Privacy Policy

Privacy Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Privacy Policy
Document type	Privacy Policy
Jurisdiction	Global
Owner	Privacy Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose
2. Scope
3. Definitions
4. Regulatory Framework
5. Our Privacy Commitment
6. The Personal Data We Collect
7. How We Collect Your Data
8. Online Collection, Cookies and Digital Services
9. How We Use Your Data and Our Lawful Bases
10. Who We Share Your Data With
11. Credit Reference Information and Your Credit Rights
12. Automated Decisions and Profiling
13. Direct Marketing and Your Choices
14. How We Protect and Retain Your Data
15. Your Rights Over Your Data
16. Making a Privacy Complaint
17. If a Personal Data Breach Occurs
18. Contact Us, Changes and Review of this Policy
Appendix A: Your Privacy Rights at a Glance
Policy Administration

1. Purpose

This Privacy Policy explains how the Company collects, holds, uses, discloses and transfers personal data, including credit-related data, and how you can exercise your rights over your data or make a privacy complaint. It is published to meet the openness and accountability principles of the OECD Privacy Guidelines and the transparency obligations of applicable data protection law in the jurisdictions where the Company operates.

The Company anchors its privacy practices to international standards — the OECD Privacy Guidelines, Council of Europe Convention 108+, and the EU General Data Protection Regulation (GDPR), which the Company applies as a reference model for lawful basis, purpose limitation, data minimisation, data subject rights, breach notification and cross-border transfer safeguards — in addition to the data protection law of each jurisdiction in which it operates. This policy reflects those standards as they stand in mid-2026.

This policy has been approved by the Board of Directors and is owned by the Privacy Officer. It describes our commitments to you. The internal procedures, roles and controls our staff must follow to meet these commitments are set out in the Company's Internal Privacy Policy, which is a separate, staff-facing document.

2. Scope

This policy applies to personal data processed by the Company and its subsidiaries and controlled entities, across every channel through which you deal with us — in person, by telephone, by mail, through our website and mobile applications, and through brokers, agents and other intermediaries acting for us.

It covers the personal data of customers and prospective customers, guarantors, account signatories, beneficial owners, directors and officers of business customers, visitors to our premises and websites, and other individuals whose data we process in the course of our business.

This policy does not cover:

- the handling of employee and job-applicant data, which is governed by our separate workforce privacy notice and applicable employment law;
- data shared under an open banking or consumer data-sharing regime operating in your jurisdiction, which is governed by our separate notice at [website address], to the extent such a regime applies; and
- internal staff procedures, roles and controls, which are set out in the Internal Privacy Policy.

If you use a third party's website or service that we link to, that party's own privacy policy applies to the data you give them.

2.1 Jurisdictional application

This policy states international best practice for the protection of personal data. The Company must map the requirements of this policy to the data protection

and privacy law of each jurisdiction in which it operates, and must maintain jurisdiction-specific supplements where local law imposes additional or different requirements — including local breach notification deadlines, data-residency rules and rights response periods. The Privacy Officer owns the mapping and the register of jurisdiction-specific supplements, must review them at least annually and within [X] business days of becoming aware of a material change in applicable local law, and must report the outcome of each review, and any gap identified, to the Board of Directors at its next scheduled meeting. Where applicable local law imposes a stricter requirement than this policy, local law prevails.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person, whether accurate or not and in whatever form recorded, including identifiers such as name, account and identification numbers, location data, online identifiers and factors specific to that person's identity, consistent with the OECD Privacy Guidelines and applicable data protection law. The terms personal data and personal information are used interchangeably.
Sensitive Personal Data	Categories of personal data that carry a higher risk of harm and attract heightened protection, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data used to identify an individual, health data, data concerning sex life or sexual orientation, and data relating to criminal convictions and offences.
Data Subject	The identified or identifiable individual to whom personal data relates, including customers, prospective customers, employees, contractors, directors, beneficial owners, guarantors and supplier contacts.
Processing	Any operation performed on personal data, whether or not by automated means, including collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, transfer, combination, restriction, erasure and destruction.
Controller	The entity that, alone or jointly with others, determines the purposes and

	means of processing personal data. The Company acts as controller for the personal data it handles in connection with its business unless expressly agreed or stated otherwise.
Processor	An entity that processes personal data on behalf of, and on the documented instructions of, a controller, including outsourced service providers and technology or cloud hosting providers engaged by the Company, and their sub-processors.
Lawful Basis	A ground recognised by applicable law that legitimises a processing activity, such as the individual's consent, performance of a contract, compliance with a legal obligation, protection of vital interests, or the legitimate interests of the controller where not overridden by the individual's rights.
Consent	A freely given, specific, informed and unambiguous indication of a person's wishes, given by a statement or clear affirmative action by a person with capacity, and capable of being withdrawn as easily as it was given. Silence, inactivity and pre-ticked boxes do not constitute consent.
Data minimisation	The principle that personal data collected and processed must be adequate, relevant and limited to what is necessary for the stated purposes.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data held by the Company or by a processor on its behalf, which may require notification to the relevant data protection authority and to affected individuals under applicable local law.
Pseudonymisation	Processing personal data so that it can no longer be attributed to a specific individual without the use of additional information that is kept separately and protected by technical and organisational controls. Pseudonymised data remains personal data.
Anonymised data	Data that no longer relates to an identifiable individual and cannot reasonably be re-identified, taking account

	of the means reasonably likely to be used. Anonymised data is not personal data.
Automated Decision	A decision, or a matter substantially and directly related to a decision, made wholly or substantially by automated processing of personal data, including profiling, where the decision produces legal effects for an individual or could reasonably be expected to affect their rights or interests significantly.
Cross-Border Transfer	Any disclosure, transfer or making available of personal data to a recipient located in a country other than the one in which the data was collected, including access to that data from another country by a service provider, group entity or cloud region.
Credit reference agency	An organisation permitted under applicable local law to collect and hold information about individuals' credit history and to provide credit reports or scores to lenders.
Privacy Officer	The person appointed by the Company as accountable for its privacy arrangements and as the first point of contact for privacy questions, rights requests and complaints, coordinating privacy compliance, privacy impact assessments, breach response and engagement with data protection authorities, and holding or overseeing the statutory data protection officer appointment where applicable law requires one.

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (as revised)	The foundational international privacy principles — collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability — on which this policy is built.
EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)	Applied by the Company as a reference model for lawful bases, data subject rights, breach notification and transfer

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com