Privacy Policy NACI

New Apostolic Church International (NACI)

Valid from

1 January 2021

Table of contents

Sources

NACI, Social Media Guideline of the New Apostolic Church, ratified in December 2017

New Apostolic Church West Germany, Privacy Policy, valid from: 20 April 2018

New Apostolic Church South Germany, Privacy Policy, valid from: 24 May 2018

New Apostolic Church Switzerland, NAC Switzerland Privacy Policy, valid from: 1 March 2019

New Apostolic Church Austria, NAC Austria Privacy Policy, valid from: 1 March 2019

Disclaimer:

The original version of this Privacy Policy was drafted in the German language. It has been translated into other languages. The German version prevails in the event of any ambiguity or discrepancy.

Foreword / Introduction

Dear Apostles, Dear Colleagues, Dear Project Workers,

The European General Data Protection Regulation (GDPR) has been applicable since 25 May 2018. It is applicable primarily in EU and EEA Member States. Under certain circumstances, it is also applicable in third countries such as Switzerland. As an association organised under Swiss law, NACI is subject in the first instance to Swiss law, and thus to the Swiss Data Protection Act (DPA). This Act has been entirely overhauled over the last few years. On 25 September 2020, Parliament enacted a new version of the Act. In terms of content it largely reflects the GDPR and is set to come into force in 2022. In view of this fact and NACI's close links with Europe, coupled with the increasing acceptance of the GDPR throughout the world, this Privacy Policy is based on the GDPR.

The rules set out in the GDPR are not entirely new. Thus, existing national data protection legislation in EU and EEA Member States, as well as in Switzerland, were already relatively clear as to the conditions under which data could be collected and processed, and for which purposes. The GDPR has tightened up these rules, and also obliges processors (any person/organisation that collects/processes data) to document how data are collected in a more transparent and traceable manner. The operative principle is data minimisation, i.e. only data that are required for a legitimate purpose should be collected, and these data should be erased as soon as possible. For all those that collect and process data, this means engaging intensively with one's own actions and work processes, and adapting them where necessary. This is because there are no generally applicable templates that are simply ready to be implemented without any additional input.

The frenetic changes in the way in which we communicate within society are very strongly influenced by technological innovation and in many cases fail to take data protection considerations on board. Precisely because we are a church, we want to make sure that personality rights do not end up falling by the wayside simply because easy and comfortable technological solutions are available. Our goal is to act responsibly also in relation to these matters.

Best wishes,

Yours,

Erich Senn
NACI Administrator

Frank Stegmaier
CFO

General principles

§ 1 General principles

(1) The New Apostolic Church International (hereafter referred to also as “NACI” or “the Controller”) follows the data protection standard of the European Union (EU) as regards the protection of personal data. This is the case in particular for the data of members of NACI and staff of the NACI Administration (administrative staff).

(2) NACI proceeds on the assumption that a privacy framework that is compliant with EU rules will largely meet with the requirements laid down in the new Swiss Data Protection Act (new DPA), which was approved by the Swiss Parliament on 25 September 2020.

§ 2 Purpose

(1) This Privacy Policy of NACI (hereafter, the “NACI Privacy Policy” or the “Privacy Policy”) constitutes a binding basis for the lawful processing of *personal data (in Switzerland: personal information)* by NACI.

(2) The aim of this Privacy Policy is to uphold and protect the basic rights and basic freedoms of data subjects, including in particular the right to the protection of personal data.

(3) A further purpose of this Privacy Policy is to enable the free movement of such data.

§ 3 Scope

(1) This Privacy Policy applies to the processing of personal data by NACI as an association organised under Swiss law with registered office in Zurich (Switzerland) as a central administrative unit.

(2) It applies personally to all administrative staff. This Privacy Policy also applies to apostles, project workers and other people associated with NACI in any way by a contractual or service relationship.

(3) The requirements and prohibitions set forth in this Privacy Policy apply to all processing of personal data, irrespective of whether this occurs electronically, on hard copy documents or orally.

§ 4 Processing and collection of data

(1) Data *processing* means any handling of personal data – from collection through archival to erasure.

(2) When processing personal data the principles laid down in the GDPR (cf. Article 5 GDPR) must be complied with: lawfulness, processing in good faith, transparency, purpose limitation, data minimisation, accuracy of personal data, storage limitation ("right to be forgotten"), integrity, confidentiality and availability ("data security" / "information security") and accountability.

