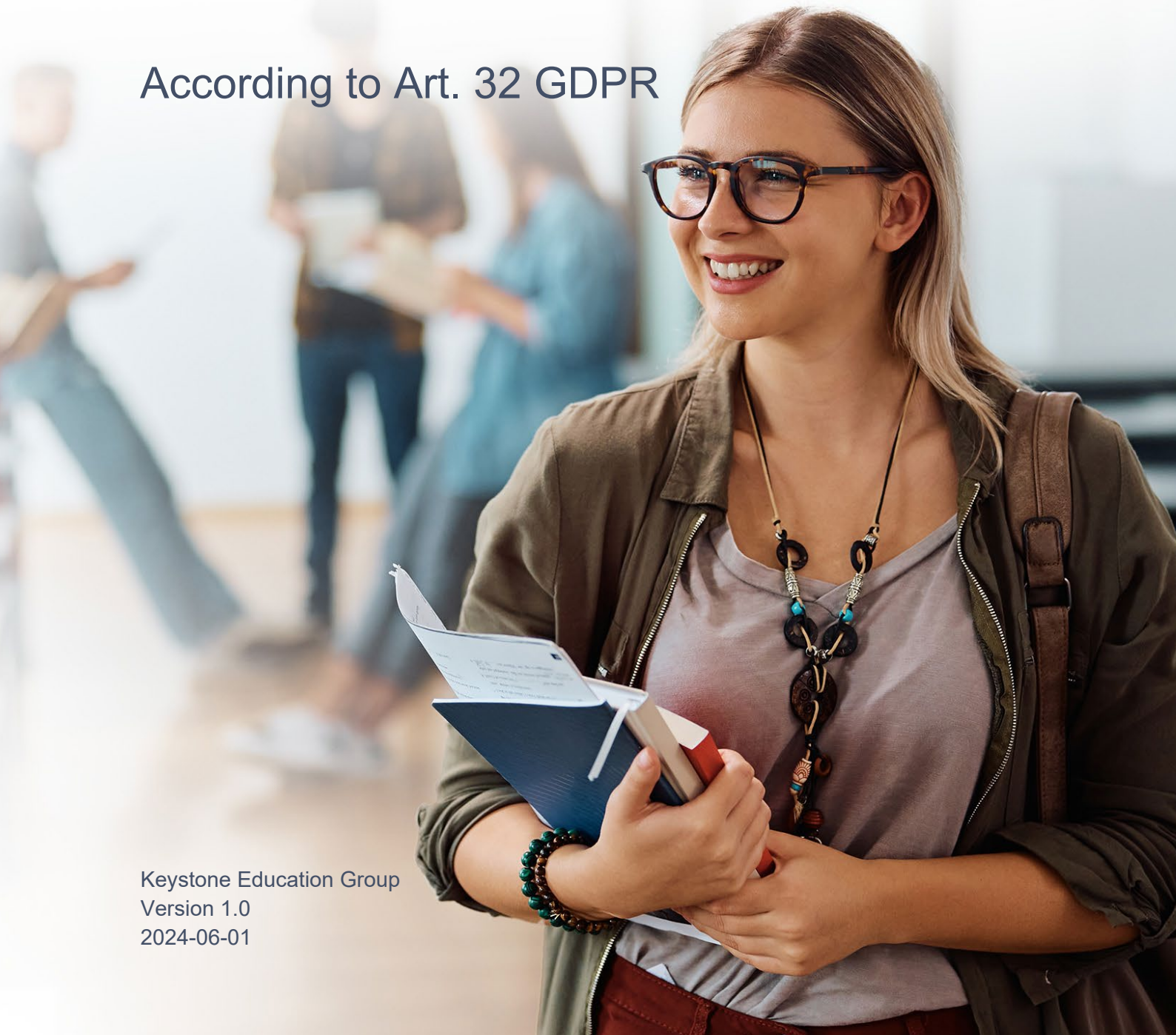
KEYSTONE
EDUCATION GROUP

Technical and organizational measures (TOM)

According to Art. 32 GDPR



Keystone Education Group
Version 1.0
2024-06-01

1 Introduction

Keystone implements appropriate technical and organisational measures to ensure the protection of personal data processed under the Data Processing Agreement. The measures are adapted to the types of processing, scope, context, categories of personal data, the cost of implementation, the purposes of the processing as well as risks, of varying probability and severity.

