

GDPR Compliance Document

Onix Work

Contents

| | |
|----------------------------------|---|
| 1. Introduction | 2 |
| 2. Scope | 2 |
| 3. Data Protection Principles | 2 |
| 4. Lawful Basis for Processing | 3 |
| 5. Data Subject Rights | 3 |
| 6. Data Security | 3 |
| 7. Data Breach Notification | 4 |
| 8. International Data Transfer | 4 |
| 9. Development and maintenance | 4 |
| 10. Support and consultancy work | 4 |
| 11. Sub-contractors | 4 |
| 12. Amendments | 4 |

1. Introduction

This document outlines the measures and commitments of Onix Work (hereinafter referred to as "the Application") to comply with the General Data Protection Regulation (GDPR). The Application is committed to ensuring the protection of personal data and the rights of individuals.

2. Scope

This document applies to all personal data processed by the Application, including data collected on users, employees, and other individuals.

The Application is not intended to contain personal information beyond a very limited selection necessary to distinguish between participants and enable administration.

The following information may be considered as personal data in the Application:

- Email address (User Name)
- Full name
- Picture
- Phone number
- Position
- Scanned signature
- Place of signature

Email Address (User Name) is the only mandatory field.

The following information may be connected to a user of the Application:

- Location
- Department
- Control categories
- User Privileges
- Change- and access Logs

3. Data Protection Principles

The Application adheres to the following principles relating to the processing of personal data:

Lawfulness, fairness, and transparency: Data is processed lawfully, fairly, and transparently in relation to the data subject.

Purpose limitation: Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimization: Only data that is necessary for the purposes of processing is collected.

Accuracy: Every reasonable step is taken to ensure that personal data that is inaccurate is erased or rectified without delay.

Storage limitation: Personal data is kept in a form which permits identification of data subjects for no longer than necessary.

Integrity and confidentiality: Data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

4. Lawful Basis for Processing

The Application processes personal data under the following lawful bases:

Consent: Clear consent has been obtained from the data subject for processing their personal data for specific purposes.

Contract: Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

Legal obligation: Processing is necessary for compliance with a legal obligation.

Vital interests: Processing is necessary to protect the vital interests of the data subject or another natural person.

Public interest: Processing is necessary for the performance of a task carried out in the public interest.

5. Data Subject Rights

Data subjects have the following rights under the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

6. Data Security

The Application implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including measures such as encryption, access control, secure software development practices, and regular security assessments.

Data is available from following environments:

- Production, including Sandbox (live data, and copy of live data)
- Development, including Beta and Test (anonymous data)

7. Data Breach Notification

In the event of a data breach, Onix will promptly notify the appropriate data protection authorities and affected individuals in accordance with GDPR requirements.

8. International Data Transfer

All data is stored within EU (Azure- Western Europe). Information can be read and maintained from all over the world. This is limited to invited users and with strict access control provided by the customer's administrators.

9. Development and maintenance

The software is developed by a dedicated team in Vietnam, using anonymized data for development and associated testing. Regression- and automated tests are conducted on actual data.

10. Support and consultancy work

To ensure that program knowledge remains integrated with our development team, support and maintenance must be conducted from the same geographical location. Therefore, Onix provides these services from Vietnam. A dedicated team, bound by a non-disclosure agreement, performs these tasks. This team cannot access customer data without explicit permission from the customer.

11. Sub-contractors

List of sub-contractors:

| Company | URL | Location | Services |
|-----------|--|-------------------------------|-----------------------|
| Microsoft | www.microsoft.com | Azure, Western Europe | Hosting, Distribution |
| Restaff | www.restaff.no | Ho Chi Minh City, Vietnam (*) | Development, Support |

(*) Written EU commission's standard contractual clauses – module 3.

12. Amendments

This document may be updated periodically to reflect changes in our data processing practices or regulatory changes.