Privacy Policy

1. Introduction

This User Privacy Policy governs your use of this website, as well as all SellOut applications, services, products, and tools (collectively, the "Services") provided by SellOut Ltd ("SellOut," "we," "us," or "our").

This policy complies with the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR), and the Platform Operators (Due Diligence and Reporting Requirements) Regulations 2023. This User Privacy Policy applies regardless of how you access or use our Services, including through mobile devices and apps. By using SellOut, you acknowledge and agree to the terms of this policy.

We reserve the right to modify this Privacy Policy at any time by publishing the updated User Privacy Policy on this website and indicating the effective date of the updated User Privacy Policy. You will be informed of any significant changes to this User Privacy Policy via our Messaging tools in My SellOut and/or by email.

2. Controller

SellOut Ltd, registered at Unit A 82 James Carter Road, Mildenhall Industrial Estate, Suffolk, United Kingdom, IP28 7DE, is the data controller for the purposes of UK data protection laws.

SellOut assumes the responsibility as the controller for gathering your personal data in direct connection with delivering our Services. This role is actively shaped by the manner in which you utilise these Services. As the controller, SellOut ensures that the collection of your data aligns with the service provision, tailoring data handling processes to correspond with your specific interactions and requirements within our platform. For data queries, contact us at support@selloutweb.com.

3. Data Processor

SellOut Ltd acts as the **Data Controller** for all personal data collected, determining the purposes and means of processing. **Amazon Web Services (AWS)** is designated as a **Data Processor**, responsible for secure data storage on behalf of SellOut.

In accordance with this Privacy Policy, Amazon Web Services, Inc. (AWS) Amazon is designated as the responsible entity for the processing of personal data of users. As the data processor, Amazon's responsibilities are centred around the storage and handling of users' personal data. This designation is based on the critical role Amazon plays in managing and safeguarding personal data within the scope of our service delivery.

In addition, you can reach out to the SellOut in charge of personal data processing at any time if you have any questions or complaints about how we handle your personal data. You can contact SellOut at support@selloutweb.com.

4. The Types of Personal Data We Collect and Process

This Policy outlines the various types of personal data that SellOut collects and processes. Our interaction with users, whether through service usage, web forms, community discussions, or account creation, involves a range of data collection and processing activities. Below, we detail the specific types of data we handle and the contexts in which they are gathered.

A. **Basic Identification Data:** When you create or update your SellOut account, or use our Services, we collect essential personal identifiers. This includes your name, address, phone numbers, email addresses, username, tax identification number. This data may be provided initially or at a later stage.

B. **Additional Seller Information:** For sellers using our Services, you may need further identification data, such as government-issued ID (e.g. social security number), birth date, tax identification numbers (such as VAT identification number), ID documents and the information they contain, selfie photos, and other information (such as bank account number) when you use our services as a seller.

C. **Transaction-Related Data:** Information related to your activities, such as bids, purchases, sales details.

D. **User-Generated Content:** Data shared through our messaging tools with other users.

E. **Financial Information:** Data related to your financial transactions such as numbers of your accounts and cards, details of your transactions, and method of payment.

F. **Transaction Logistics:** You must also provide us with information related to delivery details, billing information, customs clearance identifiers (e.g., tax IDs)
and other aspects of your transactions, as well as any identification numbers or information needed for customs clearance (such as tax IDs or other identifiers). Additionally, you must share relevant information about the delivery process (such as shipment numbers and tracking information).

G. **Demographic and Personal Preferences:** Depending on the situation, we may collect different types of data from you, such as: your age, gender, country birth, nationality, residence country, work status, family situation, hobbies and interests.

H. **Support and Issue Reporting:** If you report an issue to SellOut, we will ask you for some information that can help us identify you, such as your name and email address, and any other details that you choose to share with us in your report.

I. **Community and Customer Engagement:** You might provide further details via an online form, or by updating the information in your SellOut account. This could also include by engaging in community forums, member chats, participating in surveys or inquiries, being involved in dispute resolution procedure, or interacting with customer service on calls recorded with your permission. Additionally, this can occur if you reach out to us for any other matters related to our Services.

J. **Legal Compliance and Verification:** Additional information that we are obligated or permitted to gather and process under relevant legal provisions, necessary for your verification, authentication, or for confirming the accuracy of the data we acquire.

K. **Biometric Verification for Account Security**

   i. **Selfie Verification Across Devices:** Regardless of the device used for access – be it Apple, Windows, Android devices, or web browsers – users are required to take a selfie for identity verification purposes upon signing up. This step is integral for verifying user identity and enhancing account security.

   ii. **Data Storage and Compliance:** The biometric data (selfie) collected for this verification will be securely stored in the database. We commit to processing and safeguarding this data strictly in line with UK GDPR and the Data Protection Act 2018, ensuring compliance with relevant regulations and standards. Users will be required to provide explicit consent before their biometric data is processed, and an

alternative verification method will be available for those who do not wish to provide facial recognition data.

iii. **Retention and Deletion of Biometric Data:** The selfie image will be retained in our database only for the duration of the user's account being active. It will be permanently deleted from our system once the user decides to delete their account. This approach aligns with our commitment to data minimisation and privacy, ensuring that personal data is not held beyond the necessary period.

