Data Protection Policy

for

All Nations Church of Luxembourg

Latest update: 21 February 2024

Contents

1 Introduction

The protection of personal data is enshrined in EU law, and is also a moral responsibility that All Nations Church of Luxembourg a.s.b.l. ("**ANCL**") takes seriously. ANCL uses personal information to fulfil its vision and mission and is committed to protecting the privacy of its members, staff, volunteers, supporters and all those whose personal information it holds.

1.1 Purpose

The purpose of this policy is to describe the approach and steps ANCL takes to comply with data protection legislation.

This policy is also intended to provide us with measures to minimise risks to individuals through misuse of personal data, such as:

- personal data being used by unauthorised individuals through poor security or inappropriate disclosure;
- individuals being harmed by decisions made using inaccurate or insufficient data;
- individuals being uninformed by lack of transparency leading to unlawful practice;
- the invasion of privacy due to over-collection or over-retention of data.

1.2 Definitions

Data Controller: a body or organisation that makes decisions on how personal data is being processed. Data Controllers almost always also process data. ANCL is a Data Controller under EU law and for the purposes of this policy.

Data breach: any occasion when personal data is: accidentally or unlawfully lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or made unavailable (through being hacked or by accidental loss/destruction).

Data processing: any activity relating to the collection, recording, organising, structuring, use, amendment, storage, access, retrieval, transfer, analysis, disclosure, dissemination, combination, restriction, erasure or disposal of personal data.

Data Protection Lead: the ANCL Governing Board.

Data Subject: the individual to whom the data being processed relates.

Personal Data: any information that relates to an identifiable living individual.

Special Categories of Personal Data (also known as sensitive personal data): specific types of data that require additional care being taken when processing. The categories are race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

3rd Party Data Processors: other legal entities that process data on behalf of a Data Controller and under instruction from the Data Controller. Data Processors do not have the ability to make decisions about *how* the data should be processed, there should be documented instructions from

the Data Controller about what the processor can and cannot do with the data (known as a Data Processing/Sharing Agreement).

1.3 Scope

ANCL expects all staff and volunteers who handle personal data on behalf of ANCL to act in accordance with this policy when engaged in the business of ANCL. Those who handle personal data as part of their role will:

- make sure that data security is maintained in line with this policy and any associated guidelines or procedures that may be issued by the Data Controller from time to time;
- implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss or damage to personal data in accordance with the guidelines and good practice outlined in this policy;
- exercise particular care in protecting Special Category Data from unauthorised access, use or disclosure;
- take part in available data security training that is appropriate to their role, offered by the Data Controller; and
- keep up-to-date with the guidance and policies produced or signposted by the Data Controller.

This policy will be reviewed, and updated as required, from time to time by the Data Controller. This policy was last revised on the date stated on the front page.

2 Policy Statement

Personal data that ANCL collects, uses, stores, transfers, shares and disposes of must be handled in line with this policy.

2.1 Principles of data protection

Personal data is processed according to the following principles:

1. **Data is processed lawfully, fairly and in a transparent manner** in relation to the data subject, through the provision of clear and transparent privacy notices and responses to individual rights requests.
2. **Data is collected for specified, explicit and legitimate reasons** and not further processed for different reasons incompatible with these purposes. ANCL has created an information register that will be regularly and consistently reviewed and updated.
3. **Data is adequate, relevant and not more than is necessary** to complete the task for which it was collected and will be subject to regular review of data collection and processing needs.
4. **Data is accurate and up-to-date** and reasonable steps will be taken to ensure this through regular data quality checks.
5. **Data is not kept for longer than is necessary** to complete the task for which it was collected, by compliance with the retention procedures indicated in the information register maintained by ANCL and by regular data cleansing.

6. **Data is kept secure**, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, accidental corruption, loss or disclosure of personal data (see section 3). This will include:
    - storing paper copies of personal data in locked cabinets;
    - maintaining password protection of electronic data held on computers and online storage;
    - ensuring access to paper and electronic media is restricted only to those individuals authorised to access the data;
    - ensuring that extra precautions are taken when personal data is carried in public places, to keep the risk of data breaches to an acceptable level.

    To maintain appropriate data security, we will undertake regular risk assessments of our practices and provide awareness and training to all those processing personal data on behalf of ANCL.

