aurumbeam

LEGAL DOCUMENT

Corporate Governance and Policies

Last updated: October 2026

Aurumbeam London Ltd · 20 Wenlock Road, London N1 7GU, United Kingdom
Registered in England and Wales · Company Number 17528961 · aurumbeam.com

This document describes how Aurumbeam London Ltd is managed, controlled and supervised. It names the corporate bodies, the responsibilities and the binding internal rules.

aurumbeam is the brand and the infrastructure of Aurumbeam London Ltd. The contracting party of the customers is exclusively Aurumbeam London Ltd.

FIELD	VALUE
Company name	Aurumbeam London Ltd
Legal form	private company limited by shares under the law of England and Wales (Companies Act 2006); a limited liability company with a share capital of GBP 9,500, divided into 9,500 ordinary shares of GBP 1 each, fully paid
Registered office	20 Wenlock Road, London N1 7GU, United Kingdom
Register	Registrar of Companies for England and Wales (Companies House), Cardiff
Registration number	Company Number 17528961
Incorporation	19 October 2026
Director	Oliver Antunović
Contact	support@aurumbeam.com

1 Subject matter and scope

These policies apply to Aurumbeam London Ltd, to all employees and to all persons who perform tasks for the company on the basis of a service, work or mandate relationship. They apply to all business transactions of the aurumbeam infrastructure, that is to purchase, buy-back, custody, transfer of gold holdings between users, physical delivery, recurring purchases and the purchase of precious metals sent in from outside. The transfer of gold holdings is offered to customers under the product name beaming (beam gold, beam order, beamed); the legally decisive term is transfer of gold holdings.

Service providers are not directly bound by these policies. Their obligations arise from the respective contract. Section 14 specifies the minimum content that such a contract must contain.

In the event of conflict between these policies and mandatory law, mandatory law prevails. In the event of conflict between these policies and an individual instruction, the stricter rule prevails.

2 Legal framework of corporate governance

2.1 Mandatorily applicable requirements

BODY OF RULES	SIGNIFICANCE FOR CORPORATE GOVERNANCE
Companies Act 2006	Formation and constitution of the company, rights of the members, general duties of the directors (sections 171 to 177, in particular acting within powers, promoting the success of the company, exercising independent judgment, exercising care, avoiding conflicts of interest, not accepting benefits from third parties, declaring own interests), accounting records and annual accounts, register of people with significant control (PSC), mandatory disclosures under section 82
Articles of association	Articles based on the Model Articles for Private Companies Limited by Shares (Companies (Model Articles) Regulations 2008)
UK GDPR and Data Protection Act 2018; Regulation (EU) 2016/679 pursuant to its Article 3(2)	Responsibility, accountability, record of processing activities, technical and organisational measures, notification obligations (section 12)
Sanctions and Anti-Money Laundering Act 2018 and the United Kingdom sanctions regulations made under it	Obligation to comply with the sanctions of the United Kingdom
Regulation (EU) No 269/2014 and Regulation (EU) No 833/2014	Freezing of funds and prohibition on making funds available; prohibition on the purchase, import and transfer of gold originating in Russia (Article 3o in conjunction with Annexes XXVI and XXVII). Decisive for the sourcing and custody of the gold in Austria
Public Interest Disclosure Act 1998	Protection of workers in the United Kingdom who report wrongdoing (section 17)

2.2 What expressly does not apply

Aurumbeam London Ltd is not listed on a stock exchange. From this and from its size it follows that:

1. The UK Corporate Governance Code is addressed to listed companies and is not applicable. There is no corporate governance statement and no statement of compliance.
2. There is no obligation to provide sustainability reporting, because the relevant size thresholds are not reached.
3. The German Lieferkettensorgfaltspflichtengesetz (Supply Chain Due Diligence Act) is not applicable, because the company has neither its registered office nor a branch within the meaning of § 13d HGB in Germany and does not reach the employee threshold.
4. Aurumbeam does not hold an authorisation from the Financial Conduct Authority and is not subject to its supervision. Aurumbeam does not provide banking, financial, payment or e-money services. An acquisition via aurumbeam

results in ownership or co-ownership of physical gold, not in a claim against a credit institution.

5. Aurumbeam does not accept cash payments. The conditions under which dealers in precious metals in the United Kingdom are subject to obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLR 2017") (cash payments of EUR 10,000 or more) are not met (section 11).

