGPD, il est important de prendre en compte le fait que l’association s’adresse aux particuliers.

Compte tenu de ses activités, le traitement concerne les données personnelles qui sont saisies dans différents outils :

* Un outil obédienciel ; l’obédience est une fédération d’associations qui ont choisi d’en faire partie. C’est dans ces outils que sont généralement gérés les membres.
* Un outil propre à l’association, souvent une feuille Excel.

Les données personnelles se retrouvent dans différents documents, à savoir :

* Des comptes-rendus d’activités ou de réunions,
* Des publications (annuaires etc…)
* Une gestion des comptes
* Etc.

Autre point important : Les délais de conservation liés aux activités des associations fraternelles sont extrêmement longs comme pourrait en attester le droit coutumier. Les documents sont utilisés à fins historiques et généalogiques.

## 1.2 Description du traitement

L’activité de base des associations fraternelles est la gestion d’une association qui permet à ses membres de pouvoir s’exprimer et de débattre sur différents sujets d’actualité, politiques, philosophiques, symboliques, spirituels, religieux… Cela concerne son recrutement, sa vie associative, ses publications…

Le traitement et ses activités sont liés aux activités initiatiques de l’association, également aux activités liées à sa gestion, aux conférences et aux publications.:

### Pour la gestion des candidatures

|  |  |
| --- | --- |
|  | Gestion des candidatures |
| Description | Il s’agit de la prise en charge de la candidature d’un candidat, depuis sa candidature officielle jusqu’à son refus ou son admission. |
| Finalité | L’objectif est d’assurer la gestion des candidatures de l’association. |
| Enjeux | Avoir les informations adéquates sur le client afin de suivre de façon efficace l’évolution de sa candidature. |
| Responsable | * <PRESIDENT> |
| Sous-traitants | * Aucun |

### Pour la gestion des comptes-rendus

|  |  |
| --- | --- |
|  | Gestion des comptes rendus |
| Description | Il s’agit de la gestion des comptes-rendus et de leurs contenus. |
| Finalité | L’objectif est d’assurer le suivi des activités de l’association. Les activités sont consignées dans un cahier dédié à cet effet. |
| Enjeux | Avoir des comptes-rendus fidèles et disponibles pour les membres de l’association. |
| Responsable | * <SECRETAIRE> |
| Sous-traitants | * Aucun |

### Pour la gestion des membres

|  |  |
| --- | --- |
|  | Gestion des membres |
| Description | Il s’agit de la gestion des membres de l’association et de leurs progrès initiatiques. |
| Finalité | L’objectif est d’assurer le suivi des membres de l’association. |
| Enjeux | Avoir des informations exhaustives et intègres concernant les membres de l’association. |
| Responsable | * <PRESIDENT> |
| Sous-traitants | * Aucun |

### Pour la gestion des cotisations

|  |  |
| --- | --- |
|  | Gestion des cotisations |
| Description | Il s’agit de la gestion des cotisations des membres de l’association. |
| Finalité | L’objectif est d’assurer le suivi des cotisations des membres de l’association. |
| Enjeux | Avoir des informations complètes concernant les cotisations et versements des membres de l’association. |
| Responsable | * <TRESORIER> |
| Sous-traitants | * Aucun |

### Pour la gestion du tronc hospitalier

|  |  |
| --- | --- |
|  | Gestion du tronc hospitalier |
| Description | Il s’agit de la gestion des aides que l’association accorde à ses membres. |
| Finalité | L’objectif est d’assurer le suivi des aides que l’association accorde aux membres de l’association. |
| Enjeux | Avoir des informations complètes concernant les aides et leurs versements aux membres de l’association qui en ont besoin. |
| Responsable | * <HOSPITALIER> |
| Sous-traitants | * Aucun |

### Pour la gestion des publications

|  |  |
| --- | --- |
|  | Gestion des publications |
| Description | Il s’agit de la gestion des publications que l’association fait. |
| Finalité | L’objectif est d’assurer le suivi de la création de publications qui seront rendues publiques. |
| Enjeux | Avoir les textes qui seront publiés en tenant compte des impératifs ou demandes d’anonymisation. |
| Responsable | * <PRESIDENT> |
| Sous-traitants | * Aucun |

## 1.3 Référentiels

Il est difficile de demander à des associations de bénévoles d’avoir des référentiels de sécurisation des systèmes d’information. C’est pourquoi nous recommandons le guide d’hygiène informatique édité par l’Agence Nationale de Sécurité des Systèmes d’Information. Il est disponible ici :

<https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf>

## 1.4 Données, processus et support

### Données, destinataires et durées de conservation

|  |  |  |
| --- | --- | --- |
| Donnée | Destinataires | Durée de conservation |
| GESTION DES CANDIDATURES | | |
| Données d’état-civil : civilité, nom, prénom, photo, adresse, numéro de téléphone, état-civil, enfants. | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de l’adhésion + archivage historique. |
| Données professionnelles : CV, Société, Groupe fonction, direction, numéro de téléphone professionnel. | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de la candidature jusqu’à refus/admission. |
| Données internet : Email, site web | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de l’adhésion. |
| Données diverses : Activités extra-professionnelles, lettre de motivation. | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de la candidature jusqu’à refus/admission.. |
| Données maçonniques : Date de refus/d’admission. | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de la candidature jusqu’à refus/admission. |
| Données sensibles : Appartenances religieuses, appartenances politiques, opinions philosophiques, extrait de casier judiciaire. | * Le Président de l’association : Il collecte l’ensemble des informations. * Les 3 enquêteurs : Chacun rédige son enquête et il ignore qui sont les 2 autres. * Les membres de l’association qui ignorent qui sont les enquêteurs. * Le secrétaire et le trésorier de l’association. | Durée de la candidature jusqu’à refus/admission. |
| GESTION DES COMPTES-RENDUS | | |
| Données d’état-civil : nom, prénom. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| Données internet : Email, login et mot de passe du secrétaire. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée du mandat. |
| Données diverses : Présence des membres, participations des membres, date de la réunion concernée. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| Données maçonniques : grades concernés. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| Données sensibles : Appartenances religieuses, appartenances politiques, opinions philosophiques. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| GESTION DES MEMBRES | | |
| Données d’état-civil : civilité, nom, prénom, photo, adresse, numéro de téléphone, état-civil, enfants. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| Données internet : Email, | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée du mandat. |
| Données maçonniques : Date d’admission, Date d’initiation, Date de passage au grade de Compagnon, Date de passage au grade de Maître, Postes occupés. | * Le Secrétaire de l’Association pour archivage. * Les membres de l’association pour approbation/refus du compte-rendu. | Durée de vie de l’association et archivage historique (legs à l’obédience, archives etc…) |
| GESTION DES COTISATIONS | | |
| Données d’état-civil : nom, prénom, adresse, numéro de téléphone. | * Le Président de l’association * Le Trésorier | Durée de l’adhésion. |
| Données internet : Email, | * Le Président de l’association * Le Trésorier | Durée de l’adhésion. |
| Informations d’ordre économique et financier : Montants exigés, dates des versements, montants des versements, ribs. | * Le Président de l’association * Le Trésorier | Durée légale de 10 ans |
| Données maçonniques : Date d’initiation, Date de passage au grade de Compagnon, Date de passage au grade de Maître. | * Le Président de l’association * Le Trésorier | Durée de l’adhésion. |
| GESTION DU TRONC HOSPITALIER | | |
| Données d’état-civil : nom, prénom, adresse, numéro de téléphone, état civil. | * Le Président de l’association * L’hospitalier * Le bénéficiaire des aides | 5 ans. |
| Vie professionnelle : Statut professionnel | * Le Président de l’association * L’hospitalier * Le bénéficiaire des aides | 5 ans |
| Données internet : Email, | * Le Président de l’association * L’hospitalier * Le bénéficiaire des aides | 5 ans |
| Informations d’ordre économique ou financier : Niveau de salaire / revenus, aides sociales, ribs. | * Le Président de l’association * L’hospitalier * Le bénéficiaire des aides | 5 ans |
| Données maçonniques : assiduité aux réunions, montants versés par l’association / compensations, dates de versements. | * Le Président de l’association * L’hospitalier * Le bénéficiaire des aides | Durée légale de 10 ans |
| GESTION DES PUBLICATIONS | | |
| Données d’état-civil : nom, prénom, nom d’emprunt, photo. | * Comité de rédaction. | Jusqu’à la publication. |
| Données internet : Email, | * Comité de rédaction. | Jusqu’à la publication. |
| Données maçonniques : Textes des conférences présentées, travaux de recherche et de réflexion exclusifs. | * Comité de rédaction. | Jusqu’à la publication. |
| Données sensibles : Appartenances religieuses, appartenances politiques, opinions philosophiques. | * Comité de rédaction. | Jusqu’à la publication. |

## 1.5 Description des processus et supports

### Cartographie du système d’information

Le schéma ci-dessous représente la cartographie générale du système d’information des associations fraternelles. Il convient de remarquer qu’elles ne possèdent pas de système d’information propre et que leur système d’information est hétéroclite, qu’il dépend simplement des outils individuels des membres concernés.

