LLOYD'S

Data Protection Policy for Lloyd's South Africa (Pty) Limited

1 July 2021

Table of Contents

Document control

The Data Protection Policy (the "Policy") is part of the Data Lab Department's suite of policies. Any requests or queries should be directed to the Data Governance and Privacy Department in the Data Lab G6.

Document Properties

Policy name	Data Protection Policy for Lloyd's South Africa (Pty) Limited
Last Approval date	30 June 2021
Review frequency	Annually
Document tier	Tier 1
Documentation	n/a

Review and Approvals

Role	Name, Job Title	Status	Date
Owner	Easvarie Naidoo, General Representative, Head of Compliance and Information Officer for Lloyd's South Africa	Approved	June 2021
Author	Norton Rose Fulbright South Africa	Approved	April 2021
Independent Reviewer and Independent Approver	John Burman, Data Protection Officer	Approved	May 2021
Reviewer(s)	Eugenie Laurian, Data Privacy Manager for Global Offices, Lloyd's Data Lab	Reviewed	May 2021
Approver(s)	Easvarie Naidoo, General Representative, Head of Compliance and Information Officer for Lloyd's South Africa	Approved	30 June 2021

Version History

Version	Review/Publication Date	Approver	Status	Key changes
1.0	May 2021	John Burman	In Draft	
2.0	Review May 2021	Eugenie Laurian	In Draft	Align with the Corporation privacy framework. Corrected links from the DPO site.
3.0	30 June 2021	Easvarie Naidoo	Approved	Review and updates made.
3.0	5 July 2021	Easvarie Naidoo	Published	

Governance Process

The Policy will be reviewed and updated in response to any material changes in the organisational structure, legal or regulatory expectations or new regulations. In the absence of any such changes the Policy must be reviewed at least annually to ensure that it remains up to date and relevant. All material changes to the Policy and the annual Policy review and update must be reported to Data Governance & Privacy Team.

The review and update process for this Policy is the responsibility of **Data Governance & Privacy in Data Lab London who will liaise with the Information Officer (IO) on this.**

Key Contact

The Data Governance & Privacy Team are here to help. Please come and see us or email data.protection@lloyds.com

The IO provides independent advice and guidance to all at Lloyd's on data protection issues and has a number of responsibilities that are written into the legislation. The IO is the person that the Information Regulator (IR) will liaise with on all data protection activities.

1 Purpose

1.1 Purpose

The purpose of this Policy is to enable you to manage Lloyd's data in line with the Protection of Personal Information Act, 2013 (POPIA) and other data protection legislation and details the various conditions that must be satisfied before Lloyd's data can be processed.

This Policy is supported by a suite of policies and procedures that will enable you to manage and process Lloyd's data in accordance with current and relevant data protection legislation, including POPIA.

The confidentiality, integrity and protection of all Lloyd's data – both personal information and commercial data - is critical to the ongoing functioning and good governance of Lloyd's. Lloyd's endeavours to meet the highest standards of data protection, security and governance of all information it processes, both commercial data and personal information. Everyone has a fundamental right to have their personal information protected, and Lloyd's is committed to protecting the rights and privacy of individuals whilst carrying out its business.

THINK: Would you want your own or your children's medical or insurance records, or your pay, or claims details left lying around or sent unsecured as an attachment to an email?

1.2 Definitions

Definitions used in this Policy

This Policy covers **Lloyd's data**. Lloyd's data is any information, controlled, held or processed by the Corporation of Lloyd's and any of its subsidiaries or passed to any of its suppliers or other third parties.

data subject means the person (including a juristic person) to whom personal information relates.

data protection legislation means POPIA; and
all other applicable laws (including judgments of any relevant court of law) and regulations relating to the processing of personal information, data privacy, electronic communications, marketing and/or data security, in each case as from time to time in force and as from time to time amended, extended, consolidated, re-enacted, replaced, superseded or otherwise converted, succeeded, modified or incorporated into law and all orders, regulations, statutes, instruments and/or other subordinate legislation made under any of the above in any jurisdiction from time to time, in each case interpreted in accordance with the DP guidance.

DP guidance means legally binding guidelines, recommendations, best practice, opinions, directions, decisions, codes of practice and codes of conduct issued, adopted or approved by the Government of the Republic of South Africa and/or IR from time to time in relation to the subject matter of the data protection legislation.

lawfulness, fairness and transparency mean that information processing must be lawful and fair. The principle of transparency requires that any information and communication relating to the processing of personal information be easily accessible and easy to understand, and that clear and plain language is used.

operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, and also has the meaning given to an equivalent term under applicable data protection legislation.

personal information means all information relating to an identifiable, living natural person, and where it is applicable an identifiable, existing juristic person, and also has the meaning given to an equivalent term under applicable data protection legislation. Note the definition of **special personal** information below.