2.3 Standards applied voluntarily

1. The OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas, third edition 2016, including the Gold Supplement, as a reference framework for sourcing. The details are governed by the supply chain policy at aurumbeam.com/lieferketten-richtlinie, including the supplier's evidence of origin and refinery evidence. Aurumbeam does not describe itself as certified.
2. The procedural principles of Directive (EU) 2019/1937 on the protection of persons who report breaches as guidance for the internal reporting channel, applied irrespective of any statutory employee threshold (section 17).
3. Identity verification of customers before the first payout of a purchase price from a buy-back and before the first physical delivery, even where there is no statutory obligation (section 11).

3 Management and corporate bodies

3.1 Corporate bodies

BODY	BASIS	COMPOSITION AND FUNCTION
Member	Companies Act 2006, articles based on the Model Articles for Private Companies Limited by Shares	Oliver Antunović, sole shareholder holding all 9,500 shares. The shareholder decides by resolution on the matters reserved to the members by law and the articles, in particular amendments to the articles and the appointment and removal of directors
Director	Companies Act 2006, articles based on the Model Articles for Private Companies Limited by Shares	Oliver Antunović, sole management body. Manages the business of the company, represents it, organises day-to-day operations, is responsible for accounting records, annual accounts and filings with Companies House, hires and dismisses employees

Aurumbeam London Ltd is a company limited by shares with a share capital of GBP 9,500, divided into 9,500 fully paid ordinary shares of GBP 1 each. The sole shareholder is Oliver Antunović. The shareholder's liability is limited to the amount paid on his shares. Oliver Antunović is at the same time a person with significant control (PSC): he holds more than 75 per cent of the shares and voting rights and has the right to appoint and remove a majority of the directors.

There is no board with several directors, no supervisory body, no advisory board and no audit committee. The control function is supplemented by the external audits under section 10 and the engagement of external bodies under section 11.3.

The director is subject to the general duties of directors under the Companies Act 2006: he acts within his powers, promotes the success of the company, exercises independent judgment, acts with the requisite care, avoids conflicts of interest, does not accept benefits from third parties and declares his own interests in transactions of the company.

3.2 Areas of responsibility

The director performs the following areas of responsibility himself or delegates them in writing to employees. The delegation names the person, the tasks and the deputy.

AREA OF RESPONSIBILITY	TASK
Compliance	Monitoring compliance with these policies, sanctions screening, prevention of money laundering, documentation of conflicts of interest and benefits
Holdings and custody	Keeping the custody register, reconciliation with the holdings at the custodian, deposits into and withdrawals from storage
Data protection	Record of processing activities, data processing agreements, data subject requests, notification of personal data breaches
Information security	Rights and roles concept, logging, backup and recovery, security incidents
Customer complaints	Receipt, handling and deadline monitoring of complaints
Internal reporting office	Receipt and handling of reports under section 17
Accounting	Bookkeeping, records and vouchers, annual accounts, tax returns

From spring 2027, an external money laundering reporting officer will be engaged (section 11.3).

3.3 Register and mandatory disclosures

The details of the member, the director and the person with significant control are kept up to date in the register at Companies House. Changes are notified within the statutory time limits. The annual accounts and the confirmation statement are filed with Companies House in good time.

4 Allocation of tasks

TASK	RESPONSIBILITY
Setting the mark-ups and mark-downs on the reference price and the fees in the schedule of fees	Director; every change is published in the app and in the schedule of fees before it takes effect
Approval of a new product in the shop	Director, after confirmation of availability and of the evidence position
Keeping the custody register	Holdings and custody
Deposits into and withdrawals from storage at the custodian	Holdings and custody
Payouts to customers from buy-backs	Accounting; approval under the four-eyes principle (section 5)
Purchase of precious metals sent in from outside	Holdings and custody; identification and verification of origin in accordance with the purchase terms
Sanctions screening	Compliance; decision on hits by the director
Review of conspicuous transfers of gold holdings	manually by employees in accordance with section 11.2
Individual verification of larger incoming payments	Compliance
Granting and withdrawal of system authorisations	Information security, approval by the director
Conclusion and termination of service provider contracts	Director
Responding to customer complaints	Customer complaints; escalation to the director
Responding to data subject requests under data protection law	Data protection; decision on the refusal of a request by the director
Preparation and filing of the annual accounts	Accounting and director

5 Transactions affecting holdings

A transaction affects holdings if it changes the physical gold holding, its allocation in the custody register or the ownership and co-ownership relationships existing in it.