Le système d’information d’une association fraternelle peut être cartographié comme suit :

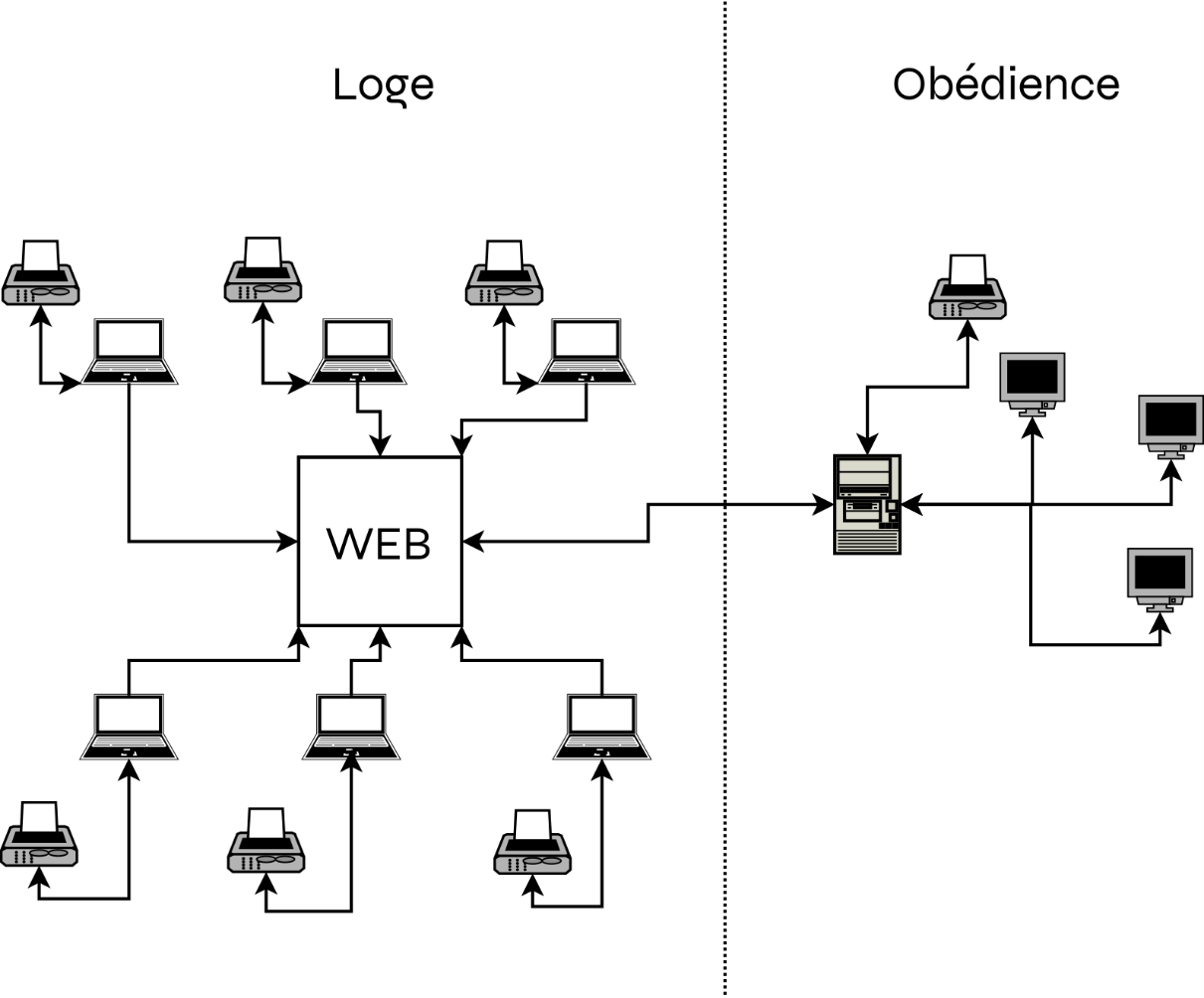


Figure 1 : Cartographie du SI

### Flux Gestion des candidatures

Cette activité concerne le recrutement associatif. La procédure standard de recrutement est la suivante :

Le candidat est généralement parrainé ; il écrit une lettre de motivation au président de l’association en y joignant :

* 2 photos d’identité
* Un cv
* Un extrait de casier judiciaire.

A la suite de sa réception l’ensemble est présenté à l’association. L’association transfert également ces informations à la fédération (obédience) si elle appartient à l’une d’entre elles. Suite à cela le président nomme 3 enquêteurs qui ont pour objectifs :

1. De rencontrer le candidat
2. De comprendre ses motivations et de voir comment le candidat va s’intégrer à l’association.
3. De rédiger un rapport sur le candidat.

