DATA PROTECTION

POLICY

Department/service:	Data Protection
Version:	1.1
Author/owner:	Sam Bull (previous DPO)/Evalian (current DPO)
Approved by:	Olivia Amartey
Date of approval	21/01/2021
Date effective from:	21/01/2021
Last reviewed:	02/07/2022

Contents

1. Introduction

Context

Data protection at Elim Foursquare Gospel Alliance ("Elim") is about ensuring people can trust it to use their data fairly and responsibly. The UK data protection regime is set out in the Data Protection Act 2018 (DPA 2018), along with the UK General Data Protection Regulation (UK GDPR) (which also forms part of UK law). It takes a flexible, risk-based approach which puts the onus Elim to think about and justify how and why it uses data.

The Information Commissioner's Office (ICO) regulates data protection in the UK. They offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

This Policy has been documented giving consideration to and in compliance with the following legislation and guidance:

Title	Body
DPA 2018	UK Government
UK GDPR	UK Government
Guidance for organisations	ICO

Aims

The aim of this policy is to set out the governing principles that ensure Elim meets its obligations under the law and adopts good practice when processing personal data. In particular, it ensures that Elim will keep the following UK GDPR key principles at the heart of its approach to processing data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

It also ensures that Elim upholds the following rights of those whose data it processes:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Scope

This policy applies to:

- all Elim employees, office holders and volunteers (personnel);
- all activities that operate under Elim, both at Elim International Centre (EIC) and at local Elim contexts, like churches, local ministries and nurseries;

This is not a legal document. It does not confer rights nor override any legal or statutory obligations.

2. Roles and responsibilities

All personnel

Before Elim personnel collect or handle any personal data as part of your work (paid or otherwise) for the EFGA, it is important that you take the time to read this policy carefully and understand what is required of you, as well as the organisation's responsibilities when we process data.

All personnel are required to comply with this policy. If you think that you have accidentally breached the policy, it is important that you contact the Data Protection Lead for your department or local Elim context or Elim's Data Protection Officer immediately so that we can take swift action to try to limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

Data Protection Officer (DPO)

The DPO's role is to assist Elim to monitor internal compliance, inform and advise on its data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Elim must ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

Elim must support the DPO in performing the tasks referred to in Article 39 of the UK GDPR by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

Elim must ensure that the DPO does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by Elim for performing his or her tasks.

The DPO is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

The DPO may fulfil other tasks and duties. Elim must ensure that any such tasks and duties do not result in a conflict of interests.

EIC Data Team

Members of the Data Team are responsible for:

- assisting the DPO with their responsibilities under this policy; and
- supporting Elim personnel with their responsibilities under this policy, where appropriate.

Data Protection Leads (DPLs)

DPLs act as the first point of contact regarding data protection issues for their department or local context. They manage requests and incidents regarding local data. They liaise with and decide whether to pass on cases to Elim's DPO.

Managers and leaders

Managers and leaders are required to make sure that any procedures that involve personal data, that they are responsible for in their area, follow the rules set out in this Data Protection Policy.

3. Training and Guidance

Elim will provide general training at least annually for all personnel to raise awareness of their obligations and responsibilities, as well as to outline the law.

Elim may also issue procedures, guidance, or instructions from time to time. Managers/leaders must set aside time for their team to look together at the implications for their work.

4. Elim's data protection responsibilities

What personal data do we process?

In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers.

We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details and visual images of people.

In some cases, we hold types of information that are called “special categories” of data in the UK GDPR. This personal data can only be processed under strict conditions. Special categories of data includes information about a person’s: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when there is a lawful basis for processing the data and when the processing is transparent. This means Elim will provide people with an explanation of how and why it processes their personal data at the point data is collected from them, as well as when data is collected about them from other sources.

How can we legally use personal data?

Processing of personal data is only lawful if one of these lawful bases, as listed in Article 6 of the UK GDPR, is met:

a) the processing is necessary for a contract with the data subject;
b) the processing is necessary for us to comply with a legal obligation;
c) the processing is necessary to protect someone’s life (this is called “vital interests”);
d) the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
e) the processing is necessary for legitimate interests pursued by the EFGA or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.
f) If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

How can we legally use special categories of data?

Processing of special categories of personal data is prohibited unless one of the conditions listed in Article 9 of the UK GDPR is met:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
b) processing is necessary for to fulfil obligations in the field of employment and social security and social protection law;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of legitimate activities with appropriate safeguards and on condition that the processing relates solely to the members or to former members of Elim or to persons who have regular contact with Elim in connection with its purposes and that the personal data are not disclosed outside Elim without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims;
g) processing is necessary for reasons of substantial public interest;
h) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Before deciding which condition should be relied upon, Elim may refer to the original text of the UK GDPR as well as any other relevant legislation or guidance and seek legal advice as required.

