SF- Group

Data Protection Policy

In line with the: General Data Protection Regulation (GDPR)
Date of first publication: 15th May 2018

Date of Most Recent Change	Details of Change
12 Jan 2022	Change to new SF-Group Template.
24 May 2023	Annual review update contact details.
25 May 2024	Annual review

Contents

1. Introduction

This policy applies to all staff and consultants who handle or have access to personal data.

There are a number of reasons why personal data is collected and kept at SF for example about employees, consultants, agents, clients and other stakeholders.

Through this policy we aim to ensure that current and future employees, consultants, agents and business partners feel confident that SF is a safe and secure place to work or do business with.

Failure to comply with data protection requirements when handling personal data is breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the company reputation. It is the responsibility of all staff or others who access or use personal information to adhere to this Data Protection Policy.

2. Summary of how SF Group uses your data

SF uses your personal data to manage and administer your involvement/employment/business with the company, and to keep in contact with you for these purposes.

Data is stored on our secure servers, we use your data to regulate, develop and manage business on your behalf.

Data is shared with our agents and as part of our operations this is a mandatory to ensure compliance. Where SF shares information with a third party a third party data processing agreement will be put in place.

Where we SF Group relies on your consent, you can withdraw this consent at any time.

Amongst the data we collect from you may be medical (including injury) information. We will hold this where you (or next of kin) have given consent, so that we can ensure we are aware of your condition and can therefore ensure that you are supported appropriately.

Where you work in a particular role within the company, you may be required to undergo criminal record background checks. The result of this check will be recorded within our records.

3. Purpose

The purpose of this policy is to:

Define the requirements of the General Data Protection Regulation (“GDPR”) as applied by UK Data Protection Legislation in the context of SF Group of companies;

Clarify responsibilities and duties, and set out the structure within which they will be discharged.

From 25 May 2018, SF will be subject to the GDPR and any other Data Protection legislation applicable in Europe and the United Kingdom.

4. Scope

This policy applies to all personal information processed by, or on behalf of, SF this includes personal information accessed or used by SF staff, as well as, for example, contractors, consultants, agents and clients.

The formats in which personal data is handled can range from electronic, hard copy, and voice recording formats, to spoken forms of communication.

Personal data is any information that can be attributed to an identifiable individual, including names, email addresses, academic performance and qualifications.

Sensitive personal data or 'special category data' includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical and religious opinions/beliefs, and details of criminal convictions or allegations. This category of data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls (e.g. a locked filing cabinet).

Other categories of data also require enhanced protection for example, bank details, other financial details and national insurance numbers.

This policy also applies to de-identified (pseudonymised) personal data where individuals can be re-identified from other information e.g. staff numbers and identification numbers.

5. Obligations

To comply with the law, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. This is captured in the data protection principles set out in the GDPR. Those handling personal data must comply with these principles.

Personal data shall:

- Be obtained, processed and used fairly, lawfully and transparently;
- Be collected for specified, explicit and legitimate purposes and not processed for any other purpose;
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Be accurate and, where necessary, kept up to date;
- Be kept for no longer than is necessary;
- Be protected by appropriate security measures to prevent loss or unauthorised access

In addition personal data should not be transferred outside of the European Economic Area. In cases where this may be necessary, please seek the advice of the Data Protection Officer.

6. Privacy notices and lawful processing

Individuals must be provided with Privacy Notices before their personal data is collected or used.

In some cases, Company Privacy Notices are already in place for the use of staff and consultants' personal data. If you need something beyond this, please seek guidance from the Data Protection Officer and follow the model Privacy Notice template.

7. What information do we collect?

We collect and process personal data from you when you join the company.
This includes:

- Your name
- Your date of birth
- Your home address, email address and phone number
- Your passport and NI details, where we have to check your eligibility or ability to work for us.
- Your payment and/or bank account details.
- Your CV's and work experience documents
- Your medical conditions or disability, where you provide this to us with your consent to ensure we are aware of any support we may need to provide to you.

8. Third party data processing

Personal data cannot be processed by a third party unless the third party Data Processing Agreement has been approved and signed on behalf of the Company by Commercial Services and the Data Processor (i.e. the third party). If you need a Data Processing Agreement or any associated advice, please contact the Data Protection Officer.

