Data protection mesasures of WaeUP Germany

We at WaeUP Germany adhere to the EU's General Data Protection Regulation (GDPR), which also affects the data of students stored in our portal software Kofa. This means that all data processed on our servers enjoys a high standard of data protection and security. As basic guidelines we only transfer the minimum amount of data necessary, avoid to generate unnecessary data and delete data whenever it is possible and legally allowed.

Our portal software runs on well secured and monitored servers. It is written in a solid programming language (Python) and implements a fine-grained system of permissions to control access to the portal data. We distribute our software as Open Source, to enable public reviews of our code and security audits. We do not believe in security by obscurity.

As we use the object-oriented database Zope for storing data, we can protect each piece of data with its own permission sets. This makes it hard for attackers to gain access to data they are not entitled to see even on a very low level.

Transport-security is ensured by requiring TLS 1.2 for all web based portal interactions. Usual additional HTTP-security measures apply. Even Kofa session-tokens are encrypted to make sure, that student data cannot be shared between online-sessions. All backup data is also encrypted before being stored. All data is stored in Germany or Nigeria.

We think out security and data protection mesasures are good and we are proud that not a single intrusion or data theft happend in the nearly 20 years of operation.

But we also take care, that things stay that way. Our software is constantly updated to meet new challenges in security, data protection and – of course – to meet our clients expectations.

As a GDPR-bound company we define and update our data protection policies regularily and have defined technical-organizational measures that can give you an insight into our mode of operation.

WAeUP Germany GbR · Marsch 5 · D-29489 Lüchow
Geschäftsführung Dr. Henrik Bettermann

Technical-organizational measures

Confidentiality (Art. 32 para. 1 lit. B GDPR)

- **Admission control**: The servers of WaeUP Germany are located in data centers of Hetzner Online GmbH in Nuremberg and Falkenstein/Germany. The data centers are protected by multiple physical access controls and additionally by 24/7 video surveillance of the servers. A video-monitored, high-security perimeter surrounds the entire data centers. Entry is only possible via electronic access control terminals with a transponder key or admission card. All movements are recorded and documented. Ultra-modern surveillance cameras provide 24/7 monitoring of all access routes, entrances, security door interlocking systems and server rooms.
- **Physical Access control**:
  Access to the servers is either via an SSH connection protected with a personal keypair with passphrase or via an HTTPS connection to a web interface. Passwords for web interfaces as well as passphrases are to be chosen according to the password guideline of WaeUP Germany.
- **Access control**: A detailed authorization concept allows only selected and instructed technical personnel to access the servers. In order to enable troubleshooting even in the event of vacation or illness, these are always at least two people. It is always communicated to customers which persons have access to protected data. Access via SSH as well as via web interfaces is logged.

  Changes to the server configuration are always carried out according to the dual control principle to prevent misconfigurations and registered in a version control system.
- **Separation control**: For each individual order, we use a separate virtual server or a seaparate instance of Kofa, so that the data raised for different purposes are strictly separated from each other.
- **Pseudonymization** (Art. 32 para. 1 lit. a DS-GVO; Art. 25 para. GDPR): Whenever it is technically and organizationally possible, the stored data is pseudonymized.

Integrity (Art. 32 para. 1 lit. b GDPR)

o Transfer control: Data is generally encrypted during transmission. This applies both to server accesses and to e-mail communication within WaeUP Germany, which is always end-to-end encrypted through the use of PGP.

WAeUP Germany GbR · Marsch 5 · D-29489 Lüchow
Geschäftsführung Dr. Henrik Bettermann

o **Input control:** If personal data is entered, changed or removed by WaeUP Germany employees, this must be recorded in a log, unless it is automatically logged by the system used.

Availability and resilience (Art. 32(1)(b) GDPR).

o Availability control: All servers of WaeUP Germany are automatically mirrored on an incremental backup system, so that in the unlikely event of a server failure, all data can be restored. The Hetzner Online GmbH data center has redundant, uninterruptible power supply, network connection, and air conditioning. All servers are constantly monitored automatically from remote for detecting unusual behaviour. All servers store all data on at least 2 disks for redundancy and quick recoverage in case of disk defects.

o Rapid recoverability (Art. 32 para. 1 lit. c GDPR): For each server component, replacement hardware is available directly in the data center, so that the permanently available personnel of Hetzner Online GmbH can immediately replace any defective hardware component on site.

Assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

o **Data protection management**: At WaeUP Germany, we follow the privacy-by-design philosophy, so that during the implementation of a software solution, it is always kept in mind whether the collected data is actually needed for the purpose. Our employees regularly attend training sessions on the subject of data protection.

o **Incident response management:** Like data privacy management, incident response management in the event of any data privacy incidents is led by the head of our technical projects, Dr. Henrik Bettermann.

- **Data protection-friendly default settings (Art. 25 (2) GDPR):** Wherever users of our systems can set the scope of the data to be collected themselves, the default setting is selected so that as little data as possible is collected.

o **Order control**: We only process order data when and where we have been explicitly instructed to do so by our clients. When selecting our service providers, we satisfy ourselves in advance of their technical and organizational measures for data protection. At the same time, we try to keep the number of external service providers processing commissioned data as low as possible as part of a simpler data protection management system.

Last updated: 1st October 2021

WAeUP Germany GbR · Marsch 5 · D-29489 Lüchow
Geschäftsführung Dr. Henrik Bettermann