POPIA means the *Protection of Personal Information Act, 2013* and its regulations.

process means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

b. dissemination by means of transmission, distribution or making available in any other form; or

c. merging, linking, as well as restriction, degradation, erasure or destruction of information,

d. and "processing" and "processed" have corresponding meanings, and also has the meaning given to an equivalent term under applicable data protection legislation.

In the case of Lloyd's, many suppliers will be our operators. Operators can only act where a written contract is first in place with the responsible party.

regulator means the Information Regulator (South Africa) or any regulatory or supervisory authority charged with enforcing data protection legislation or otherwise regulating or supervising Lloyd's in respect of its obligations under data protection legislation.

responsible party means a public or private body or any other person which, alone or in conjunction

with others, determines the purpose of and means for processing personal information, and also has the meaning given to an equivalent term under applicable data protection legislation.

special personal information means personal information including, but not limited to:

a. the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject;

b. the criminal behaviour of a data subject to the extent that such information relates to—(i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings (**criminal data**); and

c. Personal Information of children under the age of 18.

1.3 Relevant legislation

The regulation most relevant to this Policy is POPIA.

POPIA requires that personal information is processed lawfully, fairly and in a transparent manner. Infringements (non-compliance) of POPIA may result in fines, imprisonment, or both. The maximum periods of imprisonment are ten years, for serious offences and twelve months, for lesser offences and fines of up to R10 million can be imposed.

This Policy expands the personal information principles of integrity, security and transparency to Lloyd's commercial data.

2 Scope

2.1 Application

This Policy applies to all South African staff. It also applies to consultants, casual workers, fixed term contract employees, agency workers, temporary workers and service providers/third parties, whether employed directly or indirectly, who for the purposes of this Policy will be referred to as "Lloyd's staff". Members of the Board of Lloyd's South Africa (Pty) Limited are within scope of this Policy.

Please contact your local Compliance Team, Data Governance and Privacy Team or the IO. For further information via email: data.protection@lloyds.com.

This Policy applies to the processing of Lloyd's data, which includes the personal information of individuals within South Africa, and under POPIA outside South Africa where POPIA provisions are applicable.

The Policy applies to personal information held in all formats, including digital on computers, laptops, mobile devices and removable storage and servers, or held in hard copy or other paper or other physical formats.

3 Policy Statement

Everyone processing Lloyd's data (whether commercial or personal informational) must comply with this Policy.

When processing personal information (whether as a responsible party or operator) you must do in accordance with this Policy to enable you to comply with POPIA, and other applicable data protection legislation.

The following Principles must be followed:

3.1 Principles relating to the processing of personal information

All information, whether personal or commercial must be:

a) Accurate and, where necessary, kept up to date.
b) Processed in a manner that ensures appropriate data security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principles applying to personal information in compliance with POPIA, which will also apply to commercial data in order to follow a good data handling regime.

c) Processed lawfully, fairly and in a transparent manner in relation to the individual ('lawfulness, fairness and transparency');
d) Only collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
e) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
f) Kept in a form which permits identification of data subjects only for no longer than is necessary for the purposes for which the personal information is processed.

The Lloyd's Data Protection Site provides guidance and tools relating to data protection.

Below are the links to relevant section on the Data Protection Site, Tools to use. The tools have been developed with guidance notes on how to achieve and maintain compliance with the Policy.

3.2 Lloyd's Requirements relating to the processing of information to enable the Principles to be met

1. **Lawful basis for processing personal information.**
   Before processing personal information, one of the specific categories of processing **must** be met.

2. **Lawful basis for processing special personal information.**
   Before processing **special personal information** additional consideration of POPIA must be take place before processing. Until this takes place special personal information must not be processed. All such personal information must be processed for specific purposes only. When special personal information needs to be processed, it is more likely that consent will be required.

3. **Information Quality.**
   It is important that all information processed by Lloyd's is fit for purpose, particularly if it is used for decision making. Processes must be put in place to ensure information quality is maintained.

4. **Retention.**
   The Master Retention Schedule referred to in the Data and Document Retention Policy must be used to determine the retention periods for all personal information.