What must we tell individuals before we use their data?

If personal data is collected directly from the individual, Elim will inform them about its identity/contact details and those of the Data Protection Officer, the reasons for processing, and the legal bases, explaining our legitimate interests, and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement; who the data will be shared with; if the data will be transferred to countries outside of the European Union; how long the data will be stored and the data subjects' rights.

This information is commonly referred to as a 'Privacy Notice'.

This information will be given at the time when the personal data is collected.

If data is collected from another source, rather than directly from the data subject, Elim will provide the data subject with the privacy notice information as well as the categories of the data concerned; and the source of the data.

This information will be provided to the individual in writing and no later than within 1 month after Elim received the data, unless a legal exemption under the UK GDPR applies. If their data is used to communicate with the data subject, this information will be given to them at least at the time of the first communication.

When we need consent to process data

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data.

Consent can, however, be withdrawn at any time and if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

Processing for specified purposes

Elim will only process personal data for the specific purposes explained in its privacy notices or for other purposes specifically permitted by law. Elim will only collect and use personal data that is needed for those specific purposes. Elim will not collect more than is needed to achieve those purposes. Elim will not collect any personal data "just in case" it might be useful later.

Accurate data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

Keeping and destroying data

We will not keep personal data longer than is necessary for the purposes that it was collected for. We will comply with official guidance issued to our sector about retention periods for specific records.

Information about how long we will keep records for can be found in our Data Retention Schedule.

Security of personal data

Elim will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction, or damage.

The security measures implemented will provide a level of security which is appropriate to the risks involved in the processing.

Measures will include technical and organisational security measures. In assessing what measures are the most appropriate Elim will take into account the following, and anything else that is relevant:

a) the quality of the security measure;
b) the costs of implementation;
c) the nature, scope, context and purpose of processing;
d) the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
e) the risk which could result from a data breach.

Measures may include:

a) technical systems security;
b) measures to restrict or minimise access to data;
c) measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
d) physical security of information and of our premises;
e) organisational measures, including policies, procedures, training and audits;
f) regular testing and evaluating of the effectiveness of security measures.

Keeping records of our data processing

To show how we comply with article 30 of the UK GDPR, we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

5. Working with data subjects

Data subjects' rights

Elim will process personal data in line with data subjects' rights, including their:

a) right of access - to ask Elim for copies of their personal information;
b) right to rectification - to ask Elim to rectify or complete personal information they think is inaccurate or incomplete;
c) right to erasure - to ask Elim to erase their personal information in certain circumstances;
d) right to restriction of processing - to ask Elim to restrict the processing of their personal information in certain circumstances;
e) right to object to processing - to object to the processing of their personal information in certain circumstances; and
f) right to data portability - to ask that Elim transfer the personal information they gave Elim to another organisation in certain circumstances.

If any Elim personnel receives any request from a data subject that relates or could relate to their data protection rights, this will be passed on to their Data Protection Lead or Elim's Data Protection Officer immediately. Other Elim policies and procedures specific to individual rights must be followed.

Elim will act on all valid requests as soon as possible, and at the latest within one calendar month, unless there is reason to, and it is lawful to extend the timescale. This can be extended by up to two months in some circumstances.

Direct marketing

Elim will comply with the rules set out in the UK GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around direct marketing. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

Any direct marketing material that Elim sends will identify the Elim as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing, Elim will stop the direct marketing as soon as possible.

6. Working with other organisations & transferring data

Sharing information with other organisations

Elim will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice) unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed staff are allowed to share personal data.

We will keep records of information shared with third parties, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO's statutory 'Data Sharing Code of Practice' (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

Data processors

Before appointing a contractor, who will process personal data on our behalf (a data processor), we will carry out due diligence checks. The checks are to make sure the processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

We will only appoint data processors based on a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the dataprocessing, and compliance with the contract, throughout the duration of the contract.

Transferring personal data outside the European Union (EU)

Personal data cannot be transferred (or stored) outside of the European Union unless this is permitted by the UK GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU. We will only transfer ('transfer' includes making available remotely) Personal Data from countries in the UK/EEA to countries outside of the UK/EEA where:

- the transfer is to a country (or an international organisation) that the UK government/European Commission has determined ensures an adequate level of protection ("Adequacy");
- standard contractual clauses (or UK equivalent such as IDTA's) adopted by the UK government/European Commission have been put in place between the entity in the UK/EEA and the entity located outside the UK/EEA;
- binding corporate rules have been implemented, where applicable; or where
- the transfer is otherwise permitted by the law.

