aurumbeam

LEGAL DOCUMENT

Privacy and Cookies

Last updated: 29 October 2026

This Privacy Policy applies to the website aurumbeam.com including all subpages, to the aurumbeam app, to customer service, to the partner and affiliate programme and to pre-contractual communication. It fulfils the information obligations under Articles 13 and 14 UK GDPR, under Articles 13 and 14 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), under Articles 19 and 21 of the Swiss Federal Act on Data Protection, and the information obligations arising from the rules on electronic communications in Germany, Austria, Liechtenstein and the United Kingdom.

1 Controller, contact and responsibility for data protection enquiries

1.1 Controller

The controller within the meaning of Article 4(7) UK GDPR and GDPR and the controller within the meaning of the Swiss DSG is exclusively:

ITEM	DETAILS
Company name	Aurumbeam London Ltd
Address (registered office)	20 Wenlock Road, London N1 7GU, United Kingdom
Legal form	private company limited by shares under the law of England and Wales (Companies Act 2006)
Register	Registrar of Companies for England and Wales (Companies House), Cardiff
Registration number	Company Number 17528961
Body authorised to represent the company	Oliver Antunović, Director
General contact	support@aurumbeam.com
Data protection and data subject rights	datenschutz@aurumbeam.com
Website	aurumbeam.com

aurumbeam is the brand and the infrastructure of Aurumbeam London Ltd. No other companies are responsible for the processing operations described in this Policy. There is no joint controllership under Article 26 UK GDPR or GDPR.

1.2 Responsibility for data protection enquiries

Please address all data protection matters, in particular requests for access, rectification, erasure, restriction, objection and portability, as well as the withdrawal of consents, to:

Aurumbeam London Ltd, Data Protection
datenschutz@aurumbeam.com
20 Wenlock Road, London N1 7GU, United Kingdom

Enquiries are handled in German and English. The most secure route is an enquiry from your logged-in aurumbeam access or from the email address registered with us. The time limits and the procedure are set out in section 12.

1.3 Applicable data protection law

Aurumbeam London Ltd has its registered office in the United Kingdom. The UK GDPR and the Data Protection Act 2018 therefore apply to all processing operations described in this Policy, irrespective of where you live.

Insofar as we offer goods and services to persons who are in the European Union or in Liechtenstein, the GDPR additionally applies to the processing of their data pursuant to Article 3(2)(a) GDPR. In Liechtenstein, the GDPR applies by virtue of the Agreement on the European Economic Area. For persons in Switzerland, the Swiss Federal Act on Data Protection additionally applies; see section 3.

The UK GDPR and the GDPR correspond in substance and in the numbering of their articles in the provisions relevant here. Where this Policy refers to an article of the GDPR, the article of the UK GDPR with the same wording applies accordingly, unless otherwise stated.

1.4 Supervisory authorities

The competent supervisory authority for Aurumbeam London Ltd in the United Kingdom is the Information Commissioner (Information Commissioner’s Office, ICO). There is no lead supervisory authority in the European Union, because Aurumbeam London Ltd has no establishment there. Insofar as the GDPR applies, you may lodge a complaint with any supervisory authority in the European Union and in Liechtenstein, in particular with the authority at your place of habitual residence. For persons in Switzerland, the Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB, Swiss Federal Data Protection and Information Commissioner) is competent; for Liechtenstein, the Datenschutzstelle (Liechtenstein Data Protection Authority). The addresses are set out in section 13.

2 Data protection officer

Under Article 37(1) UK GDPR and GDPR, a data protection officer must be designated where the processing is carried out by a public authority (point (a)), where the core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale (point (b)), or where the core activities consist of processing on a large scale of special categories of personal data under Article 9 or of data relating to criminal convictions and offences under Article 10 (point (c)).

Aurumbeam continuously reviews and documents whether any of these conditions is met. The decisive factor in this respect is above all the scope of the review of transactions for the purpose of preventing abuse. No biometric matching takes place. No biometric data within the meaning of Article 9 GDPR are processed. Identity document images from the identity check are deleted upon completion of the check, at the latest 30 days thereafter; only the result of the check and the verified master data are retained. This considerably limits the scope of the processing.

As long as, according to this review, the conditions of Article 37(1) are not met, we do not designate a data protection officer. As soon as an obligation to designate arises, we will designate a data protection officer, publish his or her contact details at this point pursuant to Article 37(7) and communicate them to the Information Commissioner and, where required by the GDPR, to the competent supervisory authorities. The threshold in § 38(1) BDSG (Germany) relates to persons who are constantly engaged in automated processing within Germany and does not apply in the absence of an establishment in Germany.

Irrespective of the question of designation, we have set up a permanent data protection contact point. It can be reached at datenschutz@aurumbeam.com and at the address stated in section 1.2, handles all data subject enquiries and is the point of contact for the supervisory authorities.

3 Representative in Switzerland under Art. 14 and Art. 15 DSG

For users in Switzerland, in addition to the UK GDPR, the Swiss Federal Act on Data Protection (Bundesgesetz über den Datenschutz, DSG, SR 235.1) applies together with the Data Protection Ordinance (Datenschutzverordnung, DSV, SR 235.11), both in force since 1 September 2023. Under Art. 3(1) DSG, the Act applies to circumstances that have an effect in Switzerland, even if they are initiated abroad.

When the obligation to appoint a representative applies. Under Art. 14(1) DSG, private controllers with their registered office abroad must designate a representative in Switzerland if they process personal data of persons in Switzerland and **all four** of the following conditions are met cumulatively:

LETTER	CONDITION	ASSESSMENT FOR AURUMBEAM
a	connection with the offering of goods and services or with the monitoring of the behaviour of persons in Switzerland	met, because Aurumbeam sells investment gold to persons in Switzerland, holds it in custody, buys it back and delivers it
b	large-scale processing	depends on the size of the Swiss customer base; measured on an ongoing basis
c	regular processing	met, because the aurumbeam access, the custody register and recurring purchases are maintained on a permanent basis

LETTER	CONDITION	ASSESSMENT FOR AURUMBEAM
d	high risk to the personality of the data subjects	depends on whether particularly sensitive personal data are processed on a large scale. Identity and asset data are not particularly sensitive under Art. 5(c) DSG. Biometric data are not processed; no biometric matching takes place

The Swiss Federal Data Protection and Information Commissioner assesses the high risk under letter d without taking into account the protective measures taken. We take this strict view into account in our assessment.

How Aurumbeam deals with this. Aurumbeam maintains a written risk assessment under Art. 14 DSG, updates it at least annually and upon every material change to the onboarding procedure or to the Swiss customer base, and documents the result. As long as not all four conditions are met cumulatively, there is no obligation to designate a representative. As soon as a representative must be designated, we will publish the name and address pursuant to Art. 14(3) DSG in section 1.1.

Under Art. 14(2) DSG, the representative serves as the point of contact for the data subjects and for the Swiss Federal Data Protection and Information Commissioner. Under Art. 15 DSG, the representative maintains the record of processing activities containing the information under Art. 12(2) DSG, communicates this information to the Commissioner upon request, and informs data subjects upon request how they can exercise their rights. Irrespective of this, you can reach us as controller directly at any time at datenschutz@aurumbeam.com.

Supplementary information for Switzerland: we notify breaches of data security to the Commissioner under Art. 24 DSG as quickly as possible where there is likely to be a high risk to your personality or your fundamental rights; the DSG does not provide for a fixed time limit of 72 hours as in Article 33 GDPR. Your right of access under Art. 25 et seq. DSG is in principle free of charge; access is generally provided within 30 days. The disclosure of data from Switzerland to the United Kingdom is permitted because the United Kingdom is recognised under Swiss law as a state with an adequate level of data protection. Conversely, Switzerland is a state with an adequate level of protection under the law of the United Kingdom and under the adequacy decision of the European Commission; the European Commission confirmed this decision on 15 January 2024.

4 Basics: which legal bases we use and why

So that the following table remains comprehensible, we first explain the legal bases used. They apply equally under Article 6 UK GDPR and, where applicable, under Article 6 GDPR.

