Technical and Organisational Measures according to Art. 32 GDPR

Updated: November 29, 2023

ClickDimensions uses third party cloud providers to host applications and data. The certifications and controls of the cloud providers are reviewed on an annual basis including SOC 2 and ISO. Parts of the Physical Access and System Access Controls are managed by the cloud providers.

1. Confidentiality

- **Access control (Physical access)**
  No unauthorized access to data processing systems, e.g: Magnetic or chip cards, keys, electric door openers, factory security or gatekeepers, alarm systems, video systems;
-
  - ☒ Alarm system
  - ☒ Protection of building shafts
  - ☒ Automatic access control system
  - ☒ Chip card/transponder locking system
  - ☒ Locking system with code lock
  - ☒ Manual locking system
  - ☒ Biometric access barriers
  - ☒ Video surveillance of accesses
  - ☒ Light barriers / motion detectors
  - ☒ Safety locks
  - ☒ Key regulation (key handout etc.)
  - ☒ Visitor control at the porter's / reception desk
  - ☒ Logging of visitors
  - ☒ Careful selection of cleaning personnel
  - ☒ Careful selection of security personnel
  - ☒ Obligation to wear authorisation cards

- **Access control (Logical / System based access)**
  No unauthorized use of the system, e.g.: (Secure) passwords, automatic locking mechanisms, two-factor authentication, disk encryption;

  - ☒ Assignment of user rights
  - ☒ Creating user profiles
  - ☒ Assignment of credentials (Password, Username)
  - ☒ Authentication with username + strong password
  - ☒ Assignment of user profiles to IT systems
  - ☒ Use of VPN technology
  - ☒ Use of intrusion detection systems
  - ☒ Use of anti-malware software on Servers
  - ☒ Use of anti-malware software on Endpoint Devices
  - ☒ Encryption of hard disks on Endpoint Devices
  - ☒ Use of a software firewalls

- **Access control (Organisational)**
  No unauthorized reading, copying, modifying or removing within the system, e.g: Authorization concepts and demand-oriented access rights, logging of accesses;

- ☒ Using an Authorization Concept
- ☒ Administration of access rights and user lifecycle management by system administrators
- ☒ Multifactor Authentication
- ☒ Number of administrators reduced to the "bare minimum”
- ☒ Password policy incl. password length, password expiration
- ☒ Secure storage of data storage devices
- ☒ Physical deletion of data media before reuse
- ☒ Irrecoverable destruction of data storage devices
- ☒ Use of document shredders or service providers (if possible, with data protection seal of approval)
- ☒ Encryption of data storage devices
- ☒ Encryption of data in transit using TLS protocols and latest Strong Ciphers

- **Separation control**
  Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;

  - ☒ Physically separate storage on separate systems or data storage devices
  - ☒ Logical client separation (software-based)
  - ☒ Creation of an authorization concept
  - ☒ Encryption of data sets processed for the same purpose
  - ☒ Providing the data records with purpose attributes/data fields
  - ☒ Definition of database rights
  - ☒ Separation of production and development environments

- **Pseudonymisation**
  The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures;

  - ☒ Pseudonymisation of customer data (customer numbers)
  - ☒ Pseudonymization in database applications (special tables for personal data and information)
  - ☒ Data Protection Policy

2. Integrity

- Transmission control
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

  - ☒ Installation of dedicated transmission paths or VPN tunnels
  - ☒ Email encryption
  - ☒ Documentation of the recipients of data and the time periods of the planned transfer or agreed deletion periods

- **Input control**
  Determining whether and by whom personal data have been entered, changes or removed in data processing systems, e.g.: Logging, document management;

  ☒ Allocation of rights to enter, change and delete data based on an authorization concept
  ☒ Manual or automated control of the logs (according to strict internal specifications)

3. Availability and Resilience

- Availability control
  Protection against accidental or unintentionally destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), malware protection, firewall, reporting procedures, incident response and emergency plans;
- Recoverability;

  ☒ Uninterruptible power supply (UPS)
  ☒ Air conditioning in data centers
  ☒ Devices for monitoring temperature and humidity in data centers
  ☒ Fire and smoke detection systems
  ☒ Fire extinguishers in data centers
  ☒ Alarm message in case of unauthorized access to data center and similar areas
  ☒ Backup & recovery concept
  ☒ Tested data recovery processes
  ☒ Availability of an emergency plan
  ☒ Storage of data backup at a secure, external, outsourced location
  ☒ In flooded areas: data center above the waterline

4. Regular review, assessment, and evaluation procedures

☒	Review by Internal IT at the following intervals	Annually
☒	Review by external consultants at the following intervals	Annually
☒	Audit by certification authorities at the following intervals	Annually
☒	Incident Response Management System in place	

5. Privacy by design and by default;

☒ When purchasing devices and software, Privacy by Design / Privacy by Default is considered as a selection criterion
☒ During setup, the administrator activates specifically settings or options to implement Privacy by design / Privacy by default
☒ Data minimization is activated (only data necessary for the defined purpose are collected and stored..)

6. Processing on behalf of the Controller

No processors will be commissioned without privacy instructions from the controller

☒ Commission is processed via formalized evaluation process
☒ Selection of the processor / sub-processor according to data protection and data security criteria

- ☒ Preliminary examination of the data protection requirements at the order processor's premises
- ☒ Regular audits of the subcontractor / subcontractor
- ☒ The processor guarantees that the employees involved in processing the controller's data and other persons working for the processor are prohibited from processing the data outside the scope of the controller's instructions
- ☒ The Processor warrants that the persons authorised to process the personal data have been bound to confidentiality or are subject to an appropriate statutory duty of confidentiality. The obligation to maintain confidentiality and secrecy shall continue to apply even after termination of the contract

7. Personnel Security and Training

- ☒ ClickDimensions maintains personnel policies including having appropriate use guidelines, written confidentiality agreements
- ☒ Background checks are performed in accordance with Applicable Data Protection Laws
- ☒ Annual trainings on Information Security, Security Awareness, and Data Privacy are required of all employees and contractors

8. Incident Response Management

- ☒ Use of spam filter and regular updating
- ☒ Use of virus scanner and regular updating
- ☒ Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
- ☒ Formalized procedure for handling security incidents
- ☒ Documentation of security incidents and data breaches via ticket system