Legal and Compliance Department Policies

BINDING CORPORATE RULES

(for Cross Border Transfers)

Distribution	Group (All Korridor Entities)
Effective date	15 May 2025
Revision nr	V1.0
Supersedes	None
Issuing function	Legal and Compliance
Authorized by	Head: Legal and Compliance

Table of contents

1. INTRODUCTION

1.1. The Korridor Group of Companies (hereinafter for convenience referred to as "the **Company**" or "**Korridor Group**") are bound by and apply these Binding Corporate Rules for cross for border transfers of Personal Data:

1.2. The Company operates and/or has presence in various jurisdictions, and the Company understands its responsibility to ensure that the Personal Data of any Data Subject in its possession or under its control is only Processed in accordance with applicable Data Protection Laws. Where no such laws exist, the Company applies the highest standard applicable to the Company. In doing so, the Company takes guidance from the application of leading Data Protection Laws.

1.3. These Binding Corporate Rules regulate the Processing of Personal Data by the Company and its Personnel regarding cross-border transfers from one jurisdiction to another, to ensure among other things that Personal Data is transferred in a legally permissible manner and that adequate information security is afforded to the Personal Data in the recipient jurisdiction.

2. INTERPRETATION

In these Binding Corporate Rules, unless the context indicates otherwise, terms used that have different terminologies but equivalent meanings under the Data Protection Laws shall be construed to have corresponding meanings. The following capitalized terms shall have the meanings given to them below:

2.1. "**Affiliate**" means as to any Person, any other Person who, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For the purposes of this definition "control" (including, with correlative meanings, the terms "**controlling**", "**controlled by**" and "**under common control with**"), as used with respect to any Person, shall mean the possession, direct or indirect, of power to direct or cause the direction of the management and policies of such Person whether through ownership of voting securities or partnership interests, or by contract or otherwise.

2.2. "**Applicable Policies**" means all policies and procedures applicable to the Company or a Group Company, jointly or individually, depending on the context that applies to the protection of Personal Data in any manner.

2.3. **"Binding Corporate Rules"** means this set of rules, adopted by the Company to ensure compliance with Data Protection Laws when transferring Personal Data across borders within the Companies.

2.4. "**Company**" or **Korridor Group**" means collectively, all Group Companies constituting the Korridor Group, comprising Korridor Holdings Limited (incorporated in Mauritius) and its existing and future Affiliates as well as Korridor South Africa Holdings (RF) Proprietary Limited (incorporated in South Africa) and its existing or future Affiliates, including all their business operations and divisions.

2.5. "**Controller**" means a Person who, alone or in conjunction with others, determines the purpose of and means for Processing Personal Data. "Controller" shall also be construed to mean and encompass words of similar meaning as used in any other Data Protection Laws, such as "responsible party" as defined in the POPI Act.

2.6. "**Consent**" means voluntary, specific and informed expression of will in terms of which permission is given for the Processing of Personal Data.

2.7. "**Data Subject**" means any Person whose Personal Data is Processed by the Company or on behalf of the Company.

2.8. "**Data Processing Infrastructure**" means any systems, networks, servers, workstations, devices, web applications, mobile applications, cloud storages, websites and/or any other means for Processing Personal Data, which is either owned, controlled, operated or utilised by the Company.

2.9. "**Data Protection Laws**" means any data privacy and data protection law applicable to the Company or a Group Company, regulating the Processing of Personal Data of any Data Subject.

2.10. "**Group Company**" means any juristic Person which is a constituent of the Company or Korridor Group. A list of the Group Companies constituting the Korridor Group as at the Effective Date of these Binding Corporate Rules is as listed in section 1.1 above.

2.11. "**Information Officer**" means an officer of the Company duly authorised and appointed as such by the Company from time to time. The Information Officer is entrusted with a duty to*, inter alia*, ensure compliance by the Company with Data Protection Laws and may be assisted from time to time by a deputy (or deputies) duly authorised and appointed as such by the Company. "Information Officer" shall therefore equally refer to any such deputy or deputies. The details of the incumbents from time to time may be obtained from the Company's Legal and Compliance Department which may be contacted at legal@korridor.com.

2.12. "**Person**" means, where the context so requires, a natural or juristic person, whether incorporated or unincorporated and whether with or without a separate juristic personality.