LEGAL BASIS	MEANING	TYPICAL USE CASE AT AURUMBEAM
Article 6(1) (a) GDPR	your consent	newsletter, promotional push notifications, audience measurement, campaign measurement, testing of design variants, affiliate allocation
Article 6(1) (b) GDPR	performance of a contract or pre-contractual measures	aurumbeam access, purchase, custody, buy-back, delivery, recurring purchase, beaming, support
Article 6(1) (c) GDPR	compliance with a legal obligation to which we are actually subject	retention of accounting and tax records under the law of the United Kingdom, sanctions law of the United Kingdom and of the European Union
Article 6(1) (f) GDPR	legitimate interests following a documented balancing of interests	IT security, prevention of fraud and abuse, manual review of conspicuous transactions, tamper-proof logging, legal defence
Article 9(2) (f) GDPR	establishment, exercise or defence of legal claims	legal disputes in which special categories are affected

Important clarification regarding the identity check. Aurumbeam does not hold an authorisation from the Financial Conduct Authority, is not subject to its supervision and does not provide banking, financial, payment or e-money services. Aurumbeam does not accept cash payments. The conditions under which dealers in precious metals in the United Kingdom are obliged under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (cash payments of EUR 10,000 or more) are therefore not met. Payment is made exclusively by credit card; the anti-money laundering checks of the payment service provider apply in addition. We therefore do **not** base the identity check across the board on a legal obligation under Article 6(1)(c) GDPR. Aurumbeam carries out the identity check itself, predominantly as a contractual and voluntary self-commitment and for the prevention of fraud and abuse. Aurumbeam staff examine a valid official photographic identity document and compare it with the details provided; no biometric matching takes place, and no biometric data within the meaning of Article 9 GDPR are processed. Identification always takes place before any payout and delivery and before beamed quantities are allocated to the recipient. The legal basis is therefore:

- **Article 6(1)(b) GDPR**, insofar as identification is necessary for the performance of the contract. Without an established identity, we cannot allocate gold to you in the custody register, pay out the buy-back proceeds to the entitled person, make a physical delivery to the entitled person or allocate a beamed quantity with legal certainty to the entitled recipient.
- **Article 6(1)(f) GDPR**, insofar as the check additionally serves to prevent identity misuse, the takeover of other persons' accesses, multiple registrations and other abuse of the infrastructure. Our legitimate interest lies in protecting the custody holdings of all customers and in the integrity of the

infrastructure. The balancing of interests in accordance with Recital 47 is documented.

- **Article 6(1)(c) GDPR** only where a legal obligation actually exists. This is the case for the accounting and retention obligations, for screening against the sanctions lists of the United Kingdom (on the basis of the Sanctions and Anti-Money Laundering Act 2018) and of the European Union and, insofar as German VAT law applies to a supply, for the identification, recording and retention obligations which § 25c(6) UStG declares to apply accordingly to supplies of investment gold.

We take changes to the legal framework into account. Aurumbeam is aligning its processes with Regulation (EU) 2024/1624, which applies from 10 July 2027. Insofar as statutory due diligence obligations arise from it, Article 6(1)(c) GDPR in conjunction with the provisions of that Regulation will replace the bases mentioned above for those obligations. We will amend this Policy in good time and inform you accordingly.

5 Processing operations in detail

The following table describes each processing operation with the data categories, purpose, legal basis, recipients and storage period. For details of the recipients, see section 8; for supplementary information on the time limits, see section 15.

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Visiting the website and server log files	IP address, date and time of access, resource accessed, volume of data transferred, status code, referring page, browser and operating system identifier	delivery of the page, operation and stability of the systems, detection and defence against attacks	Article 6(1)(f) GDPR, Recital 49	Vercel for delivery of the website; Render for requests to the application services. Details are set out in section 8.	7 days; in the event of a documented security incident, up to 90 days
Registration and maintenance of the aurumbeam access	first name and surname, email address, telephone number, password exclusively as a hash value, custody agreement number, language setting, session and device data	creation, maintenance and securing of the aurumbeam access, provision of the app and the web application	Article 6(1)(b) GDPR	Render for application services, Supabase for the database and Vercel when the web interface is used; Resend for sending account and security emails. Details are set out in section 8.	duration of the business relationship, thereafter in accordance with the erasure policy in section 15

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Identity check by Aurumbeam, part necessary for the contract	first name and surname, date of birth, place of birth, nationality, residential address, image of the official photographic identity document, type, number and validity of the identity document, result of the check	unambiguous allocation of the gold holdings in the custody register, payout and delivery to the entitled person, allocation of beamed quantities to the entitled recipient	Article 6(1)(b) GDPR	Checks by Aurumbeam staff; Render for application services and Supabase for technical storage of documents, with Vercel also handling transmission when the web interface is used. Details are set out in section 8.	result of the check and verified master data for the duration of the business relationship and thereafter 5 years; identity document images are deleted upon completion of the check, at the latest 30 days thereafter
Identity check, abuse prevention component	result of the check, security features of the document, status reports on irregularities	prevention of identity misuse, takeover of other persons' accesses and multiple registrations	Article 6(1)(f) GDPR	no disclosure; check carried out by Aurumbeam staff	duration of the business relationship and thereafter 5 years
Purchase processing	order data, product designation, quantity in grams of fine gold, price, mark-up, processing fee, time, invoice data	conclusion and performance of the purchase contract, invoicing	Article 6(1)(b) GDPR	payment service provider, provider of the invoicing and accounting software, tax advisers	10 years as accounting record
Payment processing by credit card	tokenised card data, amount, payment status, result of strong customer authentication, payment reference, chargeback data	charging the purchase price to the credit card, charging the transfer fee where you choose this method of collection, handling of chargebacks	Article 6(1)(b) GDPR	Worldpay (UK) Limited as processor and, for its own legal obligations, as independent controller; card schemes and card-issuing banks as independent controllers	10 years, insofar as an accounting record

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Maintenance of the custody register	custody agreement number, allocated items with their markings, co-ownership shares in fractional shares, entries and withdrawals, unallocated transfer holdings, timestamps	documentation and proof of the allocation of sole ownership and co-ownership, performance of the custody agreement	Article 6(1)(b) GDPR	SOOS GmbH (Goldvorsorge, GVS Bullion Group), Vienna, as custodian, insofar as necessary for maintaining the holdings; Render for application services and Supabase for the database. Details are set out in section 8.	duration of the business relationship and thereafter 10 years, followed by erasure or an onymisation of the allocation data
Beaming (transfer of gold holdings), processing	identifiers of the transferor and of the recipient, beamed quantity, euro equivalent, transfer fee and selected method of collection, time, status of the claim, optional message	execution of the beam order, maintenance of unallocated transfer holdings, allocation to the recipient upon claim, compliance with the amount limits	Article 6(1)(b) GDPR	Render for application services and Supabase for the database, with Vercel also involved when the web interface is used. Details are set out in section 8.	10 years
Beaming, display of the other party	custody agreement number, first name and abbreviated surname of the respective other party, beamed quantity of fine gold in grams, time; the full name of the other party appears only in the tax records export	traceability for both parties involved, protection against erroneous transfers, proof of the transfer	Article 6(1)(f) GDPR	the respective other customer involved in the beaming	10 years
Buy-back and payout	order data, quantity bought back, markdown, buy-back price, processing fee, payout amount, bank details, payout record	processing of the buy-back and of the payout by bank transfer to a bank account held in your name	Article 6(1)(b) GDPR	Aurumbeam's credit institution for payouts, provider of the invoicing and accounting software	10 years as accounting record

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Physical delivery and shipping	name, delivery address, telephone number, email address, tracking number, shipment status, selected insurance level, declared value	packaging, insured and registered shipping to the verified delivery address, shipment tracking, proof of delivery, claims handling	Article 6(1)(b) GDPR	SOOS GmbH (Goldvorsorge, GVS Bullion Group), Vienna, as processor for delivery data; shipping service providers and transport insurers, each as independent controller	10 years for shipping and delivery records
Purchase of goods sent in, contractual part	description of material, weight, fineness, analysis and test result, purchase price, processing fee, payout data, return shipment data	conclusion and performance of the purchase contract	Article 6(1)(b) GDPR	refinery or testing body as processor, Aurumbeam's credit institution for payouts	10 years as accounting record
Purchase of goods sent in, identification of the sender	first name, surname, date of birth, designation and number of a photographic identity document	establishing the sender's entitlement, preventing the purchase of lost or stolen goods, proof in the purchase record	Article 6(1)(b) and (f) GDPR	authorities only where there is a legal obligation	10 years as part of the purchase record
Recurring purchases	purchase amount or target product, interval, start and end, execution dates, charge attempts and their result, status active or dormant, tokenised reference to the stored credit card	setting up and carrying out recurring purchases with a fixed amount and towards a target product, charging the stored credit card on each execution date	Article 6(1)(b) GDPR	payment service provider	tokenised card reference until the recurring purchase ends or the card is removed; data on recurring purchases and executions 10 years
Customer communication and support	master data, content of your enquiry, attachments, communication history, case number, channel	handling of and responding to your matters, traceability of the case	Article 6(1)(b) GDPR	Render for application services and Supabase for the support inbox, with Vercel also involved when the web interface is used. Details are set out in section 8.	3 years after closure of the case

