

**Data Protection Policy**

|  |  |  |  |
| --- | --- | --- | --- |
| **Created** | **May 2018** | **Signed:****Amanda Ward, CEO** | **Date:****19/6/20** |
| **Updated/Revised** | **June 2020** |  |  |

Friends at the End has reviewed and updated its Data Protection policy in line with the new General Data Protection Regulation (GDPR) which became law in May 2018.

1. **Purpose of policy**

The purpose of this policy is to:

* Comply with the General Data Protection Regulation (GDPR) regarding personal data FATE holds and processes.
* Protect the rights of individuals which FATE holds and processes data on.
* Protect the organisation from the consequences of a breach of its responsibilities.
1. **Policy Statement**

FATE recognises that it has a duty to make sure that data it holds and processes is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed.
4. Accurate and up-to-date.
5. Handled in a manner which ensures appropriate security of data, including unauthorised or unlawful access and against accidental loss, destruction or damage.

FATE will take all necessary steps to ensure it has suitable policies and procedures in place to deal with the above and that staff are fully trained to ensure they are adhered to.

1. **Lawful Processing of data**

FATE recognises GDPR regulations allow for several conditions to which data may be lawfully processed, and has reviewed these thoroughly.

FATE has conducted a full audit of data it holds and processes to determine the most appropriate lawful processing reason(s) for each category.

This data audit has determined that the vast majority of data processed by FATE can be processed under the ‘legitimate interests’ condition. The remaining categories of data processed should fall into the consent category.

* 1. Legitimate Interests

The Information Commissioner’s Office (ICO) guidance on GDPR, suggests the following on legitimate interests:

* It is likely to be most appropriate when you use people’s data in ways they would **reasonably expect** and have a minimal privacy impact, or where there is compelling justification for the processing.
* The legitimate interests can be your own interests, or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
* The processing must be **necessary**. If you can reasonably achieve the same result in another less intrusive way, legitimate interest will not apply.
* You must balance your interests against the individual’s. If they would **not reasonably expect processing, or if it would cause them unjustified harm, their interests are likely to override your legitimate interests.**

The ICO suggests a ‘legitimate interests assessment’ (LIA) should be carried out to ensure justification for using this condition.

* 1. Consent

FATE’s data audit has concluded that there are some categories of personal data for which consent must be sought.

Consent under the GDPR must be a freely given, specific, informed, unambiguous indication of the individual’s wishes.

Consent needs positive opt-in OR clear, affirmative action.

The ICO suggests that consent must be:

* Named
* Unbundled
* Granular
* Documented
* Easy to withdraw

FATE has identified the following specific areas where consent should be sought.

1. Sending direct marketing by email. This would include all newsletters, reports and updates we currently send. It will affect:
	1. Contacts we have added to our database and would like to send news to.
	2. Individuals who sign-up to receive news via the FATE website.
2. Case studies on employees or service users we support.
3. Photos & videos (for websites, reports, case studies etc).
4. Names and personal data.
5. **Privacy Statement**

FATE has developed a suitable privacy statement which is available for any data subjects to view.

The statement covers information on:

* Who we are.
* Why FATE collects privacy information.
* How information is collected.
* Types of data collected.
* Lawful basis for collecting privacy information.
* Data retention periods.
* Where data is stored.
* Individual’s rights.
* How to complain.
1. **Individual rights**

FATE recognises individual data subjects have the following rights:

|  |  |
| --- | --- |
| Right to be informed | FATE has a duty to inform individual data subjects if we are processing data on them, the reasons for this and justification for it. This will be provided through appropriate privacy statements which will be available on our website and on request for general contacts. |
| Right of access (also known as Subject Access Requests) | Individuals have the right to obtain confirmation their data is being processed, access to their data and any other supplementary information held.This can be done by writing to Friends at the End or via email – info@fate.scot. FATE will provide this information free of charge, within 30 days of receiving the request. FATE will verify the identity of the person making the request, using ‘reasonable means’ and if possible, provide the information in a commonly used electronic format.Where requests are manifestly unfounded or excessive, in particular because they are repetitive, FATE may choose to:* charge a reasonable fee, taking into account the administrative costs of providing the information; or
* refuse to respond.

