DATA PROTECTION AND RETENTION POLICY

POLICIES & PROCEDURES: Legal Risk & Compliance		**Number of pages:** 13
Effective date: 22nd March 2024	**Revised date:**	**Issued date:** 22nd March 2024
Prepared by: Assistant General Manager - Legal Head of LR&C	**Reviewed/Verified by:** Executive Committee	**Approved By:** BACC

TABLE OF CONTENTS

1. Introduction

This policy is prepared in accordance with the **General Data Protection Regulation ("GDPR")** and the **Personal Data Protection Act** No. 09 of 2022 ("Data Protection Act").

This Policy sets out the obligations which apply to Fairfirst Insurance Limited (hereinafter referred to as the "Fairfirst") its personnel, customers and third-party service providers, when dealing with the personal data of Data Subjects.

2. Scope

This policy is applicable to all Fairfirst stakeholders including Directors, Employees, Agents, Brokers, customers relevant third-party Goods and Service providers.

Each person has a personal responsibility to ensure compliance with the GDPR and the Data Protection Act and to adhere to this Fairfirst Data Protection and Retention Policy.

The respective heads of departments and Managers are responsible for ensuring awareness and compliance of this policy by members of their team and related parties.

The policy applies to data records of all types regardless of the medium on which they are held. In pursuing its business objectives, Fairfirst collects and uses personal data in conjunction with its:

1. Employment of staff and contractors.
2. Recruitment processes.
3. Regulatory obligations arising from its regulation as an Insurer namely the fitness and probity of directors and employees holding controlled functions.
4. Business related activities; and
5. Processing of reinsurance cedant statements that may include personal data of claimants.

Fairfirst may also act as a data processor for client and/or partner companies to whom it provides application hosting and related services.

3. Personal Data Protection Principles

Fairfirst performs its responsibilities under GDPR and Data Protection Act in accordance with the following eight principles:

1. Obtain and process information lawfully, fairly, and transparently.

   Fairfirst is committed to collecting and processing personal data lawfully, fairly, transparently, and only to the extent it is needed to recruit and employ its staff and contractors and satisfy its legal and regulatory obligations as an employer and an Insurer.

2. Keep it only for specified, explicit and lawful purposes.

   Fairfirst shall only keep personal data for purposes that are specific, lawful, and clearly stated. Personal data collected for a purpose other than those listed in 'Scope' above will require the approval of the Data Subject.

3. Use and disclose it only in ways compatible with these purposes.

   Unless obtained written consent of the Data Subject Personal data will not be used or disclosed for any purpose other than that for which it was obtained as listed in "Scope" above.

4. Kept safe and secure.

   Fairfirst shall implement appropriate physical and technical security measures against unauthorised access to, or alteration, disclosure, destruction, or unlawful processing of personal data and against the accidental loss or destruction of such data. Employee access to personal data held by Fairfirst shall be restricted on a need-to-know basis and access levels are reviewed periodically. Organisational and technical measures should also be implemented to ensure Fairfirst can comply with access requests from Data Subjects.

5. Ensure that it is adequate, relevant, and not excessive.

Personal data should not be collected or retained if it is not needed now or in the future, for the purpose for which it was initially obtained or which it needs to be retained for the approved references in future. Personal data held by Fairfirst will be reviewed periodically to ensure compliance with this requirement. Personnel should not store their own personal data or the personal data of other individuals on Fairfirst's systems (including but not limited to emails) unless it is necessary to do so for a specific business purpose or with written permission of Fairfirst Management.

6. Kept accurate, complete, and up-to date.

Fairfirst should ensure that all personal data it holds is accurate, complete, and up to date.

7. Retain it for no longer than is necessary.

Personal data should be retained for no longer than necessary for the purpose(s) for which it is acquired or which it needs to be retained for the approved references in future. Personal data may not be retained indefinitely unless required by law.

8. Right of access to personal data.

Any Data Subject wishing to access their personal data should put their request in writing for the attention of the Data Protection Officer in accordance with the procedure in **Appendix B.** Fairfirst will endeavour to respond to such requests as soon as is reasonably practicable but within the defined time limits of the Data Protection Act.

The requirement to retain personal data may arise in circumstances where the data in question is potentially relevant to actual, pending, or anticipated litigation and regulatory requirements.