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Complaints handling	subject matter of the complaint, custody agreement number or order number, statement of facts, review notes, decision and reasons	review, response and remedy within the promised time limit, participation in dispute resolution proceedings	Article 6(1)(b) GDPR	dispute resolution body only if proceedings are initiated, legal advisers	3 years after closure of the case
Prevention of fraud and abuse	IP address, device characteristics, login and session history, history of changes to security-relevant access data, transaction patterns in purchases, sales back to Aurumbeam and beaming, review notes	detection of and defence against fraud, takeover of other persons' accesses, automated attacks and abuse of the infrastructure; manual review of conspicuous transactions by staff	Article 6(1)(f) GDPR, Recitals 47 and 49	IT security service providers as processors, where used	login and session history 12 months; cases of irregularity until resolved and thereafter 3 years
Sanctions list screening	first name, surname, date of birth, nationality, state of residence, match status, review note	compliance with the prohibitions on making available and the asset freezes in respect of listed persons and entities under the sanctions lists of the European Union and of the United Kingdom	Article 6(1)(c) GDPR in conjunction with the directly applicable sanctions regulations of the European Union, in particular Article 2 of Regulation (EU) No 269/2014, and the sanctions provisions of the United Kingdom on the basis of the Sanctions and Anti-Money Laundering Act 2018; insofar as any of these provisions does not establish a legal obligation under the applicable data protection law, Article 6(1)(f) GDPR	service provider for list screening as processor, competent authorities in the event of a confirmed match	review notes without a match 12 months, documented matches 5 years

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Eventdriven screening for politically exposed persons and adverse media	result of the screening (passed or not passed) and the associated review note	prevention of abuse and protection of the custody holdings, only where there are specific risk indicators in the individual case; no regular or blanket screening takes place; data relating to criminal convictions and offences are not processed systematically and only insofar as permitted by Article 10 GDPR and, in the United Kingdom, Article 10 UK GDPR in conjunction with section 10 of and Schedule 1 to the Data Protection Act 2018	Article 6(1)(f) GDPR	no disclosure; screening carried out by Aurumbeam staff	duration of the business relationship and thereafter 5 years
Accounting and retention for tax purposes	invoice and credit note data, turnover, payment allocation, master data, tax identifiers	compliance with accounting, invoicing, tax and retention obligations	Article 6(1)(c) GDPR in conjunction with the obligations to keep and retain accounting records under sections 386 to 388 of the Companies Act 2006 and the tax law of the United Kingdom; insofar as the period goes beyond this, Article 6(1)(f) GDPR	provider of the invoicing and accounting software, tax advisers, auditors, tax authorities where there is a legal obligation	10 years
Newsletter and product information	email address, form of address and name where provided, time of registration and confirmation, IP address at registration, open and click data	sending product information and notices of promotions, measuring the success of mailings	Article 6(1)(a) GDPR, supplemented in Germany by § 7(2) No. 2 UWG, in Austria by § 174 TKG 2021, in Switzerland by Art. 3(1)(o) UWG, in the United Kingdom by regulation 22 PECR	service provider for sending emails as processor	until withdrawal, thereafter only inclusion in a suppression list with minimal data
Push notifications on transactions and security events	push token, device identifier, operating system version, type of event	delivery of the notifications you have requested on purchase, buy-back, beaming, delivery, login and security-relevant changes	Article 6(1)(b) GDPR; for storing and reading information on the terminal device, § 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021 and regulation 6(4) PECR	Apple Distribution International Ltd. via the Apple Push Notification service, Google Ireland Ltd. via Firebase Cloud Messaging	until the notifications are deactivated or the app is uninstalled
Push notifications with promotional content	push token, interaction data relating to the message	information about products and promotions	Article 6(1)(a) GDPR; for storing and reading information on the terminal device, § 25(1) TDDDG, § 165(3) TKG 2021 and regulation 6 PECR	Apple Distribution International Ltd., Google Ireland Ltd.	until withdrawal

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Audience measurement in the app and on the web	pseudonymous identifier, pages and views accessed, length of stay, referring page, truncated IP address, device type, screen resolution, language	analysis of usage, improvement of structure and content	Article 6(1)(a) GDPR; for storing and reading information on the terminal device, § 25(1) TDDDG, § 165(3) TKG 2021 and regulation 6 PECR	analytics service providers as processors, primarily with processing in the European Union	14 months, thereafter erasure or aggregation without personal reference
Affiliate programme, relationship with the partner	partner master data, tax and bank details of the partner, proof of referrals, remuneration statements	performance of the partner agreement, settlement of remuneration	Article 6(1)(b) GDPR	Aurumbeam's credit institution for payouts, provider of the invoicing and accounting software, tax advisers	10 years as accounting record
Affiliate allocation for the referred prospective customer	partner identifier, time of access, allocation identifier on the terminal device	allocation of a referral to the referring partner	Article 6(1)(a) GDPR; for storing and reading information on the terminal device, § 25(1) TDDDG, § 165(3) TKG 2021 and regulation 6 PECR	service provider for partner management as processor	allocation identifier 30 days, the resulting proof of referral 10 years
Measuring the advertising success of campaigns	campaign measurement identifier on the terminal device, time of access, associated registration or associated purchase	allocation of registrations and purchases to an advertising measure	Article 6(1)(a) GDPR; for storing and reading information on the terminal device, § 25(1) TDDDG, § 165(3) TKG 2021 and regulation 6 PECR	analytics service providers as processors	identifier 90 days
Testing of design variants of the user interface (A/B test)	identifier for evaluating test variants, assigned variant, interaction data	comparison of two design variants, improvement of user guidance	Article 6(1)(a) GDPR; for storing and reading information on the terminal device, § 25(1) TDDDG, § 165(3) TKG 2021 and regulation 6 PECR	analytics service providers as processors	identifier 6 months

PROCESSING OPERATION	DATA CATEGORIES	PURPOSE	LEGAL BASIS WITH PROVISION	RECIPIENTS	STORAGE PERIOD
Applications	contact details, CV, references, details of professional career, salary expectations, correspondence, notes from interviews	conducting the application process and deciding on recruitment	Article 6(1)(b) GDPR as a pre-contractual measure	no recipients beyond the processors used for hosting and sending emails; access only for the persons involved in the process	6 months after conclusion of the process; longer storage in a pool of applicants only with your consent under Article 6(1)(a) GDPR for 12 months
Logging in the closed logging system	custody agreement number as technical identifier, quantity, timestamp, transaction identifier	tamper-proof and traceable logging of movements in holdings	Article 6(1)(f) GDPR	Aurumbeam manages the business register and bookkeeping operations; Render provides application services and Supabase provides the database. Details are set out in section 8.	log entries remain unchanged for the term of the contract and the retention periods; thereafter the allocation data are erased or anonymised in accordance with section 6
Establishment and defence of legal claims	all data required for the respective subject matter of the dispute	enforcement of our own claims, defence against claims, preservation of evidence	Article 6(1)(f) GDPR; for special categories, Article 9(2)(f) GDPR	lawyers, courts, insurers, debt collection service providers	until final conclusion plus the relevant limitation period

Obligation to provide data. The details relating to registration, identity, payment and delivery address are required for the conclusion and performance of the contract. Without these details, we cannot activate an aurumbeam access, execute a purchase, make a payout or arrange a delivery. The details relating to the newsletter, promotional push notifications, audience measurement, campaign measurement, testing of design variants and affiliate allocation are voluntary; refusing them has no disadvantages for the use of the infrastructure.