This document (the "**TOM**") describes the technical and organizational measures implemented by the Keystone Education Group ("**Keystone**" or "**us**") to meet legal and contractual requirements. The measures described below apply to all data processing activities where Keystone acts as a data processor on behalf of the customer acting as data controller.

The TOM is attached to and forms part of Keystone's Data Processing Addendum.

2 Document management

Keystone validates that necessary and obligatory privacy related documentation is in place when Keystone processes personal data. Keystone stores privacy related documentation in a central repository with restricted access control. This system ensures that all necessary privacy documents are managed in a structured manner, promoting transparency and adherence to data protection regulations.

3 Access control

All data managed by Keystone is stored in cloud-based solutions. Keystone's vendors have robust access control systems in place that only allow authorized personnel to access secure areas. Only authenticated and authorized personnel can access sensitive data, such as customer and student personal data.

All access rights (both for access to IT systems and data and for access to buildings and rooms) are assigned according to the principle that employees and third-party users are only granted the level of access they need to perform their activities (principle of least privileged access). Managers within Keystone are responsible for ordering the employees' access rights to systems, applications and information at the IT service desk.

Keystone maintains proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications containing personal data. All systems used by Keystone meet corporate IT security standards and employ security configurations and security hygiene practices to protect against unauthorized access to personal data.

4 Policies and risk management

Keystone maintains and follows data protection and IT policies and practices that are integral to Keystone's business and mandatory for all Keystone employees, including consultants. These policies are reviewed periodically and amended as Keystone deems reasonable to maintain protection of personal data.

Keystone's employees take part in training to ensure compliance with Keystone's Code of Conduct, confidentiality undertakings and security policies. Additional policy and process training is provided to persons granted administrative access to security components specific to their role within Keystone's operation, as required to maintain compliance.

Keystone assesses risks related to its processing of personal data and creates action plans to mitigate identified risks. Risk assessments are a crucial part of our data protection strategy.

5 Malware and endpoint protection

Keystone has different systems and methods to protect the IT infrastructure against malicious code, including various antivirus scanners, spam filters and security updates. Keystone actively monitors to ensure that antivirus scanners and spam filters are active and updated.

6 Transfer and dissemination control

Mechanisms for securing data traffic and communication connections, as well as for monitoring and logging activities in networks, have been established to the required extent. As appropriate, firewalls and intrusion detection and prevention systems (IDS / IPS) are in place.

All data is transmitted over HTTPS (that is HTTP encapsulated over TLS) when it leaves the secure cloud area.

Paper printouts and exports of confidential data from their source system are avoided whenever possible. Hard copies and electronic exports of confidential information leaving the business premises are handled with special care, considering the relevant confidentiality level - with the aim of preventing disclosure, loss and unauthorized copying. As soon as a paper printout is no longer required, it is destroyed. Electronic data exports that are no longer required are deleted again from the respective storage location and any transport data carrier used.

7 Input control

Keystone take measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data has been processed. This is done by ensuring traceability when assigning, changing and deleting user authorizations.

8 Data segregation and retention

Keystone ensures that personal data collected for different purposes are not mixed in their processing. To this end, multitenant systems are used, or systems are physically or logically separated. The data controllers can only access personal data relating to data subjects that have explicitly consented to their data being disclosed to the data controller. Personal data that are no longer required are deleted.

9 Supplier relationship management

Keystone secures that identified security requirements are met by external suppliers during the procurement process. The supplier shall present and account for their technology, routines and processes as well as IT and information security policies. Keystone conducts regular control of suppliers' access rights and other aspects of the agreement with the supplier.