Internal 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	Internal 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

This Policy sets out how the Company and every member of its staff must handle personal data in day-to-day operations. It translates internationally recognised data protection standards — the OECD Privacy Guidelines, Council of Europe Convention 108+ and, as the Company's adopted reference model, the EU General Data Protection Regulation (GDPR) — into operable internal requirements: on what lawful basis data may be collected, how individuals must be informed, how data may be used and disclosed, how it must be secured, transferred and retained, what rights individuals can exercise, and what staff must do when something goes wrong.

This is an internal, staff-facing document. It is distinct from, and must be read alongside, the Company's customer-facing privacy notice, published separately as the document titled "Privacy Policy". That external document tells individuals how the Company processes their personal data; this Policy tells staff how to make that statement true in practice. Staff must not reproduce customer-facing wording from this Policy, and any change to practice that would make the external Privacy Policy inaccurate must be referred to the Privacy Officer before implementation.

The Board of Directors has approved this Policy. It is owned and maintained by the Privacy Officer. Compliance is mandatory: privacy failures expose the Company to administrative fines and civil penalties under applicable data protection law (under the GDPR reference model, up to the greater of EUR 20 million or 4 per cent of worldwide annual turnover), to compensation claims by individuals, to supervisory-authority enforcement including processing bans, to contractual and prudential consequences, and to loss of customer trust that no penalty scale captures.

2. Scope

This Policy applies to the Company and all of its controlled entities, and to all directors, employees (permanent, part-time and casual), secondees, contractors, consultants and agency staff (together, "staff"). It applies to processors and other third parties handling personal data on the Company's behalf through the contractual requirements described in this Policy.

It covers all personal data processed in connection with the Company's business, in any format and any system, including: customer and prospective-customer data; credit and affordability data; employee, applicant and contractor data; beneficial-owner, guarantor and supplier-contact data; government identifiers; and personal data in records, correspondence, call recordings, logs, analytics environments and backups. It covers all channels and processing contexts: branches, contact centres, digital channels, third-party and broker channels, cloud services, and analytics and model-development environments.

This Policy does not address employee-monitoring notification requirements under local employment law, which are covered in the [Acceptable Use / People

policies], nor the customer-facing disclosures themselves, which are contained in the external Privacy Policy.

Jurisdictional application. This Policy states international best practice drawn from the frameworks listed in the Regulatory Framework section. The Company must map the requirements of this Policy to the data protection, banking secrecy, credit reporting and employment law of each jurisdiction in which it operates, and record that mapping in the compliance obligations register. Where the law of an operating jurisdiction imposes a stricter or additional requirement — including shorter notification deadlines, data-residency restrictions or mandatory registration with a data protection authority — local law prevails and must be complied with.

3. Definitions

Term	Definition
Anonymised Information	Information that is no longer about an identified or identifiable individual, having regard to all means reasonably likely to be used to re-identify it. Anonymised information is not personal data while it remains anonymised; pseudonymised data remains 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.
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.
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.
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.
Data Breach Response Team (DBRT)	The cross-functional team convened by the Privacy Officer to contain, assess and remediate a suspected personal data breach, comprising as a minimum the Privacy Officer, Chief Information Security Officer, Chief Risk Officer, Head of Legal and the accountable business owner.
Data Protection Impact Assessment (DPIA)	A structured assessment of a project, system or initiative that identifies its impacts on the privacy and rights of individuals and sets out the measures required to manage, minimise or eliminate those impacts before processing begins.
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.
External Privacy Policy	The Company's customer-facing privacy notice, published as the separate document titled "Privacy Policy", which describes to individuals how the Company processes their personal data.
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.
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.
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.
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.
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.
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.
Profiling	Automated processing of personal data to evaluate personal aspects of an individual, in particular to analyse or predict creditworthiness, economic situation, behaviour, reliability, location or movements.
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.
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

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