Politique de confidentialité de l'ENAI

Église néo-apostolique internationale (ENAI)

Valable à compter du

1er janvier 2021

Table des matières

Préface / Introduction 2
Généralités 3
Organisation de la protection des données 6
Droits des personnes concernées 7
Transmission des données et communication des données à l'étranger 7
Registre des activités de traitement et des systèmes de fichiers de l'ENAI 8
Sécurité des données à caractère personnel 9
Formation des collaborateurs administratifs 10
Conséquences en cas de non-respect 10
Dispositions finales 10
Annexe: Définitions 12

Sources

ENAI, Guide des médias sociaux de l'Église néo-apostolique, édition de décembre 2017

Église néo-apostolique d'Allemagne de l'Ouest, politique de protection des données, état: vendredi 20 avril 2018

Église néo-apostolique d'Allemagne du Sud, politique de protection des données, état: jeudi 24 mai 2018

Église néo-apostolique de Suisse, politique de protection des données ENA Suisse, état: vendredi 1 mars 2019

Église néo-apostolique d'Autriche, politique de protection des données ENA Autriche, état: vendredi 1 mars 2019

Préface / Introduction

Chers apôtres, chers collaborateurs, chers collaborateurs de projets,

Depuis le 25 mai 2018, le Règlement général de protection des données (RGPD) de l'UE est en vigueur. Il est principalement applicable dans les États de l'UE et de l'EEE. Dans certains cas, il s'applique aussi aux États tiers et à la Suisse. En tant qu'association de droit suisse, l'ENAI est avant tout régie par le droit suisse et, de ce fait, par la loi suisse sur la protection des données (LPD). Cette loi a été totalement révisée ces dernières années. Le Parlement a adopté le nouveau texte de loi le 25 septembre 2020. Sur le contenu, il a repris en grande partie le RGPD et entrera probablement en vigueur en 2022. En raison de ce qui précède ainsi que des liens étroits entre l'ENAI et l'Europe et de l'acceptation croissante du RGPD dans le monde, la présente politique de protection des données s'inspire du RGPD.

Les contenus du RGPD ne sont rien de complètement nouveau. Jusqu'à présent, les lois nationales des États de l'UE et de l'EEE sur la protection des données définissaient le genre de données qui peuvent être collectées et traitées et leur finalité, ainsi que les conditions sous lesquelles ces opérations se produisent. Le RGPD renforce ces règlements et oblige également les responsables (toute personne/organisation qui collecte/traite les données) à fournir une documentation plus transparente et plus compréhensible des données. Le principe est celui de la minimisation des données, qui exige de ne collecter que des données nécessaires pour un but légitime et de les effacer immédiatement après. Pour tous ceux qui collectent et traitent les données, cela signifie qu'il faut examiner de près ses propres actions et processus de travail et les adapter si nécessaire. Car il n'y a pas de modèles généralement valables qui puissent être facilement mis en œuvre sans intervention.

Les changements rapides dans le comportement de communication dans notre société sont fortement influencés par les innovations techniques et relèguent souvent la protection des données à caractère personnel au second plan. Surtout en tant qu'Église, nous voulons nous veiller à ce que les droits de la personne ne soient pas mis de côté, simplement parce que des options faciles et confortables sont disponibles, mais nous voulons également agir de façon responsable.

Salutations cordiales

De la part de

Erich Senn	Frank Stegmaier
NACI Administrator	CFO

Généralités

§ 1 Généralités

(1) L'Église néo-apostolique internationale (ci-après désignée «ENAI» ou «le responsable») s'inspire des normes de l'Union européenne (UE) en ce qui concerne la protection des données à caractère personnel. Ceci vaut en particulier pour les données des membres de l'ENAI et des collaborateurs de l'administration de l'ENAI (collaborateurs administratifs).

(2) Aujourd'hui, l'ENAI suppose qu'une protection des données conforme à l'UE répond largement aux exigences de la nouvelle loi sur la protection des données (nLPD) adoptée par le Parlement suisse le 25 septembre 2020.

