# Table of Contents

# Information security policy of Directo OÜ

## 1. General information

Directo's mission is to provide our customers with business software that is amazingly powerful, yet incredibly easy to use. Information security has a vital role to play in our mission and we take it extremely seriously, from the Management Board down to every employee. We are committed to maintaining the confidentiality, integrity and availability of our company's and our customers' information assets. Directo may act as both the Controller and the Processor upon processing of personal data. In the context of the General Data Protection Regulation, it is our primary responsibility to implement adequate technical and organisational security measures for our services to protect the data processed by our customers against accidental or unlawful deletion, unauthorised access or disclosure. This information sheet is intended to help you better understand what we do and how we proceed to protect the data (including personal data) processed through our Directo business software. Regulation 2016/679 of the European Parliament and of the Council, known as the General Data Protection Regulation (GDPR), stipulates that:

- when entrusting a processor with processing activities, the controller should only use processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing.

Controller – that is you, i.e. the user of the Directo business software. Directo OÜ is the Processor, acting in accordance with the powers you have granted us. Your responsibility as the Controller is to make sure that the Processor, i.e. Directo protects your data. Of course, you also must know your duties and responsibilities upon processing personal data.

## 2. General description of Service

We offer Directo business software as a cloud service to our customers. As a cloud service provider, we have no control over what data you upload to or process through our service. This means that we do not know by default whether you are using our service to process personal data, what personal data you are processing and whether such processing is lawful. If required, you must assess the impact of your data processing and its compliance with the applicable legislation yourself. Depending on the impact assessment, it may prove necessary to implement additional security measures, such as introducing an ID-card-based system for logging in and/or restricting usage rights.

## 3. Information security in Directo

### 3.1. Information security policy, process, organisation and risk management

We are committed to providing secure business software. To do so, our Management Board has established a company-wide Information Security Policy, which we apply throughout the company – and we expect adherence to these principles both from Directo’s managers and employees and

contractors involved in our business activities. The Information Security Policy is reviewed at least once a year to assess its up-to-datedness, and the Chief Information Security Officer is responsible for preparation, modification and implementation of the policy.

The Chief Information Security Officer is supported in their work by a broad-based Information Security Workgroup.

All structural units and employees, and also contractors of the company are involved in the information security process.

We have created and implemented our information security policy in accordance with the ISO/IEC 27001:2013 standard and have also confirmed consistency with the standard through formal certification. The certificate is available here: https://directo.ee/wp-content/uploads/2021/12/27001_ENG_Directo.pdf.


BUREAU VERITAS
Certification

Directo OÜ

ISO/IEC 27001:2013

Our company is conducting ongoing and systematic monitoring of information security risks and updating the risk assessment, together with activities to reduce the residual risks related to information security.

## 3.2. Security of human resources

We have established information security rules and requirements for our employees and subcontractors to ensure that:

- employees, contractors and third-party users understand their responsibilities;
- employees, contractors and third-party users are fit for their roles;
- everything possible has been done to minimise the risk of theft, fraud and misuse of resources or information.

Conducting pre-employment background checks is an important part of our recruitment process and helps us to hire only those candidates who are suitable for their roles.

Non-disclosure agreements are always concluded with subcontractors before granting the subcontractor access to information assets.

Raising the security awareness is an ongoing process. Our aim is for all employees and subcontractors

to understand and be aware of the laws and regulations governing the activities of Directo OÜ, internal and contractual requirements, the implemented safeguards and the reporting methods for any related incidents. Documents regulating security (e.g. policies, guidelines and best practices) are available on the company's intranet.

## 3.3. Security of Customer’s information assets

The Customer is the responsible owner of the Customer's information assets (data, documents, files, e-mails, etc.) stored and processed in Directo's information systems. **All data belonging to our customers are treated as confidential, which is the highest security level used at Directo.**

The security level assigned in Directo is not automatically transferred out of the company. The Customer must store, process and transmit their information in Directo's IT systems in accordance with their own security levels and considered risks they have assigned to their information assets, and arrange for the implementation of appropriate security measures, which may include limitation of user rights or their scope, etc.

Directo will never sell any data uploaded to Directo's business software, uploaded by the Customer's users, or created on the server by the Customer in the course of using the Service to anyone, nor will Directo use any such data for our own direct economic benefit without the Customer's permission. Directo processes such data only to the extent necessary for providing the services of our Customers or related user support, or share the data with the appropriate law enforcement authorities in the cases prescribed in law.

## 3.4. Personal data protection in Directo

Directo OÜ uses the best available technologies and methods to protect any personal data. We keep an account of both the personal data we process and the impact of processing on these data. Read more about the processing of personal data in the terms and conditions of data protection of Directo OÜ: https://directo.ee/andmekaitsetingimused.

More details on the protection of personal data can be found here: https://wiki.directo.ee/et/gdpr

## 3.5. Data location

The servers used to provide Directo’s Service are physically located in a secure data centre in the territory of European Union.

Directo OÜ only works with recognised partners to host infrastructure. The data centre service is provided by Telia Eesti AS, whose information security management system has been certified by Bureau Veritas to comply with the ISO/IEC 27001:2013 standard: https://www.telia.ee/images/documents/sertifikaadid/iso_iec_27001_2013_est.pdf.

## 3.6. Data communication

Directo cooperates with Telia Eesti AS to mitigate information security, sustainability and business

risks related to data communication.

### 3.7. Backing up data

Under the terms of Directo's licence agreement, we create a backup copy after every 24 hours and retain the last seven backups. This means that when a data processor or controller deletes or anonymises personal data, it will take seven calendar days before it becomes impossible to recover the data from a backup copy. Directo OÜ, in cooperation with its partners, monitors the operation of the servers providing our services 24 hours a day, 7 days a week.

In order to ensure traceability, audit trails (logs) are stored and retained, reflecting performing of any operations related to managing and use of information assets, and these cannot be modified or deleted by any employee/user.

### 3.8. Customer support and incident management

Directo Customer Support is available by phone, e-mail and chat on business days between 09:00 and 17:00 (time zone EET/EEST).

The phone number of the Customer Support is +372 671 8578.

The e-mail address of the Customer Support is: info@directo.ee.

All employees of the company are responsible for reporting information security incidents. Information security incidents are handled by the User Support team in collaboration with the Chief Information Security Officer.

### 3.9. Processors involved by Directo

We may involve processors in the processing of the Customer's data. We will only do so after having acquired reasonable assurance that all parties implement appropriate technical and organisational measures in such a way that data processing meets the requirements of the applicable legislation.

## 4. Physical security

We have security measures in place to maintain business activity. Access is restricted and equipped with the necessary security devices.

## 5. Access to information systems

Our company uses role-based access, and access is granted only to the information that is necessary for performing one's tasks. This applies to all employees, contractors and third-party users of Directo.

# 6. Compliance

We continuously work to ensure compliance with all applicable laws, regulations, and contractual requirements. To ensure adherence to laws and contractual requirements, we have implemented internal management documents, security requirements and overviews in the company. To facilitate compliance, we organise training events and other security awareness activities for our employees and partners.

# 7. Constant improvement

At Directo, we are committed to continuously improving and developing our Information Security Management System to prevent information security incidents.

# 8. Business continuity

We care a lot about the operational reliability and sustainability of our product because we use exactly the same business software ourselves. We understand that disruptions can happen, and that's why we've built our systems and processes to minimise the impact on our customers when they do. To that end:

- we conduct consistent risk assessments and situation improvement to prevent materialisation of the risks;
- we ensure business continuity, which is part of our service development lifecycle;
- we test our service, and make it better through analysing and improvements;
- we work observing best practices and international standards.