Data from other sources. In three cases we do not receive data from you yourself but from other sources, and we inform you of this in accordance with Article 14 GDPR: results of screening against publicly available sanctions lists of the European Union and of the United Kingdom, details about you from a beam order that another customer places in your favour, and details from the partner and affiliate programme where a partner transmits data on prospective customers. The information is provided within one month of obtaining the data, at the latest at the time of the first communication to you.

6 Logging system and data protection

6.1 What is stored and what is not

Movements in holdings are additionally recorded in a closed, access-restricted logging system. The application services run on Render in the selected Frankfurt service region. The associated register and bookkeeping data are stored in the managed PostgreSQL database on Supabase in Frankfurt. Aurumbeam manages the business register and bookkeeping operations; Render and Supabase provide the technical infrastructure. Details are set out in section 8. The logging system is not a public blockchain. There are no tokens, no wallets and no keys held by customers. Solely the custody register is authoritative for the allocation of your gold; the logging system merely reflects it subsequently and does not establish any independent rights.

Only the following are stored in the log: the custody agreement number as technical identifier, the quantity in grams of fine gold, the timestamp and a transaction identifier. The following are not stored: name, address, email address, telephone number, date of birth, identity document data, bank details, payment data and any documents from the identity check.

The log entries are **not** anonymous. The technical identifier is a pseudonym and, under Article 4(5) GDPR, remains personal data as long as it can be attributed to a person by means of additional information. This additional information is exclusively the allocation in the custody register outside the logging system. It is stored in encrypted form, access is restricted to the roles authorised for this purpose and key management is documented.

6.2 Rectification and erasure

Rectification under Article 16 GDPR. A log entry is not altered. We rectify an inaccurate entry by means of a correcting subsequent entry; the authoritative position is derived from the custody register, which is rectified directly.

Erasure under Article 17 GDPR. Register and log entries are neither altered nor erased during the term of the contract and the retention periods under section 15; audit security is maintained by means of reversing entries. After expiry of the retention periods and upon a justified request for erasure that is not precluded by any retention obligation or legal claim, we erase the link between the technical identifier and your person, destroy the associated key material and erase all identifying data outside the logging system. The remaining log entries can thereafter no longer be attributed to any person by means reasonably likely to be used and are therefore anonymised (Article 5(1)(e) GDPR).

6.3 Guidelines of the European Data Protection Board and limits

We align the logging system with Guidelines 02/2025 of the European Data Protection Board on the processing of personal data through blockchain technologies, in the final version 2.0 of 7 July 2026. According to these: hash values, including salted hash values, remain personal data and do not constitute anonymisation. Upon a request for erasure, the data stored in the log must be effectively anonymised and all identifying data outside the log must be erased. The procedure described in section 6.2 achieves both. Personal data are not stored in the log in plain text.

The limits of this model are:

1. The log entries themselves are not erased. What is erased is the link to your person.
2. The logging system is not publicly accessible. Aurumbeam manages the business operations; the technical services used for this purpose are listed in section 8. The risk of a third party restoring the personal reference is therefore low. The architecture is documented and assessed in the record of processing activities and in the data protection impact assessment under Article 35 GDPR.
3. There is no right to data portability under Article 20 GDPR in respect of the log entries, because the logging is based on Article 6(1)(f) GDPR. By contrast, we provide you with the underlying holding and transaction data from the custody register in a structured, commonly used and machine-readable format.

---

7 Identity check, prevention of money laundering and data subject rights

7.1 Legal bases

The differentiated legal bases for the identity check are set out in section 4 and shown for each processing operation in the table in section 5. In summary: the check is based on Article 6(1)(b) GDPR insofar as it is necessary for the performance of the contract, on Article 6(1)(f) GDPR insofar as it serves to prevent abuse, and on Article 6(1)(c) GDPR only where a legal obligation actually exists. No biometric matching takes place. No biometric data within the meaning of Article 9 GDPR are processed. There is no blanket reliance on an obligation under anti-money laundering law.

7.2 Data minimisation and purpose limitation

The identity check is carried out by Aurumbeam staff themselves. They examine a valid official photographic identity document and compare it with the details provided. Aurumbeam performs the substantive review. The application and database services listed in section 8 handle technical transmission and storage; Vercel is also involved when the web interface is used. Identity document images are deleted upon completion of the check, at the latest 30 days thereafter; the result of the check and the verified master data are retained. Until deletion, the identity document images are stored in encrypted form and are accessible only to the staff entrusted with the check. Biometric comparison features are not processed. Details on identity documents that are not required are not collected or are redacted.

We use data that we process for the identity check, for the prevention of abuse or for sanctions list screening exclusively for these purposes. They are not used for advertising, for product recommendations, for creditworthiness assessments or for any other commercial evaluation. The data sets are technically separated and access rights are assigned on a role basis.

7.3 Retention periods in connection with the identity check

DOCUMENT	PERIOD	BASIS
Result of the check and verified master data held by Aurumbeam	duration of the business relationship and thereafter 5 years	Article 6(1)(f) GDPR for the defence against claims
Identity document images	deletion upon completion of the check, at the latest 30 days thereafter	Article 5(1)(c) and (e) GDPR
Identity document data in the purchase record	10 years as part of the purchase record	Article 6(1)(c) and (f) GDPR in conjunction with the retention periods for accounting records under section 15
Documented sanctions list matches	5 years	Article 6(1)(c) GDPR in conjunction with the sanctions law of the European Union and of the United Kingdom
Identification records, insofar as German VAT law applies to a supply	in accordance with the periods declared to apply accordingly by § 25c(6) UStG	Article 6(1)(c) GDPR
Records from 10 July 2027, insofar as Aurumbeam falls within the scope of Regulation (EU) 2024/1624	5 years from the end of the business relationship or the execution of the transaction; extension by a maximum of 5 further years only upon order of an authority; thereafter erasure	Article 77 of Regulation (EU) 2024/1624

7.4 Restriction of data subject rights and prohibition of disclosure

Aurumbeam is not an obliged entity under anti-money laundering law. We therefore restrict data subject rights only where, in the individual case, there is a specific statutory, regulatory or judicial basis for doing so, in particular under sanctions law or under an order of an authority or court prohibiting us from making a disclosure. The legal basis for such a restriction is, in the United Kingdom, the Data Protection Act 2018, in particular Schedule 2 to it, and, insofar as the GDPR applies, Article 23(1)(d) and (e) GDPR in conjunction with the relevant provision in each case. This may affect your right of access under Article 15, your right to erasure under Article 17, your right to restriction under Article 18 and your right to object under Article 21.

Should Aurumbeam in future become an obliged entity under anti-money laundering law, for instance under Regulation (EU) 2024/1624, which applies from 10 July 2027, the provisions then in force may oblige us to report certain matters to the competent financial intelligence unit and not to inform you of such a report, of any subsequent proceedings or of information requests from authorities. Only from the point at which we acquire such a status will we respond to access requests in this area with identically worded, standardised notices, so that no inference can be drawn from our response as to whether a report has been made in a specific case. We will amend this Policy beforehand.

As soon as a restriction ceases to apply, we will provide full access upon request. Your right to lodge a complaint with a supervisory authority remains unaffected in all cases.

8 Processors and recipients

We disclose your data only insofar as this is necessary for the purposes described. The following table identifies the technical services used and their tasks. The selected service region describes the application, database or sending location; it does not cover all processing by the platform provider.

CATEGORY	RECIPIENT	REGISTERED OFFICE AND PLACE OF PROCESSING	ROLE
Application services and background processing	Render	Selected service region: Frankfurt, Germany. The region selection does not restrict all processing by the platform provider to this location.	Technical operation of the API and background services of the aurumbeam platform.
Database	Supabase	Selected database region: Frankfurt, Germany. The region selection is not a commitment that all platform data is processed exclusively in Germany.	Operation of the managed PostgreSQL database for customer, register, bookkeeping, document and support data.

