Directive sur la protection des données ENA Suisse

Date: Valable à compter du 1er mars 2019

Sommaire

Préambule

Le Règlement général sur la protection des données (RGPD) est en vigueur dans l'EU depuis le 25 mai 2018. Par principe le droit suisse s'applique en Suisse, raison pour laquelle le RGPD n'a pas d'effet direct en Suisse. En raison de l'importante mise en réseau, de la coopération d'ENA Suisse avec l'Europe et de la complète révision de la loi suisse sur la protection des données qui reprendra le RGPD, la présente directive sur la protection des données est d'ores et déjà basée sur la nouvelle réglementation européenne.

Le RGPD n'est en soi pas complètement nouveau. La loi suisse sur la protection des données (LPD) stipule par exemple de façon très concrète sous quelles conditions des données peuvent être collectées et traitées et à quelles fins. Le RGPD consolide ces dispositions et oblige les responsables (la personne/l'organisation qui collecte/traite les données) à également fournir une documentation plus transparente et compréhensible relative aux données collectées. Le principe est la minimisation des données, c'est-à-dire ne collecter que les données nécessaires à des fins légitimes et les supprimer le plus rapidement possible. Cela signifie que toute personne collectant et traitant des données doit se préoccuper intensément de ses propres actions et processus de travail et les adapter si nécessaire, car il n'existe aucun modèle d'application générale pouvant facilement mis en œuvre sans adaptation.

§ 1 Signification, objectif, accessibilité

(1) La présente directive sur la protection des données constitue la base contraignante d'une protection légale et durable des données personnelles («données à caractère personnel») au sein de l'Église néo-apostolique Suisse (ci-après dénommée «ENA Suisse» ou «le responsable»). Elle est la base de tous les documents de mise en œuvre, comme par exemple les instructions destinées aux responsables de la pastorale (ministres).

(2) La présente directive sur la protection des données vise à protéger les droits et libertés fondamentaux des personnes concernées, en particulier leur droit à la protection des données à caractère personnel.

(3) La directive sur la protection des données doit à tout moment être facilement accessible à tous les ministres (responsables de la pastorale) responsables et employés de l'administration de l'ENA Suisse.

§ 2 Domaine d'application

(1) La présente directive sur la protection des données s'applique à tout le territoire de l'ENA Suisse. Les directives d'action «Protection des données dans le quotidien des paroisses» s'appliquent tout particulièrement aux paroisses de l'ENA Suisse.

(2) Elles s'appliquent personnellement à toutes les personnes exerçant des fonctions honorifiques, à temps partiel ou à temps plein dans le cadre de l'ENA Suisse (par exemple dans le mandatement en tant que responsable de paroisse) ou de ses structures et institutions, ainsi que tous les ministres de l'Église néo-apostolique (voir également Catéchisme, chap. 7.1, Le ministère et les services). Ces directives s'appliquent également aux personnes en relation contractuelle avec ENA Suisse.

(3) Les obligations et interdictions de la présente directive sur la protection des données s'appliquent à tout traitement d'informations à caractère personnel, que celui-ci ait lieu sous forme électronique ou papier. Elle inclut par ailleurs dans son domaine d'application toutes les personnes *concernées* (par ex., un frère/une sœur, ministre, un employé de l'administration ecclésiale, etc.).

§ 3 Définitions

(1) Les *données à caractère personnel*[1] sont des informations relatives à une personne physique identifiée ou identifiable (personne concernée). Les données relatives aux frères et sœurs font tout autant partie des données à caractère personnel que les données du personnel et les données de façon générale des ministres et responsables. Le nom d'un contact par exemple permet d'identifier une personne physique, telle que son adresse e-mail. Il suffit que les informations respectives soient associées au nom de la personne concernée ou, indépendamment de cela, puissent être déterminées dans le contexte. De même, une personne peut être identifiée si l'information doit tout d'abord être mise en relation avec des connaissances supplémentaires, telles que par exemple, la date de naissance, le numéro personnel ou l'adresse IP. L'origine de l'information n'est pas pertinente pour une référence à un individu. Les photos, les enregistrements vidéo ou audio peuvent également constituer des données à caractère personnel.

