Annex 2[1]

Processing Agreement in accordance with Article 28(3) GDPR

Preamble

This annex sets out the data protection obligations of the contracting parties. It applies to all activities related to the contract/assignment and through which the employees of the Contractor or persons contracted by the Contractor process personal data (“Data”) of the client of the Client. This Processing Agreement specifically regulates the activities of the central services of the corporate family.

1. Subject matter, duration and specification of the processing

The subject matter and duration of the processing order and the type and purpose of the processing are set out in the agreement or the order. Specifically, the Data listed in Annex 1 are a component of the data processing. If they are already regulated in the contract, the information provided in Annex 1 are for information purposes only.

The term of this Annex is based on the term of the contract unless the provisions of this processing agreement and Annex 1 to this agreement set out additional obligations.

2. Area of application and responsibility

(1) The Contractor shall process personal Data on behalf of the Client. This includes activities that are specified in the contract, in the assignment and/or in the service description. Under this contract, the Client shall be solely responsible for compliance with statutory provisions of the data protection laws, in particular for the legality of the transfer of Data to the Contractor and for the legality of the data processing (“Controller” within the meaning of Article 4 No. 7 GDPR).

(2) The instructions will initially be laid down by the contract and thereafter may be amended, supplement or replaced by the Client in written form or in electronic format (text form) to the body designated by the Contractor by means of individual instructions (individual instruction). Instructions not provided for in the contract shall be dealt with as a request for a change in performance. Oral instructions must be confirmed immediately in writing or in text form.

3. Contractor’s obligations

(1) The Contractor may only process data of data subjects within the scope of the order and of the Client’s instructions unless there is an exceptional case within the meaning of Article 28(3)(a) GDPR. The Contractor shall inform the Client without delay if it is of the opinion that an instruction breaches applicable laws. The Contractor may suspend implementation of the instruction until it has been confirmed or amended by the Client.

[1] Annex 2, Processing Agreement in accordance with Article 28(3) GDPR, is an integral part of Vers. 1-08/24 RTC User Agreement Contract

(2) The Contractor shall organise the internal organisation within its area of responsibility in such a way that it meets the specific requirement of data protection. The Contracor shall take technical and organisational measures to adequately protect the Client's Data which meet the requirements of the General Data Protection Regulation (Article 32 GDPR), The Contractor must take technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with processing on a permanent basis. The Client is aware of these technical and organisational measures and is responsible for ensuring that they provide an adequate level of protection for the risks to the Data to be processed. The measures established by the Contractor are listed in Annex 2 of this data processing agreement.

The Contractor reserves the right to make any changes to the security measures taken, but they must ensure that any security measures correspond to the state of the art and that they do not fall below the contractually agreed level of protection.

(3) The Contractor shall support the Client as agreed within the scope of its possibilities in fulfilling the requests and claims of data subjects under Chapter III GDPR and in complying with the obligations set out in Articles 33 to 36 GDPR.

(4) The Contractor shall ensure that employees and other persons working with the processing of the Client's Data for the Contractor are prohibited from processing the Data outside the scope of the instruction. In addition, the Contractor warrants that the persons authorised to process the personal data have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. This confidentiality obligation shall continue to apply after termination of the contract.

(5) The Contractor shall inform the Client without if the Contractor becomes aware of any breaches in the protection of the Client's personal data. The Contractor shall take the required measures to secure the data and to mitigate possible adverse consequences for the data subjects and shall discuss this with the Client without delay.

(6) The Contractor shall inform the Client of the name of the contact person for any data protection issues arising within the scope of the contract. These contact details are listed in Annex 1 to this agreement.

(7) The Contractor shall ensure that it complies with its obligations under Article 32(1)(d) GDPR to implement a procedure for regular review of the effectiveness of the technical and organisational measures to ensure the security of the processing.

(8) The Contractor shall correct or erase the contractual data if the Client instructs it to do so and this is covered by the instructional framework. If it is not possible to erase the data in compliance with data protection or to ensure the corresponding restriction of data processing, the Contractor shall undertake the destruction of data carriers and other materials in compliance with data protection on the basis of an individual order by the Client, or shall return these data carriers to the Client, unless already agreed in the contract. In special cases to be determined by the Client, the data carriers shall be stored or handed over. Remuneration and protective measures in relation to this shall be agreed separately, unless already agreed in the contract.