When refusing to respond to a request, FATE will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. |
| Right to rectification | Individuals have the right to have their data rectified if it is inaccurate or incomplete. FATE must do this within one month of being notified of any rectifications or inaccuracies, however, this can be extended by two months where the request for rectification is complex.If the data in question has been disclosed to third parties, FATE must inform them of the rectification where possible. FATE will also inform the individuals about the third parties to whom the data has been disclosed where appropriate.FATE will also make a decision on whether a restriction on processing should be placed while the issue is resolved. |
| Right to erasure | Or the right ‘to be forgotten’ An individual can request deletion or removal of their data if there is no compelling reason for its continued processing.The right to erasure does not provide an absolute ‘right to be forgotten’. Individuals have a right to have personal data erased and to prevent processing in specific circumstances: * Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
* When the individual withdraws consent.
* When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
* The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
* The personal data must be erased to comply with a legal obligation.
* The personal data is processed in relation to the offer of information society services to a child.
 |
| Right to restrict processing | Individuals can request processing be restricted. This means their data may still be held, but no further processing is permitted.When processing is restricted, FATE is permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in futureFATE will be required to restrict the processing of personal data in the following circumstances: * Where an individual contests the accuracy of the personal data, we will restrict the processing until we have verified the accuracy of the personal data.
* Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation’s legitimate grounds override those of the individual.
* When processing is unlawful and the individual opposes erasure and requests restriction instead.
* If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If FATE has disclosed the personal data in question to third parties, it must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. FATE must inform individuals when we decide to lift a restriction on processing. |
| Right to data portability | Individuals can obtain and reuse their personal information for their own purposes or different providers. Data must be provided in a structured, commonly used and machine-readable form. This includes CSV files.If requested, FATE may have to transfer personal data to another organisation, if technically feasible.The right to data portability only applies: * to personal data an individual has provided to a controller;
* where the processing is based on the individual’s consent or for the performance of a contract; and
* when processing is carried out by automated means.

FATE will provide any data within 30 days, however, this may be extended by two months where the request is complex, or we receive a number of requests. FATE will inform the individual within 30 days of the receipt of the request and explain why the extension is necessary. Where not taking action in response to a request, FATE will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within 30 days. |
| Right to object | Individuals have the right to object to :* Processing based on legitimate interests or the performance of a task in the public interest
* Direct marketing
* Processing for purposes of scientific/historical research and stats

FATE must stop processing the personal data unless:* **It can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual**; or
* The processing is for the establishment, exercise or defence of legal claims.
 |

Any individual wishing to register a query or request related to any of the above can do so by contacting info@fate.scot or writing to Office 7, Block 2, Kirkhill House, Broom Rd East, Newton Mearns, Glasgow, G77 5LL.

FATE will provide any information required or make any necessary adjustments free of charge within 30 days of receipt of the enquiry, unless an overriding reason to extend this deadline exists.

FATE has established appropriate processes for handling such requests.

1. **Rights related to automated decision making and profiling**

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention i.e. an automated decision.

FATE does not process any data by automated means.

1. **Data recording**
2. FATE will ensure that it has legitimate ground for collecting and processing personal data as outlined in *Section 3*, and will be clear from the outset why the data is being recorded and for what purpose.
3. Data on any individual will be held in as few places as possible and staff are discouraged from creating unnecessary additional data sets.
4. Procedures are in place to ensure all relevant systems are updated when information about an individual changes.
5. **Data accuracy**
6. FATE will regularly review procedures for ensuring that records remain accurate and consistent.
7. Data should be updated as inaccuracies are discovered.
8. Procedure are in place to ensure that regular checks of data accuracy take place.
9. **Key risks to data protection**

FATE has identified the following risks which this policy is designed to address:

1. Breaches of confidentiality. E.g. information being given out inappropriately.
2. Failure to offer choice concerning individuals’ rights e.g. right to rectification, right to erasure etc.
3. Failure to action requests from individuals concerning their rights.
4. Harm to individuals if personal data is not up to date.
5. Breach of security by allowing unauthorised access.
6. **Data storage & security**

FATE recognises it’s duty to process personal data securely by means of ‘appropriate technical and organisational measures’ and thus, has a range of policies and procedures to ensure security of data, including:

* Data Protection
* Confidentiality
* Fraud
* IT and Internet Usage and Social Media
* Risk
* Whistleblowing

A thorough risk analysis has been conducted of the main risks. This has been used to identify measures to ensure both general privacy/security and cyber security.