(3) As a general rule, personal data are collected from the data subject by the relevant local church.

(4) Master data of church members: some administrative staff have access to the master data of church members. This access is required in order to perform administrative tasks such as supporting the local churches concerned with apostles or participation in project groups by church members involved in NACI projects.

(5) Apostle files: information relating to the ordination of an apostle includes highly personal data of the data subject and is therefore particularly sensitive. These data are provided by the relevant local church as part of the ordination process. In addition, NACI holds information concerning apostles' member master data as well as their geographical areas of activity.

(6) Personnel files of administrative staff: it is not unusual for these to contain information concerning the occupation, membership of political parties, hobbies, number of children, education etc. of the data subject, which must also be guaranteed particular protection.

§ 5 Purpose limitation, data minimisation and consent

(1) The collection, processing, usage and disclosure of personal data is only permitted if this is necessary for the performance of church tasks or if the data subject has consented (purpose limitation). A data processing operation is necessary if the church purpose cannot be achieved in another manner or can only be achieved at considerable cost.

(2) The collection, processing and usage of personal data must be limited to what is necessary in relation to the purpose (data minimisation).

(3) Personal data may only be published, for example over the internet, with express consent. Any statement of intent, given in the form of a declaration or any other unequivocal confirmatory act, that is made voluntarily, in an informed manner and unambiguously with reference to the specific individual circumstances is deemed to constitute valid consent.

(4) The provision of information relating to the official events, travel and activities of apostles that is of interest for church members worldwide does not require specific consent.

§ 6 Data secrecy, pastoral secrecy and professional confidentiality

(1) Any person working for NACI is prohibited from collecting, processing or using personal data without authorisation. They must be subjected to an obligation to treat personal data in confidence before starting their work (signature of a non-disclosure agreement).

(2) Any records ("personal notes") made during the performance of professional activities within NACI must not be made accessible to third parties. This stipulation is without prejudice to the rules on the upholding of pastoral secrecy. The same applies in respect of the other duties of confidentiality necessary in order to comply with statutory duties of secrecy or confidentiality or to uphold occupational or special professional secrets that do not have a basis in law.

(3) These duties of confidentiality apply without limitation in time. They also apply to any information that was exchanged or made available before a non-disclosure agreement was signed. They are irrevocable and continue to apply also after the end of cooperation or of the employment relationship, completion of the agreed services or termination of a contract of employment, an agency agreement or a contract for services.

§ 7 Retention, archival and erasure

(1) As a general rule, any personal data that are no longer required and are not suitable for archival must be permanently erased or destroyed (e.g. by shredding).

(2) Personal data must be erased if storage is not lawful, consent to storage has been withdrawn or they are no longer required for the purposes for which they were collected.

(3) Personal data of church members are necessary in order to document membership, for the receipt of sacraments and in relation to church ordinations, assignments and appointments. This means that the withdrawal of consent to storage or departure from the church does not automatically result in the data being erased. However, access to any such personal data is limited in order to be able to provide information and issue documents to the data subject.

(4) Further exceptions to the duty of erasure apply in relation to:

- anonymised personal data
- statutory duties of retention
- personal data that must be retained as evidence or for security purposes or in order to uphold the legitimate interests of the data subject

(5) The details must be regulated in an erasure and archival concept (including data backup).

Data protection organisation

§ 8 Data Protection Officer[1]

(1) NACI shall appoint a Data Protection Officer. You can contact the Data Protection Officer as follows:

New Apostolic Church International
Data Protection Officer
Ueberlandstrasse 243
8051 Zurich / Switzerland
privacy@nak.org

(2) The Data Protection Officer monitors compliance with the European General Data Protection Regulation (GDPR) and other statutory requirements, including the terms of this Privacy Policy and other NACI policies concerning privacy-related issues. The Data Protection Officer advises and instructs the Administrative Management concerning existing data protection requirements and is responsible for communication with the data protection authorities. Selected processes are checked at random according to a risk-based approach at reasonable intervals in order to ensure compliance with data protection rules.

(3) The Data Protection Officer performs his tasks free from instruction, drawing on his own expertise. He reports directly to the Administrative Management.

(4) The Administrative Management and the administrative staff support the Data Protection Officer in the performance of his tasks.

(5) References to data protection are often made in materials released to the general public by the church. These should only indicate the NACI Data Protection Officer.