2.13. "**Personal Data**" means any information relating to an identified or identifiable Data Subject.

2.14. "**Personnel**" means in relation to the Company or Group Company, all employees, directors, officers, shareholders or other representatives.

2.15. **"Privacy Team"** means a cross functional team comprising of the main, Information Officer, the Deputy Information Officer and the Company's Information Technology and Legal and Compliance Departments responsible for overseeing data privacy and protection compliance within the Company.

2.16. **"Process"** or **"Processing**" means any operation or activity or any set of operations or activities, whether by electronic or manual means, concerning Personal Data, including but not limited to:

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

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

2.16.3. merging, linking, blocking, degradation, erasure or destruction.

2.17. "**Processor**" means a Person who Processes Personal Data for and on behalf of the Controller. "Processor" shall also be construed to mean and encompass words of similar meaning as used in any other Data Protection Laws, such as "operator" as defined in the POPI Act.

2.18. "**Recipient**" means a Group Company which receives Personal Data from a Transferor.

2.19. "**Regulator**" means the authority responsible for regulating the protection of Personal Data and ancillary matters in any jurisdiction.

2.20. "**Record of Processing Operations**" means a detailed record that documents how the Company processes Personal Data, including the purposes, categories of Data Subjects, data types, recipients, and security measures. It ensures transparency, accountability, and compliance with data protection regulations.

2.21. "**Security Breach**" means the breach of security of any Data Processing Infrastructure leading (or which may lead) to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by or on behalf of the Company ("**Data Breach**").

2.22. "**Transfer"** (including, with correlative meanings, the terms "**Transferred**" and "**Transferring**") refers to the cross-border transfer and receipt of Personal Data either between Group Companies (that is, Transferor and Recipient) or the Company/Group Company to an external third party.

2.23. "**Transfer Impact Assessment"** means an evaluation conducted to assess the legal and security implications of Transferring Personal Data from one jurisdiction to another or to an international organisation, ensuring compliance with Data Protection Law and safeguarding Personal Data.

2.24. "**Transferor**" means a Group Company which transfers Personal Data from one jurisdiction to another.

3. PURPOSE AND SCOPE

3.1. The Company strives to observe and comply with its obligations under the applicable Data Protection Laws in its Processing activities and in respect of all Data Subjects. These Binding Corporate Rules are implemented in view of the Company's obligation and its commitment to complying with the Data Protection Laws (and to the extent necessary, industry best practices) that apply to it in the course and scope of its business activities.

3.2. The Company understands and acknowledges that not all Data Protection Law requirements for a lawful Transfer of Personal Data are identical. It has, however, followed the common requirements in the development of these Binding Corporate Rules. These requirements are that:

3.2.1. Personal Data is not Transferred unless the provisions of section 7 hereof are applied, which affords Personal Data the level of protection which upholds principles that are substantially similar to those contained in the local legislation of the transferring party).

3.2.2. Where no Data Protection Law exists in a Group Company jurisdiction, these Binding Corporate Rules serve as the minimum standard applied to the protection of Personal Data by the Group Company.

3.3. The foregoing may be subject to certain exceptions such as where there are specific requirements that apply to a specific Group Company, such as:

3.3.1. Where the Data Subject is required to provide Consent to the proposed Transfer, or

3.3.2. The Transfer is necessary for the performance of a contract between the Data Subject and the Transferring party, or

3.3.3. That the Transferor is required to demonstrate to the relevant Regulator proof of appropriate safeguards in respect of Personal Data Transferred or intended to be transferred.

4. OTHER POLICIES AND PROCEDURES AND HIERARCHY

4.1. These Binding Corporate Rules must be implemented and applied by each Group Company together with any other Applicable Policies and/or procedures of the Company, or the specific Group Company.

4.2. These Binding Corporate Rules apply where Personal Data is Transferred cross-border from one Group Company (Transferor) to another Group Company or third party outside the Korridor Group (Recipient). The general principles and standards to which Group Companies are required to comply in going about a Transfer are set out in these Binding Corporate Rules.

4.3. These Binding Corporate Rules do not replace other Applicable Policies but supplements their objective by establishing a set of principles and standards to which the Company must comply with when Transferring Personal Data.