   Personal information must not be kept for longer than necessary, follow the Data and Document Retention Policy for more details, and guidance on this can be given by the Data Governance and Privacy Team or the IO.

5. **Data Subject Rights.**
   Individuals, including employees, have a number of rights about how their personal information is processed and these are set out in the Data Protection Procedure.

   If any Data Subject Access Requests (DSARs) are made to you, **you must not respond yourself, as the Data Governance and Privacy Team responds on behalf of Lloyd's.** Immediately upon receiving DSAR request, please fill out the Data Subject Access Request (DSAR) form which automatically notifies the Data Governance and Privacy Team. The team will contact the data subject and will work with you to enable a full response to be made.
   Remember strict time limits for responding apply. Do not delay in completing the DSAR request form.

6. The relationship between a responsible party and an operator (or separate and independent responsible parties) must be documented in contracts, operator agreements or data sharing agreements.

7. Processes must be in place and monitored to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

8. All personal information must be classified, protectively marked and kept secure at all times.

9. Processes must be in place to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident.

10. Processes must be in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. All system testing environments must adhere to the System Development Standards.

11. Personal information is to be kept accurate and up to date, and Lloyd's should only collect and process the minimum personal information necessary that meet the requirements for the particular process.

12. To help identify, assess and minimise or mitigate data protection risks of a new project,

process, system or technology, a Data Protection Impact Assessment (DPIA) should be conducted by filling the new SDPIA form. This form combines the security and privacy impact assessments in one single form. If you require to conduct a SDPIA for your new project, please complete the new SDPIA form. More details about DPIAs can be found here.

13. Transfers of personal information to third countries.
All transfers of personal information to third countries, or international organisations must be subject to appropriate safeguards, including standard or contractual clauses as appropriate. A SDPIA must be completed to ensure all processing risks are addressed and an appropriate level of security is maintained. See paragraph 12 above for further information on completing a SDPIA.

14. Everyone in scope of this Policy must co-operate with the Data Governance & Privacy Team and the IO in the performance of their tasks under this Policy.

4 Monitoring, Reporting and Escalation

4.1 Monitoring

Compliance with this Policy is mandatory. The IO will regularly monitor compliance with this Policy as it relates to personal information. The Head of Data Governance & Privacy will regularly monitor compliance with this Policy as it relates to commercial data and more generally.

EVERYONE is responsible for ensuring compliance with the Data Protection Procedure and we all need to implement appropriate practices, processes, controls and training to ensure compliance.

4.1.1 Information Officer (IO)

The IO is responsible for independently reviewing this Policy and will promote and monitor its compliance. The IO will act as a contact point for the regulator and will provide advice and assistance to employees on personal information protection queries. The IO carries out this and other data protection related work, together with the other mandated functions set out in POPIA in an independent way to ensure Lloyd's can comply with data protection legislation. The IO assists Lloyd's staff to follow a good personal information handling regime that will become embedded in the organisation.

4.2 Reporting Data Breaches

All data breaches (where there is a potential for unauthorised access, loss of or damage to any Lloyd's data, personal or commercial) must be reported using the Data Incident Management (DIM) Policy.

There is a one page Employee Quick Guide which gives the steps to take for reporting any data breach.

If you know or suspect that a data breach has occurred, **do not** attempt to investigate the matter yourself. Refer directly to the Employee Quick Guide for direction on how to report an incident.

4.3 Escalation

Compliance with the Data Incident Management Policy (DIM) is mandatory. Non-compliance may result in the disciplinary process being invoked. For more information, please refer to the Disciplinary Policy and Procedure.

Do not try to deal with the data breach yourself - report it!

4.4 Procedure

This Data Protection Policy has a Procedure that supports this Policy, to assist employees to comply with the principles of this Policy.

5 Training

ALL persons subject to this Policy are required to complete the mandatory internal training on Data Protection and the implications of failing to comply with the regulations.

All staff will be required to confirm completion of training. Failure to complete the training will be taken into account as part of your performance review.

Extra training on specific topics is available and is recommended depending on your work and team requirements, and detailed training on specialised topics is available. Evidence of training must be made available to the regulator if they request to see the same.

REMEMBER: by following the Data Protection Procedure you will be able to comply with all the above.

REMEMBER: Good data handling is everyone's responsibility, including YOURS!

REMEMBER: Think Privacy!

6 Glossary

A Glossary of Data Protection terms that maybe helpful to you can be found in the first section of the Data Protection Procedure.