Technical and Organizational Measures (TOM) within the meaning of Art. 32 GDPR

1. Confidentiality according to Art. 32 Para. 1 lit. b GDPR

a. Physical Access Control

Physical access controls are measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used. Physical access control measures that can be used to secure buildings and rooms include automatic access control systems, use of smart cards and transponders, control of access by security personnel and alarm systems. Servers, telecommunications equipment, network technology and similar equipment is to be protected in lockable server cabinets. In addition, it makes sense to support physical access control through organizational measures (e.g., service instructions that provide for locking service rooms when the employee is not present).

Technical measures	Organizational measures
☒ Alarm system	☒ Key regulations / list
☒ Automatic data access control system	☒ Reception / Receptionist / Security
☒ Biometric access barriers	☐ Visitors' book / Visitors' log
☒ Chip cards / transponder systems	☒ Employee / visitor badges
☐ Manual locking system	☒ Visitors accompanied by employees
☒ Security locks	☒ Care in the selection of security personnel
☒ Locking system with code lock	☐ Care in selecting cleaning services
☐ Protection of the building shafts	
☒ Doors with knob outside	
☒ Bell system with camera	
☒ Video surveillance of the entrances	

b. Data Access Control

Data access controls are measures that are suitable for preventing data processing systems (computers) from being used by unauthorized persons. Data access control refers to the prevention of the unauthorized use of equipment. Possibilities are, for example, boot password, user ID with password for operating systems and software products used, screen saver with password, the use of smart cards for logon as well as the use of call-back procedures. In addition, organizational measures may also be necessary, for example, to prevent unauthorized viewing (e.g., specifications for setting up screens, issuing guidance to users on choosing a "good" password).

Technical measures	Organizational measures
☒ Login with username + password	☐ Manage user permissions
☐ Login with biometric data	☒ Create user profiles
☒ Anti-virus software server	☒ Central password assignment
☒ Anti-virus software clients	☒ Secure password policy
☐ Anti-virus software mobile devices	☐ Deletion / destruction policies
☒ Firewall	☒ Clean desk policy
☒ Intrusion detection systems	☒ General data protection and / or security policies
☐ Mobile device management	☐ Mobile device policy
☒ Use VPN for remote access	☒ “Manual desktop locking” instructions

☒ Encryption of data carriers	
☐ Encryption smartphones	
☐ Housing lock	
☐ BIOS protection (separate password)	
☐ Locking external interfaces (USB)	
☒ Automatic desktop lock	
☒ Encryption of notebooks / tablet	

c. Data Usage Control

Data usage controls are measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage. Data usage control can be ensured, among other things, by suitable authorization concepts that enable differentiated control of access to data. It is important to differentiate between the content of the data and the possible access functions to the data. Furthermore, suitable control mechanisms and responsibilities must be defined to document the granting and withdrawal of authorizations and to keep them up to date (e.g., in the event of hiring, change of job, termination of employment). Special attention should always be paid to the role and capabilities of administrators.

Technical measures	Organizational measures
☒ File shredder (min. level 3, cross cut)	☒ Deployment of authorization concepts
☐ External document shredder (DIN 66399)	☒ Minimum number of administrators
☒ Physical deletion of data carriers	☐ Privacy vault
☒ Logging of accesses to applications, specifically when entering, modification and deletion of data	☒ Management user rights by administrators

d. Separation

Separation includes measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures	Organizational measures
☒ Separation of production and test environment	☒ Control via authorization concept
☒ Physical separation (systems / databases / data carriers)	☒ Setting database rights
☒ Multi-client capability of relevant applications	☐ Data sets are provided with purpose attributes

2. Pseudonymization (Art. 32 Para. 1 lit. a GDPR; Art. 25 Para. 1 GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without recourse to additional information, provided that such additional information is stored separately and is subject to appropriate technical and organizational measures.

Technical measures	Organizational measures

☐ In the case of pseudonymization: Separation of the assignment data and storage in separate and secure systems (possibly encrypted)	☒ Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or even after expiry of the statutory deletion period
☒ Anonymization	

3. Integrity (Art. 32 Para. 1 lit. b GDPR)

a. Transfer Control

Transfer control means measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or while being transported or stored on data carriers, and that it is possible to verify and establish to which entities personal data is intended to be transferred by data transmission equipment. Encryption techniques and virtual private networks, for example, can be used to ensure confidentiality in electronic data transmission. Measures to be taken when transporting or forwarding data media include transport containers with locking devices and regulations for destroying data media in accordance with data protection requirements.

Technical measures	Organizational measures
☒ E-mail encryption	☐ Documentation of data recipients and the duration of the planned transfer and the deletion deadlines
☒ Use of VPN	☒ Overview of regular call-off and transmission processes
☒ Logging of accesses and retrievals	☒ Disclosure in anonymized or pseudonymized form
☐ Safe transport containers	☐ Care in the selection of transport personnel and vehicles
☒ Provision via encrypted connections like sftp, https	☒ Personal handover with protocol
☐ Use of signature methods	☐

b. Input Control

Input control refers to measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g. operating system, network, firewall, database, application). It must also be clarified which data is logged, who has access to logs, by whom and on what occasion/at what time these are checked, how long storage is required and when deletion of the logs takes place.