4.4. Where there is a conflict between any provision of these Binding Corporate Rules and any Applicable Policy of the Company, these Binding Corporate Rules shall take precedence to the extent that the conflict relates to a Transfer.

5. PRINCIPLES AND CONDITIONS FOR PROCESSING PERSONAL DATA

5.1. Group Companies and their Personnel shall only Process Personal Data, whether obtained through a Transfer or otherwise, in accordance and in compliance with the principles and standards set out in the Applicable Policies, including these Binding Corporate Rules.

5.2. **Lawfulness, Fairness and Transparency, Openness:**

5.2.1. Group Companies shall:

5.2.1.1. Process Personal Data in accordance with the applicable Data Protection Laws, in a fair, open and transparent manner;

5.2.1.2. Inform Data Subjects of any Processing activity and the purpose thereof;

5.2.1.3. Maintain the documentation of all processing operations and ensure such information is easily accessible and maintained in clear and plain language;

5.2.1.4. Notify the Data Subject that they are free to refuse or withdraw Consent at any time where Consent is required; and

5.2.1.5. Notify Data Subjects, in terms of our applicable policies, of any other Recipient or category of Recipients, with whom the information shall or may be shared.

5.3. **Purpose Limitation and Purpose Specification:**

5.3.1. Personal Data must be:

5.3.1.1. Collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company or Group Company;

5.3.1.2. Processed for purposes compatible with the original purpose of collection, and may not be further processed unless such Processing is legally permissible as provide in these Binding Corporate Rules; and

5.3.1.3. Where Group Companies Transfer Personal Data to other Group Companies, they must stipulate the original purpose for collection.

5.4. **Data Minimisation:**

5.4.1. Personal Data must be adequate, relevant and limited to what is necessary in relation to achieving the original purpose for Processing. Personal Data that is not necessary to achieve the purpose must not be collected and if inadvertently collected, must be deleted.

5.5. **Accuracy:**

5.5.1. Personal Data must be accurate and updated. Group Companies are required to undergo periodic reviews and continuously establish processes to ensure that Personal Data is complete, accurate, not misleading and updated where necessary. This includes requesting information from Data Subjects, and enabling them to participate in the Processing.

5.5.2. In taking the necessary steps, the Group Company must have regard to the purpose for which Personal Data is collected or further Processed.

5.6. **Subject Participation:**

5.6.1. The Company will provide the Data Subject with all information necessary to enforce any rights available to them with respect to their Personal Data.

5.7. **Integrity and Confidentiality / Information Quality / Security Safeguards:**

5.7.1. Each Group Company must secure the integrity, availability and confidentiality of Personal Data in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent, loss, damage, unauthorised destruction or Processing of Personal Data.

5.7.2. Each Group Company must ensure that its Personnel who Process Personal Data on its behalf are aware of and committed to conforming with any Applicable Policies and these Binding Corporate Rules, and comply with the relevant security safeguards.

5.7.3. Where the Processing involves transmitting Personal Data through an information communication network, Group Companies shall, at a minimum, consider the following in determining the appropriate measures:

5.7.3.1. state of technological developments available to safeguard the Personal Data being transmitted,

5.7.3.2. special risks that exist in the processing of the Personal Data,

5.7.3.3. cost of implementing security measures, and

5.7.3.4. nature of the Personal Data being Processed.

5.7.4. The Company must continuously monitor and improve the Data Processing Infrastructure under its control. Group Companies must (to the extent practicable) ensure that their Personnel fully utilize the Company's Data Processing Infrastructure to Process Personal Data in the performance of their duties. Group Companies must comply with any Applicable Policy when utilising the Company's Data Processing Infrastructure[1].

5.8. **Retention Period Limitation**

5.8.1. Personal Data must not be retained any longer than is necessary for achieving the original purpose for which the Personal Data was collected and Processed.

6. RIGHTS OF DATA SUBJECTS

6.1. Each Group Company shall afford each Data Subject in respect of which it Processes Personal Data, the right to:

6.1.1. **Confirmation**: right of confirmation entitles a Data Subject to request and receive confirmation regarding whether their Personal Data is being Processed and what Personal Data is Processed.