Every payout to customers, in particular from buy-backs and from the purchase of precious metals sent in, is approved under the four-eyes principle: one person prepares the payout, a second person checks the recipient, the bank details and the amount and approves the payout. The approval is documented.

Entries in the custody register are not overwritten and not deleted. Every change is made by an additional entry that corrects the previous entry in a traceable manner. Entries in the closed logging system are a technical log. Only the custody register is decisive.

6 Conflicts of interest

A conflict of interest exists where personal, economic, family or other interests of a person working for the company are capable of influencing that person's decision in the interest of the company or of the customers.

1. **Duty of disclosure.** Employees notify the director in writing of any potential conflict of interest within three working days of becoming aware of it. The director declares his own interests in transactions of the company in accordance with the requirements of the Companies Act 2006.
2. **Documentation.** Notified conflicts are documented in writing with the date, the facts and the measure taken.
3. **Abstention.** Anyone affected by a conflict is excluded from handling and approving the transaction concerned, insofar as another person can take over the task.
4. **Transactions with related parties.** Contracts with the member, the director, their relatives or companies controlled by them are concluded on arm's length terms and documented in writing.
5. **Secondary activities.** A secondary activity of employees for a company that trades in, holds in custody, transports or values precious metals must be notified before it is taken up and requires the consent of the director.
6. **Separation of trading and custody.** The custodian, SOOS GmbH (Goldvorsorge, GVS Bullion Group), is a company that is legally and organisationally separate from Aurumbeam London Ltd and in which Aurumbeam London Ltd holds no interest. The details are governed by the document Custody Services at aurumbeam.com/verwahrdienste.

7 Remuneration principles

1. The remuneration of employees consists of a fixed basic remuneration. It is set at a level such that the performance of tasks does not depend on variable components.
2. Variable components are not linked to the volume of individual customer transactions, to the number of buy-backs concluded or to the turnover of individual customers.

3. Employees who perform tasks in the areas of compliance, holdings and custody, data protection, information security, customer complaints or the internal reporting office receive no sales-related remuneration for these tasks.
4. There are no targets that create an incentive to dissuade customers from a buyback, to delay a physical delivery or not to record a complaint as a complaint.
5. The remuneration of the director is governed by the articles and is documented in writing.
6. Partners and affiliates are not employees. Their remuneration is performance-related and is governed by the partner terms. Partners and affiliates may not provide investment, tax or legal advice, may not make statements about future performance and may not give the impression of acting on behalf of Aurumbeam. Breaches result in termination of the partnership and in the loss of outstanding remuneration claims.

8 Code of conduct for employees

8.1 Confidentiality

Trade and business secrets, holdings data, price calculations, custody agreements, security concepts and customer data are confidential. The duty of confidentiality applies without time limit and beyond the end of the employment relationship. Information is given to the press, authorities or third parties exclusively by the director or by a person expressly instructed by him. Requests for information from authorities are forwarded to the director without undue delay and are checked for their legal basis and scope before being answered.

8.2 Handling of customer data

1. Access only on a need-to-know basis. Anyone not handling a task does not access the associated data.
2. Customer data are not transferred to private devices, private email accounts, private cloud storage or removable storage media.
3. Printouts containing customer data are destroyed in compliance with data protection requirements once the matter has been dealt with.
4. The use of customer data for private purposes, for research without instruction or for advertising without the necessary legal basis is prohibited.
5. A breach of these rules must be reported to the director without undue delay, even if it was caused by the person reporting it. The reporting of a self-caused breach is taken into account as a mitigating factor when assessing the consequences.

8.3 Gifts and benefits

CASE	RULE
Cash payments, vouchers, precious metals, crypto assets and other cash equivalents	Acceptance and granting prohibited without exception, irrespective of value
Gifts in kind up to EUR 50 individual value	permitted without notification, provided they are a customary business courtesy
Gifts in kind above EUR 50 individual value	notification to the director within five working days, acceptance only with written approval, otherwise return
Several benefits from the same giver exceeding EUR 100 in the calendar year	notification to the director, irrespective of the individual value
Invitations to events and hospitality	permitted where there is a business occasion and a reasonable setting, notification from EUR 100 equivalent value per person
Benefits during ongoing contract or tender negotiations	prohibited, irrespective of value
Benefits to or from public officials	prohibited, irrespective of value

Notified benefits are documented in writing.

8.4 Prohibition of corruption

Offering, promising, granting, requesting and accepting advantages in order to influence business decisions is prohibited. The applicable criminal law is decisive, in the United Kingdom in particular the Bribery Act 2010, under which a company may also commit an offence if a person performing services for it commits bribery for its benefit.