Il n’existe aucune limite dans les questions qui sont posées au candidat.

Les rapports sont lus dans l’association. Les membres de l’association se prononcent à la suite de leur lecture.

S’en suit normalement un passage sous le bandeau qui n’est pas concerné par les données personnelles.

A la suite de la procédure, un avis de l’association est donnée sur l’opportunité de la candidature.

### Flux Gestion des comptes-rendus

Chaque réunion fait l’objet d’un compte rendu qui mentionne la date de la réunion, les participants, l’ordre du jours, ce qui y a été dit et fait.

Ce compte rendu prend différent nom. Il est lu dans l’association et fait l’objet d’une approbation.

Les comptes rendus sont ensuite classés dans un cahier, une pochette ou un classeur. Il peut même arriver qu’ils soient à disposition sur un hébergement commun (cloud…).

Ils sont conservés pendant toute la vie de l’association et au delà. Ils ont une valeur historique.

### Flux Gestion des membres

Notre association est essentiellement initiatique, symbolique, philanthropique, philosophique et peut aborder des sujets d’actualité avec parfois des débats pouvant toucher la politique ou la religion.

Etant initiatique, les membres se répartissent en grades qui doivent être gérés de façon spécifiques. Le terme de « grades » fait référence à la terminologie militaire qui rappelle qu’il existe une hiérarchie dans l’association.

Les grades universels sont :

* Apprenti
* Compagnon
* Maître Maçon.

D’autres grades peuvent venir s’y adjoindre selon l’association et la fédération.

Les dates de passage d’un grade à l’autre sont communiqués à la fédération.

### Flux Gestion des cotisations

Comme toute association légalement constituée, la nôtre nécessite d’avoir un budget pour fonctionner.

Ce budget est géré par le Trésorier qui tient à jour une liste des adhérents et de leurs versements.

Les cotisations sont généralement appelées en janvier, au moment de la nouvelle année fiscale.

### Flux Gestion du tronc hospitalier

L’association possède un budget destiné aux œuvres sociales ou à la détresse de ses membres.

Ce budget est géré par l’hospitalier qui tient à jour une liste des membres qui pourraient être dans le besoin et des versements qui leur ont été faits.

L’hospitalier est un officier en charge de la bienfaisance et si il détecte un membre dans le besoin ou la détresse, son rôle, outre le secours moral qu’il peut apporter aux membres, est également de voir avec eux comment ils peut les aider financièrement.

### Flux Gestion des publications.

L’association, dans le cadre de sa mission, peut décider de publier les textes des conférences qui ont marqué son année.

Les publications sont conservées pendant toute la durée de la vie de l’association. Elles ont une valeur historique.

Un comité de rédaction collecte les conférences qui lui ont semblé intéressantes ou bien il peut demander à des membres de lui soumettre des travaux de recherche ou de réflexions. Toute la partie éditoriale est confidentielle en ce sens que certains membres ne souhaitent pas voir leurs noms publiés.

# 2- Dispositif de Conformité et Principes Fondamentaux

## 2.1 Les mesures de nature juridique

Présentation des différentes mesures retenues afin de respecter les exigences légales :

* **Finalité** : finalité déterminée, explicite et légitime. Les DCP sont collectées pour des finalités déterminées, explicites et légitimes ;
* **Minimisation** : réduction des données à celles strictement nécessaires. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs (article 6 de la loi I&L et RGPD) ;
* **Qualité** : préservation de la qualité des données à caractère personnel ; les DCP sont exactes, complètes et, si nécessaire, mises à jour. L’exigence de qualité porte aussi sur le lien entre les données qui identifient les personnes et les données qui les concernent ;
* **Durées de conservation** : durée nécessaire à l’accomplissement des finalités, à défaut d’une autre obligation légale imposant une conservation plus longue. Les DCP sont conservées pendant une durée qui n’excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, à défaut d’une autre obligation légale imposant une conservation plus longue ;
* **Information** : respect du droit à l’information des personnes concernées ;
* **Consentement** : obtention du consentement des personnes concernées ou existence d’un autre fondement légal justifiant le traitement ;
* **Droit d’opposition** : respect du droit d’opposition des personnes concernées ;
* **Droit d’accès** : respect du droit des personnes concernées d’accéder à leurs données ;
* **Droit de rectification** : respect du droit des personnes concernées de corriger leurs données et de les effacer ;
* **Transferts** : respect des obligations en matière de transfert de données en dehors de l’Union européenne ;
* **Formalités** : définition et accomplissement des formalités préalables applicables au traitement.