6.1.2. **Access**: right of access to the Personal Data which right involves the provision of sufficient information about the Personal Data held about the Data Subject.

6.1.3. **Rectification**: right to request the rectification of their Personal Data which might be inaccurate, incomplete, irrelevant, excessive, out of date, misleading or obtained unlawfully.

6.1.4. **Erasure**: right to have their Personal Data erased. This right shall not apply where the Processing of Processing of Personal Data is necessary for:

6.1.4.1. reasons of public interest in the field of public health;

6.1.4.2. the purpose of historical, statistical or scientific research;

6.1.4.3. compliance with a legal obligation to process the personal data to which the Controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or

6.1.4.4. the establishment, exercise or defence of a legal claim.

[1] Refer to the **Acceptable Use Policy**, **Data Breach Protocol**, **Electronic Communications Policy** and related policies, accessible to all Personnel on the Company's intranet at https://sites.google.com/korridor.com/korridor-comms/policies-procedures or upon request for a soft/hard copy from the Legal and Compliance Department.

6.1.5. **Restriction**: right to request the restriction of the Processing of their Personal Data as provided for under any applicable Data Protection Law.

6.1.6. **Portability**: right to receive their Personal Data which they have provided to the Company/Group Company concerned, in a structured format, and to transmit such data to third parties.

6.1.7. **Objection**: right to object to their Personal Data being processed for a specific purpose.

6.1.8. **Decision Making**: subject to any exception as may be provided in terms of the applicable Data Protection Laws, right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning the Data Subject or significantly affects the Data Subject.

6.1.9. **Withdrawal of Consent:** right of a Data Subject to withdraw their Consent to the processing of Personal Data where the Personal Data is Processed on the basis of Consent.

7. CROSS BORDER TRANSFER

7.1. When the Group Company must Transfer Personal Data, the Group Company must:

7.1.1. notify the Data Subject of:

7.1.1.1. the fact or possibility that the Personal Data will be Transferred;

7.1.1.2. the level of protection afforded to the Personal Data by the Recipient (or Company at large) or third-party recipient; and

7.1.1.3. information about the identity, or category of the intended Recipient of the Personal Data.

7.1.2. Notify the Regulator of the intended Transfer of Personal Data, and submit the Binding Corporate Rules, along with a description of the purpose for Transfer and the proposed security measures and any other lawful grounds relied on.

7.1.3. Demonstrate the effectiveness of Binding Corporate Rules as a security measure, where requested by the Regulator. Where this is the case, the Group Company shall only do so in consultation with the relevant internal stakeholders and with the approval of the Information Officer.

7.2. Personal Data may only be Transferred under one or more of the following conditions:

7.2.1. where applicable, when the requirement set out in section 7.3 below has been complied with;

7.2.2. where the Data Subject has given Consent to the proposed Transfer, after having been informed of the possible risks of the Transfer in the absence of appropriate safeguards;

7.2.3. where the Transfer is necessary for:

7.2.3.1. the performance of a contract between the Data Subject and the Group Company concerned (or the Company in general) or for the implementation of pre-contractual measures taken at the Data Subject's request;

7.2.3.2. the conclusion or performance of a contract concluded in the interest of the Data Subject between the Group Company concerned (or the Company in general) and another Person;

7.2.3.3. reasons of public interest or national security as provided by the applicable Data Protection Laws;

7.2.3.4. the establishment, exercise or defense of a legal claim;

7.2.3.5. the protection of the vital interests of the Data Subject or of other natural persons, or

7.2.3.6. the legitimate interests pursued by the Group Company concerned (or the Company in general) which are not overridden by the interests, rights and freedoms of the Data Subject and where:

7.2.3.6.1. the Transfer is not repetitive and concerns a limited number of Data Subjects; and

7.2.3.6.2. the Group Company concerned has assessed the circumstances surrounding the Transfer operation and has, based on such assessment, where necessary, provided to the Regulator proof of appropriate measures with respect to the protection of the Personal Data subject to the Transfer.

7.3. Sensitive Personal Data may not be Processed (ncluding being Transferred) outside the jurisdiction in which it was collected without the Consent of the Data Subject.