§ 2 Objectif

(1) La présente politique de protection des données de l'ENAI (ci-après désignée «politique de protection des données ENAI» ou «politique de protection des données») est la base contraignante pour le traitement conforme à la loi des *données à caractère personnel (CH: données personnelles)* par l'ENAI.

(2) La présente politique de protection des données vise à préserver et à protéger les droits et libertés fondamentaux des personnes concernées, en particulier le droit à la protection de leurs données à caractère personnel.

(3) En outre, cette politique de protection des données vise la libre circulation de telles données.

§ 3 Champ d'application

(1) La présente politique de protection des données s'applique au traitement des données à caractère personnel par l'ENAI en tant qu'association de droit suisse avec siège permanent à Zurich (Suisse) et en tant qu'unité administrative centrale.

(2) Elle s'applique personnellement à tous les collaborateurs administratifs. La politique de protection des données s'applique également aux apôtres ainsi qu'aux personnes ayant une relation de mandat ou de services quelconque avec l'ENAI.

(3) Les obligations et interdictions de la présente politique de protection des données s'appliquent à tout traitement des données à caractère personnel, qu'il soit sous forme électronique, de papier ou orale.

§ 4 Traitement et collecte des données

(1) On entend par *traitement* des données toute gestion des données à caractère personnel, de la collecte à l'archivage et à la destruction.

(2) Lors du traitement des données à caractère personnel, il convient de respecter les principes du RGPD (cf. art. 5 RGPD): Licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude des données à caractère personnel, limitation de la conservation («droit à l'oubli»), intégrité, confidentialité et disponibilité («sécurité des données» / «sécurité des informations») et responsabilité.

(3) Les données à caractère personnel sont collectées en principe auprès de la personne concernée et par l'Église territoriale respective.

(4) Données de base des membres de l'Église: Certains collaborateurs administratifs ont accès aux données de base des membres des Églises territoriales. Cet accès est nécessaire pour effectuer des tâches administratives telles que l'entretien des Églises territoriales desservies aux apôtres ou pour l'adhésion aux groupes de projet des membres de l'Église qui sont impliqués dans les projets de l'ENAI.

(5) Dossiers des apôtres: Les informations relatives à l'ordination d'un apôtre sont des données à caractère très personnel et méritent donc une protection très particulière. Ces données sont mises à disposition par l'Église territoriale concernée dans le cadre de l'ordination. De plus, l'ENAI détient des informations sur les données de base de l'apôtre ainsi que sur ses aires géographiques de travail.

(6) Dossiers personnels des collaborateurs administratifs: Bien souvent, des informations portant sur la profession, l'appartenance politique, les hobbies, le nombre d'enfants, l'éducation, etc., de la personne concernée sont collectées, ce qui mérite également une protection particulière.

§ 5 Limitation des finalités, minimisation des données, consentement

(1) La collecte, le traitement, l'utilisation et la transmission des données à caractère personnel ne sont permis que si cela est requis pour accomplir le devoir de l'Église ou si la personne concernée y a consenti (limitation des finalités). Une opération de traitement des données est alors nécessaire si la finalité religieuse ne peut être atteinte d'une autre manière ou ne peut l'être qu'au prix d'efforts considérablement accrus.

(2) La collecte, le traitement et l'utilisation des données à caractère personnel doivent être restreints à la mesure nécessaire à la finalité (minimisation des données).

(3) Toute publication des données à caractère personnel, par exemple sur l'Internet, ne peut se faire que sur consentement explicite. On entend par consentement valable toute déclaration de volonté libre, spécifique, éclairée et univoque, émise par une déclaration ou par un acte positif clair.

(4) Les informations sur les événements officiels, les voyages et les activités des apôtres, présentant un intérêt pour les membres de l'Église à l'échelle mondiale, nécessitent une approbation distincte.