* 1. General privacy/security
1. Staff should adhere to a clear desk policy.
2. When not needed, paper files should be stored in cabinets/drawers/pedestals.
3. Staff should avoid leaving printouts where unauthorised people could see them e.g. on printers.
4. Data printouts with personal data should be shredded when finished with or disposed in the confidential waste bags.
5. Staff should have strong passwords on PCs and laptops. Password policies are in place which require a level of password complexity to be met.
6. Mobile phones and tablets should have a keypad lock set.
7. Staff should never write down or share passwords.
8. Staff should only use removable drives/USB drives issued by FATE. These drives will be password protected.
9. Data should only be stored on designated organisation drives, servers, removable devices or cloud services. No data should be stored directly to laptops, PCs, phones, or tablets.
10. Staff must ensure their screens are manually locked when left unattended. Staff should also have a password protected screen saver which activates after 5 minutes of inactivity
11. Servers are stored in a secure location.
12. Laptops or other mobile device users must take shared responsibility for the security of their equipment. Laptops, tablets and mobile devices must not be left in full view in a vehicle even for a short period of time, but should be locked in the boot. Laptops, tablets and mobile devices must not be left in a vehicle overnight, even in a locked boot.
13. **Data retention**
14. Data will be retained no longer than is necessary for the purpose of the business.
15. When data retention periods have been reached, data will be securely destroyed. The process for this is outlined later in the paper.
16. **Data destruction**

FATE has processes in place to ensure any personal and confidential data is destroyed securely (including at the end of data retention periods).

* On-site paper shredder for secure shredding of **ANY document or file containing personal data**
* Confidential waste collection from a certified third party. Bags are stored in a locked room until collected. **No document or file with personal data should be left in these bags for offsite destruction. They MUST be shredded on-site.**
* Once deleted from the online database recycle bin, individual data records can not be retrieved by users.
* Electronic files deleted from company servers are only recoverable by third party IT service provider.
1. **Accountability & Governance**

FATE recognises it is accountable for the data it holds and has put into place comprehensive but proportionate governance measures to minimise the risk of breaches and uphold the protection of personal data.

FATE has set up appropriate technical and organisational measures to ensure accountability, which include:

* Internal data protection policy
* Staff training
* Reviews of internal HR policies
* Use of data protection impact assessments where appropriate
	1. Records of processing activities

Any organisation with less than 250 employees is required to maintain records of activities related to **higher risk** processing, such as:

• processing personal data that could result in a risk to the rights and freedoms of individual; or

• processing of special categories of data or criminal convictions and offences.

* 1. Data protection impact assessments (DPIA)

A DPIA must be carried out when:

* using new technologies; and
* the processing is likely to result in a high risk to the rights and freedoms of individuals. Processing that is likely to result in a high risk includes (but is not limited to):
	+ systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
	+ large scale processing of special categories of data or personal data relation to criminal convictions or offences.
	+ This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
	+ large scale, systematic monitoring of public areas (CCTV).

In the event of the above scenarios materialising, FATE commits to carry out an appropriate DPIA which will include:

* A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
* An assessment of the necessity and proportionality of the processing in relation to the purpose.
* An assessment of the risks to individuals.
* The measures in place to address risk, including security and to demonstrate compliance.
	1. Data Protection Officer

Under the GDPR, an organisation must appoint a data protection officer (DPO) if:

* It is a public authority (except for courts acting in their judicial capacity);
* It carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
* If it carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

FATE is not required to appoint at DPO. Everyone who works for the organisation has a responsibility for ensuring data is collected, stored and handed appropriately.