Also prohibited are payments to expedite administrative procedures, the use of intermediaries to circumvent this prohibition and donations or sponsorship made in return for a business decision. Donations and sponsorship require the prior written consent of the director and are documented with the recipient, the amount and the purpose.

Lawful conduct takes precedence over any conflicting instruction. Anyone who receives such an instruction refuses to carry it out and reports the matter via the channel under section 17.

8.5 Private transactions in precious metals

Private purchases and sales of precious metals are in principle permitted for employees. The following restrictions apply:

1. Employees with access to price parameters, holdings data or the custody register notify the director of their own purchases and buy-backs via aurumbeam within five working days of conclusion.

2. Within two working days before the entry into force of a change to the mark-ups or mark-downs or to the fees in the schedule of fees that has already been decided but not yet published, own purchases and buy-backs via aurumbeam are prohibited.
3. The acquisition from the company's holding of items intended for allocation to customers is prohibited.
4. In private precious metals transactions, employees do not refer to their work for Aurumbeam.
5. A private transaction may not be brought forward or postponed in order to obtain an advantage from an impending customer or sourcing transaction.

8.6 Handling of knowledge about holdings

Information about total holdings, changes in holdings, planned sourcing, transport times, transport routes and security arrangements is strictly confidential. It is passed on exclusively to persons who need it to perform their tasks.

Prohibited in particular are passing on transport dates and transport routes to persons outside the transaction, giving information about the place of custody to third parties that goes beyond the information published in the document Custody Services, using holdings information for one's own or others' transactions and any publication on social networks that allows conclusions to be drawn about holdings or security arrangements.

8.7 Limits of customer communication

Employees do not provide investment, tax or legal advice, make no statements about the future development of the gold price, make no promises of returns and do not hold out the prospect of preservation or growth of value. Questions about tax treatment are referred to the customers' competent advisers.

Under competition law: no agreements are made with competitors on prices, mark-ups, terms, sales volumes, customers or territories. Even the appearance of such an agreement must be avoided. Even participation in a conversation with such content must be ended and reported to the director.

9 Risk management

The director is responsible for risk management. The following principles apply.

TYPE OF RISK	FORM AT AURUMBEAM	CONTROL MEASURE
Market price risk	The gold price may change between the customer transaction and sourcing from the supplier. Open positions also arise from buy-backs. In the case of recurring purchases, no open position arises from accumulated amounts of money, because each purchase amount triggers a purchase contract for a quantity of gold determined by fine weight and residual amounts are allocated to the gram with a resolution of 0.001 grams.	Covering customer purchases by sourcing from Goldvorsorge Österreich; monitoring of the open position by the director
Holdings and custody risk	Loss, theft, damage, shortfalls, discrepancy between the physical holding and the custody register	Reconciliation on every deposit into and withdrawal from storage; at least twice a year a physical count and weighing and at least once a year confirmation of the reconciliation by an independent auditor, in each case by an auditing body independent of Aurumbeam and of the custodian; insurance of the holding in accordance with section 15
Settlement and payment risk	Chargebacks of card payments, failed charges on recurring purchases, failed payouts, failure of the payment service provider	Payment exclusively by credit card; where there are indications of an abusive card payment, suspension of payout, delivery and beaming of the holdings acquired with it in the individual case; payouts only to a bank account in the customer's name
IT and cyber risk	Unauthorised access to customer accounts and to the custody register, manipulation of register data, failure of the infrastructure, phishing against customers and employees, malware	Measures in accordance with section 13
Compliance and sanctions risk	Breach of sanctions requirements, of consumer protection requirements or of company law notification and filing deadlines	Sanctions screening in accordance with section 11.4, review of marketing statements before publication, annual legal review in accordance with section 20
Reputational risk	Public criticism of custody, payout times or customer service, misuse of the brand by third parties, incorrect statements by partners	Response times in accordance with section 16, review of partner advertising, action against misuse of the brand, communication in a crisis exclusively via the director
Outsourcing risk	Failure or poor performance of the custodian, payment service provider, shipping service provider or hosting provider	Minimum content in every contract in accordance with section 14

10 Internal control system

The internal control system is aligned with the size of the company.

1. **Operational control.** Control takes place within the process itself: system validations, mandatory fields and plausibility checks in the aurumbeam in-

frastructure, the approval of every payout under the four-eyes principle (section 5), sanctions list screening in accordance with section 11.4 and the manual review of conspicuous transactions in accordance with section 11.2.