§ 6 Confidentialité des données, secret pastoral et secret professionnel

(1) Il est interdit aux personnes travaillant pour l'ENAI de collecter, traiter ou utiliser des données à caractère personnel sans autorisation. Avant d'entamer leurs activités, elles doivent s'engager à gérer avec confidentialité les données à caractère personnel (en signant une déclaration de confidentialité).

(2) Les documents («notes personnelles») créés dans le cadre de l'exercice des activités au sein de l'ENAI ne doivent pas être mis à la disposition de tierces personnes. Les dispositions particulières relatives à la protection du secret pastoral restent intactes. Il en va de même pour les obligations de confidentialité pour respecter les obligations légales de secret et de confidentialité ou pour des secrets professionnels particuliers, qui ne reposent pas sur des dispositions légales.

(3) Ces obligations de secret ne sont pas limitées dans le temps. Elles valent aussi pour des informations ayant été échangées ou rendues accessibles avant la signature éventuelle d'une déclaration de confidentialité. Elles sont irrévocables et persistent même à la fin de la collaboration ou du rapport contractuel ou après l'exécution des services convenus, ainsi qu'en cas de résiliation d'une relation de travail, de mandat ou de service.

§ 7 Conservation, archivage et effacement

(1) Le principe suivant s'applique: Les données à caractère personnel n'étant plus requises et n'étant pas archivables doivent être définitivement effacées ou détruites (par ex. avec une déchiqueteuse).

(2) Les données à caractère personnel doivent être effacées si le stockage est illicite, si le consentement au stockage a été révoqué ou si elles ne sont plus nécessaires pour les finalités de leur collecte.

(3) Les données à caractère personnel des membres de l'Église sont nécessaires pour la documentation de l'adhésion, de la réception des sacrements ainsi que pour les ordinations religieuses, les missions et nominations. Une révocation du consentement au stockage ou un retrait de l'Église n'entraînent donc pas automatiquement l'effacement des données. Toutefois, l'accès à ces données à caractère personnel est restreint pour pouvoir fournir des informations sur la personne concernée ou établir des certificats.

(4) D'autres exceptions à l'obligation d'effacement sont:

- Des données à caractère personnel anonymisées
- Les obligations de conservation légales

- Les données à caractère personnel devant être conservées à des fins de preuve ou de sécurité ou pour préserver les intérêts de la personne concernée méritant une protection

(5) Les détails doivent être réglés dans un concept d'effacement et d'archivage (y compris de sauvegarde des données).

Organisation de la protection des données

§ 8 Préposé à la protection des données[1]

(1) L'ENAI nomme un préposé à la protection des données. Vous pouvez contacter le préposé à la protection des données aux coordonnées suivantes:

Église néo-apostolique internationale
Préposé à la protection des données
Ueberlandstrasse 243
8051 Zurich / Suisse

privacy@nak.org

(2) Le préposé à la protection des données surveille le respect du règlement général de protection des données européen (RGPD) et d'autres dispositions légales, y compris les présentes dispositions et celles d'autres directives de l'ENAI portant sur la protection des données. Le préposé à la protection des données conseille et informe la direction administrative quant aux obligations existantes en matière de protection des données et se charge de la communication avec les autorités de protection des données. Des processus choisis sont aléatoirement axés sur des risques et il contrôle leur conformité à la protection des données à des intervalles appropriés.

(3) Le préposé à la protection des données s'acquitte de ses taches sans instructions en se servant de son expertise. Il rend directement compte à la direction administrative.

(4) La direction administrative et les collaborateurs administratifs doivent soutenir le préposé à la protection des données dans l'acquittement de ses tâches.

(5) Des références à la protection des données sont souvent faites dans l'image publique de l'Église. Le préposé à la protection des données de l'ENAI doit maintenant y être mentionné.

§ 9 Coordinateur de la protection des données

(1) L'ENAI se charge aussi de former un collaborateur administratif sur les questions de la protection des données. Ce collaborateur administratif a pour devoir de veiller à l'application de la protection des données et de communiquer des informations appropriées en interne.