In certain instances where the relationship around data sharing is more complex it may be necessary to agree a Data Sharing Agreement between the interested parties. Please contact the Data Protection Officer for advice.

Ad-hoc third party requests for personal data (for example from the police) should be referred to the Data Protection Officer.

9. How do we use this information, and what is the legal basis for this use?

We process this personal data for the following purposes as required to conduct business in pursuit of legitimate interests, in particular:

- To fulfil a contract, or take steps linked to a contract.
- As required by SF to conduct our business and pursue our legitimate interests, in particular:
- We will use your information to manage and administer your involvement with our organisation/company, and to keep in contact with you for these purposes.
- We will also use data to maintain records of our business archives.
- We use CCTV cameras to maintain the security of our premises, and may use this video to investigate incidents on our premises
- We may choose to contact you by email where we want to offer you further contracts/ products and services as previously supplied
- We use the data of some individuals to invite them to take part in research.
- Communicating with you.
- Maintaining statistics and when conducting analysis of tasking.
- Requesting your opinion on future tasking and business initiatives.
- For the purpose of invoicing.

9.1. Where you give us consent:

- We may send you direct marketing or promotional material by email.
- We may handle medical or disability information you provided to us, to ensure we support you appropriately.
- On other occasions where we ask you for consent, we will use the data for the purpose which we explain at that time.

9.2. For purposes which are required by law:

- We maintain records such as health and safety records and accounting records in order to meet specific legal requirements.
- We ensure, where you will work on tasks of a sensitive nature that you have undergone an appropriate background criminal records check – this is also carried out with your consent.
- Where you hold a role within our company requiring us to check your right to work, we may process information to meet our statutory duties.
- We may respond to requests by government or law enforcement authorities conducting an investigation.
- SF will ensure, where you will work on sensitive projects that you have undergone an appropriate background check – this is also carried out with your consent.

9.3. Withdrawing consent or otherwise objecting to direct marketing

Wherever we rely on your consent, you will always be able to withdraw that consent, although we may have other legal grounds for processing your data for other purposes, such as those set out above. In some cases, we are able to send you direct marketing without your consent, where we rely on our legitimate interests. You have an absolute right to opt-out of direct marketing, or profiling we carry out for direct marketing, at any time. You can do this by following the instructions in the communication where this is an electronic message, or by contacting us using the details set out below in the 'How do I get in touch with SF?' section.

9.4. Who will SF share this data with, where and when?

In addition we may share your data with:

- Agents – Shipping agents who provide support with our maritime operations.
- Suppliers- E.G. – vehicle security providers & Travel Agents
- Government Flag States – When SF are applying for flag state approvals and licenses personal data will be sent to flag state government bodies.
- Clients- On business proposals and risk assessments
- Gov agencies – On applications for work permits and visas

Some limited information may be shared with other stakeholders, such as other service providers so that they can respond appropriately and assist in the seamless delivery of business.

Personal data may be shared with government authorities and/or law enforcement officials if required for the purposes above, if mandated by law or if required for the legal protection of our legitimate interests in compliance with applicable laws.

Personal data will also be shared with third party service providers, who will process it on our behalf for the purposes identified above. At this moment in time SF does not use third party to process data.

Where information is transferred outside the EEA, and where this is to a stakeholder or vendor in a country that is not subject to an adequacy decision by the EU Commission, data is adequately protected by EU Commission approved standard contractual clauses, an appropriate Privacy Shield certification or a vendor's Processor Binding Corporate Rules. A copy of the relevant mechanism can be provided for your review on request.

SF sends personal data out to the below countries out of the EEA: Where data is sent to these countries it is sent to approved and vetted agents and suppliers that are used by SF operations in different countries. SF have contracts in place with these suppliers/agents as part of their supplier vendor registration and commitment to compliance.

10. Your Rights

All data subjects (an individual to whom personal data relates) have the following qualified rights:

You have the right to ask us for a copy of your personal data; to correct, delete or restrict (stop any active) processing of your personal data; and to obtain the personal data you provide to us for a contract or with your consent in a structured, machine readable format.