7.4. Transfer to external third parties which are not part of the Korridor Group should be subject to additional safeguards to ensure that the level of protection of the Personal Data by the recipient third party is adequate. Such safeguards may include but are not limited to, the Transferor entering into legally binding and enforceable instruments with the Recipient undertaking to ensure compliance with the applicable Data Protection Laws in respect of the Personal Data received and that the Personal Data is afforded adequate and appropriate protection in the Recipient jurisdiction.

7.5. Where a Recipient is acting as a Controller or joint Controller in respect of Personal Data received as a result of a Transfer, the Recipient shall:

7.5.1. comply with the obligations of a Controller set out in the Companies Privacy Policy, to the extent that such obligations are not in conflict with the applicable Data Protection Law; and

7.5.2. observe the Company's undertakings set out in the Privacy Notice[2].

7.6. Where the Recipient is acting as a Processor in respect of Personal Data received as a result of a Transfer, the Recipient shall:

7.6.1. comply with the obligations of a Processor set out in the Privacy Policy of the Company, to the extent that such obligations are not in conflict with the applicable Data Protection Laws; and

7.6.2. observe the Company's undertakings set out in the Privacy Notice[3].

8. ASSESSMENT OF RISK OF TRANSFER

8.1. The Company has taken measures to safeguard that Transfers between Group Companies and using the Company's Data Processing Infrastructure provide an adequate level of protection to the Personal Data which is the subject of the Transfer.

8.2. In the event of:

8.2.1. a Transfer to another Group Company outside of Company's Processing Infrastructure;

8.2.2. a Transfer which is not ordinarily undertaken by the Group Company; or

8.2.3. a transfer to an external third-party recipient,

the Information Officer and/or the Deputy Information Officer must be consulted by the Transferor to assess whether the applicable safeguards implemented to adequately and appropriately protect the Personal Data Transferred or intended to be Transferred and, where necessary, complete a Transfer Impact Assessment.

8.3. Where a Group Company intends to Transfer Personal Data to a third-party recipient located in a country without adequate Data Protection Laws, the Transferor shall coordinate with the Information Officer or his or her deputy to undertake a Transfer Impact Assessment to establish risks to the rights and freedoms of the Data Subjects which may result from the Transfer Impact Assessment.

8.4. No Transfer contemplated in section 8.3 above may take place unless a Transfer Impact Assessment has been conducted, and any additional safeguards that are identified as necessary pursuant to the Impact Assessment to protect the Personal Data which is subject of the Transfer have been implemented by the Transferor and the Recipient third party.

[2] https://korridor.com/privacy-notice/
[3] https://korridor.com/privacy-notice/

8.5. The outcome of the Transfer Impact Assessment must be considered when determining the appropriate measures to be implemented in terms of section 8.4. Where the Transfer Impact Assessment suggests that the Transfer is high risk and the Company/Group Company concerned is not able to mitigate such risk by reasonable measures, the Transfer may not proceed without the approval of the Information Officer.

9. RECORD OF PROCESSING OPERATIONS

9.1. Each Group Company must maintain a record of processing operations under its responsibility in which all the Processing activities of the Group Company shall be recorded. Such records shall include Transfers and the suitable safeguards undertaken.

9.2. For the time being, the record of processing operations undertaken by the Company is maintained at Group level and there is no expectation for Group Companies to maintain separate records, however Group Companies which have capacity and capability are not barred from maintaining such records.

9.3. The Record of Processing Operations shall contain among other details:

9.3.1. purpose of the Processing operations;

9.3.2. description of the categories of Data Subjects and the categories of Personal Data;

9.3.3. categories of recipients with whom Personal Data is or may be disclosed.

9.3.4. retention periods of the Personal Data; and

9.3.5. general description of the technical and organisational security measures implemented to protect Personal Data.

9.4. Subject to section 10.1 Group Companies must safeguard the confidentiality of the record of processing operations to the highest extent. Disclosure of the record of processing operations to any third party, including a Regulator or other authority for any purpose must be done in prior consultation with the Information Officer and/or the Deputy.

10. OTHER CONSIDERATIONS

10.1. Request for Disclosure of Personal Data:

10.1.1. Group Companies must not disclose Personal Data in response to requests for disclosure by any person (including Regulators and other authorities) without notifying and consulting with the Information Officer[4]. The notification must include the original request received, together with any other relevant information which may assist the Privacy Team in handling the request.