(2) Les *types spécifiques de données à caractère personnel («données sensibles»)* sont des informations susceptibles de révéler les origines raciales et ethniques, opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données génétiques, biométriques, relatives à la santé ou à la vie sexuelle, comme par exemple l'orientation sexuelle d'une personne physique, ainsi que les données relatives aux mesures d'assistance sociale ou encore des données sur les poursuites ou sanctions pénales et administratives.

(3) Le *traitement* désigne tout opération ou tout ensemble 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) La *limitation du traitement* correspond au marquage des données à caractère personnel conservées dans le but de limiter leur traitement futur.

(5) Le *profilage* désigne tout type de traitement automatisé de 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.

(6) *Anonymisation/pseudonymisation:* Les données à caractère personnel sont considérées comme étant *anonymes* si la personne ne peut plus être déterminée. L'«anonymisation» correspond à tout processus empêchant l'attribution de données à une personne spécifique ou ne la permettant que par l'exercice d'un effort extraordinaire. Dans le cas de la *pseudonymisation* en revanche, toutes les données d'identification sont remplacées par un ensemble de données neutre (pseudonyme). La pseudonymisation peut être annulée (tant qu'il existe une table de correspondance et que cette dernière est accessible et permet une fusion des deux parties de données). L'anonymisation est par contre définitive. Seules les données complètement anonymisées ne sont plus considérées comme étant des données à caractère personnel.

(7) Le *responsable du traitement* est la personne physique ou morale (dans ce cas, le responsable est uniquement l'ENA Suisse), l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermin les finalités et les moyens du traitement des données à caractère personnel.

(8) Le *sous-traitant* est la personne physique ou morale (par exemple, l'entreprise responsable de l'entretien technique de la gestion[2] informatique des membre/GIM), l'autorité publique, le service

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

[2] GIM = Gestion informatique des membres.

ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

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

(10) Un *tiers* est 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 les données à caractère personnel;.

(11) Le *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.

§ 4 Organisation de la protection des données

(1) L'ENA Suisse a mandaté un responsable la protection des données[3]. Vous pouvez le contacter à l'adresse suivante:

Église néo-apostolique de Suisse
Responsable de la protection des données
Ueberlandstrasse 243
8051 Zurich/Suisse

E-Mail: privacy@nak.ch

(2) Le responsable de la protection des données supervise le respect de la loi suisse sur la protection des données (LPD) et du règlement général sur la protection des données (RGPD), ainsi que d'autres dispositions légales, y compris les dispositions des présentes et d'autres directives de l'ENA Suisse en matière de protection des données. Le responsable de la protection des données conseille et informe le chef de l'administration ChApd CH[4] quant aux obligations existantes en matière de protection des données. Il est également responsable des communications avec le préposé fédéral à la protection des données et à la transparence (PFPDT). La conformité des processus sélectionnés à la protection des données est contrôlée par échantillonnage, en fonction des risques encourus et à intervalles raisonnables.

(3) Le responsable de la protection des données exerce ses fonctions sans instructions et par l'application de ses connaissances acquises. Il rapporte directement au chef de l'administration ChApd CH .

(4) Le chef de l'administration ChApd CH et les employés de l'administration d'ENA Suisse doivent assister le responsable de la protection des données dans l'exercice de ses fonctions.

§ 5 Traitement des données à caractère personnel

(1) Les principes de la loi sur la protection des données doivent être observés lors du traitement de données à caractère personnel (cf. art. 4 ss LDP ainsi qu'art. 5 RGPD): légalité, équité, transparence, finalités, minimisation des données, exactitude des données à caractère personnel, limite de conservation («droit à l'oubli»), intégrité, confidentialité et disponibilité («sécurité de l'information») et responsabilité.

[3] Par souci de simplicité dans le cas présent, conformément aux dispositions du RGPD, le masculin est utilisé pour désigner les deux sexes.
[4] ChApd CH = Champ d'activité de l'apôtre de disctric de Suisse

(2) Les données à caractère personnel peuvent en principe être traitées comme suit:

- En cas de relation contractuelle existante avec la personne concernée.

Exemple: L'enregistrement et l'utilisation des données à caractère personnel requises dans le cadre d'une adhésion à l'ENA Suisse, d'un contrat de travail ou encore d'un mandat de gestion pour l'administration ENA Suisse.