* 1. Staff Responsibilities

|  |  |
| --- | --- |
| **Position** | **Key Responsibilities** |
| Trustees | The Board hold ultimate responsibility for ensuring that FATE meets its legal obligations. |
|  | * Approving data protection statements attached to communications and the organisation website.
* Checking consents for case studies/photos/videos to be published.
* Liaising with Projects & IT Executive to ensure marketing materials consent are up to date.
* Addressing any data protection queries from journalists or media.
 |
| Projects & IT Executive (alongside 3rd party IT consultants) | * Ensuring all systems, and equipment used for storing data meet acceptable security standards.
* Perform regular checks to ensure security hardware and software is functioning properly.
* Evaluating any third-party services used to store data e.g. cloud services.
 |
| Staff & volunteers | * All staff are required to read, understand & accept the organisation data protection policy and procedures relating to personal data they may handle.
* Any staff utilising databases must ensure that opt out requests are appropriately dealt with and this is reflected in the databases.
 |

1. **Data Breaches**

The GDPR requires all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Types of data breach might include, but are not limited to:

* Data being destroyed
	+ Electronic
	+ paper files
* Data being lost
	+ paper files
	+ lost laptop/tablet/phone
* Data being altered without authority
	+ Intentionally
	+ accidently
* Unauthorised access to data
	+ hacking, phishing etc
* Unauthorised disclosure
	+ sending files to the wrong person
	+ giving access to a device
	1. Breaches where FATE must notify the relevant supervisory authority

FATE will notify the supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals and is likely to have a significant detrimental effect on them – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Any breaches will be assessed on a case by case basis.

* 1. Breaches where FATE must notify individuals

FATE will notify an individual where a breach is likely to result in a high risk to their rights and freedoms.

FATE will notify those concerned directly. A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

* 1. Notification of breaches

A notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows FATE to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation must do so without undue delay.

* 1. Preparing for breach reporting

As part of ongoing GDPR training and awareness, FATE will ensure that all staff understand what constitutes a data breach, and that this is more than a loss of personal data.

1. **Transfer of data**

The GDPR restricts the transfer of personal data to countries outside the EEA, or international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often you carry them out.

To make a restricted data transfer you must know whether it is covered by an EU Commission “adequacy decision”.

This decision is a finding by The European Data Protection Board (EDPB) regarding the legal framework in place in that country, territory, sector or international organisation provides ‘adequate’ protection for individuals’ rights and freedoms for their personal data.

Adequacy decisions made prior to GDPR remain in force unless there is a further Commission decision which decides otherwise. If it is covered by an adequacy decision, you may go ahead with the restricted transfer.

As at February 2019 the Commission has made a full finding of adequacy about the following countries and territories:

Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

The Commission has made partial findings of adequacy about Japan, Canada and the USA.

* The adequacy finding for Japan only covers private sector organisations.
* The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.
* The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework.

The Privacy Shield places requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals. US Government departments such as the Department of Commerce oversee certification under the scheme.

FATE recognises that some of the data it stores in online/cloud solutions are stored in datacentres outside the EU (primarily the USA). Where appropriate, FATE has reviewed the current Privacy Shield list to ensure the organisation has a current certification, and what the certification covers.

|  |  |  |  |
| --- | --- | --- | --- |
| **Service/Programme** | **Datacentre** | **Active Privacy Shield certification** | **Certification covers**  |
| **Microsoft Office 365,** covering: Microsoft Exchange (email), SharepointSkype for Business | EuropeUKUnited States | Since 12.8.2016 | HR, Non-HR Data |
| **MailChimp (The Rocket Science Group LLC d/b/a MailChimp)** | United States,Europe | Since 21.11.2016 | Non-HR data |
| **EventBrite** | United States, | Since 14.10.2016 | Non-HR data |
| **DropBox inc** | United States,Europe,JapanAustralia | Since 23.09.2016 | HR, Non-HR data |
| **Stripe inc** | United States | Since 11.7.2017 | Non-HR data |
| **Survey Monkey** | United States | Since 12.10.2016 | Non-HR data |

1. **Contracts**

As a data controller which employs data processors, FATE must have a written contract (Data Processor Agreement, or DPA) in place in order that both parties understand their responsibilities and liabilities. Data controllers must only appoint data processors who can provide ‘sufficient’ guarantees’ that they will meet the requirements of GDPR and protect the rights of individuals.