2. **External audit.** This includes the audit of holdings in accordance with section 15 and the audit of the annual accounts, insofar as this is required by law.

Accounting vouchers and accounting records are retained in accordance with the applicable commercial and tax law provisions. For customer contract documents, a uniform retention period of ten years from the end of the business relationship is applied. After the period has expired, personal data are deleted in accordance with the deletion concept.

11 Prevention of money laundering and sanctions

11.1 Starting position

Aurumbeam does not accept cash payments. Payment can be made exclusively by credit card via the payment service provider Worldpay (UK) Limited. Payments in crypto assets are not accepted. The conditions under which dealers in precious metals in the United Kingdom are subject to obligations under the MLR 2017 (cash payments of EUR 10,000 or more) are not met.

The anti-money laundering checks of the payment service provider apply in addition. This makes it possible to trace who bought which gold and when.

11.2 Voluntary due diligence measures

1. Every customer undergoes identity verification before the first payout of a purchase price from a buy-back and before the first physical delivery. Aurumbeam carries this out itself: employees of Aurumbeam check a valid official photo identity document and compare it with the details provided, without biometric matching. Images of identity documents are deleted after completion of the verification, at the latest 30 days thereafter; the result of the verification and the verified master data remain stored.
2. The basis for the data processing in the context of this voluntary verification is not a legal obligation, but the contract with the customer and the legitimate interest in preventing misuse. The details are governed by the privacy policy.
3. Larger incoming payments are verified individually.
4. **Review of beaming.** Conspicuous transfers of gold holdings are reviewed manually by employees and may be suspended. Conspicuous are in particular a sale back to Aurumbeam shortly after receipt, many transfers to changing recipients, the splitting of transactions just below the threshold of EUR 15,000, reciprocal cycles between the same customers and chains of unclaimed onward transfers.
5. Employees report conspicuous circumstances to the director without undue delay. The following are also regarded as conspicuous in particular: requests for

payout to a bank account not in the customer's name, purchases and buy-backs following one another in quick succession without economic rationale, refusal to complete identity details, and details of the source of funds that do not match the discernible background.

6. Every reported matter, the review and the result are documented. In the event of a suspicion of money laundering or terrorist financing, the transaction is suspended and, insofar as legally required, reported to the competent authority.
7. On the purchase of precious metals sent in from outside, the selling person is identified in accordance with the purchase terms. Aurumbeam does not purchase from minors.

11.3 Alignment with the EU AntiMoney Laundering Regulation

Aurumbeam aligns its processes with Regulation (EU) 2024/1624, which applies from 10 July 2027. From spring 2027, an external money laundering reporting officer will be engaged.

11.4 Sanctions

1. Customers and payees are screened against the sanctions lists of the European Union and the United Kingdom before every payout and before every physical delivery. The basis is Regulation (EU) No 269/2014 with the freezing and making-available prohibition in its Article 2 and the sanctions regulations of the United Kingdom under the Sanctions and Anti-Money Laundering Act 2018.
2. Screening for politically exposed persons and for adverse media is carried out only where there is cause.
3. The supplier, the custodian, transport and payment service providers are screened before the contract is concluded.
4. Article 3o of Regulation (EU) No 833/2014 applies to the sourcing of gold: the purchase, import and transfer of gold originating in Russia in accordance with Annexes XXVI and XXVII are prohibited. The supplier contractually confirms the origin of the goods supplied. The evidence of origin is governed by the supply chain policy.
5. In the event of a hit, the transaction concerned is suspended immediately and decided on by the director. Payouts and deliveries do not take place until the matter has been clarified. The transaction is fully documented.

12 Data protection governance

1. **Controller.** The controller is Aurumbeam London Ltd, 20 Wenlock Road, London N1 7GU, United Kingdom, datenschutz@aurumbeam.com. The UK GDPR and the Data Protection Act 2018 apply, as well as, for the offer to persons in the European Union and in Liechtenstein, Regulation (EU) 2016/679 pursuant to its Article 3(2), and for persons in Switzerland the Swiss Federal Act

on Data Protection. The competent supervisory authority for the United Kingdom is the Information Commissioner's Office (ICO).