4. Consent

Explicit consent will be obtained from the Data Subject for the processing of personal data unless processing is necessary for the performance of the underlying business contract with customers or contract of employment or if Fairfirst is pursuing its legitimate interests in seeking applications for a vacant position.

Fairfirst shall prepare a Consent Form.

This will satisfy Fairfirst's obligations to provide required information to data subjects such as job applicants, Customers. A template of Consent form included in **Appendix F** and Privacy Notice included in **Appendix C**.

5. Transfer of data to third-parties

In some circumstances it is necessary for Fairfirst to transfer personal data to third-party service providers and to affiliated group of companies of Fairfax, some of whom process data on Fairfirst's behalf ("Data Processors"), whilst other third-parties are "Data Controllers" who process data for their own purposes while providing services to Fairfirst.

Where Fairfirst engages the services of a third-party data processor, it will enter into a suitable data processing agreement which complies with GDPR requirements and requirements of Data Protection Act. Refer to **Appendix D** for a template addendum/Condition to agreements with third-party data processors. Material changes to this template when preparing the addendum to such agreements should be approved by the Data Protection Officer.

Where the service provider is itself a Data Controller, then Fairfirst will take steps to ensure that the service provider has appropriate data protection measures in place, including a privacy policy or similar document indicating compliance with GDPR and provisions of Data Protection Act.

Fairfirst shall conduct monitoring activities and periodic audits, as appropriate, to ensure that these service providers comply with their data protection obligations as Data Processors or Data Controllers, as the case may be.

6. The Data Protection Officer

The Manager Legal (in this policy referred to as the **"Data Protection Officer"**) shall be responsible for the compliance of the provisions stated herein and overseeing the processing of personal data on behalf of Fairfirst by third-party service providers.

Key responsibilities of above officers include *(inter alia the responsibilities stated in Section 20 of the Personal Data Protection Act):*

1. maintaining a record of data processing activities, a document required by GDPR and provisions of Data Protection Act which details all personal data processing activities (Refer to **Appendix E**).
2. analysis and checking the compliance of processing activities with GDPR and provisions of Data Protection Act and internal policies.
3. informing, advising, training, and issuing recommendations to management and employees of their obligations under GDPR and under the provisions of Data Protection Act.

7. Sensitive Personal Data

Fairfirst may, from time to time, be required to process sensitive personal data for which explicit consent from the Data Subject will always be obtained. Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, and criminal records and proceedings. Refer to **Appendix F** for a template consent form that should be completed by data subjects when Fairfirst collects and processes their personal data or where consent from the data subject is otherwise required.

8. Rights of Access to Information

Subject to the provisions of the law, the Data Subjects have the right of access to their personal data held by Fairfirst and, to the following information in respect of that personal data:

1. Purposes of the processing.
2. Categories of personal data held.
3. Recipients to whom personal data has been or will be disclosed.
4. The period for which personal data will be stored, if known.
5. The existence of the right to rectify, or erasure of personal data or restrict or object to the processing of such data.
6. Right to complain to the Data Protection Authority.
7. Source of personal data, if it was not provided by the data subject.

Refer to **Appendix B** for details of Fairfirst's procedures to comply with access requests from Data Subjects.

9. Data Retention

Data records should be retained in accordance with the retention periods set out in Appendix G. Retention periods should be periodically reviewed and updated to ensure compliance with legal, regulatory and tax obligations. Data records should be promptly destroyed and permanently deleted at the end of their retention period, subject to the approval of the Data Protection Officer. You may reach to the **Appendix G** for Document Management Policy of Fairfirst to check the retention periods.

10. Data Protection Breach

Any loss of personal data will be responded to and managed in accordance with GDPR and Data Protection Act.

In order for Fairfirst to be able to comply with GDPR and Data Protection Act, it is essential that all incidents (including suspected incidents which give rise to the risk of unauthorized disclosure, loss, destruction or alteration) of personal data are reported without delay to the Data Protection Officer.

After review of the breach (or suspected breach) by the Data Protection Officer, if the data breach affects the rights and freedoms of a Data Subject, the Data Protection Officer will inform the Office of Data Protection Authority of the breach accordance to the time limit and process defined in the Data Protection Act on Fairfirst becoming aware of the breach. If a data breach is likely to result in a high risk to an individuals' rights and freedoms, the Data Protection Officer must also notify affected individuals without undue delay.