If a processor uses another (sub) processor, it must obtain written permission from the controller and must also have a contract in place with that (sub) processor.

The GDPR stipulates that a processor contract should include:

* the subject matter and duration of the processing
* the nature and purpose of the processing
* the type of personal data and categories of data subject
* the obligations and rights of the controller

It should also include terms which require the processor to:

* only act on the written instructions of the controller
* ensure that people processing the data are subject to a duty of confidence
* take appropriate measures to ensure the security of processing
* only engage sub processors with the prior consent of the controller and under a written contract
* assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
* assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
* delete or return all personal data to the controller as requested at the end of the contract
* submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

FATE has identified the following sub-processors which it engages.

**Appendix 1 – Privacy Statement**

**Friends at the End**

**Privacy Statement**

**Who we are**

Friends at the End (FATE) is a Scottish Charity Incorporated Organistion (SCIO) working with end of life issues.

**Our Commitment**

FATE is committed to protecting and respecting your privacy.

FATE recognises its obligation to handle personal data it collects and uses in accordance with data protection legislation and best data protection practices. This means that your personal information will be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes.
3. Only collected so far as required for our lawful purposes.
4. As accurate and up to date as possible.
5. Retained for a reasonable period of time, in accordance with retention policies.
6. Processed in a manner which ensures an appropriate level of security

Any questions regarding this Policy and our privacy practices should be sent by email to info@fate.scot or in writing to Office 7, Block 2, Kirkhill House, Broom Rd East, Newton Mearns, Glasgow, G77 5LL.

1. **Why does FATE need to process personal information?**

FATE supports and works with people and partners across Scotland to help achieve social benefit. We need to process data from a wide range of stakeholders including personal individuals, charities, funders, suppliers and other partners to carry out our job and achieve our goals.

1. **How we collect information from you**

Like most organisations that handle personal information, there are various ways in which FATE collects information from the people we have relationships with.

* Email and written correspondence.
* Telephone conversations.
* Visitors to our website.
* Applications for funding
* Conferences & events.
* Referrals from colleagues and/or mutual contacts

In nearly all instances, it should be obvious to you that FATE is collecting your personal data.

1. **Types of information we collect from you and how we use it**

We collect data from many different groups of people to help us do our job.

I am an individual/organisation who funds FATE

* We will collect details such as your name, address, phone number, email address.
* We will keep records of your donations to FATE, but we will never disclose this information without your consent.
* Your details will be stored on paper files and via Dropbox.
* We will never ask you for your bank or credit card details.
* We will use your details to send you updates & reports on our work together. This may be by post or by email (but only if, where appropriate, we have your consent to email you)

I have donated to FATE using your website donate function

* We will collect details such as your name, address, phone number, email address and credit or debit card details.
* Your details, including payment information, will be stored securely on our website host servers and the server of our payment processing partner Stripe.
* We will keep records of your donations to FATE, but we will never disclose this information without your consent.

 I am working with you as a Pro Bono Supporter

* We will collect details such as your name, address, phone number, email address, your work skills and attributes, CVs, biogs etc.
* We might collect your details through events you attend or contacts you make with our staff and where we feel we have a legitimate interest in doing so. This might include instances where you have shared your business card or details with one of our staff.
* We will use this information to help find a match with the charity work we do.
* We will never share your CV/biog without your consent.
* Your details will be stored using our MailChimp or Dropbox database.
* We will use your details to send you updates & reports on our work together. This may be by post or by email (but only if, where appropriate, we have your consent to email you)

 I am another interested party or stakeholder

* We may collect details such as your name, address, phone number, email address.
* We might collect your details through events you attend or contacts you make with our staff and where we feel we have a legitimate interest in doing so. This might include instances where you have shared your business card or details with one of our staff.
* Your details will be stored using our own servers
* We will use your details to send you updates and news about FATE (but only if, where appropriate, we have your consent to email you)

 I have registered to receive your newsletter via the FATE website

* We will collect your name & email address, which will be stored on the servers of our third party supplier MailChimp.
* We will use your details to send you updates and news about FATE.
* We will not use your details for any other purpose.
* Your details will be held for as long as you stay subscribed.
* You can unsubscribe at any point using the unsubscribe button on our newsletters.