(9) Data, data carriers as well as all other materials shall be either surrendered or erased at the request of the Client after the end of the order. In the case of test materials and rejected materials, no individual order is required. If deviating specifications for the surrender or erasure of the data give rise to additional costs, these shall be borne by the Client.

(10) In the event of a claim being made against the Client by a data subject in respect of any claims under Article 82 GDPR, the Contractor undertakes to support the Client in defending the claim within the scope of its possibilities.

(11) The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client.

4. Client’s obligations

(1) The Client shall inform the Contractor without delay and in full if it discovers errors or irregularities in the order results in relation to provisions of data protection law.

(2) In the event of a claim against the Contractor by a data subject regarding any claims under Article 82 GDPR, Section 3(10) shall apply accordingly.

(3) The Client shall inform the Contractor of the name of the contact person for any data protection issues arising within the scope of the contract. These contact details are listed in Annex 1 to this agreement.

5. Requests from data subjects

(1) If a data subject contacts the Contractor with requests to correct or erase data or for information about their data, the Contractor shall refer the data subject to the Client, provided that it is possible to assign the data subject to the Client based on the information available. The Contractor shall forward the data subject's request to the Client without delay. The Contractor shall support the Client within the scope of its abilities on instruction as far as agreed. The Contractor shall not be liable if the request of the data subject is not answered, not answered correctly or not answered in time by the Client.

6. Verification options and control rights

(1) The Contractor shall verify compliance with the obligations set out in this contract using appropriate means to the Client.

(2) The Client shall be entitled to perform inspections or to have inspections performed by inspectors to be appointed in individual cases in consultation with the Contractor. They will be performed during normal business hours without disrupting operations, after receiving notice and taking into account a reasonable lead time. The Contractor may make this dependent on prior notice with an appropriate lead time and on the signing a declaration of confidentiality with regard to the data of other clients and the established technical and organisational measures. If the inspector engaged by the Client is a competitor of the Contractor, the Contractor has the right to object to the inspector. The Contractor may charge reasonable remuneration for support in performing an inspection. The expense and time required of an inspection shall be limited to one day per calendar year for the Contractor and Client.

(3) If a data protection supervisory authority or another sovereign supervisory authority of the Contractor carries out an inspection, the provisions of subsection 2 above shall apply accordingly. It will not be necessary to sign a confidentiality agreement if such a supervisory authority is subject to professional or statutory confidentiality where a breach is punishable under the Criminal Code.

7. Subcontractors (further processors)

(1) The use of subcontractors as further processors shall only be permitted if the Client has given its prior consent.

(2) A subcontractor relationship requiring consent exists if the Contractor engages other contractors to carry out all or part of the agreed performance. The Contractor shall enter into agreements with such third parties to the extent necessary to ensure appropriate data protection and information security measures.

The Client agrees that the Contractor may engage subcontractors. The subcontractors working at the time this agreement is concluded are listed in Annex 1. Before engaging or replacing the subcontractors, the Contractor shall inform the Client (if applicable, notice period and/or provision for emergency situations). The Client may object to the change (within a reasonable period of time) for good cause by informing the body designated by the Client. If no objection if made within the time limit, the consent to the change shall be deemed to have been given. If there is a good reason under data protection law and if it is not possible to find a mutually agreeable solution between the parties, the Client and the Contractor shall be granted a special right of termination.

(3) If the Contractor places orders with subcontractors, it shall be the Contractor’s responsibility to transfer its data protection obligations under this contract to the subcontractor.

(4) The Client agrees that the Contractor may use affiliated companies of the Contractor to perform its contractually agreed services or subcontract affiliated companies to provide the listed services. Subsection 3 above shall apply mutatis mutandis to affiliated companies.