[1] Par souci de simplification, la forme masculine est employée dans le présent document, conformément à la désignation contenue dans le RGPD.

Droits des personnes concernées

§ 10 Droits des concernés

(1) La direction administrative informe pleinement les personnes concernées sur le traitement de leurs données. Ceci a lieu au moins une fois dans le cadre d'une embauche ou aussi lors des ordinations.

(2) L'exercice des droits suivants, comme par ex. la fourniture d'informations, doit concerner la bonne personne. Pour cela, il faut vérifier au préalable, et sans ambiguïté, l'autorisation du requérant ainsi que son identité.

(3) Droit aux renseignements: Sur demande, les personnes concernées doivent être renseignées sur leurs données stockées. La fourniture de renseignements se fait normalement par écrit, à moins que la personne concernée n'ait soumis la demande par courriel. Les renseignements doivent être fournis dans les 30 jours suivant réception de la demande en ce sens.

(4) Droit à la rectification ou à la suppression: Les personnes concernées peuvent exiger de compléter des données à caractère personnel incomplètes et d'effacer les données qui ne sont plus nécessaires. Avant de procéder à un éventuel effacement de données, il convient de noter que des obligations de conservation légales ou autres ou un intérêt ecclésiastique ou autre intérêt légitime prépondérant pourraient s'y opposer.

(5) Quiconque s'estime avoir été lésé dans ses droits lors de la collecte, du traitement ou de l'utilisation de ses données à caractère personnel par un organisme religieux, peut s'adresser par écrit au préposé à la protection des données ou à la direction administrative.

Transmission des données et communication des données à l'étranger

§ 11 Transmission et communication des données

(1) La communication des données à caractère personnel à des tiers n'est permise que sur la base d'une autorisation légale, pour le compte ou sur consentement de la personne concernée.

(2) La direction administrative se trouve à Zurich (Suisse) et traite les données à caractère personnel en Suisse. La protection de ces données dans l'échange avec les Églises territoriales sises dans l'UE et dans l'EEE est garantie par la décision d'adéquation de la Commission UE ainsi que par des informations appropriées et par le consentement des personnes concernées.

(3) Toute transmission ou communication des données à une Église territoriale ou une organisation sise hors de l'UE ou de l'EEE n'est autorisée qu'avec le consentement explicite de la personne concernée.

§ 12 Prestataires externes

(1) Si des prestataires externes doivent avoir accès aux données à caractère personnel, le préposé à la protection des données doit en être informé au préalable.

(2) Les prestataires ayant un accès possible aux données à caractère personnel doivent être minutieusement sélectionnés avant passation du marché. La sélection doit être documentée et tenir compte des aspects suivants:

- L'aptitude professionnelle du prestataire pour la gestion concrète des données
- Les mesures de sécurité techniques et organisationnelles
- L'expérience du prestataire sur le marché
- D'autres aspects qui peuvent indiquer la fiabilité du prestataire (documentations sur la protection des données, volonté de coopérer, temps de réponse, etc.)

(3) Si un prestataire doit collecter, traiter ou utiliser des données à caractère personnel, il faudra conclure un contrat de traitement des commandes et établir des déclarations de confidentialité correspondantes. Les aspects relatifs à la protection des données et à la sécurité informatique doivent être réglementés dans ce cadre.

(4) Le prestataire doit passer un contrôle régulier quant aux mesures techniques et organisationnelles conclues avec lui par contrat. Le résultat doit être documenté.

Registre des activités de traitement et des systèmes de fichiers de l'ENAI

§ 13 Registre des activités de traitement

(1) L'ENAI tient un registre de tous les traitements des données effectués sous leur responsabilité et sous celle des personnes responsables de ces traitements des données (cf. art. 30 RGPD). Le préposé à la protection des données peut être appelé à donner son avis sur les informations requises par la loi (cf. document distinct «Registre des activités de traitement de l'ENAI»).

