Information Security and Data Privacy Terms

Introduction

The Information Security and Data Privacy Terms (BID) are to be filled-out as part of the procedure to ensure an adequate level of security for the protection of personal data and information security (in office IT and operational technology) by contractors who are involved in the cooperation of one or more data processing systems at RWE AG or one of its subsidiaries pursuant to secs. 15 et seq. German Stock Corporation Act (AktG) or one of its affiliated companies (hereinafter referred to as "RWE"). The Information Security and Data Privacy Terms are divided into four chapters and include a self-assessment of the technical and organizational measures you have taken to ensure the secure processing of (personal) data and, where relevant, the regulations on data processing pursuant to art. 28 in conjunction with 4 No. 8 of the GDPR:

Chapter 1: General information on the company and scope of supply and services

Chapter 2: Information on the processing of personal data

Chapter 3: Technical and organizational measures

Chapter 4: Data processing agreement pursuant to article 28(3) GDPR

RWE is required to maintain the security:

- of its IT infrastructure,
- of its operational technology used in power plants,
- of ist data processing systems it uses as well as
- its information assets

and thus protect them from loss, damage or interruption of operation.

The questionnaire, in the form in which you fill it out and with any necessary changes agreed between RWE and you, is part of a written individual or framework contract for selected services for the processing of (personal) data.

Please answer the BID as detailed, complete and solely truthful as possible in order to support us in assessing and guaranteeing the secure and compliant processing of (personal) data. Some of the following questions may not be relevant for you, in such a case please explain briefly.

Chapter 1: General information on the company and scope of supply and services

Details of the company

Name _____

Address _____

E-Mail _____

Phone _____

Details of the Data Protection Officer[1]

Name _____

E-Mail _____

Phone _____

Details of the contact person for Information Security

Name _____

E-Mail _____

Phone _____

Details on the scope of supply and services

Note: Brief description of the scope of supply and services and purposes of the commissioned data collection, processing and use.

[1] If there is no legal obligation to appoint a data protection officer, the contact person for data protection shall be named here.

Chapter 2: Information on the processing of personal data

1. Does the provision of the above-mentioned scope of supplies and services take place in whole or in part as processor pursuant to art. 28 in conjunction with 4 No. 8 of the GDPR?

◯ yes ◯ no ◯ unknown

2. Describe the scope of supply and services that will be provided as processor in accordance with the applicable data protection regulations as well as the type and purpose of the processing.

3. Location of service provision

☐ The provision of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA).

☐ The provision of the contractually agreed service takes place in a third country outside the European Union or another state party to the Agreement on the European Economic Area. The appropriate level of protection in the following countries:

- ☐ is established by Standard Contractual Clauses (Article 46 Paragraph 2 Points c and d GDPR). [2]
- ☐ is established by an adequacy decision of the European Commission (Article 45 Paragraph 3 GDPR).
- ☐ is established by approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR).
- ☐ is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR):
- ☐ is established by other means (Article 46 Paragraph 2 Point a, Paragraph 3 Points a and b GDPR):

[2] So-called EU standard contract clauses "Controller to Processor". The client's basic requirement is the signing of EU standard contract clauses in the event that the contractor intends to provide services from a so-called third country, i.e. a country outside the EU/EEA.

4. Data categories

- ☐ name, title, academic degree
- ☐ professional, industrial or business designation
- ☐ address
- ☐ date of birth
- ☐ communication data (e.g. telephone, e-mail)
- ☐ telecommunications data (traffic data, location data, inventory data, single connection data)
- ☐ Telemedia data (usage data and inventory data) or electronic communication data (electronic communication content and electronic communication metadata)
- ☐ contract reference data (contractual relation, product and/or contract interest)
- ☐ contract billing and payments data
- ☐ Special types of personal data (information on racial and ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health or sexual life, biometric data, genetic data, data about criminal convictions and criminal offences)
- ☐ personal data on bank and credit card accounts
- ☐ planning and control data (e.g. personnel operational planning)
- ☐ inquiry information (of third parties, e.g. credit agencies or of public registries)
- ☐ Other:

