Sisters of Notre Dame de Namur

Congregational

Data Protection Policy

Table of Contents

Preamble 3
1 Objective 3
2 Applicability 3
3 Terminology 3
3.1. Definitions 3
3.2. Data Protection Principles 4
3.3. Lawfulness of the Processing 5
4 Content of the Policy 6
4.1. Forwarding of and Access to Personal Data 6
4.1.1. Processing on Behalf of the Generalate 6
4.1.2. Forwarding Data to Third Parties Outside the Congregation 6
4.1.3. Transfer of Personal Data to Another Country outside the EU/EEA 6
4.1.4. Access to Data 6
4.2. Data Security 6
4.3. Rights of the Data Subject 6
5 Data Protection Organisation 7
5.1. Responsibility of the Congregation 7
5.2. IT Security Coordinator 8
5.3. Members, Collaborators and Employees 8
5.4. Changes to this Policy and Continued Applicability 8
5.5. Supplementary Detailed Guidelines 8

PREAMBLE

This **Data Protection Policy** governs the handling of personal data by the "*CASA GENERALIZIA DELL'ISTITUTO DELLE SUORE DI NOSTRA SIGNORA DI NAMUR*" ("**Generalate**") acting on the specific mandate of the Congregational Leadership Team in respect to personal data gathered, processed and stored by the Generalate in Rome, Via Raffaello Sardiello 20.

The CONGREGATION OF THE SISTERS OF NOTRE DAME DE NAMUR ("**Congregation**") and the Generalate undertake to protect the personal data and rights of data subjects in accordance with the General Decree of the Italian Episcopal Conference ("*Provisions for the protection of the right to good reputation and confidentiality*") adopted on 24 May 2018 by its 71st General Assembly, which implements the EU General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).

For the purposes of this Data Protection Policy, the Congregation is considered the **Controller** as defined below.

1 OBJECTIVE

To ensure data protection and data security by the Generalate, the objective is to protect personal data (of the members of the the Congregation and of third parties) through compliance with legal requirements.

For this purpose, this top-level policy concerning data protection and data security by the Generalate (hereinafter referred to as "**Policy**") determines fundamental rules for the handling of personal data and data security.

2 APPLICABILITY

This Policy is binding for the Congregation and the Generalate and comprises all processes in which the Generalate, its collaborators or employees automatically or semi-automatically process personal data. This Policy also applies to the manual processing of personal data, if personal data are stored or are to be stored in physical archives.

In case further regulations of the Congregation or the Generalate provide for more specific requirements for the handling of personal data than this Policy, such specific regulations shall prevail.

3 TERMINOLOGY

3.1. DEFINITIONS

"**Controller**" means the natural or legal person, service entity or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**Generalate**" means the "*CASA GENERALIZIA DELL'ISTITUTO DELLE SUORE DI NOSTRA SIGNORA DI NAMUR"*, a civilly recognized ecclesiastical entity with registered office in Rome, Via Raffaello Sardiello 20, listed in the register of juridical persons of the Prefecture of Rome at No. 1118/1987.

“**Health data**” means personal data relating to the physical or mental health of a natural person, including the provision of health care services, revealing information related to a natural person’s state of health.

"**Personal data**" are any information relating to an ecclesiastical entity, an ecclesial aggregation, an identified or identifiable natural person ("data subject").

"**Processing**" refers to 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.

"**Third party**" means the natural or legal person, service entity or other body that is not the data subject, the data controller, the person in charge of the processing and persons authorized to process personal data under the direct authority of the controller or processor.

3.2. DATA PROTECTION PRINCIPLES

The following principles shall be complied with when processing personal data:

Personal data shall be

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("**lawfulness, fairness and transparency**");

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("**purpose limitation**"); further processing of personal data for archiving purposes or for historical or statistical purposes is not considered incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**");

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("**accuracy**");

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("**storage limitation**"); personal data can be stored for longer periods if treated exclusively for archiving purposes, historical or statistical purposes, without prejudice to the implementation of adequate technical and organizational measures required by the General Decree to ensure the protection of the rights and freedoms of the data subject;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("**integrity and confidentiality**").

The Generalate and the Congregation are responsible for complying with the data protection principles and must be able to demonstrate the compliance ("**accountability**").

3.3. LAWFULNESS OF THE PROCESSING

Personal data shall only be processed if a legal basis exists for the processing. Relevant legal bases are the following:

a) The data subject has freely and specifically expressed, in an informed and unequivocal manner, through statement or unequivocal positive action, consent to the processing of personal data of the data subject for one or more specific purposes. For the purpose of an informed consent, the data subject must be made aware of at least the identity of the Controller and the purposes of the processing of the relevant personal data;

   - the Controller will have care to prepare the most appropriate means in order to be able to demonstrate that the data subject has consented to the treatment, in particular through a declaration of consent prepared by the Controller in a comprehensible and easily accessible form, using simple and clear language that does not contain unfair terms;

   - if the processing is based on a consent given under the previous General Decree of the Italian Episcopal Conference of 30 October 1999, there is no need for the data subjects to give their consent again, if it has been expressed in accordance with the provisions of the General Decree of 24 May 2018, so that the Controller can continue the processing in question.

b) The processing is required for the fulfilment of a legal obligation provided for by the canonical or civil law, which the Controller is subject to.