8. Disclosure obligation, written form clause, choice of law

(1) If the Client's data with the Contractor is endangered due to attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor must inform the Client of this without delay. The Contractor shall inform all persons responsible in this context without delay that the sovereignty and ownership of the data lies exclusively with the Client as “Controller” within the meaning of the General Data Protection Regulation.

(2) Amendment or supplement to this Annex and all its components (including any representations made by the Contractor) require a written agreement which may also be in an electronic format (text from), and express reference to the fact that it is an amendment to these terms. This also applies to the waiver of this formal requirement.

(3) In the event of any contradictions, the provisions of this data protection annex shall take precedence over the provisions of the contract. If individual parts of this Annex are invalid, this shall not affect the validity of the remainder of the annex.

(4) German law shall apply.

9. Liability and compensation

The Client and the Contractor shall be liable with respect to data subjects in accordance with the provision of Article 82 GDPR.

Annex 1

Subject of the contract

The subject matter of the contract includes:
Provision of a defined storage space on a server to store customer data.

Duration of the order

The term of the assignment is based on the contractual term of the user agreement

Type of data

The following types/categories of data are the subject matter of the processing of personal data:
Personal master data (names, user names, aliases)
Communication data (email addresses, telephone numbers)
Protocol and log files

Categories of data subjects

The categories of data subjects affected by the processing include:
Users of the portal

Subcontractor

Name and address	**Short description of the activity**
Modern Drive Technology GmbH Rettichstraße 7 92318 Neumarkt in der Oberpfalz	Provision of a defined storage space on a server to store customer data.

Contractor’s data protection officer

Name	**Address & Contact**
Markus Olbring External data protection officer	comdatis it-consulting Deventer Weg 8, 48683 Ahaus Telephone: 02561-7569986 or 0173-9799897 Email: datenschutz@ruthmann.de

*If there is no obligation to appoint a data protection officer, a contact person for data protection issues must be appointed.

Annex 2

Description	**Action**	**Yes**	**No**	**not relevant**
Access control	The company has a central and manned reception area.	x		
	An entry control system is in place in the company, i.e. door security by means of a door opener, badge reader, automatic locking system or similar.	x		
	The company's premises are always locked.		x	
	There is an entry rule for external persons.	x		
	A central key management system for issuing keys has been established in the company.	x		
	A key list is kept at a central location, showing which employee has received a key and when.	x		
	Employees have been required in writing to report the loss of a key immediately.	x		
	Visitors receive a visitor pass and return it when leaving the company.		x	
	Entry to server rooms is restricted to authorised staff.	x		
	Server rooms are always locked.	x		
	Entry to server rooms is logged.	x		
	The building is alarmed.		x	
	The building is located in a fenced area.	x		
	Building surveillance is carried out by video, site security or night watchman/guard service.	x		
Access control	Employees receive individual user names and passwords for logging on to the PC workstation.		x	
	Initial passwords must be changed by the user.	x		
	Passwords must be changed regularly.	x		
	Passwords have complexity requirements (e.g. numbers, letters, special characters).	x		
	Passwords are at least 8 characters long.	x		
	Administrative passwords are at least 12 characters long.	x		
	As an alternative to regular password changes, two-factor authentication procedures are in use.	x		
	PC workstations are automatically locked when inactive and can only be unlocked again by entering a password.	x		
	Internal networks are protected against unauthorised external access by a firewall.	x		
	External access to internal networks is only possible via encrypted connections (e.g. VPN).	x		
	Data carriers of mobile end devices (notebooks, smartphones, tablets) containing personal data are encrypted.	x		
	PC workstations and notebooks have anti-virus protection.	x		
Data access control	An authorisation concept exists in the company and contains differentiated authorisation levels.		x	
	User profiles in the applications ensure that employees only receive the rights necessary to perform their tasks.	x		
	USB connections at the PC workstations are blocked or subject to technical monitoring.	x		
	Burners at the PC workstations are locked or subject to technical monitoring.	x		
	Employees are required to use only external data carriers issued by the company.	x		
	IT-supported data carriers that are no longer needed are disposed of in accordance with data protection regulations.	x		