In addition, you can object to the processing of your personal data in some circumstances (in particular, where we don't have to process the data to meet a contractual or other legal requirement, or where we are using the data for direct marketing).

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.

To exercise any of these rights, you can get in touch with SF – or, as appropriate, our data protection officer – using the details set out below. If you have unresolved concerns, you have the right to complain to the Information Commissioner's Office.

Much of the information listed above must be provided on a mandatory basis so that we can make any appropriate legal checks as required. We will inform you which information is mandatory when it is collected. Some information is optional, particularly information such as your medical information. If this is not provided, we may not be able to provide you with appropriate assistance, services or support.

In addition, individuals can request access to the personal data held about them.

To access personal data held by the company, an access to personal data form (PDF) should be completed and sent to the Data Protection Officer. By post SF P.O. Box 15544 0509 Nairobi, Kenya or by email to feedback@salama-fikira.com

11. Retention of Personal Data

We process the majority of your data for as long as you are an Active Member and for [6] years after this.

Where we process personal data for marketing purposes or with your consent, we retain the data for [5] years unless you ask us to stop, when we will only retain the data for a maximum period of 30 days to allow us to implement your requests. We also keep a record of the fact that you have asked us not to send you direct marketing or to process your data indefinitely so that we can respect your request in future.

Where we process personal data in connection with performing a contract, we keep the data for 6 years from your last interaction with us.

We will retain information held to maintain statutory records in line with appropriate statutory requirements or guidance.

Records of your employment of involvement with particular projects may be held indefinitely by us and in order to maintain comprehensive business records.

12. Personal data breaches

In the event of breach of personal data, such as a cyber-attack, SF will notify you as soon as possible after we become aware of the breach.

It is the responsibility of all staff and consultants to immediately notify the IT department by phone if you become aware that personal data is lost, misused, compromised or stolen. This includes, for example, the loss of a laptop.

Where necessary, the Data protection Officer will report breaches to the Information Commissioner's Office (ICO) and notify all individuals affected.

Deliberate misuse of personal data will result in disciplinary action and may lead to criminal prosecution. Examples of misuse include sharing passwords between colleagues, asking a colleague to give you data about a data subject or browsing data through SFsystems/ servers about data subjects. This list is not exhaustive.

13. Data protection by design and default

It is the responsibility of all staff and consultants to incorporate data protection by design and default into all activities, processes or projects that may involve the use of personal data. This includes undertaking a Data Protection Impact Assessment (DPIA) screening assessment, and where appropriate, a full Data Protection Impact Assessment to establish the controls needed for protecting personal data. Methods of control include, for example, encryption, anonymisation and pseudonymisation.

14. Roles and Responsibilities

The Directors & compliance managers provide oversight of data protection matters in the company, with a reporting line through to the Board of Directors.

Country Directors also have oversight of data protection and are accountable for their offices and professional services.

The Data Protection Officer is the designated SF contact for all matters related to data protection and first point of contact with the regulator (Information Commissioner's Office).

Data Protection Liaison Officers are a network of contacts in individual offices and professional services that support the Data Protection Officer in fulfilment of her/his duties.

All staff are responsible for adhering to this policy as per the Terms & Conditions of employment.

15. How to get in touch with the SF Group DPO

We hope that we can satisfy queries you may have about the way we process your data. If you have any concerns about how we process your data, or would like to opt out of direct marketing, you can get in touch at feedback@salama-fikira.com or by writing to SF P.O. Box 15544 0509 Langata, Nairobi, Kenya.

If you have any concerns about how we process your data, you can get in touch at legal@salamafikira.com or by writing to The Data Protection Officer, at SF

Contact details for the Data Protection Officer are:
Crispin Kennedy
Data Protection Officer
Mobile (Ke): (+254) 702 114 144

feedback@salama-fikira.com

Policy owner
For information about this policy or data protection in general please contact:
Crispin Kennedy
COO
Mobile (Ke): (+254) 702 114 144
feedback@salama-fikira.com

16. Review

This policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.

17. Related policies

SF's Privacy Notice

18. Related procedures

SF Data Breach Procedure
SF IT Procedures
SF control of records Procedure

Signed and dated.

Crispin Kennedy
Director
SF Group
25 May 2024