L. **VAT & HMRC Reporting Compliance:** Under the Platform Operators (Due Diligence and Reporting Requirements) Regulations 2023, SellOut is legally required to report certain seller data to His Majesty's Revenue and Customs (HMRC) if specific thresholds are met. This may include:

- Seller's name and contact details.
- Transaction history, including total sales revenue.
- VAT registration status (if applicable).
- Tax identification number (if required by law).

These disclosures are made in compliance with UK tax laws and are necessary for maintaining regulatory compliance for online marketplaces.

M. **Value Added Tax (VAT) and HMRC Compliance**: All sellers on SellOut are responsible for understanding and complying with UK Value Added Tax (VAT) regulations, as governed by HM Revenue & Customs (HMRC). Failure to comply with VAT regulations can result in penalties and investigations by HMRC.

VAT Registration Threshold: Sellers whose taxable turnover exceeds the current VAT registration threshold (currently £90,000 as of March 2025, but subject to change) in a rolling 12-month period must register for VAT with HMRC. Information on VAT registration can be found on the official GOV.UK website.

VAT Responsibilities:

Sellers are required to:

- Charge VAT on applicable goods and services sold to UK customers.
- Issue VAT invoices to customers.

- Submit regular VAT returns to HMRC.
- Maintain accurate and complete records of all sales, purchases, and VAT transactions.

HMRC Guidance and Resources: Sellers should consult HMRC's resources for detailed information on VAT compliance.

Disclaimer: Sellout is not responsible for providing tax advice. This information is for guidance only, and sellers should consult with a qualified accountant or tax advisor for specific advice regarding their VAT obligations.

4.1. Automatic Collection of Personal Data in Using Our Services or Creating a SellOut Account

This section details the types of personal data that are automatically collected when you use our Services or create a SellOut account. The data collection is integral to enhancing user experience and ensuring the smooth functioning of our services.

A. **Transaction-Related Data:** During your transactions, we automatically gather generated information such as details related to bids, purchases, sales, fees, is collected. This includes data associated with your SellOut account resulting from transactions you engage in, like transaction amounts, timing and locations, and methods of payment or payout.

B. **Account Activity Data:** Data arising from your additional activities while utilising our Services, which is connected to your SellOut account. Examples include account numbers, preferred currency, activities like adding items to your shopping cart, placing items on a watch list, saving searches, following other users, or attempting to use third-party services for payments or other purposes.

C. **Service Interaction Data:** Information concerning all other interactions with our Services, including your advertising preferences and communication records with us.

D. **Geographical Information:** This encompassing both general (such as IP address) and, with your consent, precise location data from your mobile device. It's important to note that on most mobile devices, you can control or disable precise location services for all apps via the device's settings menu.

E. **Image Metadata:** Metadata related to camera settings in images you upload for items on sale.

F. **Device and Connection Information:** Information about your computer and internet connection, including usage statistics of our Services, data on web traffic, referral URLs, advertisement data, your IP address, times of access including pages visited within our Services, language preferences, and weblog information.

4.2 Collection of Personal Data Through Cookies and Similar Technologies

In the course of our Services, we employ cookies and technologies akin to cookies to gather information. This collection happens through the devices (inclusive of mobile devices) you employ to access our Services. The gathered data encompasses usage and device-specific details:

A. **Webpage Interaction Information:** Information on the webpages you visit, including times of access, frequency, duration, the links you engage with, and other actions you undertake in using our Services, as well as within advertising and email content.
B. **Advertising Interaction Details:** Details of your interactions with our advertising partners, covering information about the ads shown to you, their frequency, timing, placement, and your responses, such as clicks or purchases made.
C. **Device-Specific Information:** Information about your device is collected, including the device model, operating system and its version, browser type and settings, device ID or unique device identifier, advertising ID, specific device token, and cookie-specific data (like cookie ID).
D. **IP Address Data:** The IP address used by your device to connect to our Services.
E. **Geographical data:** Geographical data is collected in two forms: General location data (e.g., IP address), and Precise location data from your mobile device, subject to your consent. It's noteworthy that most mobile devices provide options to control or disable precise location services for all applications through the device's settings.
F. **Compliance with PECR and UK GDPR**: SellOut ensures that cookies and similar tracking technologies comply with UK GDPR and PECR regulations. Users will be required to provide **explicit consent for non-essential cookies**, including those used for targeted advertising and analytics. Users may manage their preferences through the Cookie Settings available on the platform.
G. **Third-Party Cookies and Data Sharing**: Some tracking technologies may be placed by third-party service providers, including advertising networks and analytics partners. Users will be informed about the use of such third-party cookies, and consent will be required where applicable.

