



Privacy Policy

How Infrastruct Digital processes personal information as the direct contractual seller, authorised reseller and operator of the customer storefront.

UK GDPR | DATA PROTECTION ACT 2018 | COOKIE
NOTICE

Effective date: 21 July 2026 Version: 1.3

Plain-English summary. We use personal information to operate accounts, process orders, deliver access, coordinate disclosed Product Partner fulfilment, secure Products, provide support and comply with law. Complete payment details are handled by the payment provider used at checkout. Product Partners receive only the information reasonably necessary for their disclosed role. We do not sell personal information or use it for third-party targeted advertising.

Contents

- | | |
|---|--|
| 1. Who controls your personal information | 10. International transfers |
| 2. Scope and roles of Product Partners | 11. How long we keep information |
| 3. Personal information we process | 12. Cookies, local storage and marketing |
| 4. Where information comes from | 13. Automated decision-making |
| 5. Why we use information and our legal bases | 14. Security |
| 6. Payment processing and fraud prevention | 15. Your data-protection rights |
| 7. Product Partner fulfilment and support | 16. Children |
| 8. AI inputs, files and generated outputs | 17. Complaints, changes and contact |
| 9. Who receives personal information | |



1. Who controls your personal information

Infrastruct Digital Ltd is the controller where we determine why and how personal information is processed, including through infrastructdigital.com, customer accounts, orders, billing administration, customer support and refunds. Infrastruct Digital is the direct contractual seller and an authorised reseller for Products purchased through our store. We are registered in England and Wales under company number **17331951**.

We have not appointed a statutory Data Protection Officer. Privacy responsibility is handled through the dedicated privacy contact below.

Privacy and rights requests

Infrastruct Digital Ltd

Company number 17331951

University of Kent, University Road, Keynes College, Canterbury, United Kingdom, CT2 7NP

privacy@infrastructdigital.com

2. Scope and roles of Product Partners

This notice applies when you visit our website, create or use an account, place an order, download or use a Product, link a game identifier, submit an AI request, contact support, request a refund, or communicate with us about privacy.

A **Product Partner** is a developer, licensor, server operator or supplier that authorises us to offer or resell a Product, supplies a customer entitlement, or helps fulfil, host, maintain or support it. Infrastruct Digital remains the direct contractual seller even where a Product Partner performs one of those functions.

Where a selected Product requires disclosure to a Product Partner, the recipient category is an authorised developer, licensor, server operator or fulfilment supplier. The information is limited to what is reasonably necessary for the stated function, such as an account email, order or entitlement status, a game or server identifier, or support information. Depending on the processing, the Product Partner may act as our processor or as an independent controller. You may contact us for the current recipient applicable to a Product.

3. Personal information we process

Depending on the Product and features you use, we may process the following categories. We do not collect every category in every case.

- **Account information:** name or display name, email address, password hash, account status, creation date and authentication records.
- **Order information:** Product, access period, order reference, price, currency, tax information, payment status, refund status and statement descriptor.
- **Payment metadata:** billing country, payment-method type, card brand, limited transaction identifiers and fraud signals returned by the payment provider used at checkout. We do not receive or store complete card details.
- **Technical and security data:** IP address, date and time, device or browser information, app version, operating system, security events, approximate location derived from IP, session identifiers, crash diagnostics and anti-abuse signals.
- **Product and usage data:** entitlements, activation state, feature use, usage limits, generated-item counts and operational telemetry.



- **Game identifiers:** game account name, server identifier, platform identifier or another identifier needed to grant or manage access.
- **AI content:** prompts, instructions, images, files and other inputs you choose to submit, plus resulting outputs, where needed to perform the requested function.
- **Support information:** messages, attachments, troubleshooting details, refund requests, complaints and our replies.
- **Fraud-risk, verification and dispute information:** payment-risk scores, device or account linkage, verification status, proportionate evidence of account or payment ownership, chargeback evidence and the outcome of a transaction review where reasonably required by law or a payment provider. A failed or declined review is recorded as a payment-risk outcome and is not, by itself, treated as an allegation that the customer committed a criminal offence. We do not ask you to email passwords, recovery codes, two-factor authentication codes, complete card numbers or card security codes.
- **Website storage:** necessary cookies or local-storage values used for sign-in, security, preferences and account operation.

Our Products are not designed to collect or infer special-category or criminal-offence information. Do not submit that information in prompts, files or support messages. If we discover it unexpectedly, we restrict access and delete it as soon as reasonably practicable unless limited retention is necessary for a legal claim or documented legal obligation. We will not intentionally introduce a feature designed to process such information without first documenting the required legal basis, condition, safeguards and any necessary data-protection impact assessment.

4. Where information comes from

- directly from you when you register, order, enter an identifier, use a Product or contact us;
- from the payment provider used at checkout and financial institutions when they confirm, decline, refund or dispute a payment;
- from our website, Products and infrastructure through security logs, activation records, telemetry and diagnostics;
- from Product Partners and server operators when they confirm delivery, account status, access activation, misuse or a technical problem;
- from public or officially exposed game-data sources where an analytics Product retrieves public data; and
- from you, the payment provider used at checkout, financial institutions, fraud-prevention services or lawful public records where proportionate verification is reasonably needed for an order, refund, dispute, sanctions or fraud review.