A summary of any data breach that occurs, containing the facts relating to the personal data breach, its effects and the remedial action taken, will be recorded in Fairfirst's Log of Compliance Breaches that is maintained by the Data Protection Officer.

11. Review and approval of the Policy

This policy shall be reviewed and approved by the Board of Directors every three (03) years and more frequently if required.

Appendix A – Definitions

1. "Personal data" means, any information that can identify a Data Subject directly or indirectly, by reference to -

   (a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or

   (b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of that individual or natural person.

2. "processing" means, any operation performed on personal data including but not limited to collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on personal data.

3. "controller" means, any natural or legal person, public authority, public corporation, nongovernmental organization, agency or any other body or entity which alone or jointly with others determines the purposes and means of the processing of personal data.

4. "processor" means, a natural or legal person, public authority or other entity established by or under any written law, which processes personal data on behalf of the controller; for the avoidance of doubt, a processor shall be a separate entity or person from the controller and not a person subject to any hierarchical control of the controller and excludes processing that is done internally such as one department processing for another, or an employee processing data on behalf of their employer;

   Illustration: Hospital A employs a data scientist as an employee to manage its analysis of patient records. The Hospital has decided to store its patient records on a third-party local cloud platform hosted by Company B. Hospital A is the controller, and the Company B is the processor where management of patient records are concerned. The data scientist of the hospital is only an employee of the controller and not a processor.

5. "consent" means, any freely given, specific, informed, and unambiguous indication by way of a written declaration or an affirmative action signifying a Data Subject's agreement to the processing of his personal data.

6. "Personal data breach" means, any act or omission that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Appendix B - Data Access Request Procedure

1. Data access requests directed to Fairfirst may be made in writing or verbally (by telephone or in person). If you receive a verbal access request, make a note of the request, including the name and contact details of the requesting person who should be the Data Subject together with a summary of the request. Then the personnel who obtained such request, must pass these details to the Data Protection Officer, who will respond to the request as appropriate.

2. If a written access request is received by a division within Fairfirst, ensure that the letter is date stamped on the day it is received as Fairfirst must reply to the request within 21 days of receipt (2 months of receipt if the request is complex or of a high volume with written consent of the requesting person). Forward the access request to the Data Protection Officer as soon as possible.

3. The Data Protection Officer will check the validity of the access request. The request must enable Fairfirst to definitively identify the Data Subject and to determine the scope of the data access request. Where there is doubt about either factor, the Data Protection Officer may contact the Data Subject to obtain further information.

4. Where the access request is relevant to several teams, the Data Protection Officer will contact the relevant team managers and request them, in writing, to conduct a search of all data held by them. Such searches should be conducted in accordance with guidance provided by the Data Protection Officer and all steps taken to locate and collate data should be noted and documented.

5. The Data Protection Officer must be satisfied that sufficient material has been supplied to definitively identify the Data Subject. This is most important. This may be the signature, an ID number in combination with name and address or date of birth. It should not be possible for a third-party to provide the material to lodge a false access request.

6. Check that sufficient information to locate the data sought has been supplied by the Data Subject. If it is not clear what kind of data is being requested, the Data Protection Officer will ask Data Subject for more information.

7. The Data Protection Officer will log the date of receipt of the valid request. This is the date from which the response turnaround time frame begins and can be the original date the access request was received, or the date where the request was validated with the requestor.

8. A search of all electronic files, no matter the format, and all manual files stored on the relevant filing system(s) should be undertaken. All data identified should be reviewed by the relevant team manager(s).

9. Once this review is completed the personal data that is recommended for disclosure/deletion should be forwarded to the Data Protection Officer for consideration. This step should also include an analysis of the relevant exemptions available per the GDPR and Data Protection Act being relied upon and a description of the purpose for processing the relevant personal data, to whom the data may have been disclosed and the source of the data.

10. If data to be disclosed in response to a data access request includes data relating to a third-party, this third-party data may only be disclosed with the consent of the third-party. Alternatively, the third-party data may be deleted from the document in question or anonymised if this would conceal the identity of the third-party. An opinion given by a third-party in relation to the Data Subject may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.