- Dans le cadre de mesures précontractuelles sur demande de la personne concernée ou encore de l'exécution du contrat avec la personne concernée.

Exemple: Les données à caractère personnel nécessaires dans le cadre d'un processus de recrutement pour un poste au sein de l'administration de l'ENA Suisse sont collectées.

- Si et dans la mesure où la personne concernée a consenti.

Exemple: La personne concernée accepte que les données nécessaires à l'adhésion soient collectées et traitées. L'adhésion à l'ENA Suisse est justifiée par le saint-scellé.

- S'il existe une obligation légale à laquelle est soumise ENA Suisse.

Exemple: Délais légaux de conservation.

- Si ENA Suisse a un intérêt légitime, aussi longtemps qu'il n'affecte pas les intérêts ou droits fondamentaux de la personne concernée, qui plus est, s'il s'agit d'un enfant. Le traitement des données fondé sur un intérêt légitime ne devrait toutefois pas être effectué sans la consultation préalable du responsable de la protection des données.

Exemple: L'utilisation de l'adresse postale d'anciens frères et sœurs d'une paroisse pour les inviter à une fête d'anniversaire.

(3) Par dérogation au paragraphe (2), tout ministre (responsable de la pastorale) peut conserver ses propres registres («notes à caractère personnel») aux fins de son mandat pastoral. Cela doit cependant se limiter aux membres de l'Église dont ils s'occupent personnellement dans le cadre du mandat pastoral. Le contenu de ces registres doit être directement lié à l'activité pastorale. Personne ne doit avoir accès au contenu de ces registres. Le ministre concerné (responsable de la pastorale) doit à cette fin prendre les mesures techniques ou organisationnelles appropriées.

(4) Les personnes concernées ne doivent pas faire l'objet d'une décision reposant uniquement sur un traitement automatisé, notamment le profilage, qui pourrait avoir un effet juridique sur elles ou les affecterait de manière notable.

(5) Les données à caractère personnel doivent être traitées dans un but prédéterminé, clair et légitime. Un enregistrement inutile de données, tel que la conservation de données à titre de réserve, est inadmissible.

(6) Le traitement des données à caractère personnel devrait autant que possible être évité. Les pseudonymes ou le traitement anonyme des données sont préférables.

(7) En plus du consentement déclaré de la personne concernée, le changement de finalité, qui était à l'origine basé sur le traitement des données, n'est autorisé que si la finalité du traitement ultérieur est compatible avec la finalité initiale (par exemple lors du passage à un autre niveau d'enseignement). En particulier, il convient de prendre en compte les attentes raisonnables de la personne concernée relatives à un traitement ultérieur en regard de l'ENA Suisse, du type de données utilisé, des conséquences pour la personne concernée ainsi que des possibilités de cryptage ou de pseudonymisation.

(8) La personne concernée doit être pleinement informée du traitement de ses données lors de la collecte de ses données à caractère personnel. Les informations doivent contenir l'identité de l'organe responsable ainsi que les destinataires de leurs données à caractère personnel et de toute autre information conformément à l'art. 14 de la LDP (base légale RGPD: Art. 13 RGDP) afin de garantir un traitement juste et transparent. Les informations doivent revêtir une forme

compréhensible, être facilement accessibles et être écrites dans la langue la plus simple possible.

(9) Les données à caractère personnel doivent être exactes et, si nécessaire, à jour. L'étendue du traitement des données doit être nécessaire et pertinente par rapport à l'objectif recherché. L'administration de l'ENA Suisse est en charge de la mise en œuvre par l'établissement de processus correspondants. Elle est à cette fin autorisée à donner des instructions par le Président de l'Église néo-apostolique. L'exactitude, la nécessité et l'actualité des bases de données doivent également être régulièrement vérifiées.

§ 6 Les catégories particulières de données

(1) Des catégories particulières de données à caractère personnel ne peuvent en principe être collectées, traitées ou utilisées qu'avec le consentement de la personne concernée ou, exceptionnellement, sur la base d'une autorisation légale explicite. Des mesures techniques et organisationnelles supplémentaires (par exemple, cryptage pendant le transport, attribution minimale de droits) doivent par ailleurs être adoptées afin de protéger des données à caractère personnel spécifiques.

§ 7 Transfert de données

(1) Le transfert de données à caractère personnel à des tiers n'est autorisé que par la loi ou le consentement de la personne concernée.