We do not treat private player information as public merely because it may be technically accessible.

Public game data may relate to people who are not our customers. Where that information is personal data, the applicable Product notice identifies the controller, categories and source, purpose and lawful basis, recipients and retention period. We provide the information required for data obtained from another source within the applicable time unless a documented legal exception applies, in which case we implement the required safeguards.

5. Why we use information and our legal bases

Contract and steps requested before a contract

We use account, order, payment-status, entitlement, game-identifier, support and necessary AI-input data to create an account, process an order, deliver access, operate the Product, provide support and administer a refund.



Legal obligations

We use transaction, tax, refund, complaint and limited verification records where necessary for accounting, consumer protection, sanctions compliance, fraud reporting, data-protection duties and valid legal requests.

Legitimate interests

Where those interests are not overridden by your rights, we use limited technical, security, support, verification and usage data to secure accounts, verify account or payment ownership, prevent fraud and refund abuse, diagnose failures, maintain service reliability, manage Product Partner fulfilment, defend legal claims, understand aggregate Product performance and improve support.

Consent

We rely on consent for non-essential cookies or similar technologies and for optional marketing where consent is legally required. You may withdraw consent at any time without affecting earlier lawful processing.

Information required to provide the service

To create an account and perform the contract, you must provide the account email, authentication information, order details and any Product-specific game, platform or server identifier marked as required. Payment information required by the selected payment provider is supplied directly to that provider. If required information is not provided, we may be unable to create the account, process the order, deliver or maintain the entitlement, verify payment ownership or complete a requested refund. Optional marketing choices are not required. AI prompts or files are required only if you choose to use the relevant AI feature.

6. Payment processing and fraud prevention

Infrastruct Digital is the direct contractual seller for purchases made through our store. The payment provider displayed at checkout processes payment details, performs transaction and fraud checks, returns payment status to us and supports refunds and disputes. The provider may act as our processor for some activities and as an independent controller for its own legal, security and payment-network obligations.

We use payment status, billing country, limited payment identifiers, dispute information and fraud signals to complete the order, issue receipts and refunds, prevent unauthorised transactions and respond to chargebacks. Where a transaction, refund or chargeback presents a material risk, we may ask for proportionate evidence that you control the customer account or were authorised to use the payment method. We do not store complete card numbers or card security codes.

We may pause an order, entitlement or refund while a proportionate transaction review is active. We use the least intrusive evidence reasonably available, restrict access to it, and do not retain a verification document longer than necessary merely because it was supplied. We record a decline as a risk outcome rather than an allegation of criminal conduct unless a separate legal basis and condition have been documented.

7. Product Partner fulfilment and support

A Product Partner receives only the personal information reasonably necessary for the disclosed Product-specific function, such as creating or validating an entitlement, granting server access, operating or maintaining the Product, or resolving a support request.

Before a Product Partner is permitted to process personal information on our behalf, we must put in place the confidentiality, security and data-protection terms required by applicable law. Where a Product Partner determines its own purposes as an independent controller, its own privacy information applies to that processing.



We do not authorise a Product Partner to use customer information for unrelated marketing or to sell customer lists.

8. AI inputs, files and generated outputs

When you use an AI feature, the content required to perform the request may be sent to the AI provider identified for that feature. This may include prompts, instructions, files or images that you choose to submit.

The provider category, purpose and types of content are described in this notice. The relevant provider's terms and the account, endpoint and configuration used for the feature may affect retention. We do not describe a feature as zero-retention unless that setting has been enabled and verified. You may contact us for current provider and retention information for a selected Product.

We do not use customer prompts, files or outputs to train a general-purpose model of our own. Do not submit information or material that you are not authorised to use.

9. Who receives personal information

We disclose information only where reasonably necessary, including to:

- **Payment providers** and financial institutions for payment processing, fraud prevention, refunds and disputes;
- **Proton Mail** for customer support and privacy correspondence;
- **OpenAI** and **Google Cloud/Vertex AI** where the selected Product uses their AI services;
- website hosting, authentication, database, content-delivery, logging, crash-reporting and secure-download providers;
- authorised Product Partners and community-server operators that need limited data to fulfil, operate, maintain or support the Product;
- professional advisers, insurers, auditors, accountants and tax advisers under confidentiality obligations; and
- courts, regulators, law enforcement or other recipients where required by law or needed to establish, exercise or defend legal rights.

We do not sell personal information, rent customer lists, or share personal information for third-party targeted advertising.

10. International transfers

Some providers, Product Partners or support teams may store or access information outside the United Kingdom, including in the European Economic Area, Switzerland or the United States.

Where UK data-protection law treats a transfer as restricted, we use a lawful mechanism appropriate to the destination and recipient, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another recognised safeguard. We also assess whether supplementary contractual, organisational or technical measures are needed.

