TECHNICAL AND ORGANISATIONAL STANDARD MEASURES FOR DATA PROTECTION IN ACCORDANCE WITH THE GDPR

of **Elements Group**, including **elements.at New Media Solutions GmbH**, **Punkt & Komma GmbH** and **Pimcore GmbH**, hereinafter collectively referred to as ELEMENTS.

All technical and organisational measures are assessed and updated in accordance with current standards and the state of the art on an ongoing basis.

1. Internal processing activities

- Entry control
  Protection against unauthorised access to data processing systems, in each case by keys or electrical door openers (transponders) and alarm systems. The server rooms, power distributors and telecommunications systems are located in a restricted area with limited access and are exclusively used by ELEMENTS. Additional protective systems: master key system; key regulation; customer clearance; entry control system; attendance monitoring / time recording system connected; logging; control of remote / home workers; monitoring of cleaning and maintenance work
- Admission control
  Protection against unauthorised system use by user IDs and password procedure with a validated policy in accordance with current standards (structure of characters, length, regular change, password record) or by public keys in accordance with current safety standards (SSH accesses). Further measures: two-factor authentication for administrative user accounts; screen lock for breaks with password activation; first-login procedure; regulated and secured storage of administrator passwords; single sign-on; only personalised access codes; access logging; mandatory encryption of mobile data carriers; direct connection internet service provider (glass fibre); access authorisation concepts; hardware firewalls; ongoing manual / partly automated and central installation of updates and security patches; central administration of the configuration; full-time system administrators; task-related system separation in the event of several administrators; separate user accounts for system administrators; application of the dual control principle for critical system changes; logging of the administrator activities
- Access control
  No unauthorised reading, copying, changing or removing within the systems. There are standard authorisation profiles on a “need to know basis”, a standard process for granting authorisations, regular checks of the authorisations granted. Administrative user accounts are limited to the smallest possible group of administrators and are regularly checked with particular care.
  Further measures: authorisation concepts for data, applications and operating systems; logging of file accesses, programme executions and guideline violations; retention of the records for an appropriate period; synchronisation of the clocks to evaluate logs; no administration rights for users on terminal devices; processes for obtaining / changing authorisations (new setup, change to tasks, resignation); regular check whether authorisations granted are still necessary; whenever possible, authorisations are not granted to individuals but to roles; data carrier administration; access protection by screen lock triggered automatically or by function keys with exclusive password-based or biometric procedures for verified unlocking; regulations and control for external maintenance and remote maintenance; only the company’s own devices may be connected to the internal network; open Wi-Fi segments or segments not used only internally are separated from the internal network by a firewall; communication in wireless networks is encrypted; mobile terminal devices are encrypted; internet application transfer login data only in encrypted form; publicly accessible IT systems are in an isolated DMZ;

- Transfer control
  No unauthorised reading, copying, changing or removing during electronic transmission and transport exclusively via encrypted connections (e.g. HTTPS, SFTP, VPN). Further measures: hard disk encryption for mobile terminal devices; logging of transmission; regulations for remote workers and remote maintenance (software, access rights, access path, activation / release procedure, encryption, access control, monitoring & logging);
- Input control
  Determination whether and by whom personal data was entered, changed or removed in data protection equipment, using corresponding logging methods.
- Order control
  No data processing under Art. 28 GDPR without corresponding instruction by the customer through formalised order placement or separate agreement. The following is checked and documented in each case: object and duration of processing, type and purpose of processing, type of personal data, categories of data subjects. All employees and subcontractors are obliged to maintain confidentiality.
- Availability control
  Fire protection equipment (smoke and fire detectors); fire extinguishers in the server room and in the working rooms; ban on smoking in server and PC working rooms; UPS and overvoltage protection for critical IT infrastructure; redundant air conditioning in the server room; company-wide data securing concept for all relevant IT components (storage/deletion periods, replication independent of sites, manual and automatic integration control, quick restorability); central hard disk systems with reserve capacities (RAID); centrally managed and automatically updated virus protection / protection against malicious software; spam filter; central IDS and IPS systems; emergency plans for different scenarios

2. Webserver

To the extent setup of the web server is exclusively performed by ELEMENTS, the following measures are taken initially: access only by authorised and trained staff (role concept); software firewall (only ports which are absolutely required are opened); shell / administration access only for the restricted IP area and group of persons (system administrators); access logging (storage period of 7 days); server operation only for the ordered software; data transmission only via encrypted connections;

Upon express request of the customer, changes to the measures may become necessary due to a specific assignment or occasion. There is no ongoing maintenance of the measures initially designed, unless this is separately agreed upon in a contract (maintenance contract).

3. Web applications

The web applications developed by ELEMENTS will initially be handed over to the customer with the following protective measures (upon creation of the application): standard authorisation concept based upon roles, user accounts with password authentication, personalised user accounts for all ELEMENTS employees incl. SSO login, tool for monitoring access authorisations, protection against brute-force attacks, standard mechanisms for protection against unauthorised access

4. Online campaigns, targeted advertising, newsletter / e-mail direct marketing

Transmission of personal data from the customer to ELEMENTS may only take place via encrypted transmission methods. ELEMENTS will delete such data after completion of the order. The customer will be informed of transmission to certified sub-processors in each case.