(2) Si le destinataire des données à caractère personnel se trouve en dehors de l'Union européenne ou de l'Espace économique européen, des mesures spéciales doivent être adoptées et mises en œuvre afin de protéger les droits et les intérêts des personnes concernées. Il faut s'abstenir de transférer des données si l'organisme destinataire n'a pas un niveau de protection des données adéquat ou s'il ne peut, par exemple, pas être établi au moyen de clauses contractuelles spécifiques.

§ 8 Prestataires externes

(1) Le responsable de la protection des données doit être informé au préalable si des prestataires externes devaient recevoir accès à des données à caractère personnel.

(2) Les prestataires pouvant éventuellement accéder aux données à caractère personnel doivent être soigneusement sélectionnés avant l'attribution du mandat. La sélection doit être documentée et doit en particulier tenir compte des aspects suivants:

- Qualification professionnelle du contractant quant au traitement spécifique de données
- Mesures techniques de sécurité organisationnelles
- Expérience du prestataire sur le marché
- Autres aspects impliquant la fiabilité du prestataire (documentation de protection des données, disposition à coopérer, temps de réponse, etc.)

(3) Lorsqu'un prestataire doit collecter, traiter ou se servir de données à caractère personnel dans le cadre de son mandat, un contrat y relatif doit être conclu et des déclarations de confidentialité correspondantes doivent être établies. Les aspects relatifs à la protection des données et à la sécurité informatique doivent y être réglementés.

(4) Le prestataire doit être régulièrement contrôlé quant aux mesures techniques et organisationnelles faisant l'objet de son mandat. Les conclusions doivent être documentées.

§ 9 Conservation, archivage et suppression

(1) Le principe est le suivant: les données à caractère personnel n'étant plus nécessaires et n'ayant pas de valeur archivistique doivent être supprimées ou détruites de façon permanente (par ex. en utilisant une «déchiqueteuse»).

(2) Les exceptions sont les suivantes:

- données à caractère personnel anonymisées
- données à caractère personnel collectées dans le cadre d'un service sacré irrévocable et non répétitif, tel que le baptême ou le saint-scellé, ou encore nécessaires pour des services ecclésiastiques ultérieurs, tels que mariage ou enterrement, (par ex. certificat de baptême, certificat de saint-scellé)
- données à caractère personnel devant être conservées à des fins de preuve ou de sécurité ou encore pour protéger les intérêts légitimes de la personne concernée

(3) Les détails doivent être réglés dans un concept de suppression ou d'archivage.

§ 10 Minimisation des données, Privacy by Design/Privacy by Default

(1) Le traitement des données à caractère personnel doit viser à collecter, traiter ou utiliser le moins possible de données de la personne concernée («minimisation des données»). En particulier, les données à caractère personnel doivent, dans la mesure du possible, être anonymisées ou pseudonymisées en fonction du but recherché. Il n'est par exemple pas nécessaire de connaître et d'utiliser le nom complet de la personne concernée dans le cadre d'une analyse statistique des données. Cette information peut au contraire être remplacée par une valeur aléatoire qui peut également garantir la distinction des informations sous-jacentes.

(2) Il en va de même pour la sélection et l'aménagement des systèmes de traitement de l'information (par ex. le GIM) La protection des données doit dès le départ être intégrée aux spécifications et à l'architecture des systèmes de traitement des données afin de faciliter le respect des principes de protection de la vie privée et des données, notamment le principe de la minimisation des données.

§ 11 Droits des personnes concernées

(1) L'exercice des droits énumérés ci-après, comme par exemple celui de la fourniture de renseignements, doit concerner la bonne personne. C'est pourquoi il convient de déterminer préalablement le droit et l'identité du demandeur.

(2) Les personnes concernées ont un droit d'accès à toutes les données à caractère personnel détenues et/ou traitées à leur sujet.

(3) Les informations sont normalement fournies par écrit, à moins que la personne concernée n'ait présenté sa demande par voie électronique. L'information doit être fournie dans un délai de trente jours à compter de la réception de la demande d'information. ENA Suisse communique à la personne concernée: a) toutes les données existantes à son sujet, notamment les informations disponibles sur l'origine de ces dernières; b) l'objet et, le cas échéant, la base juridique du traitement, les catégories de données à caractère personnel traitées, les personnes traitant lesdites données ainsi que tous les destinataires de ces dernières.