	Adm. rights are only available to authorised staff.	x		
Separation requirement	Personal data collected for different purposes are stored separately.	x		
	The applications allow logical client separation.	x		
	Mandate separation is implemented via the implemented authorisation concept.	x		
	A distinction is made between productive and test systems in the company.	x		
	As far as possible, data from different projects/clients are processed separately.	x		
	In the case of pseudonymised data, separation of the attribution file from the data is ensured.		x	
Transfer control	Procedures are available in the company that enable encrypted exchange of personal data (e.g. email encryption, SFTP, https).	x		
	When sending personal data (e.g. by email), employees are obliged in writing to send this data in encrypted form.		x	
	Employees have been obliged by means of a work instruction, company agreement or guideline not to exchange personal data via insecure or services that do not comply with data protection rules under any circumstances (e.g. no data transfer via social media, WhatsApp, privately used or free cloud storage services).	x		
Data entry control	There is traceability of the entry, modification and deletion of personal data on the system side by logging (Who? When?).		x	
	If standard software is used, it is ensured that logging is activated that is sufficient and that complies with data protection requirements.		x	
Availability control	There is a Doc emergency concept in the company.	x		
	Emergency drills are conducted on a regular basis.		x	
	There is redundant protection of servers and databases.	x		
	There is an adequate uninterruptible power supply (UPS) in the server rooms.		x	
	The server rooms have redundant air conditioning systems.	x		
	The server rooms have smoke detectors.	x		
	Fire extinguishing equipment is located in or directly outside the server rooms.	x		
	The server rooms have a sensor for the alarm system.		x	
	Alarm messages are sent if there is any unauthorised access to server rooms.		x	
	Data backups are stored in a secure, off-site location.	x		
	Data backups are carried out regularly through test scenarios.		x	
	Virus scanners are installed on end devices throughout the company.	x		
	Virus scanners update themselves automatically.	x		
	Operating systems on client workstations are regularly updated.	x		
	Operating systems on servers are regularly updated.	x		
	Procedures have been implemented in the company to ensure regular updates for auxiliary programmes as well (e.g. PDF readers, zip programmes, Java, Flash).		x	
	There are binding guidelines in the company for the maintenance and implementation of updates.		x	

	Automatic and permanent monitoring to detect faults means that any errors are reported quickly.	x		
	Critical IT systems in the company, especially those which are accessible via the Internet, are subjected to vulnerability tests.		x	
	The firewall and router systems are regularly updated (firmware update).	x		
Order control	External service providers are selected made with the utmost care (especially with regard to data protection and information security).	x		
	When using external service providers, it is ensured that there is no data processing outside the EU or a secure third country.	x		
	There are contractual arrangements with external service providers who process personal data or could view it in the course of their activities, in compliance with the requirements of Article 28 General Data Protection Regulation.	x		
	When using external service providers which process personal data, it is ensured that there is a legal basis for the processing (e.g. agreement on data processing, EU standard contractual clauses).	x		
	Procedures are implemented to ensure that personal data is destroyed or deleted after the order is completed. Any statutory retention periods are taken into account and complied with.	x		
	Control rights are agreed in the contractual arrangements with external service providers.	x		
	The agreed control rights are asserted at regular intervals (e.g. by obtaining a confirmation, a report)		x	
	External service providers are sworn to secrecy.	x		
Data protection management	A data protection officer has been appointed in writing in the company.	x		
	There is no legal obligation to appoint a data protection officer.			x
	A guideline on data protection and information security is used to ensure that the management has informed all employees about the need for data protection.	x		
	The company has written regulations (e.g. guidelines, company agreements) for the handling of data and IT systems.		x	
	Employees are sworn to secrecy in writing.	x		
	Employees are made aware of data protection in training courses.		x	
	There is a documented register of processing activities in the company. Where necessary, processing activities are also documented in the order.	x		
	The company has documentation of the measures for the security of processing activities (so-called TOMs)		x	
	Regular audits ensure that the established data protection compliance measures are adequate.		x	
	The data protection officer prepares an annual report.	x		
	The company has certification in the area of information security (e.g. ISO/IEC 27001, IDW PS 951, VdS 3473).		x	
	The company is certified in the area of data protection.		x	