Data Protection Statement

Introduction

Ormonde Technologies (SurfBox) Ltd (the 'Company') needs to collect information (User Data) for limited purposes from a Customer (the 'Customer') using its services in public libraries, shopping centres, airports, hotels and other public venues (the 'Location Provider') hosting its services. The purpose of processing User Data is for the delivery of internet, print, copy and scan services at these venues. Data Protection is the safeguarding of the privacy rights of the Customer in relation to the processing of User Data.
This is a statement of the Company's commitment to protect the rights and privacy of the Customer in accordance with the General Data Protection Regulation (GDPR).

Data Protection Principles

The Company will administer its responsibilities under the regulation in accordance with the stated data protection principles as follows:

Legal Basis for Processing

The Company processes User Data under the following legal bases:

- Performance of a contract: To provide printing, scanning, and related services requested by the Customer.
- Legitimate interests: To maintain service quality, security, and support.
- Legal obligations: To comply with applicable laws and regulations.

Data Collected

The Company will obtain and process User Data fairly and in accordance with the fulfilment of its functions. The User Data collected during the fulfilment of its functions during a Customer session are as follows:

- **Printing**: The Customer's documents submitted for print purposes. Additionally, the Customer's email address is required to be submitted for the purpose of submission of print jobs via email.
- **Scanning / Copying**: The Customer's documents submitted for scanning purposes. Additionally, the Customer's email is required to be submitted for the purpose of scanning document to email.
- **Public Internet & PC Access**: The Company does not obtain any User Data in the provision of public internet & PC access services. No usernames, email addresses or passwords are required to use these services.

Data Retention

The Company will keep data for purposes outlined in the previous section that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes. The Company will not retain or disclose User Data for any purpose other than for delivery of its services.

The Company will only retain data for the duration of its service delivery and for any support purposes relating to the services. Specifically, data is retained temporarily for the purposes outlined in the previous Section as follows:

- **Documents for Printing**: Documents submitted for printing are retained in electronic format, to allow Customers to collect and, where required, reprint, documents in print (hard copy) format, for a period of (maximum) three days. Hard copy print copies can only be obtained by the Customer by means of a unique release code that has been returned to their email address, mobile app or desktop PC. While troubleshooting Customer Service requests, such documents may need to be viewed or reprinted on behalf of the Customer, but this is only carried out with the prior consent of the Customer.
- **Documents for Scanning / Copying**: Documents submitted for scanning or copying purposes are stored temporarily for the duration of the Customer's session. They are permanently deleted at the end of the session.
- **Documents on Public PCs:** Documents may be downloaded during Customer sessions on public internet PCs. These may be accessed by the Customer for viewing, editing and printing purposes. Such documents are permanently deleted at the end of each Customer session.
- **User Email Addresses**: User email addresses are retained for a period of fourteen days for follow-up Customer Service, support and other operational purposes. Such data will not be used for other purposes, including marketing, either by the Company, or 3rd party companies.
- **Card Payments:** The Company does not record or store Customers' card details in the delivery of its services. Card details are forwarded to a PCI compliant payment gateway provider for payment processing.

Data Protection Statement

Security Measures

The Company will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The Company is aware that high standards of security are essential for all personal information.

Document Submission by Email

The Company recognises that Customers may submit documents for printing either via email or through the Company's secure web upload service. Scanned documents may be submitted to the Customer via email or directly to the Customer's USB device. While email submission remains available for convenience, the Company advises that email transmission may involve routing through third-party networks not controlled by the Company. Customers should therefore avoid sending documents that contain sensitive or confidential information by email. All such emails and attachments are automatically deleted from Company systems after processing and are not retained longer than necessary. For enhanced security, Customers are encouraged to use the secure web upload or USB scanning service for documents that contain sensitive or confidential information.

Company Responsibilities

The Company has overall responsibility for ensuring compliance with the Data Protection Regulation. All employees of the Company who collect and/or control the contents and use of User Data are also responsible for compliance with the Regulation. The Company will provide support, assistance, advice, and training to all staff to ensure it is in a position to comply fully with the legislation. A Data Protection Officer has been appointed to assist the Company and its staff in this regard.

In addition, the Company is responsible for implementing and maintaining appropriate technical and organisational measures to protect Customer data against accidental loss, mis-delivery, or unauthorised access. These measures include, but are not limited to, the use of job release codes, automatic deletion of uncollected documents, system monitoring, and regular audits of equipment and processes.

In the event of a system error, technical fault, or other issue resulting in the unintended release or disclosure of a Customer's document, the Company will treat the matter as a potential data breach. Such incidents will be logged, investigated, and, where required, reported to the Data Protection Commission and the affected Customer(s) in accordance with Articles 33 and 34 of the GDPR. The Company is committed to ensuring that any misdelivered documents are securely disposed of and that corrective measures are taken to prevent recurrence.

Through these actions, the Company seeks to ensure that responsibility for data protection is not placed solely on the Customer, but is actively managed and overseen by the Company in line with its legal obligations under the GDPR.

Customer Responsibilities

The Customer is responsible for ensuring that they retrieve their own documents at the end of each session and for verifying that any printed, scanned, or copied documents obtained through use of the Company's services are solely their own.

If, on occasion, other documents are received in error (for example, due to a system fault or a mistake by another Customer), the Customer must notify the Location Provider staff and/or the Company immediately. Such documents must not be retained or further disclosed and should be securely disposed of or handed to staff for secure disposal.

The Customer is also responsible for reporting any service issues (e.g., no document received, paper jam, system fault) to the Location Provider staff and/or the Company so that the matter can be investigated and resolved.

While the Company has primary responsibility for implementing safeguards and managing risks in accordance with data protection legislation, Customers play an important role in promptly identifying and reporting unexpected outcomes (such as receipt of another Customer's documents). This shared responsibility helps ensure that incidents are contained quickly and handled securely in line with GDPR requirements.

Data Subject Rights

Customers have the following rights concerning their data under GDPR:

- Access to their personal data
- Rectification of inaccurate data

- Erasure ('right to be forgotten')
- Restriction or objection to processing
- Data portability

To exercise these rights, contact our Data Protection Officer (DPO):

Email: dpo@surfbox.ie | Phone: +353 56 7793788

Procedures and Guidelines

This Statement supports the provision of a structure to assist in the Company's compliance with the Data Protection regulation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

Review

This Statement will be reviewed regularly considering any legislative or other relevant indications.

Last Updated

This document was last updated on Wednesday 12 November 2025.