2. **Data protection officer.** There is no obligation to designate a data protection officer under Article 37(1) UK GDPR and Article 37(1) of Regulation (EU) 2016/679, because the core activity consists neither of large-scale regular and systematic monitoring of individuals nor of large-scale processing of special categories of personal data. Data protection enquiries are handled at datenschutz@aurumbeam.com.
3. **Record of processing activities.** The record of processing activities under Article 30 is maintained and updated with every new processing operation.
4. **Processing on behalf.** With every service provider that processes personal data on behalf of Aurumbeam, a contract under Article 28 is concluded before processing begins. This applies in particular to the hosting provider, the custodian for delivery data and providers of email and customer service systems. Subprocessors require prior consent. The processors are listed in Annex 1 to our data processing agreement.
5. **Transfers to third countries.** A transfer to a third country takes place only on the basis of an adequacy decision or appropriate safeguards. Before every new transfer, the basis is documented.
6. **Technical and organisational measures.** The measures under Article 32 are documented and reviewed in the event of material changes to the processing.
7. **Personal data breaches.** Every personal data breach must be reported to the director without undue delay. In the case of notifiable matters, notification is made to the competent supervisory authority within 72 hours of becoming aware of it under Article 33, for the United Kingdom to the Information Commissioner's Office. Where there is a high risk to the data subjects, they are notified under Article 34. All incidents are documented irrespective of the notification obligation.
8. **Data subject rights.** Requests for access, rectification, erasure, restriction, data portability and objection are answered under Article 12(3) without undue delay, at the latest within one month of receipt. An extension by up to two further months is possible in the case of complexity and is communicated to the data subject within one month.
9. **Data protection impact assessment.** Before introducing processing that is likely to result in a high risk to the rights and freedoms of the data subjects, an impact assessment under Article 35 is carried out and documented.
10. **Deletion concept.** The deletion concept assigns a period to each category of data and takes into account the retention periods under commercial and tax law.

References to Articles in this section refer equally to the UK GDPR and to Regulation (EU) 2016/679.

13 Information security

1. **Roles and rights.** Access is granted via roles. Administrative rights are granted separately and logged separately. When a person leaves, all access is deactivated on the last working day.
2. **Authentication.** Two-factor authentication is mandatory for all administrative access and for access to the custody register. Two-factor authentication is available to customers for their access.
3. **Separation of environments.** Development, testing and production are separated. Real customer data are not used in test and development environments.
4. **Logging.** Security-relevant events and all changes to the custody register are logged and protected against subsequent alteration.
5. **Backup and recovery.** Data are backed up regularly.
6. **Vulnerabilities and changes.** Security-relevant updates are installed according to criticality. Changes to production systems are made in accordance with an approval procedure with a fallback route.
7. **Security incidents.** Security incidents are reported to the director without undue delay, contained, documented and followed up. If an incident affects personal data, section 12 No. 7 applies in addition.
8. **Customer access.** Each customer is recorded in the custody register exclusively under his or her custody agreement number. It is the sole identifier for custody holdings and for orders for the transfer of gold holdings; there are no external addresses. Changes to security-relevant master data, in particular the stored bank details, are confirmed to the customer.
9. **Closed logging system.** The entries in the closed, access-restricted logging system are a technical log. Only the custody register is legally decisive. This order of precedence must be ensured with every system change.

14 Outsourcing and management of service providers

14.1 Categories

Outsourcing arrangements are regarded as material if their failure would directly impair business operations, the security of the holdings or the rights of the customers. These include custody, payment processing, transport and shipping as well as hosting and operation of the infrastructure.

14.2 Selection

Before engagement, suitability, reliability, insurance cover, sanctions list screening and, where personal data are processed, compliance with data protection law are

checked. The director makes the decision.

14.3 Minimum content of the contract

SUBJECT MATTER	REQUIREMENT
Description of services	clear description of the tasks assumed and of the quality of service
Instruction and control	right of Aurumbeam London Ltd to give instructions, rights to information and audit, access for appointed auditors within the framework of the security requirements
Subcontracting	permissible only with prior consent, flow-down of all obligations to the subcontractor
Confidentiality and data protection	duty of confidentiality, contract under Article 28 UK GDPR and Article 28 of Regulation (EU) 2016/679, insofar as personal data are processed
Notification obligations	notification without undue delay of security incidents, discrepancies in holdings, insolvency applications and measures by authorities
Insurance	evidence of adequate insurance cover
Sanctions and origin	confirmation of compliance with the applicable sanctions requirements, in the case of the supplier additionally evidence of origin in accordance with the supply chain policy
Term and termination	termination rights, transition support, return of data and holdings in a usable format

15 Custodian governance

The sole place of custody is Vienna, Austria. The custodian is SOOS GmbH (Goldvorsorge, GVS Bullion Group), Handelskai 94-96, Stiege 4, 5. OG, 1200 Vienna, Austria, Firmenbuch (commercial register) FN 371831k (Handelsgericht Wien, Vienna Commercial Court). The gold is sourced from Goldvorsorge Österreich, a precious metals dealer registered in Vienna, from the holdings of the GVS Bullion Group and remains in Austria. The details are governed by the document Custody Services at aurumbeam.com/verwahrdienste.