(4) Les personnes concernées ont droit à la rectification de leurs données à caractère personnel si celles-ci devaient s'avérer être inexactes. Elles peuvent par ailleurs également demander à ce que des données à caractère personnel incomplètes soient complétées.

(5) La personne concernée a le droit de supprimer ses données à caractère personnel dans les conditions suivantes:

– la connaissance des données n'est plus nécessaire à la réalisation de l'objectif de la conservation,

– la personne concernée a retiré son consentement, et il n'existe donc plus aucun fondement juridique pour le traitement,

- leur traitement est interdit,

– la personne concernée s'oppose au traitement ou invoque un droit d'opposition au motif d'une situation personnelle particulière qu'elle doit pouvoir justifier,

– il s'agit de données à caractère personnel spécifiques dont l'exactitude ne peut être prouvée, ou

– il existe une autre obligation légale de suppression des données.

S'il existe une obligation de suppression et si les données à caractère personnel ont déjà été rendues publiques, les autres responsables du traitement des données doivent être informés de la demande de la personne concernée de supprimer toutes les copies de ses données et tous les liens vers ces données.

(6) La personne concernée peut demander la limitation du traitement de ses données si:

– l'exactitude de ses données à caractère personnel est contestable (erreur dans la saisie du nom après la célébration d'un mariage). Cette limitation du traitement n'est cependant valable que jusqu'à ce que l'exactitude ait été vérifiée par l'unité d'organisation responsable (par exemple, l'administration de l'ENA Suisse ou à la paroisse à laquelle appartient la personne en question), ou

– le traitement n 'est pas autorisé, mais que la personne concernée refuse la suppression desdites données, ou

– l'ENA Suisse n'a plus besoin des données à caractère personnel à des fins de traitement, mais la personne concernée a besoin desdites données pour faire valoir, exercer ou défendre des droits, ou

– la personne concernée a fait opposition au traitement desdites données en raison d'une situation particulière et que l'unité d'organisation responsable (par exemple, l'administration de l'ENA Suisse ou la paroisse à laquelle appartient la personne en question) est encore dans l'examen de ladite opposition.

(7) La personne concernée doit être informée, au plus tard dans un délai d'un mois, de toutes les mesures prises à sa demande.

(8) Le responsable de la protection des données se tient à disposition pour donner des conseils quant au respect des droits des personnes concernées.

§ 12 Demandes de renseignements de tiers relatifs aux personnes concernées

(1) L'ENA Suisse ne transmet en principe aucune donnée à caractère personnel à des tiers. Dans le cas où un organisme demanderait des informations sur des personnes concernées, telles qu'une autorité publique ou un institution socials, la communication desdites informations ne serait autorisée que si:

– l'organisme requérant peut démontrer un intérêt légitime à cet égard; et

– une norme juridique oblige à fournir des informations; et

– l'identité du demandeur ou de l'organisme requérant est clairement établie.

§ 13 Liste des activités de traitement

(1) ENA Suisse tient un registre de tous les traitements de données et de toutes les personnes responsables de ces traitements (cf. art. 30 RGPD). Le délégué à la protection des données peut être consulté pour donner des conseils quant aux informations requises par la loi.

(2) ENA Suisse met, sur demande, la liste à la disposition des autorités compétentes en matière de protection des données. La responsabilité en incombe au délégué à la protection des données en accord avec le chef de l'administration ChApd CH .

§ 14 Formation

(1) Les personnes ayant un accès permanent ou régulier aux données à caractère personnel de l'ENA Suisse, collectant de telles données ou mettant au point des systèmes de traitement de ces données doivent recevoir une formation appropriée quant aux exigences en matière de protection des données. Le délégué à la protection des données décide, en accord avec le chef de l'administration ChApd CH , de la forme et du roulement de la formation.

§ 15 Confidentialité des données, secret pastoral et secret de fonction

(1) Les personnes travaillant pour l'administration de l'ENA Suisse ne peuvent ni collecter, traiter ou utiliser des données à caractère personnel sans autorisation. Elles doivent accepter de traiter les données à caractère personnel de manière confidentielle avant le début même de leur fonction (signature d'une déclaration de confidentialité).