4.4 Collection of Personal Data from other Sources

We may additionally acquire personal data pertaining to you from various external sources and third parties, as allowed under relevant laws. This encompasses the following types of information:

A. **Data from Public Sources:** We collect personal data from publicly accessible sources such as publicly available sanctions lists. This helps us to stay compliant with legal requirements and maintain the integrity of our services.
B. **Information from Credit Agencies:** We obtain data from credit agencies or bureaus, including credit evaluations/checks, verification of identity, information useful for risk assessment, and determination of credit limits.
C. **Information from data providers:** We acquire information from data providers, which might include identity verification (**Know Your Customer - KYC** procedures), demographic data, and details pertinent to interest-based and online advertising. This enhances our ability to tailor our services to your needs and preferences.
D. **Information from government or other authorised entities:** We access information from government or other authorised entities regarding any past convictions of the respective seller, within the bounds of applicable laws. This is essential for legal compliance and ensuring the safety of our platform. In compliance with UK tax regulations, we may also collect VAT registration details and tax-related information where required.
E. **Integration with Data from Additional Sources:** We integrate or link the personal data we collect directly from you with the data obtained from these additional sources. When receiving personal data from third parties, we ensure that these entities are legally allowed to share this information with us. We also have access to personal data about you from SellOut Affiliates. We ensure that all third-party data sharing complies with UK GDPR and Data Protection Act 2018.
F. **Data from Payment Processors & Financial Institutions**: If you make or receive payments through SellOut, we may collect and verify payment-related information from payment processors such as PayPal or Stripe. This includes transaction history, account verification, and fraud prevention data, in compliance with **Financial Conduct Authority (FCA) regulations** if applicable.

5. The legal basis and purposes for Data processing

We engage in the processing of your personal data for multiple objectives, grounded on various legal bases that authorise such processing. These purposes include, but are not limited to, delivering and enhancing our Services, offering a tailored user experience on the SellOut website and app, communicating with you about your SellOut account and our Services, customer support, personalised marketing and advertising communications, and for the identification, prevention, and investigation of fraudulent or illegal activities. We also distribute your information to third-party entities including service providers acting on our behalf for these purposes.

Herein is a summary of the purposes for processing your personal information, including the types of recipients to whom we transfer personal information for the stated purposes, categorised by our legal basis for this processing or sharing:

A. **Contractual Necessity**: Processing your data is necessary to fulfill our contractual obligations when providing our services, such as:

- Facilitating transactions and processing payments.
- Managing your account and providing customer support.
- Delivering goods and services purchased through the platform.

B. **Legitimate Interests**: We process your data based on our legitimate business interests, including:

- Fraud detection and prevention.
- Enhancing security and verifying user identities.
- Conducting analytics and improving platform functionality.
- Sending relevant notifications and service updates.

C. **Legal Compliance**: We process and share data where required to comply with legal obligations, including:

- Complying with **HMRC reporting requirements** for VAT and seller transactions.
- Verifying seller identity and compliance with **anti-money laundering (AML) regulations**.
- Ensuring compliance with **Financial Conduct Authority (FCA) regulations** where applicable.

D. **User Consent**: In certain situations, we process personal data based on explicit consent, including:

- Marketing communications and advertising.
- Use of biometric data for identity verification.
- Cookies and tracking for analytics and advertising (opt-in required under PECR).

E. **Automated Decision-Making & Profiling**: In some cases, we may use automated processes to assess transaction risks, prevent fraudulent activities, or provide personalised experiences. Users have the right to request human intervention in any automated decision that significantly affects them.

5.1 Data Processing for Contractual Compliance and Service Provision

A. **Contractual and Service-Related Data Management:** We engage in processing your personal data to fulfill our contractual obligations with you and to deliver our Services effectively.

B. **Service Delivery and Transaction Facilitation:** Our services involve enabling and conducting transactions with other users. This involves transferring your personal data to other users when necessary for completing the transaction, even in instances of terminated, unsuccessful, or later invalidated transactions, such as sharing your return address to facilitate item returns. Additionally, we process transaction-related data to:

- Showcase your transaction and feedback history.
- Enhance features like payment processing, ratings, authentication services, and SellOut account management.
- Offer other services as detailed in connection with those services.
- Maintain the functionality of our Services.
- Notify you about transaction execution and Service usage based on the communication preferences set in your SellOut account.

C. **Delivery Coordination and Notifications:** Facilitation of item delivery via logistics and delivery service providers, including delivery-related notifications (e.g., tracking details), as permitted by law without requiring your consent.

D. **Comprehensive Customer Support:** Offering comprehensive customer support, which covers resolving issues with your SellOut account, mediating disputes, providing other customer service-related services, and pursuing fee claims. For these purposes, we may reach out to you through notifications in My SellOut, email, phone, SMS, push notifications on your mobile device, or postal mail. If we contact you by phone, for efficiency, we may utilise automated calls with recorded messages or automated texts to the extent permitted by applicable law without your consent.

E. **Processing Location Information for Service Enhancement:** We may process general location information (like IP address or postal code) to offer location-based services.

F. **Tax Compliance & HMRC Reporting:** Where required under UK tax regulations, SellOut may process and share seller VAT details and transaction history with His Majesty's Revenue and Customs (HMRC). This ensures compliance with Platform Operators (Due Diligence and Reporting Requirements) Regulations 2023.

G. **Financial Conduct Authority (FCA) Compliance:** If SellOut facilitates financial transactions, we process user payment details in accordance with FCA guidelines, ensuring secure handling of payment data and fraud prevention measures.

When required, we may transfer your personal data to processors and various recipients for one or more of the outlined purposes. These recipients include:

- Other SellOut users.
- Third-party service providers, partners for authentication, physical storage services, and delivery firms (like DHL, UPS, etc.).
- Government bodies or official agencies (inclusive of customs and taxation authorities).
- Providers of payment services.
- External entities operating websites, applications, services, and tools.

5.2 Processing Personal Data for Legal Compliance

We process your personal data to adhere to legal obligations we are subject to. This involves various purposes, such as:

A. **Legal Investigations and Proceedings:** We process your personal data for participating in and aiding investigations and legal proceedings conducted by public or governmental bodies, primarily for detecting, investigating, and prosecuting illegal actions.

B. **Prevention and Mitigation of Illegal Activities:** Our processing activities include efforts to prevent, identify, and reduce unlawful activities, such as fraud, money laundering, financing of terrorism, child exploitation, and violations of sanctions laws, in line with compulsory reporting duties.

C. **Third-Party Information Requests:** We respond to valid requests for information from third parties who hold legal claims to such data, particularly in cases involving intellectual property infringement, counterfeiting, or other unlawful acts.

D. **Compliance with Laws:** We fulfill our obligations related to data collection, verification, disclosure, and reporting under laws in connection with consumer protection, anti-fraud measures, online platform operations, and taxation. This includes obligations under the Online Safety Act 2023, which imposes duties on online platforms to ensure user safety by monitoring and removing harmful content.

E. **Financial & Credit Reporting Compliance:** Where legally required, we may share relevant data with credit reporting agencies or bureaus, including information on delayed payments or defaults.

F. **Regulatory Data Transfers:** When necessary, we transfer your personal data to:
   - Law enforcement, courts, government entities, and public authorities (including tax and financial bodies).
   - Intergovernmental or supranational organisations for regulatory compliance.
   - Third-party service providers explicitly chosen by you, subject to your consent.
   - Third parties involved in legal proceedings if required under court orders or similar legal requests.

G. **Automated Decision-Making for Fraud Detection:** SellOut may use automated processing to detect suspicious transactions and prevent fraudulent activities. Users have the right to request human intervention in cases where automated decisions significantly impact them.

5.3 Processing Personal Data for Protecting Vital Interests

Our processing of your personal data focuses on protecting your vital interests or those of another person, involving the prevention, detection, mitigation, and investigation of illegal activities that could impact these vital interests, unless legally obliged otherwise. As needed, we share your personal data with processors and recipients for the aforementioned purposes, which include:

- **Law Enforcement and Governmental Authorities:** Data may be transferred to UK law enforcement agencies, courts, government bodies, or public authorities, including intergovernmental or supranational organisations, in accordance with the Online Safety Act 2023. We cooperate with UK regulators such as the Information Commissioner's Office (ICO) and Ofcom in cases involving fraud, online harm, or illegal activities.
- **Parties in Legal Proceedings:** We provide personal data to third parties engaged in legal proceedings, ensuring compliance with the UK GDPR's data minimisation principle.
- **SellOut Affiliates:** Your personal data might also be shared with SellOut Affiliates as part of this protective process, subject to data processing agreements that align with UK data transfer laws.
- **External Third-Party Service Providers:** We may transfer personal data to third-party service providers who assist in these protective efforts, ensuring they comply with UK International Data Transfer Agreements (IDTAs) or equivalent safeguards.

5.4 Data Processing for Legitimate Interests

We process your personal data when it's necessary for the legitimate interests pursued either by us or a third party, provided these interests are not outweighed by your own interests, rights, and freedoms. In accordance with the UK GDPR, we have conducted Legitimate Interest Assessments (LIAs) to ensure compliance. Based on this, we process your data for the following reasons:

1. **Legal Investigations and Proceedings:** We engage in processing personal data for involvement in investigations and proceedings by UK courts, law enforcement agencies, and government bodies to identify, investigate, and prosecute unlawful activities. We disclose data only when necessary to prevent imminent harm or to report suspected illegal activities, and within the bounds of applicable UK laws. This may include your name, city, postcode, phone number,

email address, (previous) usernames, IP address, fraud complaints, and bidding and listing history.

2. **Protecting Third-Party Interests in Civil Disputes:** To safeguard the interests of third parties in civil disputes, we may disclose necessary information to these third parties to prevent imminent harm. Data such as the seller's name, address, city, postcode, country, phone number, email address, and company name is shared under strict confidentiality agreements.
3. **Fraud and Crime Prevention:** Our processing activities include preventing, detecting, mitigating, and investigating fraud, financial crimes, security incidents, and other illegal or prohibited activities. Automated decision-making systems, including fraud detection algorithms, may be used. Users have the right to request human intervention in cases where decisions impact their rights.
4. **Service Security Enhancement:** We actively work on enhancing the security of our Services by monitoring and implementing security measures, unless legally required otherwise.
5. **Identity and Credit Checks:** Conducting identity verification, creditworthiness assessments, and financial background checks, evaluating applications, and comparing information for accuracy and verification under UK financial regulations.
6. **Message Review for Security:** We may automatically filter and, when needed, manually review messages sent via our messaging tools to prevent fraudulent or suspicious activities or breaches of our rules and policies.
7. **Service Improvement Analysis:** We analyse and improve our Services by evaluating site usage data or feedback on blocked or crashed pages to enhance user experience, including as part of product development.
8. **Marketing Communications:** Communicating with you via email, text message, or phone, to present vouchers, discounts, special offers, conduct surveys and opinion polls, and inform you about our Services (based on your SellOut account preferences). If you choose to opt out of marketing emails, you can unsubscribe via the link in the email's footer. Please note, customisation of webpage and app content to show items and services that might interest you based on your activities.
9. **Evaluating the effectiveness of our email marketing:** We assess the effectiveness of our email marketing, targeted advertising, and promotional campaigns to ensure compliance with UK regulations, including the UK GDPR and the Online Safety Act 2023. This involves analysing engagement metrics, optimising campaign performance, and ensuring that marketing communications align with legal consent requirements. We implement clear opt-in and opt-out mechanisms, provide users with greater transparency on how their data is used for

targeted marketing, and ensure compliance with profiling regulations. Additionally, we evaluate automated decision-making processes in advertising to safeguard user rights, including the ability to object to personalised marketing strategies.

10. **Service Delivery Monitoring:** We monitor service delivery status, including tracking information when sellers use delivery labels from carriers through SellOut or provide tracking numbers. This ensures compliance with the UK Online Safety Act 2023, particularly in relation to safeguarding consumers against fraudulent transactions and ensuring transparency in digital commerce.
11. **Content Sharing with Affiliates and Providers:** We share content related to service registration, transaction handling, and customer support with SellOut or our payment service providers. In accordance with the UK GDPR and the Data Protection Act 2018, we ensure that any data sharing is conducted under strict data protection agreements and that users retain control over their personal information.
12. **Legal Claim Management:** We manage legal claims, including those between SellOut users, in compliance with UK data protection laws and consumer protection regulations. This includes securely processing and storing personal data for legal purposes while ensuring users' rights under the UK GDPR.

When required, we share your personal data with processors and various entities for one or multiple purposes as previously outlined:

● **Third-party service providers** – Ensuring compliance with updated UK privacy regulations, including the UK Online Safety Act 2023 and the Data Protection Act 2018.

● **Other SellOut users** – Facilitating transactions in line with consumer rights and dispute resolution frameworks.

● **Law enforcement bodies, judicial courts, governmental bodies, or public authorities, intergovernmental or supranational organisations** – Meeting legal obligations such as fraud prevention and financial crime investigations.

● **Third parties engaged in legal proceedings** – Ensuring due process and data security in legal claims.

● **Other entities in cases of investigations into fraud, intellectual property violations, retail crime, possession of stolen goods, counterfeiting, or other illegal activities** – Enhancing compliance with the UK's latest regulations on digital commerce.

● **Providers of payment services –** Ensuring adherence to financial regulations, including UK anti-money laundering (AML) laws.

● **Credit reporting agencies or bureaus, data verification services, risk assessment entities, and collections agencies** – Processing details regarding late payments, defaults, or other anomalies that may impact credit scores, in accordance with UK credit and financial regulations.
● **Other corporations in the event of a business acquisition** – Conducting data transfers in compliance with UK data protection laws.

5.5 Processing of Your Personal Data with Consent

A. **Location-Based Services:** We use your precise location data, with your consent, to provide services tailored to your location. In compliance with UK GDPR, most mobile devices allow you to manage or disable precise location services for all applications and webpages.
B. **Financial Information Retention:** With your consent, we retain your financial information, such as credit card and bank account numbers, to streamline future transactions while ensuring compliance with UK financial security regulations.
C. **Biometric Data for Fraud Prevention:** We process biometric data for identification purposes to help prevent fraud and minimise risks on our platform, particularly in connection with Know Your Customer (KYC) and similar regulatory requirements under UK financial laws.
D. **Consent-Based Data Processing for Service Provision:** We process your personal data based on the consent you've provided, enabling us or third parties to offer or make available specific services while ensuring compliance with UK GDPR and the Online Safety Act 2023.

6.2 International Data Transfers

A. **Global Data Transfers:** We may transfer your personal data to recipients worldwide. Transfers from the United Kingdom to countries outside the UK, including the EEA and other third countries, are conducted based on appropriate safeguards or as permitted by the UK Data Protection Act 2018 and ICO guidelines.
B. **Transfers to the EEA:** For data transfers to the EEA, we adhere to the UK's adequacy regulations and decisions, ensuring a level of data protection comparable to UK standards.
C. **Transfers to Adequately Regulated Countries:** The UK Information Commissioner's Office (ICO) adequacy regulations recognise certain jurisdictions as providing an adequate level of data protection, including Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, and the Republic of Korea.

D. **Country-Specific Data Transfer Provisions:** Additionally, the ICO's adequacy recognition extends to certain countries with specific limitations:
    - Canada: Adequacy applies only to data under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
    - Japan: Adequacy is limited to personal data transferred to private sector entities under Japan's Act on the Protection of Personal Information, excluding types of transfers covered by the EU's adequacy decision for Japan.
    - USA: Data transfers to the USA are governed by the UK Extension to the EU-US Data Privacy Framework.

E. **Transfers to Non-Adequate Countries:** In cases where transfers are made to countries not recognised as providing adequate protection, we implement necessary safeguards such as data protection agreements incorporating standard data protection clauses recognised by the UK data protection authorities with the recipients, or through other measures provided for by UK law.

7. Data Storage and Deletion

A. We retain your data only as long as necessary for the purpose it was collected. If you have an account, we keep your data while your account is active. In cases where your account is deactivated, either by you or due to prolonged inactivity, we retain your data for a reasonable period thereafter. Additionally, we may retain your data for legal, regulatory, or technical reasons, in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

B. The determination of the data retention period considers the volume, nature, and sensitivity of the data, potential risk from unauthorised use or disclosure, the purposes for which we use your data, whether these purposes can be achieved through other means, and any applicable legal obligations. Additionally, under HM Revenue & Customs (HMRC) requirements, we may be required to retain certain transaction and financial data for at least six years for tax and audit purposes.

C. For active accounts, your data is retained throughout the account's active status. If your account is deactivated, we retain your data for a certain period post-deactivation, subject to the lawful basis for retention. Data necessary for fraud prevention, security, and dispute

resolution may be stored longer, in line with the UK Information Commissioner's Office (ICO) guidelines on lawful retention periods.

D. Post-deactivation, your data may be retained for legal, regulatory, or technical reasons, including in backup systems, to preserve transaction records, enforce rights, comply with anti-money laundering (AML) regulations, and enable access to historical transaction data when required by law. Following this period, we will either delete or anonymise the data, with or without notice, ensuring that it can no longer be linked to an identifiable individual.

E. Should your account be deactivated, some of your data might remain visible within the Service, for example, if other users have shared your data in public interactions such as reviews or discussions. If your account is banned due to policy violations or security concerns, we retain certain data indefinitely to prevent new account creation, safeguard SellOut, its users, and the overall security of the platform. Additionally, under UK law, data related to fraud, abuse, or disputes may be retained for a longer period to comply with legal investigations or regulatory requirements.

F. Specific Data Retention Periods

To ensure compliance with UK law, we retain different types of data for the following periods:

Data Type	Retention Period	Legal Basis
User Account Data (Name, Email, Address)	Until account deletion + up to 2 years	Necessary for fraud prevention & service continuity
Transaction Records (Orders, Sales, Payments)	6 years	Required under UK tax & financial regulations (HMRC)
Messaging & Communications (Chats, Emails with Support)	3-6 months after account deletion	For dispute resolution & customer service
Fraud Prevention & Security Logs (IP addresses, Login History)	Up to 5 years	To detect fraudulent activities
Banned Accounts & Policy Violations	Indefinitely or at least 5 years	To prevent re-registration & protect users

For specific retention periods of different data aspects, please contact us at support@selloutweb.com.

8. Your Rights as a Data Subject

As a data subject under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, you have several rights concerning your personal data. These rights include access to your data, correction, deletion, restriction of processing, and data portability. Additionally, you have the right to withdraw consent, object to processing based on legitimate interests, and file a complaint with a regulatory authority. Your rights are subject to limitations where processing is necessary for legal compliance, public interest, or the protection of other individuals' rights and freedoms.

A. **Withdrawal of Consent:** You can revoke your consent for us to process your personal data at any time. Consequently, we will no longer process your data based on this consent moving forward. The withdrawal of consent does not affect the lawfulness of processing that occurred before the consent was withdrawn. If processing relies on another legal basis, such as contractual necessity or compliance with legal obligations, we may still process certain data despite your withdrawal of consent.
B. **Right to Access:** You have the right to request and obtain a copy of your personal data that we process. This includes:

- The purposes of data processing.
- The categories of personal data being processed.
- The recipients or categories of recipients to whom data has been disclosed or will be disclosed.
- The intended retention period for storing personal data or, if not possible, the criteria used to determine this period.
- The rights available to you, including rectification, erasure, restriction of processing, and objection.
- The source of the data, if not collected directly from you.
- Any information regarding automated decision-making, including profiling.

This right is subject to limitations, including cases where disclosing data would adversely affect the rights and freedoms of others, national security, or ongoing investigations. We will process requests within one month, with possible extensions under complex circumstances, as permitted by UK GDPR.

C. **Right to Rectification:** If your personal data is inaccurate or incomplete, you have the right to request its correction without undue delay. Where necessary for verification purposes, we may ask you to provide supporting documentation to validate the correction request. If we

have shared incorrect data with third parties, we will inform them of the correction unless it is impractical.

D. **Right to Erasure:** You You can request the deletion of your personal data in specific circumstances, including:

- The data is no longer needed for its original purpose.
- You withdraw consent, and there is no other legal basis for processing.
- You object to processing, and there are no overriding legitimate grounds.
- The data has been unlawfully processed.
- The data must be erased to comply with a legal obligation under UK or EU law.

This right does **not** apply where processing is necessary for:

- Freedom of expression and information.
- Legal compliance (e.g., financial or tax record retention under HMRC requirements).
- Public interest or scientific/historical research.
- The establishment, exercise, or defense of legal claims.

E. **Right to Restrict Processing:** You may request that we limit the processing of your personal data in certain situations, such as:

- If you contest the accuracy of your data (restriction applies while verification is ongoing).
- If processing is unlawful, but you prefer restriction instead of deletion.
- If we no longer need the data, but you require it for legal claims.
- If you have objected to processing and we are assessing whether our legitimate interests override your rights.

During a restriction period, your data will only be stored and not processed, except with your consent or for legal claims. If the restriction is lifted, we will inform you before resuming processing.

F. **Right to Data Portability:** You have the right to receive your personal data in a **structured, commonly used, and machine-readable format** and transmit it to another data controller where:

- The processing is based on consent or contractual necessity.
- The processing is carried out **by automated means**.

This right does not apply to data processing based on legal obligations, public interest, or security-related processing.

G. **Rights Related to Automated Decision-Making & Profiling:**

You have the right not to be subject to a decision based solely on automated processing, including profiling, if it produces legal effects or similarly affects you. However, exceptions apply where:

- Automated processing is necessary for contract performance.
- It is authorised by law.
- You have given explicit consent.

In such cases, you have the right to obtain human intervention, express your views, and contest the decision.

H. **Right to Lodge a Complaint:** You have the right to lodge a complaint with a supervisory authority. If you have concerns regarding our data handling, you're entitled to file a complaint with the UK's Information Commissioner's Office (ICO). The ICO offers a detailed process for lodging complaints, accessible in their "for the public" section. For further information and to initiate a complaint, please visit the ICO website here.

To act upon any of the rights outlined in this section, you may reach out to SellOut and forward your request via support@selloutweb.com.

9. Use of Cookies and Comparable Technologies

In our Services, both SellOut and authorised third parties employ cookies and related technologies (collectively referred to as "cookies") to enhance your experience, making it faster and more secure, and to deliver tailored advertising to you. You can access comprehensive details on the usage of cookies and similar technologies, along with your choices, in our User Cookie Policy.

A. **The Functions of Cookies and Similar Technologies:**

- Some are essential for operating our Services.

- Others aid in technical optimisation of our Services (like tracking error notifications and load times).
- Several enhance user experience (for example, remembering font size preferences and data entered in forms).
- Certain cookies are used to present you with more relevant advertisements.

B. Types of Cookies:

- **Session Cookies:** Active only while your browser is open.
- **Persistent Cookies:** Remain on your device for an extended period. We implement robust security measures to safeguard against unauthorised access to our cookies and similar technologies.

C. Managing Cookies:

You have the option to disable cookies and similar technologies if your device supports it. Cookie settings can be managed through your browser or device settings. Under the UK Privacy and Electronic Communications Regulations (PECR) and the UK GDPR, we are required to obtain your explicit consent for the use of non-essential cookies. When you first visit our website or app, we will present a cookie consent banner that allows you to accept or reject different categories of cookies.

- You can withdraw or modify your cookie preferences at any time through our Cookie Settings tool.
- Essential cookies, which are strictly necessary for the operation of our Services, cannot be disabled.

D. Third-Party Cookies:

Third-party cookies may be used in connection with advertising, analytics, and social media integration. These cookies are subject to the privacy policies of the third parties placing them. For details on third-party cookies and opt-out options, visit:

www.youronlinechoices.com
www.aboutads.info/choices
www.networkadvertising.org/choices

E. **Note on Advertisements Without Third-Party Cookies:**

Opting out of third-party data processing for advertising purposes via cookies does not eliminate advertisements. It simply means that the ads you see will not be personalised based on cookie data or similar technologies.

F. **Compliance with UK Law & ICO Guidelines:**

- Our cookie policy aligns with the **UK GDPR**, the **Data Protection Act 2018**, and the **Privacy and Electronic Communications Regulations (PECR)**.
- The UK Information Commissioner's Office (**ICO**) has set out strict guidelines on obtaining consent for cookies, which we fully adhere to.
- If you have concerns about our use of cookies, you can file a complaint with the ICO at www.ico.org.uk.

10. Data Security

At SellOut, safeguarding your personal data is a top priority. Our security strategy includes utilising Amazon Web Services (AWS) for data storage and processing, taking advantage of AWS's extensive security features. We implement robust network security measures and data encryption technologies to enhance protection. AWS provides stringent physical access controls to its data centres and robust logical access controls to data and systems. These combined efforts ensure a high level of data security, keeping your personal information secure and protected. In compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, we continuously assess and update our security measures to mitigate risks and protect your rights.

11. Information Visibility Among Users

A. **Shared Information on SellOut Platform:** As a member of SellOut, the information you post or share, either on the SellOut platform or with other members, is visible to others. This transparency includes details like: Your bids and purchases, Items you are selling, your saved interests and favourite sellers, search history and storefronts. Feedback you've provided, your ratings, product reviews, and associated comments. Furthermore, any personal details you choose to display in your profile are accessible to other users.

B. **Display of Public User ID:** Your public user ID is a visible element associated with all your public activities on SellOut. When we notify other users about potential suspicious activities or policy

violations, these notices may include your public user ID and reference specific listings. It's important to note that if your username is easily identifiable, it may allow others to associate it with your SellOut activities.

C. **Access to Personal Data in Transactions:** While we strive to protect your personal data, it's necessary for other users to access certain information to facilitate transactions and payments. This access is limited to essential data only. During transactions, users have access to each other's: Names and user IDs. Email addresses, other contact and shipping information. For example, it's possible for users to exchange phone numbers to communicate about a transaction, such as a seller providing their number to a buyer for queries about an item for sale. However, it's mandatory that such personal contact information is solely used for the intended transaction on SellOut. Sellers are prohibited from using a buyer's phone number for unrelated purposes, including transactions outside SellOut or for adding the buyer to marketing lists. Users must comply with the UK GDPR when processing or handling personal data acquired from other users.

D. **Data Exchange in Transactions:** In any transaction on SellOut, whether completed, cancelled, unsuccessful, or invalidated, we will provide you with the personal information of the other user involved. This includes Name, username, email address, contact details, shipping and billing information, return address, if applicable. Upon receiving this data, you assume the role of data controller. This designation brings the responsibility for any subsequent data handling, ensuring adherence to the guidelines set forth in this User Privacy Policy and relevant policies. Under the UK GDPR, you are responsible for ensuring the lawful processing of this data and responding to any data subject requests, such as access or erasure requests, within the legally required timeframes.

E. **Beyond Personal Use:** If your usage extends beyond personal purposes, it is recommended to detail your data processing activities within the Privacy Policy. Ensure the protection of other users' privacy. For sellers, compliance with applicable data protection laws is mandatory, particularly in upholding the rights of other users as data subjects. This encompasses facilitating user access to their personal data under your control and arranging for data erasure upon user request. Sellers and other business users must also register with the UK Information Commissioner's Office (ICO) if required.

F. **Permissible Use of User Data:** Personal data obtained from other users must only be employed for SellOut transaction-related activities, Services provided via SellOut, such as delivery logistics, fraud complaint resolution, and user-to-user communications. Purposes for which the data subject has explicitly given consent. Any use of other users' personal data for

alternate objectives, like adding them to a mailing list without clear consent, is a violation of our User Agreement and may be subject to penalties under the UK GDPR.

12. Essential Personal Information and Its Use

A. **Mandatory Personal Information for Service Agreements:** Certain personal information you provide to SellOut is required to comply with our policies. This information is necessary for our operations. You are required to provide identifiable information like your legal name, date of birth, and either a tax identification number or social security number. This is a requirement for us to meet our "Know Your Customer" (KYC) legal obligations under UK financial regulations, including the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

B. **Sharing of Personal Information Within SellOut and With Service Providers**: As per our Privacy Policy, we may need to share some of this essential information with other SellOut Affiliates. This facilitates various transaction processes. Additionally, this information may be shared with external service providers, including but not limited to payment processors, credit agencies, and bureaus, to ensure seamless transaction experiences. Any sharing of personal data will be done in accordance with the UK GDPR, ensuring appropriate safeguards and lawful bases for processing.

C. **Voluntary Provision of Additional Personal Data:** Providing other types of personal data, such as your address and delivery details, while voluntary, can be important for the full use of our Services. This additional information may be required for activities within our Services, including but not limited to bidding, purchasing, and selling, which are integral to completing transactions on the SellOut platform. Any optional personal data you provide will be handled under the principles of data minimisation and purpose limitation as required by UK GDPR.

13. Children use of SellOut

Our services are not intended to be accessible to children, in accordance with the relevant national laws defining a child. Our services are tailored for users who are legally not considered children. We do not knowingly collect personal data from users classified as children. In compliance with the UK Children's Code (Age Appropriate Design Code), we ensure that our platform does not target or encourage engagement from individuals under the age of 18. If we become aware of personal data belonging to a child being processed, we will take immediate steps to delete such information in accordance with applicable laws.