CATEGORY	RECIPIENT	REGISTERED OFFICE AND PLACE OF PROCESSING	ROLE
Website and web interface	Vercel	Frankfurt, fra1, is configured for server-side functions. Delivery and platform operations are not restricted exclusively to this region.	Delivery of the website and web interface and technical forwarding of their requests to the application services. Native app requests go directly to the application services on Render.
Transactional email delivery	Resend	Selected sending region for the domain: Ireland, eu-west-1. According to the provider, account data including email metadata, logs and API records is stored in the United States regardless of the sending region.	Delivery of account and security emails, involving recipient addresses, message content and technical delivery data.
Payment processing by credit card	Worldpay (UK) Limited, The Walbrook Building, 25 Walbrook, London EC4N 8AF, United Kingdom	United Kingdom; an adequacy decision of the European Commission exists for transfers from the European Union	processor for the processing of credit card payments and chargebacks; independent controller for the fulfilment of its own legal obligations, in particular its own anti-money laundering checks
Custody, delivery and shipping	SOOS GmbH (Goldvorsorge, GVS Bullion Group), Handelskai 94-96, Stiege 4, 5. OG, 1200 Vienna, Austria, Firmenbuch (Austrian Companies Register) FN 371831k	Austria	processor for delivery data. Custody of the holdings, placing into and removal from storage, reconciliation of holdings, insured and registered shipping. GVS Austria GmbH, likewise part of the GVS Bullion Group, may perform processing tasks for SOOS GmbH. Details at aurumbeam.com/verwahrdienste
Delivery of push notifications	Apple Distribution International Ltd. (Apple Push Notification service), Google Ireland Ltd. (Firebase Cloud Messaging)	Ireland, with processing in the United States of America, see section 9	processor or independent controller, as the case may be, for the operation of the delivery services

Further recipients by category. In addition, we use service providers for sending emails, customer service and ticketing, invoicing and accounting, audience measurement, campaign measurement and testing of design variants (only with your consent), partner management in the affiliate programme, technical screening against the sanctions lists of the European Union and of the United Kingdom, IT security, and for the testing, analysis and valuation of goods sent in for purchase (refinery). Independent controllers are the credit institution through which we make payouts in the case of sales back to Aurumbeam, purchases of precious metals sent in and partner remuneration; the

shipping service providers and transport insurers that transport, deliver and insure shipments; the card scheme of your credit card and your card-issuing bank; tax advisers, auditors and legal advisers; and the testing body independent of Aurumbeam and of the custodian that carries out the verification of holdings; they are bound to confidentiality by professional rules or by contract. Authorities and courts, in particular the Information Commissioner's Office, tax, sanctions and law enforcement authorities and enforcement bodies, receive data as independent controllers only where there is a legal obligation.

Aurumbeam performs the substantive identity review itself. The data processed technically for that purpose passes through the application and database services listed in this table; Vercel is also involved when the web interface is used.

We will provide you with an up-to-date list of the processors used, including sub-processors, upon request to datenschutz@aurumbeam.com.

9 Transfers to third countries

Aurumbeam London Ltd processes your data as controller in the United Kingdom. Frankfurt regions are selected for application services on Render and the database on Supabase. The website and web interface are provided through Vercel. The sending region selected for email delivery through Resend is Ireland, eu-west-1; according to the provider, account data including email metadata, logs and API records is stored in the United States. A selected service, database or sending region does not mean that all data is processed exclusively in Germany or the European Union.

United Kingdom. For the transfer of personal data from the European Union and the European Economic Area to the United Kingdom, there is an adequacy decision of the European Commission under Article 45 GDPR. It was renewed on 19 December 2025 and is valid until 27 December 2031. Under Swiss law, the United Kingdom is recognised as a state with an adequate level of data protection.

Insofar as personal data are transferred to other countries, this takes place only subject to the conditions of Articles 44 to 49 UK GDPR and, where applicable, Articles 44 to 49 GDPR.

RECIPIENT AND PURPOSE	THIRD COUNTRY	BASIS FOR THE TRANSFER
Aurumbeam London Ltd as controller	United Kingdom	adequacy decision of the European Commission under Article 45 GDPR, renewed on 19 December 2025, valid until 27 December 2031; for data from Switzerland, recognition as a state with an adequate level of data protection

RECIPIENT AND PURPOSE	THIRD COUNTRY	BASIS FOR THE TRANSFER
Apple Push Notification service for the delivery of notifications to devices running iOS and iPadOS. The device token and the message content are transferred	United States of America, with processing of certain functions in the European Union	under the GDPR, primarily the adequacy decision of the European Commission of 10 July 2023 on the EU-US Data Privacy Framework under Article 45 GDPR and, under the law of the United Kingdom, its UK Extension, in each case insofar as the recipient is certified; additionally and in the alternative, standard contractual clauses under Article 46(2)(c) GDPR in the version of Implementing Decision (EU) 2021/914, for the United Kingdom together with the International Data Transfer Addendum of the Information Commissioner
Google Firebase Cloud Messaging for the delivery of notifications to devices running Android. The registration token, device identifiers and the message content are transferred	United States of America, with processing of certain functions in the European Union	as above
Recipients in Switzerland, for instance delivery services for deliveries to Switzerland	Switzerland	adequacy decision of the European Commission under Article 45 GDPR; under the law of the United Kingdom, Switzerland is likewise regarded as a state with an adequate level of protection

Certification status. Before the transfer begins and at least annually thereafter, we check whether a recipient in the United States is certified under the EU-US Data Privacy Framework and its UK Extension by reference to the public list at dataprivacyframework.gov. If a certification lapses, the agreed standard contractual clauses apply and we reassess the continuation of the transfer.

Transfer Impact Assessment. For each transfer on the basis of standard contractual clauses, we carry out an assessment of the legal situation in the recipient country in accordance with Recommendations 01/2020 of the European Data Protection Board, document it and repeat it in the event of material changes. Supplementary measures for the push services are in particular: encryption of the transmission, omission of any confidential content in the message text, and restriction of the data transferred to what is technically necessary for delivery. For this reason, our notifications contain no amounts, no information on holdings and no access data, but only a general notice that an event has occurred.

Switzerland. For transfers subject to the Swiss Federal Act on Data Protection, we use the version of the standard contractual clauses recognised by the Swiss Federal Data Protection and Information Commissioner, with the necessary adaptations under Art. 16(2) DSG, in particular the reference to the DSG, the competence of the Commissioner and the inclusion of data of legal persons.

You may obtain a copy of the agreed safeguards upon request to datenschutz@aurumbeam.com. We redact trade secrets and personal data of third parties in doing so.

10 Cookies, SDKs and similar technologies

10.1 Legal framework

The storing of information on your terminal device and access to information already stored there are governed, in the United Kingdom, by regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and, in the European Union and in Liechtenstein, by Article 5(3) of Directive 2002/58/EC as amended by Directive 2009/136/EC in its respective national implementation. These provisions apply irrespective of whether the information is personal data, and they apply in a technology-neutral manner, including in apps and not only in the browser.

COUNTRY	PROVISION	REQUIREMENT
Germany	§ 25(1) of the Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG, Telecommunications Digital Services Data Protection Act), which has been the authoritative title of this Act since 14 May 2024; the numbering of the sections has remained unchanged	consent on the basis of clear and comprehensive information. Exceptions under § 25(2): sole purpose of carrying out the transmission of a communication, or strict necessity for a service explicitly requested by you
Austria	§ 165(3) TKG 2021	a separate obligation to provide information on the data processed, the legal basis, the purposes and the storage period, and in addition **actively** given consent. Continuing to browse or scrolling is not sufficient. The same two exceptions as in Germany
Switzerland	Art. 45c of the Fernmeldegesetz (FMG, Swiss Telecommunications Act, SR 784.10)	no obligation to obtain prior consent. Processing data on third-party devices is permitted if it is indispensable for the transmission or display of the requested information, or if information is provided on the processing and its purpose and on the possibility of refusal. The information obligation under Art. 19 DSG continues to apply
Liechtenstein	national implementation of Directive 2002/58/EC by virtue of the Agreement on the European Economic Area	consent, in substance as in Germany and Austria
United Kingdom	regulation 6 PECR	consent on the basis of clear and comprehensive information. Exceptions under regulation 6(4): sole purpose of carrying out the transmission of a communication, or strict necessity for a service explicitly requested by you

Notice for users in Switzerland. Switzerland thus has an opt-out model and no obligation to obtain prior consent. We nevertheless apply the stricter consent model uniformly. Accordingly, in Switzerland too you can decide in advance and change your selection at any time. With this section, we inform you of the processing, its purposes and the possibility of refusal within the meaning of Art. 45c(b) FMG and Art. 19 DSG.

