GLAZIE

Data Processing Terms

The controller-to-processor terms on which an approved GLAZIE supplier handles customer and fulfilment personal data: what they receive, what they may never use it for, how breaches and data-subject requests are handled, how long they keep it, and the security measures required of them.

Version 1.0 · Effective 1 September 2026
Published at https://glazie.co.uk/sell/agreements/data-processing-terms
GLAZIE LTD · Company No. 12310620 · VAT No. GB 336090512 · Registered in England & Wales · 56 Ashgrove Road, Ilford, London, IG3 9XD

Parties

Party	Details
GLAZIE (controller)	GLAZIE LTD, company number 12310620, registered in England and Wales, registered office at 56 Ashgrove Road, Ilford, London, IG3 9XD (GLAZIE).
Supplier (processor)	The approved supplier identified in the supplier application through which these Terms are accepted, as confirmed in its Commercial Schedule (the Supplier).

1. Parties, scope and status

1.1 These Data Processing Terms (Terms) form part of the Supplier Service Agreement between GLAZIE and the Supplier.

1.2 For the processing described in Schedule 1, GLAZIE acts as controller and the Supplier acts as processor. The Supplier must process GLAZIE Personal Data only to manufacture, fulfil, deliver, support and resolve marketplace Orders in accordance with GLAZIE's documented instructions.

1.3 These Terms do not make either party a processor for every item of information exchanged between them. Each party remains an independent controller for personal data it processes for its own employment, corporate administration, legal compliance and business-contact purposes.

1.4 Where the Supplier is required by applicable law to process limited information for its own statutory product-safety, traceability, tax or regulatory obligations, it acts as an independent controller for that specific processing only. It must minimise the personal data used, must not use that exception for marketing or customer acquisition, and must tell GLAZIE where reasonably required.

1.5 If these Terms conflict with the Supplier Service Agreement on the protection or processing of personal data, these Terms prevail to the extent of the conflict. Commercial liability and payment matters remain governed by the Supplier Service Agreement unless these Terms expressly state otherwise.

2. Definitions

Applicable Data Protection Law: all data-protection and privacy laws applicable to the processing, including the UK GDPR, the Data Protection Act 2018, amendments made by the Data (Use and Access) Act 2025 and related regulations, and PECR where applicable, in each case as amended or replaced.

Business Day: as defined in the Supplier Service Agreement.

Customer: the individual end customer, business customer contact, delivery recipient, authorised collector or

other person whose personal data is supplied to the Supplier through a GLAZIE marketplace Order.

GLAZIE Personal Data: personal data processed by the Supplier on behalf of GLAZIE under these Terms, including the data categories in Schedule 1.

Personal Data Breach: a personal data breach within Applicable Data Protection Law affecting GLAZIE Personal Data.

Restricted Transfer: a transfer of personal data for which Applicable Data Protection Law requires an adequacy decision, approved safeguard, exception or other lawful transfer mechanism.

Sub-processor: another processor engaged by the Supplier to process GLAZIE Personal Data on behalf of GLAZIE.

Words defined in the Supplier Service Agreement have the same meaning here unless these Terms say otherwise.

3. Documented instructions and purpose limitation

3.1 The Supplier must process GLAZIE Personal Data only on documented instructions from GLAZIE, including the Order, canonical specification, Supplier Portal workflow, approved support instructions, these Terms and any written instruction capable of being retained as a record.

3.2 The Supplier must not use GLAZIE Personal Data for any independent commercial purpose, including:

- direct marketing, remarketing, advertising, profiling or lead generation;
- opening a direct customer account or adding a Customer to the Supplier's own CRM or mailing list;
- cross-selling, upselling or soliciting future direct orders;
- matching Customer information against external databases or enriching a customer profile;
- training, fine-tuning or evaluating any public, shared or third-party AI model, or uploading Customer data to an AI service that GLAZIE has not approved in writing;
- selling, licensing, disclosing or otherwise monetising Customer data; or
- using Customer data to determine or reveal GLAZIE's retail pricing, marketplace margin, routing logic or other confidential marketplace information.