(2) Les personnes ayant des obligations de confidentialité particulières (par ex. responsables GIM) sont tenues de le faire par écrit.

(3) Les dossiers («notes personnelles») établis dans le cadre de l'exercice de fonctions pastorales ne peuvent être accessibles à des tiers. Les dispositions particulières relatives à la protection du secret pastoral restent inchangées. Il en va de même pour les autres obligations de confidentialité (par exemple les obligations contractuelles de confidentialité) qui ne sont pas fondées sur des dispositions légales.

(4) Ces obligations de confidentialité ne sont pas limitées dans le temps. Elles s'appliquent également aux informations échangées ou rendues accessibles avant la signature d'une potentielle déclaration de confidentialité. Elles sont irrévocables et restent en vigueur même après la fin de la coopération, respectivement de la relation contractuelle ou l'exécution des prestations convenues, et après la fin d'un contrat de travail ou d'une relation contractuelle..

§ 16 Plaintes

(1) Toute personne concernée a le droit de déposer une plainte relative au traitement de ses données au cas où elle se sentirait atteinte dans ses droits.

(2) L'organe compétent pour les plaintes susmentionnées est le délégué à la protection des données en tant qu'instance indépendante interne non dirigée.

§ 17 Audits

(1) Les processus pertinents peuvent être contrôlés par des audits réguliers effectués par des organismes internes ou par des auditeurs externes afin d'assurer un niveau élevé de protection des données. Des mesures correctives immédiates doivent être prises en cas de découverte d'une possibilité d'amélioration.

(2) Les enseignements apportés par l'audit doivent être documentés. La documentation doit être remise au délégué à la protection des données, au chef de l'administration ChApd CH ainsi qu'au responsable technique du processus concerné.

(3) Un audit est achevé avec succès lorsque toutes les mesures décrites dans le rapport ont été mises en œuvre. Des audits de suivi sont, le cas échéant, effectués en examinant la mise en œuvre des recommandations de l'audit initial.

§ 16 Enquêtes internes

(1) Les mesures visant à élucider l'examen des faits et à prévenir ou à détecter des infractions pénales ou des violations graves aux obligations doivent être mises en œuvre dans le strict respect de la législation applicable en matière de protection des données. En particulier, la collecte et l'utilisation des données qui en découlent doivent être nécessaires pour atteindre l'objectif de l'enquête, appropriées et proportionnées aux intérêts légitimes de la personne concernée.

(2) La personne concernée doit être informée dès que possible des mesures prises à son égard.

(3) Quelle que soit la forme de l'enquête interne, le délégué à la protection des données doit être préalablement associé au choix et à l'organisation des mesures à mettre en œuvre.

§ 19 Disponibilité, confidentialité et intégrité des données

(1) En fonction de la nature, de l'étendue, des circonstances et des objectifs du traitement, ainsi que de la probabilité d'occurrence, chaque procédure (par exemple la création d'une nouvelle base de données contenant les données personnelles des membres de l'Église) doit être accompagnée d'une évaluation documentée du besoin de protection et d'une analyse des risques pour les personnes concernées..

(2) Un concept général de sécurité relatif au constat de besoin de protection et à l'analyse des risques est élaboré afin de garantir la disponibilité, la confidentialité et l'intégrité des données («Sécurité de l'information»). Ce concept est contraignant dans toutes les procédures. L'état actuel de la technique doit notamment être pris en considération, de même que les moyens et les mesures de cryptage et de sauvegarde des données. Le concept de sécurité doit régulièrement être contrôlé et évalué par rapport à l'efficacité des mesure techniques et organisationnelles prévues.

(3) Il convient d'éviter que des personnes non autorisées puissent utiliser les systèmes de traitement de données. Les portes des locaux non occupés doivent être fermées. Des mesures efficaces de contrôle d'accès aux équipements doivent être mises en place et activées. Les accès au système doivent toujours être bloqués en cas d'absence.

(4) L'accès aux systèmes et des données à caractère personnel qu'ils contiennent ne doit se faire que par l'utilisation de mots de passe. Ils requièrent l'identifiant personnel de l'utilisateur et ne sont pas transférables. Il faut s'assurer que les mots de passe soient toujours sous clé. Les mots de passe doivent avoir une longueur minimale de huit caractères et être composés d'un mélange de caractères (majuscules, minuscules, chiffres et caractères spéciaux). Les mots de passe ne doivent pas figurer dans un lexique ou être formés à partir de termes faciles à deviner et surtout ne pas correspondre à des termes et expressions liés à l'ENA Suisse.

