IGUAKO CAPITAL · Group policy

Data Protection and Privacy

This policy sets the standard for the collection, use, storage, transfer and deletion of personal data across every entity in the group's 28 jurisdictions. It gives effect to the third, fourth, sixth and seventh principles of the Ethical Technology Charter: provenance of data, restraint in inference, transparency to clients and the right to a human decision. It sets the group minimum; where the law of a jurisdiction requires more, the local rule applies and is recorded in the processing register maintained by the Group Data Protection Officer.

CODE	CATEGORY	VERSION
IGC-DT-001	Data and technology	3.1
EFFECTIVE	**REVIEW**	**OWNER**
2022-10-01	Annual, with an interim review whenever the processing register changes materially. Next review due October 2026.	Group Data Protection Officer

1. Purpose and the Charter basis

The group processes personal data because it must identify its clients, run their mandates and meet its legal obligations. It processes personal data for no other purpose. This policy exists to make that limit operational: every item of personal data the group holds must be traceable to one of those purposes, to a documented origin and to a lawful basis. Data that cannot be traced is deleted.

The Ethical Technology Charter, adopted by the Board in 2023, supplies the principles. Provenance of data requires a documented origin for every dataset. Restraint in inference forbids conclusions about an individual beyond what a mandate requires. Transparency to clients requires that a client can see which decisions were model-assisted. The right to a human decision means any client can require a named person to review any decision that affects them. Each principle is given a control in this policy.

The policy is owned by the Group Data Protection Officer, who reports to the Information Governance Committee and has direct access to the Chair of the Board. Local data protection officers in Singapore, Luxembourg, London, Dubai and Toronto report to the Group Data Protection Officer on this subject and to their entity boards on all others.

2. The processing register and lawful basis

Every processing activity in the group is entered in the processing register before it begins. The register held 84 activities at 30 June 2026. Each entry records the categories of data, the categories of individual, the purpose, the lawful basis in each jurisdiction where the activity runs, the origin of the data, the systems that hold it, the recipients, the retention period and the named owner. An activity without a named owner cannot be entered.

The origin field is the Charter's provenance principle made concrete. It states whether the data came from the individual, from a public register, from a screening provider under contract or from a counterparty in a transaction. The group does not buy personal data in bulk, does not scrape it from public networks and does not accept a dataset from a vendor that cannot state where it came from. The Third-Party Risk and Outsourcing policy carries the matching contractual requirement.

A new processing activity, or a material change to an existing one, requires a privacy assessment signed by the activity owner and the Group Data Protection Officer before it starts. Where the activity involves a model, profiling of any kind or a transfer to a new jurisdiction, the assessment goes to the Information Governance Committee for approval. Nineteen assessments were completed in the twelve months to 30 June 2026 and two proposals were declined.

- No processing activity begins before its register entry is complete and its owner named.
- Every dataset carries an origin statement; a dataset without one is not admitted.
- Privacy assessment before any new activity, with committee approval where a model or transfer is involved.

3. Restraint in inference

The group draws conclusions about a person only where a mandate, a legal duty or a contract requires it. Client due diligence requires an assessment of source of wealth and of sanctions and political exposure; that assessment is permitted. A conclusion about a client's health, beliefs, family circumstances or personal habits is not required by any mandate the group holds and is not permitted, whether it would be drawn by a person or by a model.

No system in the group builds a behavioural profile of a client, an employee or a member of the public. Screening tools match names and identifiers against lists; they do not score propensity. Marketing to eligible counterparties is addressed to firms and roles, not to inferred interests. The group does not use facial recognition, voice identification or any other biometric inference in any office or system.

Where a client volunteers information beyond what the mandate needs, the information is recorded only if the client asks for it to be recorded, and it is never used as an input to any decision. Staff monitoring is limited to the access logs and communications surveillance required by the Market Abuse Prevention and Information Security policies, and the scope of that monitoring is published to staff.

4. Rights of individuals and the human decision

Any individual whose data the group holds may ask what is held, ask for it to be corrected, object to a use of it, ask for it to be erased where no legal obligation requires retention, and ask for it to be transferred in a usable form. Requests are addressed to privacy@iguako.tech or to the local privacy contact in any office. The group answers within 30 days, or within the shorter period a local law sets. In the twelve months to 30 June 2026 the group received 47 requests and answered every one within the period.