11. A final decision on disclosure/deletion of the requested information will be taken by the Data Protection Officer, in conjunction with the team manager(s) as required.

12. The extracted data is then collated into an intelligible form (including an explanation of terms and abbreviations if necessary) and sent electronically to the Data Subject unless otherwise requested by the Data Subject.

13. If the Data Subject has instead requested the deletion or rectification of personal data held by Fairfirst, the identified information is deleted from or updated (as appropriate) on each of the systems on which it is located. Hard copy documents should be updated or deleted as appropriate. The Data Protection Officer should take steps to ensure such data is also deleted/amended by third-party data processors used by Fairfirst.

14. The Data Protection Officer will keep copies of all related correspondence on a file and record access, deletion, and other requests in a Data Request Register similar below:

Data request register

Date Received	Business Unit	Data Request	Details (Type of Request)	Date Responded	Further Action Taken	Status - Resolved/ Unresolved

Appendix C - Template Privacy Notice

Introduction

We at Fairfirst Insurance Limited (**"Fairfirst"**) care about your privacy and we respect your privacy rights.

By submitting your personal data including cover letters/emails, curriculum vitae, references, educational certificates, and details such as name, address, telephone number, email address, gender and date of birth or any other personal data relevant to the business transactions of the Customers, whether directly or through a another controller or processor, you permit the collection and use of your personal information as outlined below and you signify your agreement to this Privacy Notice. If you do not agree with these terms, you should not submit your personal data to Fairfirst.

By submitting your personal data including cover letters/emails, references, educational details such as name, address, telephone number, email address, gender and date of birth and any other relevant details which is relevant in obtaining the Insurance Service provided by Fairfirst, (whether directly or through an Agent, Broker or any other authorized party by the Fairfirst), and/or when providing goods or services to Fairfirst in day to day business process, you permit the collection, use and further processing of your personal information as outlined below and you signify your agreement to this Privacy Notice. If you do not agree with these terms, you should not submit your personal data to Fairfirst.

Your personal data

Upon receipt of the Recruitment Information, Information relates to providing Insurance Services and Information relates to providing goods or services to Fairfirst, Fairfirst will process the information that you submitted in accordance with Fairfirst internal process and Fairfirst responsibilities under the General Data Protection Regulation ("GDPR"), provisions of Personal Data Protection Act No. 09 of 2022 and other applicable data protection legislation. Fairfirst will not use the data you submitted for any other purpose.

Fairfirst may also process proof of identity that Fairfirst request from you before Fairfirst disclose personal information to you that Fairfirst hold (in order to establish that Fairfirst is disclosing the personal data to you and not to someone pretending to be you).

Purpose of and legitimate interests for processing

Fairfirst process the information provided by you or obtained from publicly available third-party sources to evaluate your suitability for recruitment, provide Insurance services and obtain goods or services for Fairfirst. This processing is conducted in the pursuit of Fairfirst' s legitimate interest in the above requirements.

Disclosure of your information to other people

Fairfirst does not disclose personal data received from above sources to any third-parties unless Fairfirst have your express permission, or Fairfirst believe the law permits or requires it.

Retention period

Fairfirst shall destroy the personal data of unsuccessful recruitment, Insurance businesses and goods or service providing subject to your rights as set out below. The personal data of successful recruitment, Insurance Policies and goods or serve provides will be retained for the duration of their employment with Fairfirst, within the term of the Contract of Insurance, within the term of the contract for providing goods or service and for a further 6 years period from end of such terms or any further time which law permit Fairfirst to retain those data for further time.

IP ADDRESSES AND COOKIES

When browsing Fairfirst **https://www.fairfirst.lk/privacy-policy/** website or systems Fairfirst may collect information about your computer, including (where available) your IP address, operating system, and browser type, for system administration and statistical purposes. This is statistical data about Fairfirst users' browsing actions and patterns and does not identify any individual.

For the same reason, Fairfirst may obtain information about your general internet usage by using a cookie file which is stored on the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive. On revisiting the Website or systems Fairfirst computer server will recognise the cookie, giving Fairfirst information about your last visit. They help Fairfirst to improve the Website and systems and to deliver a better and more personalised service. They enable us:

- to estimate Fairfirst' s audience size and usage pattern.
- to store information about your preferences, and so allow Fairfirst to customise the Website and systems according to your individual interests and make your usage of the Website and systems more enjoyable; and
- to speed up your searches.