 I have completed an enquiry form/pledge your support on the FATE website

* We will collect your name, email address & phone number.
* We will use this information to contact you about your enquiry.
* Your details will be stored on our website host servers, where they will be stored for 3 months. They may also be stored on our internal systems if necessary
* We will not use your details for any other purpose unless agreed with you during any follow-up discussions.
* We will not share your details with anyone unless agreed with you during any follow-up discussions.
1. **What is our lawful basis for processing personal information?**

As mentioned previously, FATE supports and works with people and organisations across Scotland to help achieve social benefit. In the majority of cases, processing of data is therefore necessary for FATE to meet its **legitimate interests** as a voluntary sector partner helping make positive changes to people’s lives.

**Legitimate interest**

Where using legitimate interest as a lawful reason for processing data, FATE will ensure that:

* The legitimate interests are those of FATE, or the interests of third parties. Legitimate interests might include commercial interests, individual interests or broader societal benefits.
* The processing is necessary and can not be achieved in another less intrusive way.
* The interests of FATE are fairly balanced against of those of individuals concerned, the individual would reasonably expect the processing, and processing would not cause unjustified harm to the individual.

Examples of when we might use legitimate interest as a lawful reason for processing can include, but are not limited to:

* Processing applications for funding
* Processing details of donations to FATE
* Contacting charities or other organisations we work with
* Arranging conferences/events/training
* Follow up to meetings you may have had with our colleagues

**Consent**

In some cases, we will require consent to use your data. Common scenarios where we would seek this include:

* To send you updates/reports/newsletters by email
* If you are a staff member or service user we work with and we are publishing a case study about you
* If you are a staff member or service user we work with and we would like to use a photo or video of you in a publication or website.

There may be other instances where consent is needed, but we will always contact you to do this.

1. **Opt-in to receive news and updates**

You have a choice about whether or not you wish to receive information from us. In many cases, but not all, we can not send you news and updates without your consent. If you would like to hear from us about the vital work we do, you can opt-in using our web form <https://fate.scot/contact/>

If you change your mind and do no longer want to receive marketing communications from us, you can unsubscribe using the link at the bottom of any material we send you.

You can also change your marketing preferences at any time by contacting us by email at info@fate.scot

1. **How long do we keep your data for?**

The periods for which FATE retains personal information depend on the purpose for which the information was obtained but, in general terms, we will retain personal data for so long as required by law, or as may be required for record keeping or contractual obligations.

1. **Where does FATE store personal information?**

Personal information is processed by staff at our office in the UK.

We sometimes need to store information in servers located outside the UK, but within the United States of America and European Economic Area (EEA).

There may also be occasions when data we process is stored on servers outside the EEA. Where this happens, we will take all reasonable steps to ensure that your personal information is properly protected.

1. **Who has access to your information?**

Your information is suitably and securely stored and only accessible by staff members as deemed appropriate to your relationship with us.

In some circumstances outlined in Section 3 of this document, your details may be stored on third party software platforms where FATE trusts that suitable data security is in place.

FATE will never sell or rent your information to third parties.

1. **Your rights**

You have several rights regarding your data and how it is processed. A summary of these is shown below.

Right to be informed

FATE has a duty to inform you if we are processing your personal data and why. This information is available in section 3 of our Privacy Statement. If you have any concerns about this you can contact us at info@fate.scot

Right of access

You have the right to obtain confirmation of any personal data we are processing and to access it. We will provide you with a copy of any data we hold in an electronic and/or paper format and let you know why we have it, who (if anyone) it has been shared with, and how long we will store it. We will provide this information free of charge, within 30 days of receiving your request.