c) The processing is necessary for the performance of a duty of public interest or related to the exercise of official authority the Controller is vested with. Performance of institutional activities including those related to relations between the public authorities and the churches, religious associations or communities shall be considered purposes of public interest. The processing of personal data is carried out for reasons of public interest if carried out by public authorities in order to achieve the mission, provided for by constitutional law or by public international law, or of officially recognized religious associations. The processing must be proportionate to the purposes pursued, respect the essence of the right to data protection and has to provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject;

d) the processing is necessary for archiving purposes in the public interest, for scientific or historical research or for statistical purposes in compliance with Article 24 of the General Decree, is proportionate to the purpose pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to protect the fundamental rights and interests of the data subject;

e) the processing is necessary to pursue the legitimate interests of the Controller or of third parties, unless the interests or fundamental rights and freedoms of the data subject, in particular if the person concerned is a minor, prevail;

f) the processing is necessary to ascertain, exercise or defend a right in court or whenever the court or tribunals exercise their judicial functions;

g) the processing regards personal data that have manifestly been made public by the data subject.

4 CONTENT OF THE POLICY

4.1. FORWARDING OF AND ACCESS TO PERSONAL DATA

4.1.1. Processing on Behalf of the Generalate

Data processing is regularly carried out directly by the Generalate that legitimately acquired and holds them.

The assignment of data processing to an entity not belonging to the Generalate is subject to the provisions referred to in Article 15 of the General Decree and must be done through a contract stipulated in accordance with can. 1290 CIC and can. 1034 CCEO, provided that the assignee shall always be obliged to observe the regulations of the General Decree and in particular the provisions of Article 15. Processors shall be selected carefully with a view of the technical and organisational measures they take.

4.1.2. Forwarding Data to Third Parties Outside the Congregation

If personal data of members are forwarded to third parties outside the Congregation (including other Congregations), the Generalate shall do so only upon the documented request and with the consent of the relevant data subject (i.e. the member), if not otherwise permitted or required by law.

4.1.3. Transfer of Personal Data to Another Country outside the EU/EEA

If personal data are transferred to another country outside the EU/EEA, the recipient must have appropriate safeguards in place, e.g. standard data protection clauses, binding contracts with the Generalate etc. Moreover, the data subject should be granted effective and enforceable rights as well as effective administrative and judicial legal remedies.

4.1.4. Access to Data

Access permissions must be clearly and comprehensively determined and documented.

4.2. DATA SECURITY

Every member and/or employee involved in the processing of personal data shall comply with the data security requirements in his field of activity and is thus responsible for the dutiful handling of personal data. Fundamental data security requirements include, but are not limited to the following:

a) Access control and encryption of personal data

b) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

4.3. RIGHTS OF THE DATA SUBJECT

In accordance with Article 7 of the General Decree, the data subject has the right to obtain from the Controller confirmation whether or not personal data is being processed that concerns the data subject and, if so, to receive the following information:

a) the purposes of the processing;

b) the categories of personal data processed;

c) the recipients or categories of recipients to whom personal data have been or will be communicated, in particular if these recipients are based in third countries or if they are international organizations;

d) when possible, the retention period of personal data or, if this is not possible, the criteria used to determine this period;

e) if the data are not collected from the data subject, all the information available on the origin.

The data subject has also the right to request:

a) the rectification of errors;

b) the cancellation of personal data, to the extent permitted by the provisions of the General Decree;

c) the cancellation of personal data and the limitation of the processing of the personal data concerning the data subject, to the extent permitted by the provisions of the General Decree.

The data subject is also entitled to:

a) oppose the processing, to the extent permitted by the provisions of the General Decree;

b) to propose a complaint to the supervisory authority.

Where personal data is transferred to a third country or a to an international organization, the data subject has the right to be informed of the existence of adequate guarantees.

Enquiries or requests of the data subjects shall without delay and without being prompted to do so be forwarded to the Secretary General.

5 DATA PROTECTION ORGANISATION

5.1. RESPONSIBILITY OF THE CONGREGATION

The Congregation shall:

a) implement suitable measures to comply with the statutory and internal data protection requirements;

b) ensure the implementation and establishment of the regulations of this Policy as well as of the further instructions, guidelines and standards as they may be enacted from time to time;

c) provide the resources required for the performance of the data protection duties by the members and/or employees involved in the processing of personal data;

d) enforce data protection requirements and monitor on a regular basis relevant data protection issues and statutory data protection requirements.

5.2. IT SECURITY COORDINATOR

As regards IT security, the Generalate or the Congregational Leadership Team may appoint an IT Security Coordinator, whose duties and competencies shall be regulated separately. The IT Security Coordinator shall closely and trustingly collaborate with the Generalate and the Congregational Leadership Team.

5.3. MEMBERS, COLLABORATORS AND EMPLOYEES

Every member of the Congregation, collaborator and employee shall comply with the requirements of this Policy as well as data protection requirements, guidelines and standards as they may be enacted from time to time. Any errors or deficiencies identified shall be reported directly to the Secretary General.

5.4. CHANGES TO THIS POLICY AND CONTINUED APPLICABILITY

The Congregation is responsible for the creation, formal enactment, revision (substantial material changes to the content) and, if necessary, repeal or replacement of this Policy.

5.5. SUPPLEMENTARY DETAILED GUIDELINES

The Congregation shall define the essential data protection requirements, guidelines and standards in supplementary detailed guidelines or instructions. This Policy is the basis for supplementary detailed guidelines.

Approved and adopted by the Congregational Leadership Team on January 9, 2024.