3.3 If the Supplier believes an instruction infringes Applicable Data Protection Law, it must promptly inform GLAZIE before carrying it out unless the law prohibits that notification.

3.4 If the Supplier is legally required to process GLAZIE Personal Data other than on GLAZIE's instructions, it must tell GLAZIE before the processing unless the law prohibits it.

4. Data minimisation and supplier access

4.1 GLAZIE will expose only the information the Supplier reasonably needs for fulfilment. The Supplier must likewise limit access internally to personnel who need the information for the relevant Order.

4.2 The Supplier acknowledges that the GLAZIE marketplace is deliberately separated into customer, supplier and internal commercial views. Unless expressly required for fulfilment, the Supplier must not receive or seek access to Customer card or payment details, GLAZIE retail prices, GLAZIE margin, refund economics, cross-supplier pricing or private administrative notes.

4.3 Delivery and collection details are withheld until the Supplier has positively accepted the Order. Once disclosed, they may be used only for the fulfilment purpose for which they were disclosed.

4.4 Special-category data and criminal-offence data are not intentionally required for ordinary marketplace fulfilment. If such information is incidentally included in a Customer instruction or support message, the Supplier must restrict use to the minimum necessary for the specific fulfilment task, protect it as highly

confidential, and not retain or reuse it for any unrelated purpose.

5. Confidentiality and personnel

5.1 The Supplier must ensure that every person authorised to process GLAZIE Personal Data is subject to an appropriate duty of confidentiality.

5.2 The Supplier must give access only to trained personnel with a genuine operational need, and must promptly remove access when that need ends or employment or engagement changes.

5.3 Named accounts must be used where available, and credentials must not be shared between individuals.

5.4 The Supplier remains responsible for the acts and omissions of its personnel in relation to GLAZIE Personal Data.

6. Security

6.1 Taking account of the state of the art, implementation cost, the nature, scope, context and purposes of processing and the risks to individuals, the Supplier must implement appropriate technical and organisational measures to protect GLAZIE Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

6.2 The baseline measures in Schedule 3 apply unless the Commercial Schedule or a written security addendum imposes stronger controls.

6.3 The Supplier must maintain reasonable incident-response, continuity and recovery procedures appropriate to the data and systems it uses for GLAZIE Orders.

6.4 The Supplier must not deliberately weaken, bypass or disable a security control provided by the Supplier Portal or another GLAZIE system.

7. Personal Data Breaches

7.1 The Supplier must notify GLAZIE without undue delay after becoming aware of a Personal Data Breach. As a contractual operating target, the Supplier must make the initial notification within 24 hours of awareness, even if the investigation is incomplete.

7.2 The initial notification must, so far as known at the time, include:

- what happened, when it was discovered and whether it is ongoing;
- the categories and approximate number of affected people and records where known;
- the systems, Orders and Sub-processors involved;
- the likely consequences or risks;
- containment and remedial actions already taken or planned; and
- a named incident contact for follow-up.

7.3 The Supplier must preserve relevant evidence, provide updates as material facts become known, and cooperate with GLAZIE’s investigation, risk assessment, regulatory notification and Customer communication.

7.4 The Supplier must not notify the ICO, another regulator or an affected Customer on GLAZIE’s behalf unless GLAZIE instructs it to do so or the Supplier is independently required by law. If independently required, the Supplier must coordinate with GLAZIE where legally permitted.

7.5 Notification is made by the route in Schedule 5. A notification sent to any other GLAZIE address does not start the 24-hour clock.

8. Data-subject rights and complaints

8.1 If the Supplier receives a request, complaint or enquiry from a Customer concerning GLAZIE Personal Data, it must not substantively respond on GLAZIE's behalf unless instructed. GLAZIE is the customer-facing point for data-protection rights and complaints.

