

DATA RETENTION POLICY

1. INTRODUCTION

This Data Retention Policy ("Policy") sets out how Wondr Technologies UK Limited (the "Company") retains, reviews, and securely deletes personal data in accordance with applicable data protection legislation, including the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable, the EU General Data Protection Regulation.

The Company recognises that personal data must not be retained for longer than is necessary for the purposes for which it is processed. This Policy reflects the storage limitation principle and ensures that retention periods are clearly defined, justified, and consistently applied across the organisation.

2. PURPOSE

The purpose of this Policy is to ensure that personal data processed by the Company is retained only for lawful and legitimate purposes, that appropriate retention periods are applied to different categories of data, and that secure deletion or anonymization is carried out once those purposes have been fulfilled. This Policy also aims to reduce legal, regulatory, financial, and reputational risk by ensuring systematic and documented retention management.

3. SCOPE

This Policy applies to all personal data processed by the Company in its capacity as data controller. It covers personal data relating to users of the REVELTRY platform, prospective users, employees, contractors, shareholders, directors, service providers, and business contacts. It applies to personal data processed directly by the Company as well as data processed on its behalf by authorised processors, including group entities and contracted service providers.

4. GENERAL RETENTION PRINCIPLES

The Company retains personal data only where there is a lawful basis for doing so. Personal data shall be kept for no longer than is necessary to fulfil contractual obligations, comply with legal requirements, protect legitimate business interests, or establish, exercise, or defend legal claims. Where personal data is no longer required, it shall be securely deleted or irreversibly anonymised. Where legal or regulatory

obligations require retention, the data shall be restricted to those statutory purposes only and shall not be used for any unrelated processing activities.

5. RETENTION OF USER ACCOUNT DATA

Personal data collected in connection with user accounts on the REVELTRY platform includes identification details such as name, email address, telephone number, authentication information, social login identifiers, device identifiers, IP address data, and associated profile information.

Such personal data shall be retained for the duration of the user's active account and for a period for which it is necessary for the purpose it was collected. This retention period reflects the applicable limitation period for contractual claims under English law and the Company's legitimate interest in defending potential disputes.

Where a user requests account deletion, the account shall be deactivated without undue delay. Personal data shall be restricted from active processing and retained only where necessary to comply with legal obligations or to defend legal claims during the applicable retention period. You may request account deletion by accessing this [link](#).

6. RETENTION OF FINANCIAL AND TRANSACTION DATA

The Company processes financial data relating to deposits, withdrawals, prize payments, wallet balances, payment processor references, and transaction histories. Such data forms part of the Company's accounting and financial reporting records.

Financial transaction data shall be retained for a for a period for which it is necessary for the purpose it was collected in accordance with statutory accounting and tax obligations, including obligations imposed by HM Revenue & Customs.

Where required by law or regulatory investigation, data may be retained for a longer period. Financial records shall not be erased where statutory retention requirements apply.

7. RETENTION OF GAME PARTICIPATION AND COMPETITION DATA.

The Company processes personal data relating to participation in competitions, including pool entries, scores, rankings, leaderboard positions, and prize allocations. Where such records are linked to financial transactions, they shall be retained for a period for which it is necessary for the purpose it was collected.

Statistical or analytical data that has been irreversibly anonymised may be retained indefinitely, provided that individuals are no longer identifiable.

8. RETENTION OF IDENTITY VERIFICATION DATA

Where identity verification or know-your-customer procedures are implemented, personal data may include receipt of copies of limited identification documents, proof of address documentation, and verification reports from third party providers. Such data shall be retained for a period for which it is necessary for the purpose it was collected.

ID documents and verification reports will be stored on third party vendor's platform. We will not store any such data on our database. We may retrieve such data from third party vendor only when required for regulatory compliance.

9. RETENTION OF MARKETING DATA

Personal data processed for marketing purposes includes contact details, consent records, and records of marketing engagement. Where an individual withdraws consent, their contact details may be retained on a suppression list for an indefinite period to ensure compliance with opt-out requirements and to prevent further marketing communications.

10. RETENTION OF CUSTOMER SUPPORT RECORDS

Customer support records, including correspondence, complaints, and support tickets, shall be retained for a period for which it is necessary for the purpose it was collected. Where a complaint or support interaction relates to a dispute, regulatory matter, or potential legal claim, the relevant records shall be retained for a period for which it is necessary for the purpose it was collected.

11. RETENTION OF EMPLOYEE AND CONTRACTOR DATA

Personal data relating to employees and contractors, including employment contracts, payroll information, and performance records, shall generally be retained for a period for which it is necessary for the purpose it was collected. Payroll and tax records shall be retained in accordance with statutory requirements imposed by UK tax legislation.

Certain records may be retained for longer periods where required by law.

12. RETENTION OF CORPORATE GOVERNANCE RECORDS.

The Company retains personal data relating to directors, shareholders, and corporate governance matters in accordance with the Companies Act 2006 and other applicable legislation. Certain corporate records are required to be retained permanently. Financial and supporting documentation shall be retained for a period for which it is necessary for the purpose it was collected.

13. VENDOR AND PROCESSOR RETENTION OBLIGATIONS

Third-party processors such as payment providers, KYC vendors, cloud providers, and analytics partners should be contractually required to follow equivalent retention and deletion standards.

14. DATA REVIEW AND MONITORING

The Company shall conduct periodic reviews of retained personal data to ensure that retention periods remain appropriate and that unnecessary data is securely deleted. Dormant accounts and inactive records shall be subject to review procedures to determine whether continued retention is justified.

Compliance with this Policy shall be monitored by the Company's designated Data Protection Lead or Compliance Officer.

15. SECURE DELETION AND ANONYMISATION

When personal data reaches the end of its retention period, it shall be securely deleted from live systems and removed from backup systems in accordance with the Company's backup lifecycle procedures. Secure deletion methods may include cryptographic erasure, secure overwrite, or controlled database purging.

Where appropriate, personal data may be irreversibly anonymised so that individuals can no longer be identified.

16. CROSS-BORDER PROCESSING

Where personal data is accessed or processed outside the United Kingdom, including by group entities such as Wondr Technologies LLC FZ or such other service providers, the Company ensures that appropriate safeguards are in place. Such safeguards may include International Data Transfer Agreements, Standard Contractual Clauses, and documented transfer risk assessments.

17. RESPONSIBILITIES

The Board of Directors retains ultimate responsibility for compliance with this Policy.

Operational responsibility for implementation, monitoring, and review rests with the designated Compliance Officer or Data Protection Lead. All employees, contractors, and authorised processors are required to comply with this Policy.

18. POLICY REVIEW

This Policy shall be reviewed annually or sooner where required due to changes in legislation, regulatory guidance, or business operations.

19. PERIODIC DATA AUDITS

Periodic audits or reviews of stored personal data will occur to ensure data is not retained longer than necessary and that deletion procedures are functioning correctly.