## 2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

Les mesures sont présentées par activité. Il y a 6 activités.

La licéité de la collecte des DCP des deux activités est fondée sur l’exécution du contrat (Art. 6.1-b du RGPD)

### Concernant la gestion des candidatures

**Les mesures doivent être explicitement écrites dans les dossiers de candidature.**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des candidatures |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de candidatures. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion du candidatures. Les données sont apportées par le candidat lui-même. Toutes les données sont présentées à l’association. |
| Qualité | Données | L'accès aux DCP de cette activité est limité aux membres de l’association. La qualité même des DCP est communiquée par le candidat lui-même dans le cadre de la finalité qui le lie à l’association. |
| Durée de conservation | Données | Les durées de conservation sont liées à la durée de la candidature. Le dossier collecté par l’association est transféré à la confédération dans le cas où elle est liée à elle. L’acceptation ou le refus de la candidature conditionnent la conservation des données liées à la candidature au niveau de l’association fraternelle. |
| Droit à l'information | Données | Le respect du droit à l'information est inscrit dans les dossiers d’inscription. |
| Consentement | Données | Le consentement est explicitement donné. Le traitement des DCP s'inscrit dans l'Art. 6.1-a du RGPD qui stipule : "la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;". Il convient en outre de préciser que les DCP traitées sont celles qui sont communiquées par le candidat dans le cadre de sa procédure d’admission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition des candidats. En cas d'opposition le traitement du dossier de candidature est interrompu et fermé, les éléments et données sont intégralement restitués au candidat. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les candidats disposent d'un droit de rectification en communiquant des DCP modifiées au président de <ASSOCIATION>. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne |
| Formalités | Données | Les candidats sont informés dans leurs dossiers qu'ils peuvent saisir l'autorité compétente, à savoir la CNIL, en cas de contestation. |

### Concernant la gestion des comptes-rendus

**Les mesures sont explicitement écrites dans le règlement intérieur de <ASSOCIATION>**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des comptes-rendus |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de gestion des comptes rendus de <ASSOCIATION>. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion des comptes-rendus. |
| Qualité | Données | Les DCP sont nécessaires à l’intérêt légitime de <ASSOCIATION> dans sa mission. Elles sont fournies par le membre lui-même lors de sa conférence. |
| Durée de conservation | Données | Les durées de conservation sont les durées légales qui peuvent varier d'un document à l'autre. La loi coutumière pour les associations fraternelles est que les comptes rendus sont conservés de façon indéfinie à fins de recherche historique ou généalogique. |
| Droit à l'information | Données | Le respect du droit à l'information figure dans le règlement intérieur de <ASSOCIATION>. |
| Consentement | Données | L'obtention du consentement des membres n'est pas nécessaire ; la licéité repose l’intérêt légitime de l’association dans le cadre de la réalisation de sa mission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition de ses membres. Cependant, cette opposition ne saurait être liée à l'un des éléments nécessaires à l'intérêt légitime de sa mission, sauf à vouloir démissionner. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les membres disposent d'un droit de rectification en communiquant des DCP modifiées au secrétaire de l’association. C’est fait à la fin de chaque réunion au cours de la lecture du compte-rendu. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne. |
| Formalités | Données | Les membres sont informés par le règlement intérieur qu'en cas de désaccord il peuvent saisir l'autorité de contrôle qui est la CNIL pour la France. |

### Concernant la gestion des membres

**Les mesures sont explicitement écrites dans le règlement intérieur de <ASSOCIATION>**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des comptes-rendus |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de gestion des membres de <ASSOCIATION>. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion des membres. |
| Qualité | Données | Les DCP sont nécessaires à l’intérêt légitime de <ASSOCIATION> dans sa mission. Elles sont fournies par le membre lui-même lors de sa conférence. |
| Durée de conservation | Données | Les durées de conservation sont les durées légales qui peuvent varier d'un document à l'autre. Les documents concernant la gestion des membres sont conservés pendant toute la durée de l’adhésion. |
| Droit à l'information | Données | Le respect du droit à l'information figure dans le règlement intérieur de <ASSOCIATION>. |
| Consentement | Données | L'obtention du consentement des membres n'est pas nécessaire ; la licéité repose l’intérêt légitime de l’association dans le cadre de la réalisation de sa mission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition de ses membres. Cependant, cette opposition ne saurait être liée à l'un des éléments nécessaires à l'intérêt légitime de sa mission, sauf à vouloir démissionner. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les membres disposent d'un droit de rectification en communiquant des DCP modifiées au secrétaire de l’association. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne. |
| Formalités | Données | Les membres sont informés par le règlement intérieur qu'en cas de désaccord il peuvent saisir l'autorité de contrôle qui est la CNIL pour la France. |