In addition to section 14, the following principles apply to the management of custody:

1. Customer holdings are kept at the custodian as holdings for the account of Aurumbeam's customers, separately from Aurumbeam's own holdings. The custodian does not acquire ownership of the gold held in custody. These requirements are laid down in the storage agreement.
2. The custodian is contractually obliged not to lend, pledge, lease or encumber gold held in custody or to use it in its own transactions.
3. Reconciliation between the physical holding and the custody register takes place on every movement, at least twice a year by a complete count and weighing, and where there is cause in the event of discrepancies. At least once a year,

an independent auditor confirms the reconciliation. The auditing body is a body independent of Aurumbeam and of the custodian.

4. Discrepancies are documented, corrected by a counter-entry and reported to the director without undue delay. Existing entries are not overwritten and not deleted.
5. Under the custodian's terms, the holdings in custody are insured at their current raw material value against burglary, robbery and fire.
6. The director decides in writing on the appointment or a change of the custodian. The document Custody Services is updated before the change takes effect.

16 Complaint and escalation procedures

16.1 Customer complaints

STAGE	RESPONSIBLE	TIME LIMIT
Receipt and acknowledgement	Customer complaints, support@aurumbeam.com	acknowledgement of receipt within two working days
Examination of the merits and response	Customer complaints	reasoned written response within 14 days of receipt
Escalation	Director	decision within ten working days of escalation
Out-of-court dispute resolution	reference to the competent body in text form, insofar as the applicable law so provides	with the rejecting or partially rejecting response

The 14-day period is a contractual commitment to customers under the General Terms and Conditions.

For consumers with habitual residence in Germany, § 37 of the Verbraucherstreitbeilegungsgesetz (Consumer Dispute Resolution Act) applies in addition: if a dispute concerning a consumer contract could not be settled, reference must be made in text form to a competent consumer arbitration body, stating its address and website, and it must at the same time be stated whether Aurumbeam will participate. This obligation is an integral part of the complaints process.

Every complaint is recorded with the date of receipt, the facts, the person handling it, the time limits, the result and the date of completion, even if it is received by post.

16.2 Internal escalation

1. An employee who identifies a breach of rules, an error in holdings or a security problem reports this to the director without undue delay.

2. Discrepancies in holdings, security incidents affecting customers, sanctions hits and personal data breaches are reported directly to the director without any waiting time.
3. If the matter concerns the director himself, the report is made to the internal reporting office under section 17.

17 Whistleblower protection

17.1 Basis

Aurumbeam operates an internal reporting channel and aligns its procedures with the principles of Directive (EU) 2019/1937 on the protection of persons who report breaches, irrespective of whether there is a statutory obligation to establish an internal reporting channel. For workers in the United Kingdom, the protection under the Public Interest Disclosure Act 1998 is decisive. More extensive mandatory protective provisions of the state in which the reporting person works remain unaffected.

17.2 Who can report and what can be reported

Reports can be made by employees, former employees, applicants, trainees and interns, freelancers, contractors, suppliers and their employees, as well as customers.

Breaches of legal provisions and of these policies can be reported, in particular corruption, bribery and acceptance of bribes, embezzlement or manipulation of holdings, incorrect entries in the custody register, breaches of anti-money laundering and sanctions requirements, breaches of data protection or of product safety, as well as attempts to prevent a report.

17.3 Reporting channel

CHANNEL	DETAILS
Email	meldestelle@aurumbeam.com. The mailbox is accessible exclusively to the persons of the internal reporting office and is technically separated from the general mailboxes
Post	Aurumbeam London Ltd, Internal Reporting Office, 20 Wenlock Road, London N1 7GU, United Kingdom. The envelope must be marked “Confidential, personal to the Internal Reporting Office” and is opened exclusively by that office
In-person meeting	at the request of the reporting person, appointment within seven days of the request, on request with minutes, which are submitted to the reporting person for review and correction

Reports can be made by name or anonymously. Anonymous reports are handled in the same way as named reports. In the case of an anonymous report, feedback is possible only if the reporting person provides a return channel.