§ 9 Data Protection Coordinator

(1) NACI also commits to providing data protection training to an administrative staff member. The task of this administrative staff member is to ensure compliance with data protection rules and to issue instructions within the organisation in order to ensure this outcome.

[1] For the sake of simplicity, any male pronouns used below refer to both men and women without distinction.

Rights of data subjects

§ 10 Rights of data subjects

(1) The Administrative Management informs data subjects comprehensively concerning the processing of their data. This occurs at least once in relation to appointment as well as upon ordination.

(2) Related rights, such as e.g. the right of access, may only be exercised by the entitled person. Therefore, the applicant's entitlement and identity must be established unequivocally in advance.

(3) Right of access: upon request, data subjects must be provided with access to personal data stored that concern them. Access is provided as a general rule in writing, unless the data subject has requested access electronically. Information is provided within 30 days of receipt of a request for access.

(4) Right to rectification or erasure: data subjects may have incomplete personal data completed and obtain the erasure of data that are no longer required. Prior to any erasure of data is it necessary to ensure that erasure is not potentially precluded by statutory or other retention requirements or any overriding interest of the church or any other legitimate interest.

(5) Any person who considers that his rights have been violated in relation to the collection, processing or usage of his personal data by a church body may contact the Data Protection Officer or the Management Board in writing.

Disclosure and transmission of data abroad

§ 11 Disclosure and transmission of data

(1) The transfer of personal data to a third party is only permitted if provided for by law or on behalf of or with the consent of the data subject.

(2) The Administrative Management is situated in Zurich (Switzerland) and processes personal data in Switzerland. The protection of these data when they are exchanged with local churches based in the EU or the EEA is guaranteed under the terms of an adequacy decision of the EU Commission and by the provision of reasonable information to and the grant of consent by the data subject.

(3) Any disclosure or transmission of data to a local church or organisation based outside the EU or the EEA is only permitted with the express consent of the data subject.

§ 12 External service providers

(1) Should any external service providers gain access to personal data, the Data Protection Officer must be informed in advance.

(2) Service providers that may gain access to personal data must be selected carefully before an order is placed. The selection must be documented, and should take account in particular of the following aspects:

- the professional competence of the service provider for the specific data processing operation
- technical and organisational security measures
- the service provider's experience on the market
- other aspects pointing to the reliability of the service provider (data protection documentation, willingness to cooperation, response times, etc.)

(3) Should a service provider collect, process or use personal data on an outsourced basis, it is necessary to conclude a data processing agreement ("DPA") in addition to related non-disclosure agreements. These must regulate all data protection and IT security aspects.

(4) Compliance by the service provider with the technical and organisational measures agreed to with it must be reviewed at regular intervals. The result must be documented.

Record of processing activities and NACI file systems

§ 13 Record of processing activities

(1) NACI keeps a record of all processing activities falling under its competence along with the persons responsible for the relevant data processing (cf. Article 30 GDPR). Advice may be sought from the Data Protection Officer concerning the information required by law (cf. separate document "Record of NACI Processing Activities").

(2) NACI shall provide the record to the competent data protection authority upon request. This is the responsibility of the Data Protection Officer, acting in consultation with the Administrative Management.

§ 14 The concept of "file system"

(1) A file system is any structured collection of personal data that are made accessible according to particular criteria, irrespective of whether the collection occurs centrally, locally or on a functional or geographical basis. Examples of file systems may include personnel files or databases containing members' data.

(2) The members of NACI are the apostles living around the world. Their data are collected at the latest at the time they express a desire to take up this position. These data are stored by NACI in the dedicated database on the NAC portal.

Security of personal data

§ 15 Data security

(1) Personal data must be processed in such a manner as to ensure the reasonable security of the personal data, including protection by appropriate technical and organisational measures (TOM") against unauthorised or unlawful processing and against unintentional loss, unintentional destruction and unintentional damage.

(2) The IT Department adopts the necessary TOM in order to provide an appropriate guarantee of the security of the personal data stored.

(3) Administrative staff are obliged to handle personal data with care and using the technical instruments of the employer when performing their tasks under their employment contracts.

§ 16 Personal data breaches

(1) Should any NACI data be disclosed unlawfully to a third party, the Management Board must be informed of this fact without undue delay. The Management Board involves the Data Protection Officer in order to clarify the facts without undue delay.

(2) The report must contain all relevant information in order to clarify the facts, including in particular the recipient, the data subjects and the type and nature of the data transmitted.

