# 

# 

# 

# 

# **Privacy Policy**

| **Introduction** Elim and its affiliates, subsidiaries and related entities (“Elim”, “we, “our”) are committed to protecting the privacy and security of the personal data we collect about our members and employees.  The right to be informed covers some of the key transparency requirements of the UK General Data Protection Regulation (UK GDPR). We are committed to providing individuals with clear and concise information about how we use, obtain, and retain personal data.  Personal data is defined in the UK GDPR as any information relating to an identified or identifiable natural person (data subject); a person who can be identified directly or indirectly in particular by reference to an identifier such as a name, identification number, location data, an online identifier or factors relating to physical, physiological, genetic, mental, economic, cultural, or social identity.  Please read this privacy notice carefully as it provides important information about how we handle your personal information and your rights. If you have any questions about any aspect of this privacy notice you can contact us by emailing us at dpo@elim.org.uk. **Personal data we collect and use**  * **Information about you** - such as your name, date of birth, email address, phone number * **Special category data** - this is personal data that needs more protection because it is sensitive. Where it is relevant for example as part of providing pastoral services, * **Government identifiers** – for example, information from your identification documents, such as your driving license, national insurance number or passport. * **Online information** – for example, Cookies and IP address (your computer’s internet address), if you use our websites * **Financial information** – for example, salary, bank account details and information from fraud prevention or credit reference agencies for employment purposes, gift aid or products purchased through our shop * **Video recordings** – for some church services/congregations * **Family & beneficiaries’ information** – for example, your marital status, dependents, next of kin, family medical history or nominated beneficiaries (where relevant). If you provide information on another individual, it’s important you ensure they are aware of the detail you`ve provided to us. Their personal data will be processed in accordance with this Privacy Notice, so please let them know it’s important that they read this policy * **Employee information** – for example DBS information, passport details, employment history, medical information, emergency contacts, application information * **Ministry application information** – for example church attendance details, marital status, employment history, nationality, gender, spouse/children, salary details * **Personal data about other named individuals as required** - Where you provide the personal data of others you must have their authority to provide their personal data to us and share this Privacy Statement and any related data protection statement with them beforehand together with details of what you’ve agreed on their behalf.    **Purposes for which we use personal data and the legal basis** When providing services to you, we may use your personal data for the following purposes and on the following lawful bases:   | **Purpose** | **Lawful Basis for Processing** | | --- | --- | | Carrying out pre-employment checks including processing driving licenses and passports for identification purposes and processing employee information such as applications, CV’s, and DBS check information | Legitimate interest | | Processing overseas missionaries’ applications | Legitimate Interest | | Issuing relevant communications and marketing information | Consent | | Processing membership records e.g. name, address, email address, contact number | Legitimate Interest | | To provide an interactive website where email is used to communicate with the users | Legitimate Interest | | To provide a security mechanism whereby we can restrict content to certain groups of users | Legitimate Interest | | Processing medical or religious information for employment purposes or providing support to our members in relation to counselling or pastoral services | Consent | | Processing employee information including bank details for the purposes of paying employees | Performance of a contract | | Videoing key church services or events | Consent | | Processing payments for our online shop | Legitimate Interest |    **Transferring your personal data** In some instances, your personal data may be transferred outside the UK and the European Economic Area. While some countries have adequate protections for personal data under applicable laws, in other countries steps will be necessary to ensure appropriate safeguards apply to it.  If it becomes necessary for the purposes of fulfilling our charitable objectives, we will only share your personal data with organisations in countries benefiting from a European  Commission adequacy decision or on the basis of Standard Contractual Clauses (SCC’s) approved by the European Commission/UK which contractually obliges the recipient to process and protects your personal data to the standard expected within the UK/EU.   **How long we keep your personal data** We will retain your personal data for as long as is necessary to provide you with our services and for a reasonable period thereafter to enable us to meet our contractual and legal obligations and to deal with complaints.  At the end of the retention period, your personal data will be securely deleted or anonymised, for example by aggregation with other data, so that it can be used in a non-identifiable way for statistical analysis and business planning.  Some of the key considerations when we are determining data retention periods for your personal data are below;   * whether we are retaining personal information for archiving, scientific or statistical purposes * relevant guidance from the Information Commissioners Office (ICO) or the National Archives * whether we have a legal or regulatory requirement to retain your personal data once your relationship with us has ended   We implement appropriate technical and organisational measures to protect data that we process from unauthorised disclosure, use, alteration or destruction.   **Your rights and options** You have the following rights in respect of your personal data:   * You have the right of access to your personal data and can request copies of it and information about our processing of it. * If the personal data we hold about you is incorrect or incomplete, you can ask us to rectify or add to it. * Where we are using your personal data with your consent, you can withdraw your consent at any time. * Where we are using your personal data because it is in our legitimate interests to do so, you can object to us using it this way. * Where we are using your personal data for direct marketing, including profiling for direct marketing purposes, you can object to us doing so. * You can ask us to restrict the use of your personal data if:   + It is not accurate.   + It has been used unlawfully but you do not want us to delete it.   + We do not need it anymore, but you want us to keep it for use in legal claims, or   + if you have already asked us to stop using your data but you are waiting to receive confirmation from us as to whether we can comply with your request. * In some circumstances, you can compel us to erase your personal data and request a machine-readable copy of your personal data to transfer to another service provider. * You have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.   You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.  If you wish to exercise your rights, please contact us at: dpo@elim.org.uk or please write to us at Elim International Centre, De Walden Road, West, Malvern, WR14 4DF.  You can also lodge a complaint with the Information Commissioner’s Office. They can be contacted using the information provided at: [ico.org.uk/concerns](https://ico.org.uk/concerns/). **Cookies** Cookies are text files containing small amounts of information that are downloaded to your device when you visit our website. Cookies do lots of different jobs, like letting you navigate between pages efficiently, remembering your preferences, and generally improving the user experience.  Cookies can be "First Party", i.e. set by us, or "Third Party" – set by another company to perform the function, for example, Google Analytics.  When someone visits our website, we collect standard internet log information. We do this to find out things such as the number of visitors to the various parts of the website. We collect this information in a way that does not identify anyone.  We also allow cookies to be set by a number of independent measurement and research companies. These companies read and write their own cookies onto your devices.  For example, these cookies are used to track the adverts and keep a count of the number of times that each advert is viewed by users.  We use this type of information to help improve the services the website provides to you.  If we do want to collect personally identifiable information through any of the website, we will be upfront about this. We will make it clear when we collect personal information and will explain what we intend to do with it.  For further information [please click the link to our cookie notice](https://www.elim.org.uk/User/CookiesPolicy.aspx).   **How to help keep your personal information secure** There are some things you can do to protect your personal information online.   1. Never share a One Time Passcode (OTP). 2. Never enter your details after clicking on a link in an email or text message. 3. Always send confidential information by encrypted email where possible this reduces the risk of interception. 4. If you’re logged into any online service do not leave your computer unattended. 5. Close down your internet browser once you’ve logged off. 6. Never download software or let anyone log on to your computer or devices remotely, during or after a cold call.  **Secure Online Services** You can easily identify secure websites by looking at the address at the top of your browser which will begin https:// rather than http://.   **Changes to this privacy notice** We will regularly review and update this privacy notice at least annually and align it to regulatory changes.  Last modified: 30 December 2021. |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |