Facial Scan Privacy Notice

Effective Date: 03/03/2025

1. Scope and Purpose

This Facial Scan Privacy Notice ("Notice") governs SellOut Limited's ("we," "us," or "our") use of facial recognition technology ("FRT") on our marketplace platform. It is issued in compliance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and relevant guidance from the Information Commissioner's Office ("ICO"). It supplements our Privacy Policy and User Agreement, and is intended to provide users with clear and transparent information about how we collect, use, secure, and share biometric data.

2. Legal Framework

The processing of facial scan data and other biometric identifiers is governed by the following laws and regulatory instruments:

- The UK General Data Protection Regulation (UK GDPR), including Articles 5 (principles), 6 (lawful basis), 9 (special category data), and 35 (Data Protection Impact Assessment);
- The Data Protection Act 2018, particularly Part 2, Chapter 2, which supplements and applies the GDPR in UK domestic law;
- The ICO's "Biometrics and Data Protection" guidance (2024), which sets out expectations for fair, transparent, and proportionate use of facial recognition systems.

We commit to reviewing this Notice regularly and updating it to reflect legal and regulatory developments.

3. Data Controller

SellOut Limited is the data controller responsible for the collection and processing of biometric data under this Notice.

Registered Office: Unit A 82 James Carter Road, Mildenhall Industrial Estate, Suffolk, United Kingdom, IP28 7DE
Company Number: 13640565
Data Protection Officer: support@selloutweb.com

4. Types of Biometric Data Processed

We process facial geometry data to enable secure user authentication, prevent fraud, and enhance account protection. This data is classified as "biometric data" under Article 9 of the UK GDPR and is only processed where we have obtained your explicit consent.

At this time, we do not process behavioural biometrics (such as typing rhythm or mouse dynamics). If that changes, we will first conduct a Legitimate Interests Assessment (LIA) and update this Notice accordingly.

5. Lawful Basis and Conditions

Explicit Consent

We rely on your explicit, informed, and freely given consent before collecting or processing any facial scan data. Consent is obtained through a clear and separate opt-in mechanism that is distinct from general platform acceptance. You have the right to withdraw your consent at any time through your account settings or by contacting support@selloutweb.com. Withdrawal of consent will not affect the lawfulness of processing carried out prior to such withdrawal.

Automated Decision-Making

We do not make any fully automated decisions that produce legal or similarly significant effects based solely on facial scan data. Where automated processing supports security-related decisions (e.g., flagging a high-risk login), a human review will always be included in the final decision-making process, in accordance with Article 22 UK GDPR.

6. Data Sharing and Third Parties

Biometric data is used strictly for the purposes described above and is not disclosed to third parties unless required by law or contractually necessary.

Where disclosure is required, it may be shared with (i) government authorities such as HMRC or the police under a lawful request; or (ii) trusted fraud prevention partners, under strict confidentiality and data protection obligations.

If biometric data is transferred outside the United Kingdom, such transfers will be governed by appropriate safeguards in accordance with Chapter V of the UK GDPR, including the use of Standard Contractual Clauses (SCCs) or a UK adequacy decision.

7. Data Retention and Deletion

Facial scan data associated with active accounts will be retained until the data subject withdraws consent or closes their account. In the event of a fraud investigation, biometric data may be retained for up to 90 days following the conclusion of the investigation. Where we are under a legal obligation to retain biometric data, such retention will be limited to the minimum period required under applicable UK law.

All biometric data is permanently erased using secure deletion methods consistent with NIST Special Publication 800-88 Revision 1 (media sanitisation standards).

8. Security Measures

We implement robust security protocols to protect biometric data:

- **Technical measures** include AES-256 encryption, pseudonymisation, secure network transmission, and multi-factor authentication.
- **Organisational controls** include role-based access restrictions, staff confidentiality agreements, and audit trails of all access to biometric data.
- **Incident response** measures ensure that any personal data breach involving biometric data is promptly investigated and, where applicable, reported to the ICO within 72 hours, as required by Article 33 UK GDPR.

9. Data Subject Rights

You have the following rights under the UK GDPR in relation to your facial scan data:

- **Right of access:** You may request confirmation of whether we process your facial scan data and obtain a copy in a structured, commonly used, and machine-readable format.
- **Right to rectification:** You may request that we correct any inaccuracies or complete any incomplete biometric data.
- **Right to erasure:** You may request deletion of your facial scan data, subject to legal or regulatory retention obligations.
- **Right to object:** Where our processing is based on legitimate interests (if applicable in the future), you may object to that processing.
- **Right to restriction:** You may request a temporary pause in processing under specific circumstances, such as during the resolution of a data accuracy dispute.

To exercise these rights, please contact us at support@selloutweb.com. We will respond to your request within one month, in accordance with Article 12(3) UK GDPR.

10. Data Protection Impact Assessment (DPIA)

We have conducted a Data Protection Impact Assessment (DPIA) for our use of facial recognition technology, which identified the following potential risks:

- Unauthorised access to biometric databases;

- Algorithmic bias leading to false positive or false negative matches;
- Residual retention of biometric templates after deletion.

To mitigate these risks, we have implemented quarterly penetration testing, bias and accuracy audits of our algorithms, and strong encryption protocols for data in transit and at rest.

11. Updates and Complaints

We review this Notice at least twice annually or sooner where there are significant changes in law, guidance, or operational practices. Future amendments to UK data protection law—including any new statutes relevant to biometric data—will be incorporated as and when they come into force.

If you have any concerns or complaints regarding our use of biometric data, you may contact the Information Commissioner's Office (ICO) via: https://ico.org.uk/concerns

Annex A: Cross-Referenced Policies

- Dispute Resolution Policy – Section 4.3: Fraud Handling
- User Agreement – Clause 12: Data Security Obligations
- Privacy Policy

Accessibility Statement

We are committed to ensuring this Notice is accessible to all users. It has been prepared in accordance with **WCAG 2.1 AA** accessibility standards. If you require this document in an alternative format (such as large print or plain English), please contact support@selloutweb.com.

We maintain a timestamped record of consent for each user's biometric enrolment, which is stored securely alongside the user profile.

All decisions involving biometric data that could affect access or account status include a meaningful opportunity for human review prior to action.

A large print or plain language version of this Notice is available at: www.selloutweb.com/facial-privacy-easyread