### Concernant la gestion des cotisations

**Les mesures sont explicitement écrites dans le règlement intérieur de <ASSOCIATION>**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des comptes-rendus |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de gestion des cotisations de <ASSOCIATION>. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion des cotisations. |
| Qualité | Données | Les DCP sont nécessaires à l’intérêt légitime de <ASSOCIATION> dans sa mission. Elles sont fournies par le membre lui-même lors de sa conférence. |
| Durée de conservation | Données | Les durées de conservation sont les durées légales qui peuvent varier d'un document à l'autre. Les documents concernant la gestion des cotisations sont légalement conservés pendant la période de 10 ans. |
| Droit à l'information | Données | Le respect du droit à l'information figure dans le règlement intérieur de <ASSOCIATION>. |
| Consentement | Données | L'obtention du consentement des membres n'est pas nécessaire ; la licéité repose l’intérêt légitime de l’association dans le cadre de la réalisation de sa mission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition de ses membres. Cependant, cette opposition ne saurait être liée à l'un des éléments nécessaires à l'intérêt légitime de sa mission, sauf à vouloir démissionner. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les membres disposent d'un droit de rectification en communiquant des DCP modifiées au secrétaire de l’association. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne. |
| Formalités | Données | Les membres sont informés par le règlement intérieur qu'en cas de désaccord il peuvent saisir l'autorité de contrôle qui est la CNIL pour la France. |

### Concernant la gestion du tronc hospitalier

**Les mesures sont explicitement écrites dans le règlement intérieur de <ASSOCIATION>**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des comptes-rendus |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de gestion du tronc hospitalier de <ASSOCIATION>. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion du tronc hospitalier. |
| Qualité | Données | Les DCP sont nécessaires à l’intérêt légitime de <ASSOCIATION> dans sa mission. Elles sont fournies par le membre lui-même lors de sa conférence. |
| Durée de conservation | Données | Les durées de conservation sont les durées légales qui peuvent varier d'un document à l'autre. Les documents concernant la gestion du tronc hospitalier sont légalement conservés pendant une période légale de 10 ans. |
| Droit à l'information | Données | Le respect du droit à l'information figure dans le règlement intérieur de <ASSOCIATION>. |
| Consentement | Données | L'obtention du consentement des membres n'est pas nécessaire ; la licéité repose l’intérêt légitime de l’association dans le cadre de la réalisation de sa mission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition de ses membres. Cependant, cette opposition ne saurait être liée à l'un des éléments nécessaires à l'intérêt légitime de sa mission, sauf à vouloir démissionner. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les membres disposent d'un droit de rectification en communiquant des DCP modifiées au secrétaire de l’association. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne. |
| Formalités | Données | Les membres sont informés par le règlement intérieur qu'en cas de désaccord il peuvent saisir l'autorité de contrôle qui est la CNIL pour la France. |

### Concernant la gestion des publications

**Les mesures sont explicitement écrites dans le règlement intérieur de <ASSOCIATION>**

|  |  |  |
| --- | --- | --- |
| Libellé | Effet principal | Activité : Gestion des comptes-rendus |
| Finalité | Données | Finalité du traitement est déterminée, explicite et légitime. Les DCP sont collectées uniquement pour le processus de gestion des publications de <ASSOCIATION>. Les DCP sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs |
| Minimisation | Données | Les données récoltées sont les DCP strictement nécessaires à la mise en œuvre du processus de gestion des publications. |
| Qualité | Données | Les DCP sont nécessaires à l’intérêt légitime de <ASSOCIATION> dans sa mission. Elles sont fournies par le membre lui-même lors de sa conférence. |
| Durée de conservation | Données | Les durées de conservation sont les durées légales qui peuvent varier d'un document à l'autre. Les documents concernant la gestion des publications sont conservés jusqu’à la publication effective. |
| Droit à l'information | Données | Le respect du droit à l'information figure dans le règlement intérieur de <ASSOCIATION>. |
| Consentement | Données | L'obtention du consentement des membres n'est pas nécessaire ; la licéité repose l’intérêt légitime de l’association dans le cadre de la réalisation de sa mission. |
| Droit opposition | Données | <ASSOCIATION> respecte le droit d'opposition de ses membres. Cependant, cette opposition ne saurait être liée à l'un des éléments nécessaires à l'intérêt légitime de sa mission, sauf à vouloir démissionner. |
| Droit d'accès | Données | <ASSOCIATION> respecte le droit d'accès des personnes à leurs DCP. Une demande de l'intéressé est formulée. Une personne qui exerce son droit d’accès obtient la communication de l’intégralité des données qui la concerne, qu’elles soient stockées en base active ou archivées. |
| Droit de rectification | Données | Les membres disposent d'un droit de rectification en communiquant des DCP modifiées au secrétaire de l’association. |
| Transferts hors UE | Données | Les DCP de <ASSOCIATION> ne sont pas communiquées hors de l'Union Européenne. |
| Formalités | Données | Les membres sont informés par le règlement intérieur qu'en cas de désaccord il peuvent saisir l'autorité de contrôle qui est la CNIL pour la France. |