8.2 The Supplier must forward the request to GLAZIE promptly and, as an operating target, within 2 Business Days of receipt.

8.3 The Supplier must provide reasonable assistance so GLAZIE can respond to requests for access, rectification, erasure, restriction, portability, objection and rights relating to automated decision-making where applicable.

8.4 Assistance includes locating relevant information in Supplier systems and approved Sub-processor systems, implementing a deletion or restriction instruction, and providing evidence reasonably needed to demonstrate completion.

9. Assistance with compliance

9.1 The Supplier must provide information and reasonable assistance requested by GLAZIE in relation to:

- security and Article 32 risk controls;
- records of processing and accountability evidence;
- data protection impact assessments and, where required, prior consultation with the ICO;
- investigation of complaints, regulatory enquiries or suspected unlawful processing; and
- verification that the Supplier continues to provide sufficient guarantees for compliant processing.

9.2 The Supplier must promptly tell GLAZIE of any material change in its processing, systems, Sub-processors, locations or security posture that could materially affect the risk to GLAZIE Personal Data.

10. Sub-processors

10.1 The Supplier must not appoint a Sub-processor without GLAZIE's prior specific or general written authorisation.

10.2 GLAZIE gives general written authorisation for the categories of Sub-processor in Schedule 4, on condition that the Supplier maintains the register described there and gives GLAZIE at least 14 calendar days' written notice before adding or replacing a Sub-processor, so that GLAZIE has a reasonable opportunity to object on data-protection grounds.

10.3 Where a Sub-processor must be engaged at once to maintain continuity — for example a replacement carrier after a sudden failure — the Supplier may do so before the notice period expires, but must notify GLAZIE immediately and must stop using that Sub-processor if GLAZIE reasonably objects.

10.4 The Supplier must enter into a written contract with each Sub-processor imposing data-protection obligations that are, in substance, no less protective than those imposed on the Supplier by these Terms for the processing delegated to that Sub-processor.

10.5 The Supplier remains responsible to GLAZIE for the performance of its Sub-processors.

10.6 Carriers, logistics providers, cloud and IT providers and specialist processors are Sub-processors where they process GLAZIE Personal Data on the Supplier's behalf. Being commercially involved does not by itself remove the need to assess the role correctly.

10.7 A GLAZIE objection must be based on a reasonable data-protection concern. The parties will work in good faith on a compliant alternative; if none is reasonably available, GLAZIE may restrict the affected processing or service.

11. International access and transfers

11.1 The Supplier must not make a Restricted Transfer of GLAZIE Personal Data, or permit routine remote access from a location that creates a Restricted Transfer, without GLAZIE's prior written authorisation.

11.2 Where a Restricted Transfer is authorised, the Supplier must ensure a lawful transfer mechanism is in place, complete any transfer risk assessment required by law, implement any additional safeguards that assessment identifies, and provide GLAZIE with reasonable evidence on request.

11.3 Where appropriate, the parties may use the then-current UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, an applicable adequacy regulation or another lawful safeguard recognised under Applicable Data Protection Law.

11.4 The Supplier must not change the country or region from which GLAZIE Personal Data is materially processed without first considering whether the change affects the transfer analysis, and notifying GLAZIE where required.

12. Retention, return and deletion

12.1 The Supplier must not retain identifiable Customer information for longer than needed for fulfilment, an open complaint, remake or warranty case, a documented GLAZIE instruction or a legal obligation.

12.2 The retention rules in Schedule 2 apply. They are deliberately shorter for direct Customer identifiers than for technical manufacturing records: GLAZIE keeps the long-lived order and accounting record, and the Supplier does not need a copy of it.

12.3 On termination of the Supplier relationship, or earlier on GLAZIE's written instruction, the Supplier must return or securely delete GLAZIE Personal Data unless applicable law requires retention.

12.4 If law requires retention, the Supplier must isolate the retained information, use it only for the legally required purpose, and delete it when that requirement ends.