(2) Sur demande, l'ENAI met le registre à la disposition de l'autorité compétente de protection des données. La personne compétente à ce titre est le préposé à la protection des données, en accord avec la direction administrative.

§ 14 Terme «système de fichiers»

(1) Un système de fichiers est une collecte structurée de données à caractère personnel qui sont accessibles selon certains critères, que cette collecte soit gérée de façon centralisée, décentralisée ou selon des aspects fonctionnels ou géographiques. Comme exemples de systèmes de fichiers, on peut citer les dossiers personnels ou aussi les banques de données contenant des données de base des membres.

(2) Les membres de l'ENAI sont les apôtres, qui sont répartis partout dans le monde. Leurs données seront collectées plus tard si jamais il y a l'intérêt de les nommer à ce poste. Ces données sont stockées à l'ENAI dans une base de données prévue à cet effet dans le portail de l'ENA.

Sécurité des données à caractère personnel

§ 15 Sécurité des données

(1) Les données à caractère personnel doivent être traitées d'une manière garantissant une sécurité appropriée des données à caractère personnel, y compris la protection contre tout traitement non autorisé ou illicite et contre toute perte, destruction ou endommagement involontaires, par des mesures techniques et organisationnelles («TOM»).

(2) La division IT prend les TOM nécessaires pour garantir de façon appropriée la sécurité des données à caractère personnel.

(3) Dans le cadre de leurs tâches contractuelles, les collaborateurs administratifs sont obligés de gérer minutieusement les données à caractère personnel et les ressources de l'employeur.

§ 16 Manquements à la protection des données («violation des données»)

(1) Si des données de l'ENAI ont été divulguées de façon illicite à des tiers, la direction administrative doit en être immédiatement informée. La direction impliquera directement le préposé à la protection des données dans la clarification des faits.

(2) Le signalement doit mentionner toutes les informations pertinentes sur la clarification des faits, notamment l'organisme récepteur, les personnes concernées ainsi que le type et la portée des données communiquées.

(3) L'exécution d'une éventuelle obligation d'information vis-à-vis de l'autorité de protection des données est effectuée exclusivement par le préposé à la protection des données, en accord avec la direction administrative. Les personnes concernées sont informées par la direction administrative, le préposé à la protection des données étant appelé à donner son avis.

Formation des collaborateurs administratifs

§ 17 Formation à la protection des données et à la sécurité

(1) Les personnes ayant constamment ou régulièrement accès aux données à caractère personnel de l'ENAI, collectent ces données ou développent des systèmes de traitement de ces données, doivent être dûment formées aux prescriptions en matière de protection des données. En accord avec la direction administrative, le préposé à la protection des données décide de la forme et du cycle des formations correspondantes.

(2) Les cybercriminels exploitent très souvent les caractéristiques humaines telles que la serviabilité, la confiance, la peur ou le respect de l'autorité. C'est pourquoi il est important de former correctement les collaborateurs administratifs aussi sur les thèmes tels que la cybersécurité.

Conséquences en cas de non-respect

§ 18 Conséquences en cas de non-respect

(1) Une violation négligente ou même délibérée de la présente politique de protection des données peut donner lieu à des mesures relevant du droit du travail, y compris une résiliation sans préavis ou en temps opportun. De même, des sanctions pénales et des conséquences civiles, telles que les dommages et intérêts, peuvent être envisagées.

Dispositions finales

§ 19 Responsabilité

(1) Le respect des prescriptions de la présente politique de protection des données doit pouvoir être prouvé à tout moment. Ce faisant, il faut particulièrement veiller à la traçabilité et à la transparence des mesures prises, par exemple via les documents correspondants.

§ 20 Modifications

(1) Dans le cadre de l'évolution de la législation sur la protection des données et des modifications technologiques ou organisationnelles, la présente politique de protection des données est régulièrement contrôlée quant au besoin d'adaptation ou de complément.