You may refuse to accept cookies by activating the setting on your browser which allows you to refuse the setting of cookies. However, if you select this setting, you may be unable to access certain parts of the Website or system. Unless you have adjusted your browser setting so that it will refuse cookies, Fairfirst system will issue cookies when you log on to the Website or system.

Your rights

At any time, you can make a request for access to all the personal data that Fairfirst hold about you. Fairfirst will provide this information to you as soon as Fairfirst is reasonably able and may request payment of a small administrative charge as per the provisions of Data Protection Act.

You may inform Fairfirst of any changes in your personal data and in accordance with Fairfirst's obligations to you, Fairfirst will update or delete your personal data accordingly. You may also object to or restrict the processing of your personal data by Fairfirst.

The Data Protection Officer are responsible for data protection at Fairfirst. If you wish to exercise your rights as described above, please write to: **Data Protection Officer, Fairfirst Insurance Limited, Access Tower II (14th Floor), No. 278/4, Union Place, Colombo 02.; or email: dataprotection@fairfirst.lk.**

Complaint process

Should you be unhappy with how Fairfirst has handled your personal data, you have the right to make a complaint to the Data Protection Authority of Sri Lanka and according to the provisions of Personal Data Protection Act No.9 of 2022.

Changes to Privacy Notice

Our Privacy Notice may change from time to time and any changes to the notice will be posted on Fairfirst's website.

Appendix D - Condition which covers the Personal Data Protection contained in Fairfirst Contracts

DATA PROTECTION

In the event that any Party to this agreement discloses Confidential Information that contains Personal Data and the Receiving Party processes such Personal Data on behalf of the Disclosing Party for the implementation of business purposes mentioned herein, then the Receiving Party shall:

a) act only on instructions from the Disclosing Party regarding access to, or the processing, erasure, disclosure, transfer or other use of such data;

b) comply with any request made or direction given by the Disclosing Party in connection with its obligations under any current and/or any future applicable statute, law, regulation or regulatory obligations relating to the protection of Personal Data;

c) take appropriate technical and organizational security measures against unauthorized or unlawful processing of such Personal Data and against accidental loss or destruction of or damage to such Personal Data;

d) comply with all applicable laws and regulations relating to holding, retrieval, processing and use of such Personal Data.

DEFINITIONS

Personal Data - means any information relating to an individual.

Processing - means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Appendix E - Register for Data Processing Activities

Data Processing Activity Register

Date of inception	Department applicable	Reason for the activity	Details of the activity	Actions taken	Date of completion	Status

Appendix F - Data Processing Consent forms

Insured

TP Service Providers

Employees

Appendix G - Personal Data Retention Period

You may reach to the Document Management Policy of Fairfirst to check the retention periods of data via the **DMS Policy.**

Appendix H - Personal Data Breach Inquiring Procedure

i. Any breach of personal data within the company could be notified by the data subject who is in breach of personal data directly to the Data Protection Officer of Fairfirst in writing via an E-mail - **dataprotection@fairfirst.lk** or via registered post **Data Protection Officer, Fairfirst Insurance Limited, Access Tower II (14th Floor), No. 278/4, Union Place, Colombo 02** with proof of the notified personal data breach.

ii. The Data Protection Officer of Fairfirst shall immediately enter the complaint in the Data Complaint management system with the available proof of the personal data breach.

iii. The Data Protection Officers shall create a separate case record for each such complaint and maintain the same till the finalization of the complaint.

iv. The Data Protection Officers shall coordinate with the internal departments and gather relevant information regarding the complaint and inquired into the same.

v. Once analysed all the facts and details available to the complaint the Data Protection Officers shall respond to the complainant in writing addressing the complainant with appropriate response.

vi. If there is a breach of Personal Data recognized through such investigation the Data Protection Officers shall take immediate action to remediate such gaps if identified and strengthening the internal processors with notice to respective departments.

vii. The response for the complaint shall be finalized within Twenty One (21) working days from the date of receipt of the complaint to the Data Protection Officer of Fairfirst.

- END -