Where Elim is a Data Processor, transfers of Personal Data outside the UK/EEA shall only be made with the controller's agreement.

Where a transfer is not based on Adequacy, we will undertake a transfer impact assessment ("TIA") using our TIA Template to ensure that Data Subjects (whose Personal Data is transferred) continue to have a level of protection essentially equivalent to that under the UK or EU GDPR (whichever is applicable). If the TIA outcome is that the appropriate safeguard does not provide the required level of protection, we will implement supplementary measures e.g. encryption.

We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the UK GDPR.

7. Managing change & risks

Data protection impact assessments (DPIAs)

When we are planning to carry out any data processing which is likely to result in a high risk, we will carry out a DPIA. These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains, we will consult with the ICO.

DPIAs will be conducted in accordance with the ICO's Code of Practice, 'Conducting privacy impact assessments'.

Dealing with data protection breaches

Where Elim personnel or contractors working for Elim, think that this policy has not been followed, or data might have been breached, this will be reported immediately to a Data

Protection Lead or Elim's Data Protection Officer.

We will keep records of personal data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when Elim becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

Glossary of terms

Data breach

A personal data breach is when a breach of security affects the confidentiality, integrity or availability of personal data. This could happen when personal data is accidentally or unlawfully:

- lost or destroyed;
- made unavailable;
- altered; or
- disclosed to or accessed by an unauthorised individual.

Data controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The charity, Elim Foursquare Gospel Alliance, is data controller for all churches and activities that operate under this charity.

Data processing

Any operation which is performed on personal data, such as collecting, recording, using, storing, altering, disclosing or destroying.

Data processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller. In doing so, they serve the controller's interests rather than their own.

Data Protection Act 2018 (DPA 2018)

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the UK GDPR.

Data Protection Impact Assessment (DPIA)

A DPIA is a risk assessment that provides a way to systematically and comprehensively analyse data processing activities and helps identify and minimise data protection risks. It is a legal requirement in some circumstances

Data Protection Lead (DPL)

Each EIC department or local Elim context has a member of personnel designated as the DPL. This defaults to the Head of Department, Minister in charge, or most senior manager unless otherwise designated. They act as the first point of contact regarding data protection issues for their department or context. They manage requests and incidents regarding local data. They liaise with and decide whether to pass on cases to Elim's DPO.

Data Protection Officer (DPO)

Elim's DPO assists with monitoring internal compliance, informing and advising on its data protection obligations, providing advice regarding DPIAs and acts as a contact point for data subjects and the supervisory authority. Elim's DPO is independent and performs the role for all churches and activities that operate under the Elim Foursquare Gospel Alliance.

Data subject

The individual to whom the personal data relates.

Direct Marketing

The communication (by whatever means) of advertising or marketing material which is directed to particular individuals. This includes the promotion of aims and ideals as well as advertising goods or services.

Elim International Centre (EIC) department

All national ministries and departments based at EIC.

Elim personnel

All employees, office holders and volunteers who work for Elim Foursquare Gospel Alliance or any of its churches or other activities.

UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data and came into effect on 25 May 2018.

Information Commissioner's Office (ICO)

The UK's independent supervisory authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO regulates data protection in the UK. They offer advice and guidance, promote good practice, carry out audits, consider complaints, monitor compliance and take enforcement action where appropriate.

Legitimate Interest Assessment (LIA)

A type of light-touch risk assessment based on the specific context and circumstances of the processing used to demonstrate that legitimate interests apply.

Local Elim context

- Churches
- Non-EIC Ministries
- Nurseries
- Nursing homes
- Shops
- Cafes
- Community centres

Personal data

Any information relating to an identified or identifiable natural (living) person.

Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, like a key.

Special category data

Personal data that needs more protection because it is sensitive. This includes data about an individual's racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); genetic data; biometric data; sexual life and sexual orientation.

Subject Access Request (SAR)

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why an organisation is using their data, and check they are doing it lawfully.

ICO Registration

Data Controller

Organisation Name: Elim Foursquare Gospel Alliance

Registration Number: Z5192422

Tier: Tier 1

Contact

Data Protection Officer (DPO)

Name: Evalian – Laura Hastie

Address:

Elim International Centre
De Walden Road
West Malvern
Worcestershire
WR14 4DF

Email: dpo@elim.org.uk

Telephone: 01684 588 983