Reports concerning the director are forwarded by the reporting office to Aurumbeam's external legal adviser.

In addition to the internal reporting channel, the external bodies competent under the applicable law are available. A prior internal report is not a precondition for using the external channel.

17.4 Time limits

STEP	TIME LIMIT
Acknowledgement of receipt to the reporting person	within seven days of receipt of the report
Initial assessment of whether the matter falls within the scope, and start of the investigation	within ten working days of receipt
Feedback on follow-up measures planned or already taken and the reasons for them	within three months of the acknowledgement of receipt
Interim notification if the review takes longer	at the latest on expiry of the three months, stating the reason and the expected completion
Final notification of the result	within five working days of completion of the review

The time limits for the acknowledgement of receipt and the feedback correspond to Article 9(1)(b) and (f) of Directive (EU) 2019/1937.

17.5 Confidentiality

1. The identity of the reporting person, the identity of the person concerned and all information that allows conclusions to be drawn are treated confidentially.
2. Only the persons of the internal reporting office have access to reports. Disclosure to other persons takes place only insofar as it is strictly necessary for the investigation, and only after prior information to the reporting person, unless the information would jeopardise the investigation.
3. The identity is disclosed to authorities or courts only insofar as this is mandatorily required by law and proportionate. The reporting person is informed in advance, insofar as the information does not jeopardise the investigations.
4. Reports and the associated documentation are kept separately from personnel files.
5. Reports and the associated documentation are retained for five years and deleted thereafter, unless ongoing proceedings preclude this.

17.6 Prohibition of retaliation

Detrimental measures because of a report are prohibited. Prohibited in particular are dismissal, formal warning, transfer, withdrawal of tasks, demotion, refusal of promotion or training, reduction or withholding of remuneration, change of working hours, negative performance assessment, exclusion, coercion, intimidation, damage

to reputation, blacklisting and the termination or non-renewal of a supply or service contract.

The protection also applies to persons who assist a reporting person, to relatives and to colleagues in the professional environment.

The protection applies if the reporting person had reasonable grounds to believe at the time of the report that the information reported was true. It does not cease to apply if the report subsequently proves to be unfounded. There is no protection in the case of knowingly false reports; these have consequences under employment law.

17.7 Documentation

The internal reporting office documents every report with the date of receipt, the category of the matter, the time limits, the investigation steps, the result and the measures taken. The documentation is kept under case numbers; the link to persons is kept separately and protected against access.

18 Training and further training

These policies are made available to all employees before they take up their duties.

19 Reporting

The following must be reported to the director immediately: discrepancies in holdings, sanctions hits, notifiable personal data breaches, security incidents affecting customers, inspections and requests for information by authorities and the failure of a material service provider. Reports under section 17 that concern the director are dealt with in accordance with section 17.3.

The director ensures that the company law filings with Companies House, in particular the annual accounts and the confirmation statement, are made in good time.

20 Review of the policies

1. **Annual legal review.** These policies and all legal texts of the aurumbeam infrastructure are reviewed legally at least once a year. The legal review covers the currency of the legal bases in all sales markets and the question of whether responsibilities and procedures are applied in practice as laid down here.

2. A review for cause takes place in the event of a change in the legal position in one of the sales markets Germany, Austria, Switzerland, Liechtenstein and the United Kingdom, on the introduction of a new product or service, on a change of the custodian or of a material service provider, after a loss event and after an objection by an authority.
3. A separate review with regard to Regulation (EU) 2024/1624 takes place before 10 July 2027 (section 11.3).
4. Changes are versioned. Each version is documented with the date, the reason for the change and the sections changed. Earlier versions are retained for ten years.
5. The version in force at any given time is available on aurumbeam.com and accessible to all employees. Material changes are actively communicated to all employees.
6. Breaches of these policies are investigated and, depending on their severity, have consequences under employment law up to and including termination of the employment relationship. Claims for damages and the possibility of a criminal complaint remain unaffected.

Last updated: October 2026

aurumbeam

Aurumbeam London Ltd
20 Wenlock Road
London N1 7GU
United Kingdom

Registered in England and Wales
Company Number 17528961

CONTACT

support@aurumbeam.com
datenschutz@aurumbeam.com

aurumbeam.com

LAST UPDATED: OCTOBER 2026