# 3- Les atteintes potentielles à la vie privée

Les associations loi 1901 qui ne possèdent pas de salariés n’ont pas les moyens de payer un consultant qui fera une étude sérieuse de sécurité.

Ces atteintes ont été identifiées et constatées grâce à des entretiens et à l’expérience (de plus de 30 ans) des rédacteurs de ce document.

Notre méthodologie est donc empirique. Le tableau suivant identifie les atteintes constatées.

**Les biens essentiels pris en compte pour le PIA sont les données à caractère personnel.**

## 3.1 Les vulnérabilités identifiées

Le but est d’identifier ce qui pourrait porter atteinte aux données à caractères personnels dans les traitements identifiés.

Le tableau suivant liste les vulnérabilités identifiées.

|  |  |
| --- | --- |
| Vulnérabilité | Description |
| V1 | Ordinateur des utilisateurs non sécurisé |
| V2 | Cloud non sécurisé |
| V3 | Messagerie non sécurisée |
| V4 | Cahier des comptes rendus non mis en sécurité |
| V5 | Utilisateurs non sensibilisés |

## 3.2 Les événements redoutés – Identification des risques

Acronymes utilisés :

D : Disponibilité  
I : Intégrité  
C : Confidentialité

La liste des risques. Le but recherché est d’identifier les sources qui impactent des événements et de les mettre en lien avec la disponibilité, l’intégrité et la confidentialité des événements redoutés.



## 3.3 Les menaces sur la vie privée

Le but est d’identifier les menaces qui peuvent intervenir sur les données à caractères personnels. Les DCP font appel à du matériel et des procédures pour être stockées ou bien être traitées. Le but de cette partie est d’identifier les menaces afférentes à <ASSOCIATION>.

Les menaces sont catégorisées de la façon suivante :

* EHI : Erreur Humaine Interne
* EHE : Erreur Humaine Externe
* MHI : Acte de malveillance Humaine Interne
* MHE : Acte de malveillance Humaine Externe
* CM : Code malveillant
* ENV : Environnement

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Description | Risque | Menace |
| M1 | Hackers | D/I | EHE |
| M2 | Extrémistes | C/D | EHE |
| M3 | Code malveillant | D/I | CM |
| M4 | Membre (erreur) | D/I/C | EHI |



## 3.4 Etude des risques sur la vie privée

### Tableau des risques selon la criticité et la vraisemblance.

L’échelle va de 1 à 4, du moins critique au plus critique, du moins vraisemblable au plus vraisemblable.

Tableau détaillé :

3 risques pèsent sur les Données à Caractère Personnel :

* Risque de Divulgation
* Risque de Modification
* Risque d’Indisponibilité

L’axe des abscisse représente la vraisemblance

L’axe des ordonnées représente la criticité



Le tableau laisse apparaître les zones à risques suivantes :

Les catégories qui doivent être traitées en priorité sont :

* La lutte contre la divulgation des données à caractères personnels
* La modification des données à caractères personnels.

Les catégories qui devront traitées ensuite sont :

* La lutte contre l’indisponibilité des DCP.

# 4- Validation du PIA

## 4.1 Formalisation des mesures de sécurité à déployer

Les priorités sont définies comme suit :

1. Peu prioritaire
2. A traiter
3. Très prioritaire

|  |  |  |  |
| --- | --- | --- | --- |
| Mesure | Description | Traitement | Priorité |
| 1 | Divulgation de la liste des membres | Chiffrement des supports concernés | 3 |
| 2 | Divulgation des emails des membres | Utilisation des emails en copie cachée ou utilisation d’une mailing list sécurisée | 3 |
| 3 | Accès aux comptes rendus des réunions | Procédure stricte de rédaction des comptes-rendus qui suppose leur effacement numérique après impression et validation.  Mise sous clé du cahier des délibérations. | 2 |
| 4 | Divulgation des adresses des membres | Chiffrement des supports concernés | 3 |
| 5 | Suppression des dossiers des membres | Mise en place d’un système de sauvegarde chiffré. | 1 |
| 6 | Effacement des comptes et des données qui leurs sont liées | Mise en place d’un système de sauvegarde chiffré | 1 |
| 7 | Chiffrement des données de la loge (cryptolocker) | Mise en place d’un système de sauvegarde chiffré | 2 |
| 8 | Accès aux coordonnées bancaires des membres | Chiffrement des supports concernés | 2 |