The seventh Charter principle is applied without qualification. Any client may require that a decision affecting them, whether or not a model assisted it, be reviewed by a named person with authority to change it. The reviewer is not the person who made the original decision. The review is completed within ten business days and the outcome, with reasons, is given to the client in writing.

Client reports identify each decision in which a model assisted, using the assistance statement defined in the Artificial Intelligence Governance policy. The group makes no automated decision about a client, a counterparty or an employee. Every decision has a human author whose name is on the record, and the record can be produced to the individual on request.

- Requests to privacy@iguako.tech answered within 30 days or the shorter local period.
- Human review of any decision within ten business days by a person who did not make it.
- Model-assisted decisions identified on client reports; no automated decisions about any person.

5. Retention, storage and transfers

Personal data relating to a client relationship is kept for seven years after the relationship ends and is then deleted, unless the law of the booking jurisdiction requires a longer period, in which case the longer period is recorded in the register and applied. Data collected for a prospective relationship that does not proceed is deleted after twelve months. Recruitment data for unsuccessful candidates is deleted after six months. The full schedule is in the Records Management and Retention policy.

Client records are held on the group's primary systems in George Town and Luxembourg, with a copy at the regional hub that serves the booking entity. Data is encrypted at rest and in transit. Every access to a client record is logged with the identity of the person and the reason, and the logs are reviewed monthly by the local data protection officer. Personal data is not stored on portable media or on personal devices.

Personal data moves between group entities only under the intra-group data transfer agreement, which binds every entity to this policy regardless of local law. Data leaves the group only to a custodian, administrator, counterparty or screening provider that needs it to perform a mandate, or to a public authority with a lawful demand. Each external transfer is made under a written agreement and is logged with the recipient, the purpose and the legal basis.

6. Breaches and incidents

A personal data breach is any loss, unauthorised access, unauthorised disclosure or unlawful destruction of personal data, whether caused inside the group or by a third party holding data on its behalf. Any member of staff who becomes aware of a suspected breach reports it to the Group Data Protection Officer within 24 hours of discovery. Delay to gather more facts is not permitted; the first report may be incomplete.

The Group Data Protection Officer assesses the breach within 72 hours, decides with the General Counsel whether a supervisory authority or the affected individuals must be notified under the law of each jurisdiction concerned, and records the decision and its reasons. Notification, where required, is made within the statutory period. Affected clients are told what was lost, what the group has done and what they can do, in plain language, without waiting for the regulatory process to finish.

Every breach, notifiable or not, is logged in the breach register with its cause and the corrective action taken. The register is reviewed quarterly by the Information Governance Committee. Three breaches were recorded in the twelve months to 30 June 2026. None met the threshold for supervisory notification; each was reported to the individuals affected within five business days.

7. Governance and training

The Information Governance Committee, chaired by the independent director Priya Vantongeren, approves this policy, receives the breach register each quarter and the processing register each year, and hears any dispute between the Group Data Protection Officer and a business division. The Group Data Protection Officer presents an annual report to the Board covering requests, breaches, assessments and declined proposals.

Every member of staff completes data protection training within one month of joining and annually thereafter. Staff in roles that handle client data, screening data or model inputs complete an additional module on inference and provenance. Completion was 100 per cent of the 312 people at 30 June 2026. Internal Audit

tests the register, the access logs and the retention schedule on a two-year cycle under the Internal Audit Charter.

Key controls

- Processing register with origin, lawful basis, retention and named owner for each of the 84 activities.
- Privacy assessment before any new processing, with Information Governance Committee approval where a model or transfer is involved.
- Prohibition on behavioural profiling, biometric inference and inference outside the mandate, enforced by system design review.
- Requests to privacy@iguako.tech answered within 30 days; human review of any decision within ten business days.
- Encryption at rest and in transit with monthly review of client-record access logs.
- Intra-group data transfer agreement binding every entity, and logged written agreements for every external transfer.
- Breach reporting to the Group Data Protection Officer within 24 hours and assessment within 72 hours.
- Annual training for all staff with 100 per cent completion, and Internal Audit testing on a two-year cycle.

Related policies

- Information Security (IGC-DT-002)
- Records Management and Retention (IGC-DT-003)
- Artificial Intelligence Governance (IGC-DT-005)
- Third-Party Risk and Outsourcing (IGC-DT-006)

Colophon

IGUAKO Capital is a work of institutional fiction by the Iguako Institute for Applied Unreality (iguako.tech). This document is part of that work. It creates no rights or obligations, describes no licensed entity and is not an offer, a contract, a client record or advice.