(3) Compliance with any duty to inform the data protection authority is a matter exclusively for the Data Protection Officer, in consultation with the Administrative Management. Data subjects are informed by the Administrative Management, and the Data Protection Officer is involved on an advisory basis.

Training of administrative staff

§ 17 Training, data protection and security

(1) Persons with ongoing or regular access to NACI personal data, who collect such data or who develop systems in order to process such data must receive appropriate training concerning requirements under data protection law. The Data Protection Officer decides in consultation with the Administrative Management concerning the form and frequency of the relevant training.

(2) Human qualities such as helpfulness, trust, fear or respect for authority are often exploited by cyber-criminals. It is therefore important for administrative staff to be trained also in relation to cyber-security issues.

Consequences of breaches

§ 18 Consequences of breaches

(1) Any negligent or deliberate breach of this Privacy Policy may give rise to disciplinary measures, including termination with or without notice. It may also result in criminal penalties and consequences under civil law, such as liability to pay damages.

Concluding terms

§ 19 Accountability

(1) It must be possible to demonstrate at all times that this Privacy Policy is being compiled with. In order to ensure this, any action taken to ensure traceability and transparency, such as for example concerning the relevant documentation, is particularly important.

§ 20 Amendments

(1) This Privacy Policy will be reviewed regularly in order to determine whether it needs to be adjusted or supplemented due to further developments in data protection law or any technological or organisational changes.

(2) The amendment of this Privacy Policy is not subject to any specific formal requirements. Administrative staff will be informed promptly in a suitable manner concerning the amended requirements.

§ 21 Implementation and entry into force

(1) The Administrative Management is authorised to issue supplementary regulations in the form of service instructions.

(2) This Privacy Policy shall take effect on 1 January 2021 and replaces all previous privacy policies of NACI.

Zurich, December 2020

For the New Apostolic Church International (NACI):

Erich Senn
NACI Administrator

Frank Stegmaier
CFO

Annex: definitions

(1) *Personal data (in Switzerland: personal information)*[2] means any information relating to an identified or identifiable natural person (data subject). Data relating to brothers and sisters also constitute personal data, as do personal information and data concerning office holders and functionaries. For example, it is also possible to make inferences concerning a natural person, such as a contact person's email address, from his name. It is sufficient for the relevant information to be associated with the name of the data subject, or to be inferred from the circumstances independently of the person's name. Similarly, a person may be identifiable if the information first has to be associated with additional knowledge, such as e.g. date of birth, ID number or IP address. The manner in which the information was obtained is irrelevant for the purpose of establishing whether there is an association with a particular person. Photographs as well as video or sound recordings can also contain personal data.

(2) *Special types of personal data (in Switzerland: particularly sensitive personal information)* mean information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or the membership of political parties or trade unions, and genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, special categories of personal data may only be collected, processed or used with the consent of the data subject or exceptionally under the terms of an explicit statutory authorisation. Moreover, additional technical and organisational measures (e.g. encryption during transportation, minimal assignment of rights) must be taken in order to protect particularly sensitive personal data.

(3) *Processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission , dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(4) *Restriction of processing* means the marking of stored personal data with the aim of limiting their processing in future.

(5) *Profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. However, as a responsible organisation, NACI does not engage in any automated decision making or profiling.

(6) *Anonymisation / pseudonymisation:* personal data are deemed to have been *anonymised* if the person is no longer identifiable. "Anonymisation" means the process by which the allocation of data to a specific person is prevented or is only thereafter possible with extraordinary effort. In the event of *pseudonymisation* on the other hand, all identifiable data are replaced by a neutral dataset (pseudonym). Pseudonymisation can be reversed (provided that a correspondence table enabling the two data sets to be cross-referenced exists and is accessible).

[2] In English: "personal data" or "personal information".

On the other hand, anonymisation is definitive. Only data that have been entirely anonymised no longer constitute personal data.

(7) *Controller* means the natural or legal person (in this case, the Controller is NACI), authority, agency or other body that decides, either alone or in conjunction with others, for which purposes and by which means personal data are to be processed.

(8) *Processor* means any natural or legal person (e.g. the company charged with technological maintenance of the member management system / MMS[3]), public authority, agency or other body which processes personal data on behalf of the Controller.

(9) *Recipient* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

(10) *Third party* means a natural or legal person, public authority, agency or body other than the data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data.

(11) *Consent* of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him.

[3] MMS = Member Management System.