Two-tier model. Storing and reading information on your terminal device is governed by the above provisions. The subsequent processing of the personal data read requires an additional legal basis under Article 6 GDPR. Both levels are shown in the following table. For users in the United Kingdom, regulation 6 PECR applies in every row in place of § 25 TDDDG and § 165(3) TKG 2021: where the table refers to § 25(2) TDDDG, the exception under regulation 6(4) PECR applies; otherwise, consent under regulation 6(1) and (2) PECR applies. For technologies requiring consent, we do not rely on a legitimate interest.

10.2 Cookie table

CATEGORY	TECHNOLOGY AND CONTENT	PURPOSE	STORAGE PERIOD	LEGAL BASIS
Strictly necessary	session cookie with session identifier	maintaining the login, allocating requests to the session	session; deleted when the browser is closed	§ 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021, Art. 45c(a) FMG; for the processing, Article 6(1)(b) GDPR
Strictly necessary	security token against cross-site request forgery	protection of forms and orders against manipulation	session	§ 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021; for the processing, Article 6(1)(f) GDPR
Strictly necessary	cookie for server allocation in load balancing	even distribution of requests, stability	session	§ 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021; for the processing, Article 6(1)(f) GDPR
Strictly necessary	cookie for storing your selection in the consent banner	proof and implementation of your decision, avoidance of repeated requests	6 months	§ 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021; for the processing, Article 6(1)(f) GDPR in conjunction with the obligation to demonstrate consent under Article 7(1) GDPR
Strictly necessary	cookie for the purchase order after active selection of a product	retaining the selection until the order is completed	session	§ 25(2) No. 2 TDDDG, § 165(3) last sentence TKG 2021; for the processing, Article 6(1)(b) GDPR
Functional	cookie for language and region selection	displaying the user interface in the selected language and currency	12 months	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR
Functional	cookie for display settings, for instance display mode, table view, chart period	retaining your settings beyond the session	12 months	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR
Functional	loading of embedded external content, for instance maps or videos	displaying external content only after your approval	session up to 12 months, depending on the provider	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR

CATEGORY	TECHNOLOGY AND CONTENT	PURPOSE	STORAGE PERIOD	LEGAL BASIS
Statistics	pseudonymous audience measurement identifier, pages and views accessed, length of stay, referring page, truncated IP address, device type	analysis of usage, detection of errors in user guidance, improvement of content	14 months	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR
Statistics	identifier for evaluating test variants of the user interface (A/B test)	comparison of two design variants	6 months	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR
Marketing	allocation identifier of the partner and affiliate programme	allocation of a referral to the referring partner, settlement of remuneration	30 days	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR
Marketing	identifier for measuring the advertising success of campaigns	allocation of registrations and purchases to an advertising measure	90 days	§ 25(1) TDDDG, § 165(3) TKG 2021; for the processing, Article 6(1)(a) GDPR

Session recording, heatmaps, cross-device profiling and the sale of usage data to third parties do not take place. We do not use a device-based advertising identifier.

10.3 Requirements for the consent banner

Our consent banner meets the following requirements:

1. On the first level, the buttons for rejecting and for accepting are placed side by side with equal prominence: the same size, the same design, the same contrast, the same number of clicks. All non-essential technologies can be rejected with a single click.
2. There are no pre-ticked boxes. Silence, scrolling and continuing to browse do not constitute consent.
3. The selection is separated by purpose: strictly necessary, functional, statistics, marketing. Strictly necessary technologies cannot be deselected because they are permitted without consent; this is explained in the banner.
4. Already on the first level, we state the categories of data processed, the legal basis, the purposes and the storage period. In doing so, we also fulfil the separate information obligation under § 165(3) first sentence TKG 2021.
5. There is no design that pushes you towards consent, no misleading colour contrasts, no hidden links and no additional effort required for rejecting.
6. Access to aurumbeam.com does not depend on your consent. We do not use a cookie wall in the event of rejection.

7. We log your decision with the time, the version of the banner, the version of the texts, the purposes selected and a technical identifier, in order to be able to demonstrate consent under Article 7(1) GDPR.
8. We ask again after 6 months and upon every material change to the technologies used.

10.4 Withdrawal and change of your selection

You may withdraw your consent at any time with effect for the future. Withdrawing consent is as easy as giving it (Article 7(3) GDPR):

- on the website via the permanently accessible link “Cookie Settings” in the footer of every page,
- in the app under “Settings”, sub-item “Privacy”,
- additionally, informally by message to datenschutz@aurumbeam.com.

The lawfulness of the processing carried out until withdrawal remains unaffected. In addition, you can delete cookies and prevent them from being set via the settings of your browser. If strictly necessary cookies are blocked, logging in and placing orders are not possible.

11 Specific information on the aurumbeam app

11.1 Permissions

The app requests permissions only when the associated function is used and explains the purpose beforehand. You can revoke any permission at any time in the system settings of your device.

PERMISSION	WHAT WE NEED IT FOR	CONSEQUENCE OF REFUSAL
Camera	capturing the identity document as part of the identity check, scanning order codes	the identity check is then only possible via the web browser or by uploading existing images
Photo library	selecting existing images for the identity check or for a purchase of precious metals sent in	you can instead capture files directly or upload them via the web application
Notifications	delivery of notices on transactions, logins and security-relevant events	you will then receive these notices only by email and in the app
Unlocking via device authentication (fingerprint or facial recognition of the operating system)	convenient and secure unlocking of the app via device authentication	the app is then unlocked exclusively with password and second factor

Important distinction. Unlocking via the fingerprint or facial recognition of your device is carried out exclusively by the operating system on the device. Aurumbeam receives no biometric data in this process, only the response as to whether unlocking was successful. This local device authentication must be

strictly distinguished from the identity check, which is carried out by Aurumbeam staff as an examination of the official photographic identity document and comparison with the details provided; no biometric matching takes place, and no biometric data within the meaning of Article 9 GDPR are processed.

The app does not collect location data. It does not access contacts, calendar, microphone or telephone functions.

11.2 Push notifications

For the delivery of notifications, a device token or a registration token, as the case may be, and the message content are transmitted to the Apple Push Notification service or to Google Firebase Cloud Messaging. The token is a pseudonymous identifier that is linked to your aurumbeam access and is therefore personal data. For the legal bases, see section 5; for transfers to third countries, see section 9.

Notifications contain no amounts, no information on holdings, no access data and no details of individual products, but only a general notice of an event. You see the details only after logging in to the app. You can deactivate transaction and security notifications and notifications with promotional content separately from each other in the app.

The analytics module within the messaging service used is deactivated. Automatic initialisation of analytics functions when the app is started is switched off; analytics functions are only activated after your consent.

11.3 Device identifiers and access to the terminal device

The app stores on your device a randomly generated installation identifier, the login credentials in the secure storage area of the operating system, your privacy selection and display settings. The same rules apply to storage and access as to cookies, namely regulation 6 PECR, § 25 TDDDG and § 165(3) TKG 2021. When first started, the app therefore displays the same consent dialogue as the website, with an equivalent option to refuse.

The installation identifier is not the advertising identifier of the operating system and is not disclosed to third parties for advertising purposes. It is deleted when the app is uninstalled.

11.4 App Tracking Transparency

Aurumbeam does not carry out cross-device advertising tracking. We use neither Apple’s advertising identifier nor Android’s advertising ID, and we do not combine your data with data of third parties for advertising purposes. A dialogue under the App Tracking Transparency framework is therefore not displayed, because no tracking requiring permission within the meaning of this framework takes place. Should this change, we will obtain, before any such processing, both permission via the operating system dialogue and consent under Article 6(1)(a) GDPR. Permission in the system dialogue does not replace consent under data protection law.

11.5 Information in the app stores

In the Apple App Store, we maintain the app privacy details (Privacy Nutrition Labels) with the data types collected, their purpose and their linkage to your person. For the aurumbeam app, these are in particular contact information, financial information, identifiers, purchases, usage data and diagnostics. The category “Data Used to Track You” is not populated, because no advertising tracking takes place. The app and the integrated software libraries maintain a Privacy Manifest containing the information on data types collected and the justification for the use of the interfaces that require a justification.

On Google Play, we maintain the data safety section with the same information on data types collected and shared, the purposes, encryption in transit and the option of deletion.

The information in both stores is congruent with this Privacy Policy. If store information temporarily deviates following an update, this Policy is authoritative.