You can make a request by writing to info@fate.scot or Office 7, Block 2, Kirkhill House, Broom Rd East, Newton Mearns, Glasgow, G77 5LL.

If we feel that requests are manifestly unfounded or excessive, FATE may choose to charge a reasonable fee or refuse to respond.

If we choose to refuse to respond to a request, FATE will explain why and make sure you know about your right to complain to the supervisory authority. FATE will do this within 30 days of your original request.

Right to rectification

You have the right to have your data rectified if it is inaccurate or incomplete. FATE will do this within one month of you telling us about any rectifications or inaccuracies, although this can be extended by two months if the request is complex.

If your data has been disclosed to third parties, FATE will inform them of the rectification where possible.

Right to erasure

Or the right ‘to be forgotten’ You can request deletion or removal of your data if there is no compelling reason for us to continue using it.

The right to erasure does not provide an absolute ‘right to be forgotten’. You have a right to have personal data erased and to prevent processing in specific circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
* When you withdraw consent.
* When you object to the processing and there is no overriding legitimate interest for continuing the processing.
* The personal data was unlawfully processed
* The personal data must be erased to comply with a legal obligation.
* The personal data is processed in relation to the offer of information society services to a child.

Right to restrict processing

You can request processing of your data be restricted. This means your data may still be held by FATE, but no further processing is permitted.

FATE will be required to restrict the processing of personal data in the following circumstances:

* Where someone contests the accuracy of the personal data
* Where someone has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether your organisation’s legitimate grounds override those of the individual.
* When processing is unlawful and the individual opposes erasure and requests restriction instead.
* If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If FATE has disclosed your personal data in question to third parties, it must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

FATE must inform individuals when we decide to lift a restriction on processing.

Right to portability

You can obtain and reuse the personal data we hold on you for own purposes or for different providers. FATE must provide this in a structured, commonly used and machine-readable form. This includes CSV files.

If requested, FATE may have to transfer personal data to another organisation, if technically feasible.

The right to data portability only applies:

* to personal data you have provided to us;
* where the processing is based on your consent or for the performance of a contract; and
* when processing is carried out by automated means.

FATE will aim to provide any data within 30 days, however, this may be extended by two months where the request is complex. FATE will inform you within one month of the receipt of the request and explain why the extension is necessary.

Where not taking action in response to a request, FATE will explain why to you, and make you aware of your right to complain to the supervisory authority without undue delay and at the latest within one month.

Right to object

You have the right to object to

* Processing based on **legitimate interests** or the performance of a task in the public interest
* Direct marketing
* Processing for purposes of scientific/historical research and stats

FATE must stop processing your personal data unless:

**It can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms**; or, the processing is for the establishment, exercise or defence of legal claims.

1. **Use of 'cookies'**
* A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site.
* We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes. Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.
* You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.
1. **Links to other websites**

Our website may contain links to other websites run by other organisations. This privacy policy applies only to our website‚ so we encourage you to read the privacy statements on the other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website.

In addition, if you linked to our website from a third-party site, we cannot be responsible for the privacy policies and practices of the owners and operators of that third-party site and recommend that you check the policy of that third-party site.

1. **16 or Under**

We are concerned to protect the privacy of children aged 16 or under. If you are aged 16 or under‚ please get your parent/guardian's permission beforehand whenever you provide us with personal information.

1. **Review of this Policy**

We keep this Policy under regular review and will post and updated versions on our website. This Policy was last updated in June 2020.

1. **Contact Information**

If you have any questions which are not covered in this notice, you can send them to info@fate.scot or Office 7, Block 2, Kirkhill House, Broom Rd East, Newton Mearns, Glasgow, G77 5LL.

1. **Complaints**

If you have raised an issue regarding the handling of your data which you feel has not been suitably addresses by FATE, you can contact the Information Commissioner’s Office on 0303 123 1113 to raise a complaint. You can also find useful information on the ICO website at <https://ico.org.uk/concerns/>