7. **Data that is transferred outside the European Union** will only take place with appropriate safeguards to protect the rights of individuals.
8. **Accountability**. ANCL responsible for, and will demonstrate, compliance with the principles by:
    - adopting and implementing this data protection policy;
    - publishing privacy notices to explain our data protection practices to those whose personal data we process
    - putting in place written contracts with 3rd party Data Processors that process personal data on our behalf;
    - implementing regular reviews, to update the measures we have put in place.

2.2 Collecting personal data

Data protection legislation requires that the collection and use of personal data is fair and transparent. If we acquire any personal data related to an individual (including employees, officer holders, volunteers, suppliers, supporters or other external contacts), either directly from the data subject or from a third party, we must do so in line with the above 'Principles of Data Protection'.

If we acquire data in error (that is, data we should not have access to), by whatever means, we will assess whether the data should be retained and, if so, arrange for it to be given to the appropriate individual.

2.3 Privacy Notices

Individuals have the right to be informed about the collection and use of their personal data and ANCL will be open and transparent about its use of personal data in line with this Policy. Our current privacy notice can be found here: https://www.allnationschurch.com/privacy/.

If our data processing practices change, causing a Privacy Notice to be updated, we will reissue the notice to the affected data subjects, by email.

2.4 Lawful bases

Personal data must only be processed once we have identified an appropriate lawful reason to do so. There are six available lawful bases for processing (Appendix 1). No single basis is 'better' or more important than the others, therefore we must decide which basis is most appropriate depending on our purpose and relationship with the individual.

The lawful basis for different areas of our data processing are included in the information register maintained by ANCL and indicated in the relevant Privacy Notice.

2.5 Individual rights

Data protection legislation gives individuals specific rights regarding their personal data:

1. The right to be informed
2. The right to access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability (unlikely to be relevant to parishes or deaneries)
7. The right to object
8. Rights in relation to automated decision making and profiling (unlikely to be relevant to ANCL).

3 Data Security

3.1 Confidentiality, integrity and availability

We will maintain data security by protecting the confidentiality, integrity and availability of personal data. This means that:

- only people who have a need to know and are authorised to use the personal data can access it. People who are not authorised should not be able to access the personal data, or alter, disclose ore delete it;
- personal data is accurate and suitable for the purpose for which it is processed e.g. personal data is kept up to date and can only be updated by authorised staff, leadership and volunteers; and
- personal data is accessible and usable by authorised users when they need it for authorised purposes.

3.2 Technical measures

The measures we use to minimise risk to the confidentiality, integrity and availability of personal data include:

- personal data is only shared amongst those members of staff, leadership[1] and volunteers who have a need to know the information to fulfil a specific task;
- databases (e.g. Planning Center) and electronic document storage/sharing systems (e.g. Google Drives) are password protected and permissions (e.g. to access, view, edit, delete) are set appropriately;
- all devices (including personal devices used by staff, leadership and volunteers in carrying out ANCL business) are password protected;
- passwords to databases, document storage/sharing systems and devices containing personal data are not shared;
- as far as practicable, documents relating to ANCL business are saved to ANCL's document storage/sharing systems and links sent to recipients (i.e. we avoid sending attachments as this creates duplicated data);
- staff and other individuals with official ANCL email accounts use these accounts (and not personal email accounts) for ANCL business and do not use their ANCL email accounts for personal purposes;
- personal email accounts used by volunteers for the purposes of ANCL business are not shared with any other individual(s) and are password protected;
- avoiding downloading and storing information on personal devices;
- avoiding printing information containing personal data unless necessary and ensuring that it is kept (and disposed of) securely;
- taking care when typing email addresses and using the BCC field for general correspondence;
- avoiding recording more personal data than is required (e.g. medical information is not relevant to ANCL membership applications);
- email accounts (including personal email accounts), databases, document storage/sharing systems are regularly reviewed and information deleted if no longer required;
- paper documents containing personal data are kept in lockable filing cabinets, for which keys are held only by those who need access;
- paper files are regularly reviewed and documents containing personal data are disposed of by shredding if no longer required;
- being vigilant of our surroundings, in particular when working outside of normal office locations, being careful not to place any personal data in a position where it can be viewed, stolen or lost; and
- desks are kept clear of personal data when not occupied.

3.3 Data Sharing

As a Data Controller, we recognise that when we share personal data with third parties, we are responsible for:

- ensuring the third party complies with GDPR, and
- stating any constraints or requirements about what the third party can or cannot do with our data.