(5) L'accès aux données à caractère personnel ne doit être accordé qu'aux personnes qui, dans le cadre de l 'exercice de leurs fonctions, doivent avoir connaissance de ces données (principe du «besoin de savoir»). Les autorisations d'accès doivent être précises, déterminées et documentées.

(6) Les transmissions de données par les réseaux publics doivent, dans la mesure du possible, être cryptées. Le cryptage est obligatoire si le besoin de protection des données à caractère personnel l'exige.

(7) Les travaux de maintenance des systèmes ou des équipements de télécommunication par des prestataires externes sont à superviser. Il convient également de veiller à ce que les prestataires de services n'aient pas un accès non autorisé à des données à caractère personnel. Les opérations de téléassistance ne doivent être autorisées qu'au cas par cas et doivent respecter le principe de l'attribution minimale de droits. Les opérations de téléassistance doivent, si possible, être enregistrées ou inscrites au procès-verbal.

§ 20 Analyse d'impact relative à la protection des données

(1) L'ENA Suisse peut effectuer des analyses d'impact sur la protection des données relatives aux procédures relevant de sa responsabilité lorsqu'un risque élevé pour les droits et libertés des personnes concernées est prévisible suite au traitement des données. L'analyse d'impact de la protection des données contient toutes les descriptions requises par la loi en vertu de l'article 35, § 7 RPGD.

(2) Le délégué à la protection des données conseille l'ENA Suisse lors de la mise en œuvre de l'analyse d'impact relative à la protection des données ainsi que sur la question de savoir quand les traitements représentent un risque élevé pour les personnes concernées.

§ 21 Violations de la protection des données («perte de données»)

(1) Le chef de l'administration ChApd CH doit immédiatement être informé du fait que des données de l'ENA Suisse ou d'une paroisse auraient été révélées à un tiers. Ce dernier impliquera immédiatement le délégué à la protection des données dans le cadre de l'examen des faits.

(2) La notification doit comprendre toutes les informations pertinentes permettant à l'examen des faits, notamment l'organisme destinataire, les personnes concernées ainsi que la nature et l'étendue des données transmises.

(3) Le respect d'un éventuel devoir d'information envers le PFPDT s'effectue exclusivement par le délégué à la protection des données, en accord avec le chef de l'administration ChApd CH . Les personnes concernées sont informées par la direction de l'ENA Suisse et le délégué à la protection des données consulté.

§ 22 Conséquences des infractions

(1) Une infraction par négligence ou encore volontaire à la présente directive peut entraîner des mesures de droit du travail, notamment un licenciement sans délai ou dans les délais prescrits. Les sanctions pénales, conséquences civiles et dommages et intérêts sont également à prendre en considération.

§ 23 Responsabilité

(1) Le respect des exigences de la présente directive sur la protection des données doit pouvoir être démontré à tout moment. Il convient à cet égard de veiller de façon particulière à la traçabilité et à la transparence des mesures prises, par exemple par le biais de documents connexes.

§ 24 Mise à jour de la directive; traçabilité

(1) La présente directive sur la protection des données sera régulièrement révisée et complétée conformément à l'évolution de la protection des données et des changements techniques ou organisationnels.

(2) Les modifications apportées à la présente directive sur la protection des données prennent effet de façon informelle. Les ministres, responsables et employés de l'administration de la ENA Suisse doivent être informés sans délai et de manière appropriée des modifications apportées.

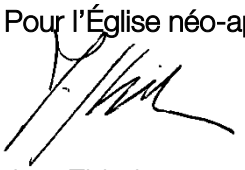
§ 25 Dispositions finales et entrée en vigueur

(1) La présente directive sur la protection des données remplace la directive actuelle (dernière mise à jour datant du 1er janvier 2009).

(2) Elle entrera en vigueur le 1er mars 2019.

Zurich, le 13 février 2019

Pour l'Église néo-apostolique de Suisse:



Jürg Zbinden
Président de l'Église néo-apostolique