12.5 The Supplier may retain technical manufacturing, product and traceability records for legitimate legal or warranty purposes where permitted, but must key them to the GLAZIE Order number or another non-direct identifier and remove Customer name, contact details and delivery address unless those identifiers are genuinely required.

12.6 On request, the Supplier must provide reasonable written confirmation of deletion or return.

13. Audits and compliance evidence

13.1 The Supplier must make available information reasonably necessary to demonstrate compliance with these Terms and Applicable Data Protection Law.

13.2 GLAZIE will use security questionnaires, policy evidence, certifications, penetration-test summaries, independent assurance reports or other proportionate evidence before requiring an on-site audit.

13.3 Where reasonably necessary, GLAZIE or an independent auditor bound by confidentiality may audit the Supplier's relevant processing on reasonable notice and during normal business hours. Notice need not be given where an urgent security incident, credible regulatory concern or material suspected breach makes advance notice impracticable.

13.4 An audit must be scoped to relevant processing and conducted so as to avoid unreasonable disruption or disclosure of unrelated confidential information.

13.5 The Supplier must promptly address material deficiencies identified through a justified audit or compliance review.

14. Records and evidence

14.1 The Supplier must maintain records sufficient to identify its processing activities, authorised Sub-processors, material security incidents and completion of material deletion or return instructions.

14.2 Order, access, handover and operational records may be retained by GLAZIE as marketplace transaction and audit records under GLAZIE's own controller responsibilities.

14.3 Nothing in these Terms requires GLAZIE to disclose allocation logic, cross-supplier benchmarking, private administrative notes or another supplier's confidential data.

15. Changes to processing

15.1 GLAZIE may issue reasonable documented instructions that are consistent with the Supplier Service Agreement and the agreed processing purpose.

15.2 A material expansion of processing purpose, personal-data categories, international transfer location or use of sensitive data will be documented through an updated schedule, a written addendum or a new version of these Terms.

15.3 The Supplier must not treat a new commercial opportunity as an implied instruction to reuse Customer data.

16. Liability and regulatory rights

16.1 The parties' commercial liability allocation is governed by the Supplier Service Agreement and Commercial Schedule, subject to any liability that cannot lawfully be limited or excluded.

16.2 Nothing in these Terms limits the rights of data subjects, the powers of the ICO, or obligations imposed directly on a controller or processor by Applicable Data Protection Law.

16.3 Each party remains responsible for the regulatory obligations that apply to it in its actual role.

17. Term and survival

17.1 These Terms take effect on the same date as the Supplier Service Agreement or the date the Supplier validly accepts these Terms, whichever is later.

17.2 They continue for as long as the Supplier processes GLAZIE Personal Data.

17.3 Confidentiality, deletion and return, audit evidence, liability and any provision that by its nature must continue remain effective after termination for as long as relevant GLAZIE Personal Data is retained.

18. Governing law

18.1 These Terms and any non-contractual obligations arising from them are governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction, subject to mandatory data-protection law and regulatory powers.

Schedule 1 — Processing details and role matrix

Processing activity	Role	Purpose and limits
Marketplace Customer fulfilment	GLAZIE: controller. Supplier: processor	Manufacture, prepare, deliver or make available for collection a paid GLAZIE Order; communicate only as needed for fulfilment.

Processing activity	Role	Purpose and limits
Delivery or collection handover	GLAZIE: controller. Supplier: processor	Use delivery address, recipient and contact information and handover evidence only to complete and evidence delivery or collection.
Complaint, remake or warranty investigation	GLAZIE: controller. Supplier: processor	Investigate manufacturing and fulfilment issues and provide evidence and remedial support on GLAZIE instructions.
Supplier staff and representatives	Each party: independent controller	Contract administration, account security, business communications, and legal and compliance records relating to the other party's personnel.
Supplier statutory manufacturing or traceability processing	Supplier: independent controller, only where law genuinely requires	Limited statutory processing only. Minimise direct Customer identifiers, and do not use this role for marketing, solicitation or commercial profiling.

