IRIS – Data Security & Privacy Policy

System Description: Algorithm to improve truck fill rate
Prepared by: Prospero Networks Ltd.
Initial Date: November 13, 2024
Version: 3
Version Date: February 4, 2025

1. Information IRIS Collects

IRIS collects only minimum information required to authenticate users and operate the platform effectively. This includes:

- User email address (used for authentication via Firebase).
- Files uploaded by the user for processing.

IRIS does not:

- Use cookies
- Track browsing activity
- Collect data from non-authenticated users visiting public parts of the website

2. Purpose of Data Collection

IRIS collects user-uploaded files and associated session details for the following purposes:

- To execute the IRIS algorithm based on user-initiated actions
- To isolate access per customer for confidentiality
- To support monitoring and ensure service quality and abuse prevention

3. How IRIS Protects Your Data

- Data is hosted and processed in secure infrastructure provided by Google Cloud Platform (GCP), certified under internationally recognized standards:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security Controls)
- ISO/IEC 27018 (Protection of Personal Data in the Cloud)
- SOC 1, SOC 2, and SOC 3 Reports
- FedRAMP (for U.S. government cloud services)

- Files are encrypted in transit (HTTPS) and at rest (AES-256 encryption).

- Physical data centers are protected with multi-layered access control.

- Google Cloud undergoes regular third-party audits and penetration tests.

- All uploaded files are malware-scanned prior to processing.

- IRIS regularly applies security patches and conducts internal assessments.

- Uploaded files are automatically deleted after a retention period of 30 days unless requested earlier.

- Access to data is governed by the principle of least privilege.

- All user interactions are authenticated using Firebase Authentication.

- Secure session tokens are used and validated for every action.

- Sessions expire after a period of inactivity, and tokens can be revoked immediately.

- Access is role-based and scoped per customer; cross-customer access is blocked by design.

- All user and system activities are captured in secure audit logs and monitored for anomalies.

- Only select employees at Prospero Networks have access to sensitive data, under strict confidentiality agreements and access logs.

- Multi-Factor Authentication (MFA) is used for admin access.

- IRIS has an internal incident response protocol to rapidly address potential security events.

- Customers are notified without undue delay if a data breach affecting their information is confirmed.

- IRIS has a tested backup and recovery procedures in place.

4. Sharing Your Information

IRIS does not share personal information or user-uploaded content with third parties without explicit user consent.

5. User Controls & Rights

- Users have the right to access, rectify, or request deletion of their data at any time, in accordance with applicable data protection laws.

- Users may request deletion of any uploaded file.

- No personal data is retained beyond what is operationally necessary.

- IRIS does not collect or retain location, search, or device metadata.

6. Security Monitoring & Logging

- All user activity, including login and uploads, is logged for security auditing purposes.

- Repeated failed login attempts or invalid session usage are flagged for review.

7. Data Retention & Deletion

- Uploaded files are auto-deleted after a pre-defined window of 30 days unless requested earlier.

- Users may request manual deletion of uploaded files before auto-expiration.

- Users may request full account deletion by contacting support. Upon verification, all associated credentials and user data will be securely deleted in accordance with our retention policy, which ensures data is not kept longer than necessary and is permanently removed from active and backup systems.

- Backup data is also purged in accordance with retention policies to ensure complete deletion.

8. Advertising and Personalization

- IRIS does not use third-party trackers, analytics, or behavioral profiling tools.

- IRIS does not serve personalized content or advertising. No user behavior is tracked or profiled.

9. Legal & Regulatory References

- Compliant with UK Data Protection Act 2018 and GDPR (EU) principles:
    - Data minimization
    - Storage limitation
    - Integrity and confidentiality
    - Lawfulness and transparency

- Data is hosted and processed in secure environments compliant with:
    - ISO/IEC 27001 – Information Security Management
    - ISO/IEC 27017 – Cloud Security Controls
    - ISO/IEC 27018 – Protection of Personal Data in the Cloud
    - SOC 1, SOC 2, and SOC 3 reports
    - FedRAMP – U.S. government cloud compliance

10. When This Policy Applies

This Data Security & Privacy Policy applies solely to the IRIS platform operated by Prospero Networks Ltd., including its web interface, file upload functionality, and algorithmic processing engine. It does not apply to any third-party services or websites that may be linked to from the IRIS platform.

11. Updates to This Policy

This policy may be updated from time to time to reflect changes in system features, legal requirements, or best practices. When updates are made, the version number and revision date will be updated accordingly.The ‘last updated’ date will be visible at the top of this policy. Significant changes will be communicated through official customer channels.

12. Contact Information

For any privacy-related inquiries, data access requests, or concerns regarding your information, please contact:

Email: info@iristfr.com

Phone: +44 20 3092 2545

Website: www.iristfr.com

Company Information: Prospero Networks Ltd.

Company Number: 11487433

VAT Number: GB327 5122 20

Registered Office: Unit Da2 Sutherland House,
43 Sutherland Road,
London, England, E17 6BU