Deletion of the aurumbeam access. You can have your aurumbeam access deleted directly in the app under “Settings”, sub-item “Access”. Without installing the app, deletion is also possible via the deletion page on aurumbeam.com, which can be accessed without logging in; deletion is carried out as soon as your identity has been confirmed. We acknowledge receipt, settle any outstanding holdings at your choice by sale back to Aurumbeam, physical delivery or beaming to another customer, and then delete your data. Data for which a statutory retention obligation exists are blocked from further use and deleted only after the period has expired; which data these are is set out in section 15.

12 Your rights

12.1 Overview

You have the following rights under the UK GDPR and, insofar as the GDPR applies, the same rights under the GDPR. The rights under the Swiss DSG are listed in the last row; details of all rights are contained in the document “GDPR: Your Rights and How to Exercise Them”.

RIGHT	PROVISION	CONTENT AND TIME LIMIT
Access	Article 15 GDPR	information about the data processed and the circumstances of the processing, and a first copy free of charge. Response within one month; in the case of complexity or a large number of requests, extension by up to two further months with an interim notice within the first month

RIGHT	PROVISION	CONTENT AND TIME LIMIT
Rectification	Article 16 GDPR	rectification of inaccurate data and completion of incomplete data, without undue delay
Erasure	Article 17 GDPR	erasure, without undue delay, unless an exception under Article 17(3) GDPR applies, in particular statutory retention obligations (point (b)) and the establishment, exercise or defence of legal claims (point (e))
Restriction	Article 18 GDPR	restriction of processing, for instance while a request for rectification or an objection is being examined
Notification to recipients	Article 19 GDPR	we communicate rectifications, erasures and restrictions to all recipients to whom the data have been disclosed, and inform you of these recipients upon request
Data portability	Article 20 GDPR	provision of the data that you have provided to us and that we process by automated means on the basis of consent or a contract, in a structured, commonly used and machine-readable format; upon request, direct transmission to another controller
Objection	Article 21 GDPR	objection to processing based on Article 6(1)(f) GDPR on grounds relating to your particular situation; objection to direct marketing without giving reasons and always effective
Automated decisions	Article 22 GDPR	see section 14
Withdrawal of consent	Article 7(3) GDPR	at any time with effect for the future, as easy as giving consent
Complaint	Article 77 UK GDPR and GDPR	to the Information Commissioner's Office or to a supervisory authority in the European Union or in Liechtenstein, see section 13
Judicial remedy	Article 79 UK GDPR and GDPR	proceedings before the courts in the United Kingdom or, insofar as the GDPR applies, before the courts of the state of your habitual residence (Article 79(2) GDPR)
Compensation	Article 82 GDPR	compensation for material or non-material damage
Access under Swiss law	Art. 25 et seq. DSG	in principle free of charge; response generally within 30 days (Art. 25(7) DSG in conjunction with Art. 18(1) DSV)

Information on your right to object under Article 21 GDPR

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data which is

based on Article 6(1)(f) GDPR. This concerns in particular the prevention of fraud and abuse, the server log files, logging in the logging system and the event-driven screening for politically exposed persons and adverse media. We will then no longer process the data concerned, unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the establishment, exercise or defence of legal claims.

Where we process your data for direct marketing, you have the right to object to this processing at any time without giving reasons. Following your objection, we will no longer process your data for this purpose.

Please send your objection informally to datenschutz@aurumbeam.com.

12.2 How to exercise your rights

Send your request to datenschutz@aurumbeam.com or by post to Aurumbeam London Ltd, Data Protection, 20 Wenlock Road, London N1 7GU, United Kingdom. No particular form is required, and handling is free of charge for you. It is helpful to state your custody agreement number or the email address registered in your aurumbeam access and to give a brief description of your request.

We acknowledge receipt and respond within one month. If an extension under Article 12(3) GDPR is necessary, we will inform you of this within that first month, stating the reasons.

Verification of identity for requests. Where there are reasonable doubts as to your identity, we will request additional information under Article 12(6) GDPR. The simplest route is a request from your logged-in aurumbeam access or from the email address registered with us. We do not require a fresh copy of your identity document if your identity has already been established via the aurumbeam access.

Possible restrictions of these rights are set out in section 7.4.

---

13 Complaint to a supervisory authority

You may lodge a complaint with a supervisory authority irrespective of other remedies. The competent authority for Aurumbeam London Ltd in the United Kingdom is the Information Commissioner’s Office. There is no lead supervisory authority in the European Union, because Aurumbeam London Ltd has no establishment there. Insofar as the GDPR applies, you may, under Article 77(1) GDPR, lodge a complaint with any supervisory authority in the European Union and in Liechtenstein, in particular with the authority of your place of habitual residence, your place of work or the place of the alleged infringement.

COUNTRY	AUTHORITY	ADDRESS AND WEBSITE
Germany	the Landesdatenschutzbehörde (state data protection authority) competent for your place of residence or place of work	The addresses of all German supervisory authorities can be found at datenschutzkonferenz-online.de. Further information is provided by the Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Federal Commissioner for Data Protection and Freedom of Information), Graurheindorfer Straße 153, 53117 Bonn, bfdi.bund.de
Austria	Datenschutzbehörde (Austrian Data Protection Authority)	Barichgasse 40 bis 42, 1030 Vienna, Austria, dsb.gv.at
Switzerland	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Swiss Federal Data Protection and Information Commissioner)	Feldeggweg 1, 3003 Bern, Switzerland, edoeb.admin.ch
Liechtenstein	Datenschutzstelle (Liechtenstein Data Protection Authority)	Kirchstrasse 8, FL-9490 Vaduz, Liechtenstein, datenschutzstelle.li
United Kingdom	Information Commissioner's Office (ICO)	Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom, ico.org.uk

14 Automated decisionmaking and profiling

14.1 No solely automated decisions

We do not take decisions which produce legal effects concerning you or similarly significantly affect you based solely on automated processing within the meaning of Article 22(1) GDPR. Conspicuous transactions are reviewed manually by staff. Technical tools such as sanctions list screening only provide indications; the decision is always taken by a person responsible for it after a substantive review and with access to all relevant information.

PROCESS	PROCEDURE
Rejection in the course of the identity check	Before a final rejection, a person responsible for it reviews the facts substantively. A mere confirmation of a technical check result is not sufficient
Suspension of a purchase, a sale back to Aurumbeam, a delivery or a beam order; blocking of the aurumbeam access	decision by staff after manual review, documented. You will be informed insofar as we are legally permitted to do so
Blocking following a match in the sanctions list screening	the match is always reviewed by a person, because identical names are common. The blocking itself is based on sanctions law
Limits on beaming and on payouts	no decision within the meaning of Article 22 GDPR, because the limits apply generally and are not set on the basis of an evaluation of your person

PROCESS	PROCEDURE
Pricing, mark-up, mark-down and fees	no decision within the meaning of Article 22 GDPR, because prices and fees are set for all customers according to the same rules and are displayed in the app before conclusion
Product suggestions in the user interface	no decision within the meaning of Article 22 GDPR, because no legal effect and no significant impact result from them; can be switched off at any time

No assessment of your creditworthiness, no scoring of your financial circumstances and no disclosure of assessment results to credit reference agencies take place.

14.2 Your rights

You may express your point of view on any decision under section 14.1, request a fresh review by another responsible person and contest the decision. To do so, contact datenschutz@aurumbeam.com. The explanation of the reasons may be restricted in individual cases insofar as provided for in section 7.4.

15 Retention and erasure policy

We erase personal data as soon as the purpose has ceased to apply and no statutory retention obligation and no need for legal defence precludes erasure (Article 5(1)(e) GDPR). The retention obligations under the law of the United Kingdom are authoritative, because Aurumbeam London Ltd has its registered office there and keeps its books there. Insofar as we retain records for longer than these obligations require, this is based on Article 6(1)(f) GDPR: the records serve you and us as proof of the allocation, the holding period and the acquisition data, including vis-à-vis tax authorities in your state of residence, and for the defence against claims within the limitation periods. The periods run from the end of the calendar year in which the respective transaction was completed.

We work with separate erasure classes for each data category and not with a blanket erasure run for each customer. Data whose period has expired are erased, even if other data of the same aurumbeam access must still be retained. Until the period expires, blocked data are excluded from further use and kept available only for the purpose of retention.