10.1.2. Where the Privacy Team determines that the Company or a Group Company may disclose the Personal Data, it may only be on grounds that:

10.1.2.1. a legal obligation exists, requiring the Personal Data to be disclosed;

10.1.2.2. there exists an imminent risk of serious harm to the Data Subject or another natural person, which merits compliance with the requests for disclosure [5].

10.1.3. In any event, only the Personal Data that is necessary to meet the purpose of the disclosure may be disclosed.

10.1.4. Where a request is made by a Data Subject to facilitate any of their rights in respect of Personal Data Processed by the Company or Group Company, such request may be handled in accordance with the prescripts of other Applicable Policies regarding the handling of such request.

10.2. External Communication:

10.2.1. Only the Information Officer or the Deputy Information Officer are authorised to contact Persons outside of the Company about Security Breaches or Data Breaches. Security Breaches and/or Data Breaches must be reported to the Company in accordance with Applicable Policies.

10.2.2. External communication of Security Breaches or Data Breaches to Regulators and/or Data Subjects by Group Companies should only be made with the approval of the Information Officer or the Deputy Information Officer.

11. PRIVACY TEAM, ESCALATIONS AND DEVIATIONS

11.1. Implementation of these Binding Corporate Rules and data protection compliance within the Company shall be driven by the Privacy Team with the support of the management committee of the Company.

[4] This provision does not prohibit disclosure of information in the ordinary course and scope of operations of the Company or the Group Company concerned such as for purposes of KYB/KYC requirements undertaken by the Company or Group Company in the ordinary course and scope of business.
[5] Taking into consideration the nature, context, purposes, scope and urgency of the request for disclosure and the privacy rights and freedoms of any the Data Subject.

11.2. Group Companies and each of their Personnel are responsible for escalating and communicating any non-compliance or potential non-compliance with these Binding Corporate Rules or any other Applicable Policy of the Company to the Privacy Team which is responsible for documenting and investigating such reports.

11.3. Any conflicts or queries relating to requirements under these Binding Corporate Rules, Applicable Policies or other matters that relate to Personal Data privacy/protection matters should be referred to the Privacy Team for resolution and/or clarification.

11.4. Any requests for exceptions or deviations from these Binding Corporate Rules should be referred first to the Information Officer or Deputy, who shall consult other relevant stakeholders as they deem appropriate before granting any approval.

12. CONSEQUENCES OF NON-COMPLIANCE

12.1. All Group Companies and their Personnel are committed and are obligated to comply with these Binding Corporate Rules.

12.2. Personnel who do not comply with these Binding Corporate Rules and other Applicable Policies of the Company will be subject to disciplinary action, up to and including dismissal where it is warranted.

12.3. Failure to comply with these Binding Corporate Rules may also result in risks or harm to Data Subjects, fines, penalties, criminal sanctions being imposed on the Company or a Group Company, loss of business or adverse publicity against the Company.

13. PUBLICATION AND AMENDMENTS

13.1. The latest version of these Binding Corporate Rules is made available via the Company's intranet[6] and will be publicly available on the Company's website.

13.2. These Binding Corporate Rules will be reviewed frequently at intervals to be determined by the Privacy Team to assess their compliance with Data Protection Laws and industry standards. They will be updated based on the findings of the review.

13.3. These Binding Corporate Rules may be amended from time to time when circumstances necessitate changes such as when there are changes in Data Protection Laws or of the Company structure.

13.4. Any amendment shall be approved by the Head: Legal and Compliance and will be communicated to all Group Companies.

13.5. Where the local Data Protection Laws applicable in the jurisdiction of any Group Company require that a Regulator be notified of the changes, the Privacy Team shall be responsible for ensuring that the relevant Regulator is timeously notified.

[6] https://sites.google.com/korridor.com/korridor-comms/policies-procedures

APPROVAL AND VERSION CONTROL

Approval:

	Date	Name	Position
Created:	July 2024	Ntsako Ngonyama	Legal and Compliance Advisor
Reviewed:	May 2025	Mitchell Levieux	In-House Legal Advisor
Approved:	May 2025	Christi Botha	Head: Legal & Compliance