Subject matter, nature and purpose

Processing of limited Customer and fulfilment information necessary to perform marketplace manufacturing, delivery and collection, support, remake and warranty tasks under the Supplier Service Agreement.

Duration

From disclosure of the relevant GLAZIE Personal Data until the operational purpose ends and the data is deleted or returned under Schedule 2, subject to an open case, a documented instruction or a legal retention obligation.

Categories of data subjects

- individual consumers purchasing from GLAZIE;
- employees or representatives of business and trade Customers;
- delivery recipients and authorised third-party recipients;
- persons authorised to collect an Order;
- Customer contacts involved in a complaint, remake or warranty case; and
- other individuals incidentally named in delivery or support instructions where necessary for fulfilment.

Categories of personal data

- GLAZIE Order number and fulfilment identifiers;
- name or recipient name where operationally necessary;
- delivery or collection address and postcode;
- telephone number and email address only where necessary for delivery, collection or an authorised support workflow;
- delivery or collection instructions and availability information;
- support correspondence or complaint details provided to the Supplier for resolution;

- handover information such as delivery or collection time, recipient name, authorised-third-party status and evidence references; and
- images or documents supplied for a complaint or remake where they incidentally contain personal data.

Data not provided to the Supplier

- payment-card or bank-payment credentials;
- Customer retail price and GLAZIE marketplace margin;
- full Customer billing and accounting data where it is not required for fulfilment;
- marketing profiles, browsing history or unrelated account history;
- another supplier's confidential information; and
- private GLAZIE administrative notes or liability deliberations.

Sensitive data

No special-category or criminal-offence data is intentionally required. Any incidental sensitive information must be handled under clause 4.4 and must not be copied into local systems unless strictly necessary.

Schedule 2 — Retention and deletion

These are the Supplier's retention rules for GLAZIE Personal Data. They are deliberately shorter for direct Customer identifiers than for technical manufacturing records. Where the Supplier's own law or a recognised product-safety obligation requires a different period, the Supplier must document the basis and minimise the personal data retained.

Data class	Supplier retention	End-of-period action
Live order contact and delivery details	Until confirmed delivery or collection plus 30 days, or until a blocking operational case is resolved, whichever is later.	Delete from local operational copies; retain only the GLAZIE Order reference where possible.
Recipient and handover evidence	90 days after confirmed handover, or until any related dispute is resolved, whichever is later.	Delete direct identifiers and signatures unless GLAZIE instructs otherwise or law requires retention.
Complaint or remake case personal data	Until the case is closed plus 90 days.	Delete direct identifiers; retain non-personal technical defect and remake evidence where legitimately required.
Email and local message copies containing Customer data	No longer than necessary for the active task, and in any event delete within 30 days after closure.	Move any required evidence into the approved Order or case record, then delete the local copy.
Technical manufacturing and traceability records	For the period reasonably required by applicable law, product traceability or the agreed warranty.	Key to the GLAZIE Order number or product identifier; remove Customer contact and delivery details unless genuinely required.
Backups	Normal secure backup cycle after live deletion, and no more than 90 days.	Expire automatically. No restoration for ordinary use after deletion, except disaster recovery.