DATA CATEGORY	PERIOD	LEGAL BASIS OF THE PERIOD
Invoices, credit notes, payment records and other accounting records	10 years	Article 6(1)(c) GDPR in conjunction with sections 386 to 388 of the Companies Act 2006 and the tax retention obligations of the United Kingdom; insofar as the period goes beyond this, Article 6(1)(f) GDPR for the purpose of proof vis-à-vis you and the tax authorities of the sales markets

DATA CATEGORY	PERIOD	LEGAL BASIS OF THE PERIOD
Ledgers, tax records, inventory and reconciliation records relating to custody	10 years	as above
Contracts with customers, including custody, purchase contracts and contracts for the purchase of precious metals sent in, and the associated acceptance records	10 years from the end of the contract	Article 6(1)(f) GDPR for the purpose of proof and the defence against claims
Custody register and transaction history, including beaming	duration of the business relationship and thereafter 10 years. Entries are neither altered nor erased during this time; rectifications are made by means of reversing entries; after expiry, the allocation data are erased or anonymised	Article 6(1)(c) GDPR in conjunction with the above retention obligations and Article 6(1)(f) GDPR, because the history serves you and us as proof of the allocation, the holding period and the acquisition data
Transfer confirmations for beaming	as for the custody register and transaction history. The confirmation identifies the other party only by custody agreement number, first name and abbreviated surname; the full name appears only in the tax records export	Article 6(1)(f) GDPR, Article 5(1)(c) GDPR
Purchase records containing identity document data	10 years	as for accounting records
Master data of the aurumbeam access without a record function	duration of the business relationship, thereafter erasure after expiry of the longest period applicable to the associated records	Article 5(1)(e) GDPR
Result of the check and verified master data from the identity check	duration of the business relationship and thereafter 5 years	Article 6(1)(f) GDPR; from 10 July 2027, Article 77 of Regulation (EU) 2024/1624, insofar as Aurumbeam falls within the scope of that Regulation
Identity document images	deletion upon completion of the check, at the latest 30 days thereafter	Article 5(1)(c) and (e) GDPR
Documented matches from sanctions list screening	5 years	Article 6(1)(c) GDPR in conjunction with the sanctions law of the European Union and of the United Kingdom
Review notes from sanctions list screening without a match	12 months	Article 5(1)(e) GDPR
Tokenised reference to the stored credit card for recurring purchases	until the recurring purchase ends or the card is removed	Article 5(1)(e) GDPR
Server and security log files, IP addresses	7 days; in the event of a documented security incident, up to 90 days	Article 6(1)(f) GDPR, Recital 49
Login and session history	12 months	Article 6(1)(f) GDPR

DATA CATEGORY	PERIOD	LEGAL BASIS OF THE PERIOD
Fraud and abuse prevention cases involving an irregularity	until resolved and thereafter 3 years	Article 6(1)(f) GDPR in conjunction with the limitation periods
Support and complaint cases	3 years after closure of the case	Article 6(1)(f) GDPR in conjunction with the limitation periods
Records of consents, including the cookie selection	duration of the consent and thereafter 3 years	Article 7(1) in conjunction with Article 5(2) GDPR
Cookie selection stored on the terminal device	6 months, then a fresh request	Article 5(1)(e) GDPR
Newsletter and advertising data	until withdrawal, thereafter inclusion in a suppression list with minimal data	Article 6(1)(a) and Article 21(3) GDPR
Audience measurement data	14 months	Article 5(1)(e) GDPR
Allocation identifier in the affiliate programme	30 days	Article 5(1)(e) GDPR
Campaign measurement identifier and associated registrations and purchases	90 days	Article 5(1)(e) GDPR
Identifier for testing design variants (A/B test) and associated interaction data	6 months	Article 5(1)(e) GDPR
Applicant data	6 months after conclusion of the process; in the pool of applicants, with consent, 12 months	Article 6(1)(b) and (a) GDPR in conjunction with the time limits for asserting claims
Records relating to pending or announced legal disputes	until final conclusion and thereafter until expiry of the relevant limitation period	Article 6(1)(f) and Article 9(2)(f) GDPR
Entries in the logging system	unchanged during the term of the contract and the retention periods; thereafter erasure or anonymisation of the allocation data in accordance with section 6.2	Article 17(1) in conjunction with Article 5(1)(e) GDPR

As soon as Aurumbeam becomes an obliged entity under anti-money laundering law, the periods in section 7.3 additionally apply to the records concerned. We apply retention obligations of other states insofar as they apply irrespective of an establishment, for instance under § 25c(6) UStG.

16 Minors

Use of aurumbeam requires the user to be of full age and to have unrestricted legal capacity. Our offering is not directed at children and young persons. An aurumbeam access can only be opened by persons who have reached the age of 18; age is established in the course of the identity check on the basis of the identity document.

We therefore do not knowingly collect personal data from minors. If it emerges that an aurumbeam access has been opened by a minor contrary to these requirements, we block the access, settle any outstanding holdings in favour of the entitled person and erase the data, unless a statutory retention obligation exists. We do not base any processing on the consent of a child in relation to information society services under Article 8 UK GDPR or GDPR, the age limit for which is 13 years in the United Kingdom (section 9 of the Data Protection Act 2018) and is set differently in the Member States of the European Union. We accept notices of use by minors at datenschutz@aurumbeam.com.

17 Data security

We take technical and organisational measures under Article 32 UK GDPR and GDPR and under Art. 8 DSG in conjunction with Art. 1 to 6 DSV that are appropriate to the risk. These include in particular:

Encryption. All connections to aurumbeam.com and from the app are established exclusively using state-of-the-art transport encryption; unencrypted connections are rejected. Stored data are encrypted on the storage media. Particularly sensitive fields, in particular the link between technical identifier and person in the custody register and payment details, are additionally encrypted at field level. We store passwords exclusively as a hash value with a random salt and a computationally intensive method suitable for this purpose, never in plain text. Backup copies are encrypted and stored separately. Key management is documented; keys are rotated regularly.

Access control. Access rights are assigned on a role basis and in accordance with the principle of least privilege, are reviewed at least every six months and are revoked without undue delay upon departure or change of role. Administrative accesses are restricted to named persons and require multi-factor authentication. The data sets for the identity check, abuse prevention and marketing processing are technically separated. All employees and processors are bound to confidentiality in writing and receive training.

Logging. Access to personal data by administrative accounts, changes to permissions, login attempts and security-relevant system events are logged in a tamper-protected manner and evaluated. The logs are themselves access-restricted and are erased in accordance with the periods in section 15.

Two-factor authentication. Two-factor authentication is available for your aurumbeam access, and a second factor is required for security-relevant transactions, in particular payouts, changes to bank details, changes to the email address and beam orders. We expressly recommend activating two-factor authentication permanently. We additionally inform you of every security-relevant change by email and, if activated, by notification.

Further measures. Separation of development, test and production environments; use of exclusively synthetic or anonymised data in test and development environments; regular updating of the software used; security audits and penetration tests by external specialists; detection of and defence against automated attacks; a documented process for security incidents with notification to the Information Commissioner's Office under Article 33 UK GDPR within 72 hours, insofar as the GDPR applies, to the competent supervisory authorities in the European Union and in Liechtenstein under Article 33 GDPR within 72 hours, and to the Swiss Federal Data Protection and Information Commissioner under Art. 24 DSG as quickly as possible; communication to the data subjects under Article 34 GDPR in the event of a high risk; contingency plans and regularly tested recovery procedures.

No procedure offers complete protection. Please therefore keep your access data safe, do not use them anywhere else and report any suspicion of unauthorised access to us without undue delay at support@aurumbeam.com.

18 Changes to this Privacy Policy

We amend this Privacy Policy when the processing, the service providers used or the legal position change. The version published on aurumbeam.com and in the app, bearing the date stated at the end, applies in each case.

In the event of material changes, in particular new processing purposes, new categories of recipients, changed legal bases or changed storage periods, we will inform you before they take effect by email to the address registered in the aurumbeam access and by a notice in the app. If a purpose is to be changed for which your data were not originally collected, we will inform you of this in advance under Article 13(3) GDPR; if consent is required for the new purpose, we will obtain it beforehand. If the range of cookies and similar technologies requiring consent changes materially, we will ask for your selection again.

We will provide earlier versions of this Policy upon request to datenschutz@aurumbeam.com.

This Policy is provided in German and English. In the event of discrepancies between the language versions, the German version shall prevail.

Last updated: 29 October 2026

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