



# Fin d'accompagnement et archivage des données

Voir référentiel / III. Mission d'une cellule / 4. Conserver les données

## I. Protection et conservation des données recueillies sur support papier

---

1. Dès le premier contact, un dossier « papier » est constitué. Il comporte une édition de tous les documents concernant les propos exprimés de chaque personne victime : mails, notes écrites après un contact téléphonique, document final, etc. Ce dossier est conservé pendant six ans par le référent dans une armoire fermée à clé et dans une pièce fermée à clé également. Un sommaire est réalisé dans chaque dossier afin de faciliter le repérage des différents documents.
2. Les dossiers individuels sont versés aux archives diocésaines au terme d'une DUA (Durée d'Utilité Administrative) de six ans, sauf s'ils sont toujours actifs. Les archives diocésaines assurent la conservation et la protection des dossiers clos. Les documents liés au fonctionnement de la cellule d'accueil et d'écoute (comptes-rendus de réunion, contacts avec les différentes instances, articles de journaux...) seront également versés aux archives diocésaines au terme d'une DUA de six ans.
3. La cellule envoie systématiquement une copie du document final de chaque écoute à l'autorité dont elle dépend. Sur chacun des envois, la nécessité de prévoir des modalités de confidentialité et de conservation appropriées est rappelée au destinataire. La personne victime est avertie de cette démarche.
4. La cellule édite un dossier par personne victime. Ces dossiers sont identifiés et classés selon un codage déterminé. Ils sont ensuite regroupés par année dans

des boîtes d'archives. La gestion de ces dossiers respecte les principes définis par le Règlement Général pour la Protection des Données (RGPD - mai 2016). La section III de cette fiche détaille cette organisation.

5. La cellule n'édite pas de dossier par auteur. Il revient aux responsables diocésains ou congréganistes de compléter, avec les renseignements qui leur sont transmis par la cellule, leurs dossiers des clercs, laïcs ou religieux incriminés.
6. Si des instances judiciaires ou des chercheurs souhaitent consulter les archives de la cellule d'accueil et d'écoute, ils s'adresseront par écrit à l'évêque.

## II. Protection et conservation des données recueillies sur support numérique

---

7. Un double du dossier « papier » en format numérique est également créé pour chaque personne victime.
8. Dès le premier contact, le nom de la personne victime est inscrit dans un fichier qui permet de garder trace de la demande et du suivi qui se met en place. Par exemple, ce fichier peut se présenter sous la forme d'un tableur qui permet de faire des tris selon le critère souhaité (personne victime, diocèse, auteur, laïc ou clerc, etc.). Afin de respecter les règles en matière de confidentialité, trouver un chiffrement ou codage pour que ce ne soit pas directement identifiable. Ce fichier anonymisé est géré selon les normes RGPD.
9. Chaque document final, en version informatisée, est transmis au référent de la



cellule et n'est conservé que par ce dernier. Le rédacteur ne garde aucune trace de la fiche transmise, ni dans le disque dur de son ordinateur, ni dans sa boîte mail.

10. Pour assurer la sécurité de toutes les données recueillies, l'ensemble des documents numériques est conservé sur un serveur accessible via Internet et protégé par un VPN. Parmi les membres de la cellule, seul le référent peut accéder à ce serveur. L'ordinateur du référent est protégé par un mot de passe.
11. L'évêque peut également consulter le fichier informatisé en ayant accès aux données via le serveur accessible par VPN. Cet accès est contrôlé par un mot de passe. Lorsqu'un nouvel évêque est nommé, le code d'accès est modifié.
12. Lorsqu'un référent cesse sa mission, son accès au fichier est supprimé. Un nouveau profil est créé pour son successeur. Le référent ne conserve aucun document : il transmet à son successeur tous les documents « papier » ou numériques concernant l'activité de la cellule et non encore transmis aux archives diocésaines.
13. Les messages de la boîte mail de la cellule seront détruits par année glissée sur 6 ans.
14. Tout échange de mails sur les boîtes mails personnelles des membres de la cellule sera archivé si nécessaire par le référent et détruit.
15. Les archives du diocèse conserveront les dossiers sur support papier et/ou support informatique (version PDF uniquement). Lors du versement du dossier papier d'une personne victime aux archives, celles-ci communiqueront au référent la cote d'archivage. Cette cote de classement sera insérée dans le fichier anonymisé (cf. n°8).

### III. Références au Règlement Général de la Protection des Données.

---

16. Lors de l'entretien en présentiel, les règles de confidentialité et les mesures de conservations des données sont annoncées oralement à la personne victime. Lors de l'adoption du document définitif, une lettre est envoyée à la personne victime. Ses droits y sont précisés ainsi que les mesures de protection des données prises par la cellule. Un document semblable est adressé aux personnes qui n'ont contacté la cellule que par téléphone ou par courriel (cf. **a2** - *Modèle de lettre RGPD*).
17. Les documents conservés dans les archives diocésaines ne sont pas consultables avant un délai de 120 ans. Mais une personne victime peut demander à consulter son propre dossier avant la fin du délai officiel en s'adressant par courrier à l'évêque du diocèse.
18. Aucune demande de destruction d'un dossier ne sera prise en compte pour permettre d'éventuelles enquêtes judiciaires ultérieures. Dans le cadre de recherches historiques, les dossiers seront anonymisés.
19. L'ensemble des règles de protection des données appliquées dans la cellule vaut également pour toute autre personne impliquée dans l'instruction ou la conservation des dossiers (secrétariat, archives...).
20. Une fois par an, le référent de la cellule et le responsable des archives se rencontrent et vérifient l'application des règles énoncées.



	Réfèrent de la cellule		Évêque
	Conservation des documents	Suite	Accès aux document
<b>Dossier individuel des personnes victimes</b>	6 ans Papier <sup>1</sup>	Versés aux archives	Oui
	6 ans Informatique <sup>2</sup>	Versés aux archives ou détruits	Oui
<b>Documents de fonctionnement de la cellule</b>	6 ans Papier <sup>1</sup>	Versés aux archives	Oui
	6 ans Informatique <sup>2</sup>	Versés aux archives	Oui
<b>Fichier anonymisé</b>	Tenu à jour Informatique <sup>2</sup>		Consultation
<b>Mails de la cellule</b>	6 ans Informatique <sup>2</sup>	Versés aux archives si nécessaire puis détruits	Oui

(1) Armoire fermée à clé

(2) Ordinateur du réfèrent ; serveur sécurisé, VPN, mot de passe



## Fiches et annexes

**a2** - Modèle de lettre RGPD