(2) Les modifications apportées à cette politique de protection des données sont efficaces de façon informelle. Les collaborateurs administratifs doivent être informés immédiatement et de façon appropriée des prescriptions modifiées.

§ 21 Exécution et entrée en vigueur

(1) La direction administrative est autorisée à édicter des règlements complémentaires sous forme d'instructions de service.

(2) La présente politique de protection des données entre le 1er janvier 2021 en vigueur et remplace toutes les politiques de protection des données antérieures de l'ENAI.

Zurich, décembre 2020

Pour l'Église néo-apostolique internationale (ENAI):

Erich Senn	Frank Stegmaier
NACI Administrator	CFO

Annexe: Définitions

(1) *Données à caractère personnel (CH: données personnelles)*[2] sont toutes les informations concernant une personne physique identifiée ou identifiable (personne concernée). Les données des frères et sœurs font tout autant partie des données à caractère personnel que les données personnelles et les données des ministres et titulaires de fonctions. Par exemple, le nom d'un interlocuteur est tout aussi révélateur d'une personne physique que son adresse électronique. Il suffit que les informations respectives soient liées au nom de la personne concernée ou puissent être établies indépendamment de celui-ci à partir du contexte. De même, une personne peut être identifiable si l'information doit d'abord être liée à des connaissances supplémentaires, par ex. dans le cas de la date de naissance, du numéro de matricule ou de l'adresse IP. L'obtention de l'information n'a pas d'incidence sur une référence personnelle. Même les photos, les enregistrements vidéo ou sonores peuvent constituer des données à caractère personnel.

(2) *Certains types de données à caractère personnel (CH: données sensibles)* sont des informations pouvant révéler l'origine raciale et ethnique, les opinions politiques, les convictions religieuses ou philosophiques ainsi qu'une éventuelle appartenance à des partis politiques ou à des syndicats, de même que les données génétiques, données biométriques, des données sur la santé ou des données sur la vie sexuelle ou sur l'orientation sexuelle d'une personne physique. Certaines catégories de données à caractère personnel ne peuvent en principe être collectées, traitées ou utilisées qu'avec le consentement de la personne concernée ou, à titre d'exception, que sur la base d'une autorisation légale explicite. En outre, des mesures techniques et organisationnelles supplémentaires (par ex. le cryptage lors du transport, cession minimale des droits) doivent être adoptées pour protéger des données à caractère personnel particulières.

(3) *Traitement,* toute opération ou toute série d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

(4) *Limitation du traitement,* le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

(5) *Profilage* désigne toute forme de traitement automatisé des données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique. Toutefois, l'ENAI en tant qu'organisation responsable renonce à une prise de décision automatique ou au profilage.

[2] En anglais: «personal data» ou «personal information».

(6) *Anonymisation / pseudonymisation:* Les données à caractère personnel sont considérées comme *anonymisées* lorsque la personne ne peut plus être identifiées. On entend par «anonymisation» toute opération empêchant d'attribuer des données à une personne spécifique ou ne rendant cela possible qu'avec un effort extraordinaire. Dans la *pseudonymisation*, par contre, toutes les données d'identification sont remplacées par un enregistrement neutre de données (pseudonyme). La pseudonymisation peut être inversée (si un tableau de correspondance permettant un regroupement des deux parties de données existe et est accessible). L'anonymisation, cependant, est définitive. Seules les données entièrement anonymisées ne sont plus considérées comme des données à caractère personnel.

(7) *Responsable du traitement*, la personne physique ou morale (l'ENAI est ici le seul responsable), l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

(8) *Sous-traitant,* la personne physique ou morale (par ex. l'entreprise mandatée pour l'entretien technologique de la gestion des membres/MDV[3]), l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

(9) *Destinataire,* la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers.

(10) *Tiers,* une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter des données à caractère personnel.

(11) Un *consentement* de la personne concernée est toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle 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.

[3] MDV = gestion des données des membres.