Technical measures	Organizational measures
☒ Technical logging of the input, modification and deletion of data	☒ Overview, with which programs which data has been entered or changed or can be deleted
☒ Manual or automated control of the logs	☐ Traceability of input, modification and deletion of data by individual user names (not user groups)

	☒ Assignment of rights for input, modification and deletion of data on the basis of an authorization concept
	☒ Storage of forms from which data have been transferred to automated processing operations
	☒ Clear responsibility for carrying out deletions

4. Availability and Resilience (Art. 32 Para. 1 lit. b GDPR)

a. Availability

Availability refers to measures that ensure that personal data is protected against accidental destruction or loss. This covers topics such as an uninterruptible power supply, air-conditioning systems, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, and so on. This information refers to the data center.

Technical measures	Organizational measures
☒ Fire and smoke detection systems	☒ Backup & Recovery Concept (formulated)
☒ Fire extinguisher in server room	☒ Control of the backup process
☒ Monitoring temperature and humidity of the server room	☒ Regular tests for data recovery and logging of results
☒ Server room air conditioned	☒ Storing the backup media in a safe place outside the server room
☒ UPS system	☐ No sanitary connections in or above the server room
☒ Protective socket strips in server room	☒ Existence of an emergency plan (e.g. BSI IT-Grundschutz 100-4)
☐ Data protection safe (S60DIS, S120DIS, other suitable standards with special seals etc.)	☒ Separate partitions for operating systems and data
☒ RAID system / hard disk mirroring	
☒ Video surveillance server room	
☒ Alarm message in case of unauthorized access to server room	

5. Procedures for Regular Review, Assessment and Evaluation (Art. 32 Para. 1 lit. d GDPR; Art. 25 Para. 1 GDPR)

a. Data Protection Management

Technical measures	Organizational measures

☒ Software solutions for data protection management in action	☒ Internal / external data protection officer Christian Volkmer Project 29 GmbH & Co. KG Ostengasse 5 93047 Regensburg Tel.: 0941-298693-0 Fax: 0941-298693-16 E-mail: info@projekt29.de Web: www.projekt29.de
□ Central documentation of all procedures and regulations on data protection with access for employees according to need / authorization (e.g. Wiki, Intranet)	☒ Employees trained and committed to confidentiality/data secrecy
□ ISO 27001 security certification, BSI IT-Grundschutz or ISIS12	☒ Regular training of employees at least annually
□ Other documented security concept	□ Internal / External Information Security Officer/ CISO name / company contact
☒ A review of the effectiveness of the technical protective measures is carried out at least once a year	☒ The data protection impact assessment (DPIA) is to be carried out if necessary
	☒ The organization complies with the information obligations according to Art. 13 and Art. 14 GDPR
	□ Formalized process for handling requests for information from data subjects is in place

b. Incident Response Management
Support for security breach response

Technical measures	**Organizational measures**
☒ Use of firewall and regular updating	□ Documented process for detecting and reporting security incidents / data breakdowns (also with regard to the obligation to report to the supervisory authority)
☒ Use of spam filters and regular updating	□ Documented procedure for handling security incidents
☒ Use of virus scanners and regular updating	☒ Involvement of ☒ DPO and ☒ ISO in security incidents and data breaches
☒ Intrusion Detection System (IDS)	☒ Documentation of security incidents and data breakdowns e.g. via ticket system

☒ Intrusion Prevention System (IPS)	☐ Formal process and responsibilities for following up on security incidents and data breaches

c. Privacy-friendly Default Settings (Art. 25 Para. 2 GDPR)

Privacy by design / Privacy by default

Technical measures	Organizational measures
☒ No more personal data is collected than is necessary for the respective purpose	
☐ Simple exercise of the right of withdrawal of the data subject by technical measures	

d. Order Control (outsourcing to third parties)

Order control refers to measures that ensure that personal data processed on behalf of a customer can only be processed in accordance with the customer's instructions. In addition to data processing done on behalf of the data controller, this item also includes the performance of maintenance and system support work both on site and via remote maintenance. If the contractor uses service providers in the sense of commissioned processing, the following points must always be regulated with them.

Technical measures	Organizational measures
	☒ Prior verification of the safety measures taken by the contractor and their documentation
	☒ Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
	☒ Conclusion of the necessary order processing agreement or EU standard contractual clauses
	☒ Written instructions to the contractor
	☒ Obligation of the contractor's employees to maintain data secrecy
	☒ Obligation to appoint a data protection officer by the contractor if the obligation to appoint exists
	☒ Agreement on effective control rights vis-à-vis the contractor
	☒ Regulation on the use of further subcontractors
	☒ Ensuring the destruction of data after the completion of the order

	☒ In case of a longer collaboration: Ongoing review of the contractor and its level of protection