When sharing or disclosing personal data we shall ensure that:

[1] ANCL Governing Board and Leadership Team

- we consider the benefits and risks, either to individuals or ANCL, of sharing the data, along with the potential results of not sharing the data;
- we are clear about with whom we can share the data. If we are unsure, we check with the data owner, or our Data Protection Lead;
- we do not disclose personal data about an individual to an external organisation without first checking that we have a legitimate reason to do so (see above 'Lawful bases' section);
- if we must transfer or share data, we do so using appropriate security measures;
- if we are sharing data outside of the EU, we take particular care to ensure that the destination country meets all the necessary requirements to protect the data.

If we are unsure whether or not we can share information, we will contact our Data Protection Lead.

Data Sharing statements

We may state any constraints or requirements on the use of data shared with third parties in the following ways, depending on the level of risk:

- Through the use of disclaimer-type statements in emails or on contractor job sheets

The following is an *example* of what is meant by 'disclaimer type statement': The attached personal data is provided by [name_of_data_controller] to [third_party_name] for the purposes of [state_the_purpose_here]. To comply with General Data Protection Regulation 2016/679, this data is only to be used for [insert_name_here] to contact the persons listed in the attached data file for the above stated purpose. You must not share it with any other third party; you must store it securely and take all reasonable steps to prevent its unauthorised access, accidental deletion or corruption. When you no longer need this data, it must be deleted and any paper copies you have made destroyed. Should this data suffer an unauthorised disclosure (data breach), you are to notify [name and contract detail for lead data protection person].

- By the inclusion of a 'Data Protection' section of a contract with a third party (such as a leasing agreement)
- By a standalone 'Data Sharing Agreement'

3.4 Fact versus Opinion

When using personal data, it is our policy not to write comments about any individual that are unfair, untrue or offensive and that you would not be able to defend if challenged. In general we:

- express facts, not opinions
- work on the basis that anything written about an individual might be seen by that individual.

This includes emails. Although a certain amount of informality attaches to email writing, it should not be overlooked that these can provide a written record of our comments and, in the event of a Subject Access Request, they are subject to disclosure if they contain personal data.

3.5 Data Breaches

A personal data breach means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Any data breach, as described above, is to be reported to the Data Protection Lead.

Where a breach is known to have occurred which is likely to result in a high risk to the rights and freedoms of individuals, our Data Protection Lead will report this to the National Commission for Data Protection (Luxembourg) within 72 hours and will co-operate with any subsequent investigation. We will contact the affected data subject(s) where it is necessary to do so.

3.6 Awareness and training

We recognise the importance of ANCL staff, leadership and volunteers being aware of data security good practice and their responsibilities under this policy. We raise awareness by:

- putting in place this policy, making it available to staff, leadership and volunteers and keeping it under review; and
- arranging training sessions for those handling personal data on behalf of ANCL.

4 Approval and review

Approved by	ANCL Governing Board
Policy owner	ANCL Governing Board
Policy author	Julia Kennedy
Date	31 May 2021
Latest Review date	21 February 2024

5 Revision History

Version No	Revision Date	Previous revision date	Summary of Changes

APPENDIX 1 – Lawful bases (Article 6 of GDPR)

Legitimate interest

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate Interest Assessment. When can you rely on legitimate interests?

- When processing is not required by law but is of benefit to you
- When there is a limited privacy impact on the data subject
- When the data subject would reasonably expect your processing to take place

In order to use legitimate interests as your lawful basis for processing, your processing must therefore meet all of the following criteria:

- Have a specific purpose with a defined benefit
- Be necessary – if your defined benefit can be achieved without processing personal data then legitimate interests is not appropriate
- Be balanced against, and not override, the interests, rights and freedoms of data subjects

Contract

The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation

The processing is necessary for you to comply with the law (not including contractual obligations).

Consent

The individual has given clear consent for you to process their personal data for a specific purpose.

If consent is used it must be valid (freely given, unambiguous, actively selected, can easily be withdrawn); Both giving and withdrawing consent must be recorded.

For consent to be valid, i.e. the correct basis, it must be a choice - so if the data subject refuses to give consent, does that mean that the service can't be provided? If it is an essential service (e.g. pension, payroll etc) then the data controller cannot refuse the service, so there is effectively no choice, so consent is not valid.

Vital interests

The processing is necessary to protect someone's life.

Public Task

The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.