## 4.2 Préconisations de sécurisation

Ces préconisations sont rapides et peu coûteuses :

* Les responsables / officiers concernés doivent être équipés d’outils légalement acquis dont ils possèdent les licences.
* Les équipements des personnes concernées doivent être correctement sécurisés (antivirus mis correctement à jour et chiffrement des ordinateurs).
* Si des solutions de partages sont utilisées, ces solutions doivent être chiffrées par défaut. Il suffit pour cela de l’activer dans les paramètres.
* Les cahiers de délibérations doivent être mis sous clés. Le Secrétaire en est le responsable et un double est confié au président.
* Dans la mesure du possible pour les communications internes les membres doivent utiliser une mailing list sécurisée qui dissimulera leur email.
* Dans le cadre de communications vers plusieurs destinataires externes à l’association, les destinataires des emails doivent être en copie cachée.

Un comportement lié aux systèmes d’information peut également figurer dans le règlement intérieur de l’association.

# 5- Réagir en cas de violation des données personnelles

**Définition :**

Une violation de Données à Caractères Personnels se définit comme étant une perte de disponibilité, d’intégrité ou de confidentialité de ces données, que ce soit de manière illicite ou accidentelle.

**Nous vous recommandons de réunir en urgence un comité pour effectuer les opérations suivantes. Ces opérations sont obligatoires.**

## 5.1 Documenter la violation

Cette documentation est impérative. Elle doit permettre de renseigner les autorités compétentes sur la violation. Vous devez préciser :

1. La nature de la violation (Disponibilité, Intégrité ou Confidentialité, illicite ou accidentelle).
2. Si possible, les catégories et le nombre approximatif de personnes concernées par la violation (employés, clients, grands comptes -lesquels- …). Les catégories de clients se trouvent dans le registre des traitements.
3. Les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ; (Il s’agit de quantifier les données et les informations concernées).
4. Décrire les conséquences probables de la violation de données ; (les impacts possibles qui figurent normalement dans le PIA – exemple vol de données…)
5. Décrire les mesures prises ou que vous envisagez de prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives. (Les mesures que vous comptez mettre en place pour éviter que cela se reproduise et pour limiter l’impact. Cela figure dans le PIA).

Le document récapitulatif de votre notification à la CNIL permet de répondre à l’obligation de documentation interne.

**Si l’incident constitue un risque au regard de la vie privée des personnes concernées, vous devrez notifier l’incident à la CNIL.**

**En cas de risque élevé, vous devez également notifier les personnes concernées**.

En cas de doute, notifiez à la CNIL qui vous indiquera s’il est nécessaire d’informer les personnes.

## 5.2 Délais

La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d’une violation présentant un risque pour les droits et libertés des personnes.

Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

1. Une notification initiale dans les meilleurs délais à la suite de la constatation de la violation ;
2. Puis, une notification complémentaire dans le délai de 72 heures si possible après la notification initiale.

IMPORTANT : Si le délai de 72 heures est dépassé, il conviendra d’expliquer, lors de votre notification, les motifs du retard.

## 5.3 Notifier à la CNIL

Cela se fait en ligne, à l’URL suivante

<https://notifications.cnil.fr/notifications/index>

## 5.4 Action de la CNIL

Dès réception, la CNIL va instruire la notification. La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que :

* La violation ne porte pas atteinte aux données personnelles ou ne présente pas de risque pour les droits et libertés des personnes.
* Vous avez correctement informé les personnes concernées.
* Vous avez mis en place, préalablement à la violation, des mesures techniques de protection appropriées.

La CNIL pourra vous imposer d'informer les personnes concernées si elle constate que :

* Vous ne les avez pas correctement informées.
* Les mesures techniques de protection que vous avez mises en place préalablement à la violation ne sont pas appropriées.

## 5.5 Cadre Légal

L'obligation de notifier à la CNIL les violations de données à caractère personnel est prévue à l’article 33 du règlement général sur la protection des données (RGPD). Elle concerne tous les responsables de traitement de données à caractère personnel. Dans le cas où la violation de données à caractère personnel est susceptible d’engendrer un risque élevé pour les droits et libertés d’une personne physique, l’article 34 du RGPD impose de notifier ces dernières.

# Révisions du Document

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Auteur | Modifications |
|  |  |  |  |
|  |  |  |  |