Schedule 3 — Minimum technical and organisational measures

Control	Minimum expectation
Identity and access	Named accounts where available; least-privilege access; strong unique passwords; multi-factor authentication where supported; prompt joiner, mover and leaver access changes; no credential sharing.
Device protection	Supported operating systems; security patches applied on a reasonable risk-based schedule; screen lock; device encryption where supported; malware protection appropriate to the device type.
Network and transmission	Encrypted transport such as HTTPS and TLS for portal access; no unencrypted transfer of Customer data; no Customer data in consumer or public file-sharing or messaging services unless GLAZIE has approved the workflow.
Storage and local copies	Minimise downloads, spreadsheets, screenshots and printouts; store only in controlled business systems; restrict access; securely delete when no longer needed.
Email and messaging	Business-managed accounts; verify recipients before sending; never send Customer data to personal email or personal cloud storage.
AI and automated tools	Do not submit GLAZIE Personal Data to public or shared generative-AI systems, AI training datasets or model-development services unless specifically approved in writing and contractually protected.
Staff confidentiality and training	Relevant staff receive privacy and security guidance and are bound by confidentiality.
Physical security	Reasonable controls for offices, factories, dispatch areas and paper records; prevent public or visitor access to Customer documents or screens.
Incident response	A documented route for reporting suspected loss, misdelivery, phishing, compromised credentials or unauthorised access, and the ability to meet the 24-hour notification target in clause 7.
Resilience and recovery	Reasonable backups, continuity procedures and recovery arrangements for systems whose failure could materially affect fulfilment or data protection.
Disposal	Secure deletion of electronic data and secure destruction of paper and media containing Customer data.
Sub-processor governance	Written terms, due diligence proportionate to risk, a current register, change notification and transfer compliance.

Schedule 4 — Sub-processor register

GLAZIE gives general authorisation under clause 10.2 for the following categories of Sub-processor, provided the Supplier keeps a current register and notifies changes as that clause requires:

- carriers and logistics providers used to deliver or collect an Order;
- cloud, hosting, IT support and order-management providers used to run the Supplier’s own systems; and

- specialist processors engaged for a specific fulfilment task, such as toughening, laminating or installation, where they receive Customer data.

The register must be provided to GLAZIE on request and before the Supplier's first Order, and must record, for each Sub-processor:

Field	What it records
Sub-processor	Legal name of the entity processing GLAZIE Personal Data.
Service	What it does for the Supplier, and which processing activity in Schedule 1 it touches.
Processing location	Country or countries from which the data is accessed or stored.
Transfer mechanism	Where the location makes the processing a Restricted Transfer: the adequacy regulation, UK International Data Transfer Agreement, UK Addendum or other lawful safeguard relied on.
Status	Whether GLAZIE has been notified and whether the 14-day objection period in clause 10.2 has run.

A Sub-processor GLAZIE has not been told about is not authorised, whatever category it falls into.

Schedule 5 — Contacts and escalation

Purpose	GLAZIE route	Supplier obligation
Personal Data Breach, within 24 hours (clause 7)	Email sales@glazie.co.uk with "DATA BREACH" in the subject line, and raise a ticket in the Supplier Portal. Use both.	Send from a monitored address and give a named incident contact who can be reached the same day.
Data-subject request received by the Supplier (clause 8)	Forward to sales@glazie.co.uk within 2 Business Days. Do not reply to the Customer substantively.	Forward the request in full, including anything the Customer attached.
Sub-processor change notice (clause 10.2)	Email suppliers@glazie.co.uk at least 14 calendar days before the change.	Send from the Supplier's contractual contact and include the Schedule 4 register fields.
Privacy or data-protection question	Email sales@glazie.co.uk.	Ask before processing, not after.
Supplier's own privacy contact	Recorded from the Supplier's application and kept current in the Supplier Portal.	Tell GLAZIE when the contact changes.

GLAZIE is the customer-facing point for data-protection rights and complaints. A Customer who contacts the Supplier must be directed to GLAZIE, not answered on GLAZIE's behalf.

Acceptance

These Terms are accepted electronically. By ticking the Data Processing Terms box in the supplier application, the person completing the application confirms on behalf of the Supplier that they have read these Terms, have authority to bind the Supplier to them, and accept them.

GLAZIE records the version number and a SHA-256 fingerprint of the exact text accepted, the accepting

user and account, the date and time, and, where available, the IP address and browser used. An earlier acceptance is never overwritten by a later version: each accepted version remains provable, and a copy of the accepted version can be downloaded from the published page at any time.

For GLAZIE LTD: Rehan Jamil, Director.

Version history

- Version 1.0, 1 September 2026: first published version.