You may ask privacy@infrastructdigital.com for more information about relevant safeguards, subject to protection of confidential and security-sensitive terms.

For each restricted transfer, we record the actual recipient, destination and transfer mechanism and provide the applicable information in this notice or a Product-specific notice. If we intentionally offer Products to people in the European Union in circumstances requiring an EU representative, we will appoint that representative and publish its contact details before the relevant processing begins.



11. How long we keep information

We keep personal information only for as long as reasonably necessary for the purpose for which it was collected and for applicable accounting, tax, consumer-protection, security, dispute and legal requirements.

- **Account and entitlement information:** for the life of the account or entitlement and afterwards only where needed for support, security, disputes or legal obligations.
- **Order, payment, refund and accounting records:** for the statutory accounting and tax retention period that applies to the record.
- **Support, complaint and dispute records:** for as long as needed to resolve the matter and establish, exercise or defend legal claims.
- **Security, verification and anti-abuse information:** for a period proportionate to the relevant security risk, review or incident.
- **Game identifiers:** while required to provide or support the purchased access, and afterwards only where needed for an unresolved matter or legal obligation.
- **AI inputs and outputs:** according to the feature, provider and settings disclosed before submission, unless you choose to save the content or provide it to support.
- **Backups:** until overwritten or securely removed through the normal backup cycle.

When information is no longer required, we delete or anonymise it. We may retain a minimal record where necessary to honour an opt-out, document a refund, prevent duplicate recovery or comply with law.

12. Cookies, local storage and marketing

Our website and account area use cookies or browser storage where needed for sign-in, security, checkout, preferences and account operation.

We do not use non-essential analytics, advertising or marketing technologies unless the required information and consent controls are in place. Where such technologies are used, the current categories, providers, purposes and available controls are shown in the website's cookie notice or consent interface.

We send necessary service messages about accounts, orders, access, security and support. Marketing messages are sent only where permitted by law and include a way to opt out.

13. Automated decision-making

We do not ourselves use solely automated decision-making with legal or similarly significant effects. Payment providers and financial institutions may use automated systems to authorise or decline transactions under their own privacy notices. If our own use of an automated signal restricts an existing account or entitlement, you may contact support and request meaningful human review.

14. Security

We use proportionate technical and organisational measures designed to protect personal information against accidental or unlawful loss, alteration, disclosure or access. Measures are selected for each live system according to risk and may include encryption in transit, password hashing, access controls, least-privilege access, logging, backups, provider and Product Partner review, and incident response.



No online system is completely risk-free. Use a unique password, protect your email account and notify support promptly about suspected unauthorised access. If a personal-data breach creates a legal notification duty, we will notify the ICO and affected individuals in the required time and manner.

15. Your data-protection rights

Under UK data-protection law, you have the following rights, subject to the conditions and exemptions that apply to each right:

- be informed about our use of your information;
- request access to and a copy of your personal information;
- correct inaccurate or incomplete information;
- request deletion in applicable circumstances;
- restrict processing or object to processing based on legitimate interests;
- receive information you supplied in a portable format where the right applies;
- withdraw consent at any time where processing relies on consent; and
- request human intervention where applicable automated-decision rights arise.

Your right to object

Where we rely on legitimate interests, including account security, fraud prevention, service reliability and Product improvement, you may object by emailing privacy@infrastructdigital.com. We will stop the relevant processing unless we demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed for legal claims. If you object to direct marketing, we will stop it.

Email privacy@infrastructdigital.com to exercise a right. State the right and the relevant account email. We may request proportionate information to verify identity. We normally respond within one month, subject to lawful extensions for complex or numerous requests.

Rights are not absolute. We may need to retain transaction records required by law or information needed to establish or defend a legal claim. If we cannot fulfil all or part of a request, we will explain why and identify available complaint rights.

16. Children

Accounts, purchases and Products are intended only for people aged 18 or over. We do not knowingly create accounts for children. If you believe a person under 18 has provided information, contact the privacy address so that we can investigate and take appropriate action.

An age statement does not remove responsibilities where an online service is in fact likely to be accessed by children. We will review audience and design and introduce appropriate age-assurance and child-protection measures before intentionally serving under-18 users.

17. Complaints, changes and contact

You may make a data-protection complaint to privacy@infrastructdigital.com. You do not have to complain to us before contacting the ICO. We investigate complaints and respond within the period required by applicable law.



You may also complain to the UK Information Commissioner's Office at ico.org.uk/make-a-complaint. If EU data-protection law applies, you may contact the supervisory authority in your EEA country. You may seek a judicial remedy where the law permits.

We may update this notice when our Products, providers or legal obligations change. We will update the effective date and provide an appropriate notice where a change materially affects you.

Privacy and rights requests

Infrastruct Digital Ltd

Company number 17331951

University of Kent, University Road, Keynes College, Canterbury, United Kingdom, CT2 7NP

privacy@infrastructdigital.com