5. Categories of data subjects

- ☐ employees
- ☐ relatives of employees
- ☐ pensioners/survivors
- ☐ applicants
- ☐ customers
- ☐ employees of external companies
- ☐ interested persons
- ☐ tenants/landlords, lessees/lessors
- ☐ suppliers
- ☐ contact persons

☐ children (i.e. persons under age)

☐ Other:

6. Representative within the Union pursuant to Article 27 Paragraph 1 GDPR

Name _____

Address _____

E-Mail _____

Phone _____

7. Sub-contractual relations

The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address	Service

Chapter 3: Technical and organizational measures

1. Confidentiality

1.1. Physical access control	yes	no	not relevant
1.1.1. Does saving and/or processing of Client data take place? ☐ In the Contractor's offices ☐ In the Contractor's data centre or server rooms ☐ At the following IT service provider (e.g., cloud provider):	☐	☐	☐
1.1.2. Are buildings secured by the following measures? Offices: ☐ Alarm system ☐ Video monitoring Server rooms: ☐ ☐ Data centres: ☐ ☐ Technical rooms: ☐ ☐ Production facilities: ☐ ☐ Repair shops: ☐ ☐	☐	☐	☐
1.1.3. Is access to the premises secured by the following measures? Offices: ☐ Manual lock system ☐ Smart card entry system Server rooms: ☐ ☐ Data centres: ☐ ☐ Technical rooms: ☐ ☐ Production facilities: ☐ ☐ Repair shops: ☐ ☐	☐	☐	☐
1.1.4. Is authorised access documented on a name-specific basis?	☐	☐	☐
1.1.5. Are access rules in place for third parties/guests/visitors? Offices: ☐ Name-specific documentation yes ☐ no ☐ Entry/ stay only accompanied by supervisory staff Server rooms: ☐ ☐ ☐ Data centres: ☐ ☐ ☐ Technical rooms: ☐ ☐ ☐ Production facilities: ☐ ☐ ☐ Repair shops: ☐ ☐ ☐	☐	☐	☐
1.1.6. Are access rules in place for cleaning and maintenance staff? Offices: ☐ Name-specific documentation yes ☐ no ☐ Entry/ stay only accompanied by supervisory staff ☐ Server rooms: ☐ ☐ ☐ Data centres: ☐ ☐ ☐ Technical rooms: ☐ ☐ ☐ Production facilities: ☐ ☐ ☐ Repair shops: ☐ ☐ ☐	☐	☐	☐

[3] e.g. turnstiles, biometric access control

1.1.7. Are there regulations concerning the withdrawal of building access authorisations and access rights to computer systems including documentation for employees upon termination of employment?	☐	☐	☐
1.1.8. Aysasare there processes in place to maintain security (e.g. lock desk, empty desks ('clean desk policy', empty screen, etc.)? Office buildings: Yes ☐ No ☐ — Third parties (service providers): Yes ☐ No ☐ Offices Server rooms	☐	☐	☐
1.1.9. Are systems physically protected where necessary? At your sites: Yes ☐ No ☐ — Third parties (Service providers): Yes ☐ No ☐ Offices Server rooms Data centres	☐	☐	☐
1.1.10. Are technical controls in place for securing devices that have been inadvertently left unattended? Example: sign-out when the session has ended or configuration of automatic sign-out, sessions end when work is finished. At your sites: Yes ☐ No ☐ — Third parties (Service providers): Yes ☐ No ☐ Offices Server rooms Data centres	☐	☐	☐
1.2. Control to prevent unauthorised systems access (blacklist)	**yes**	**no**	**not relevant**
1.2.1. Is the company network protected from the public network and monitored by a firewall? (IDS/IPS)? Type: _____ Update procedure and frequency:	☐	☐	☐
1.2.2. Are penetration tests for all IP addresses exposed to the Internet carried out regularly?	☐	☐	☐
1.2.3. Are mobile clients such as technician notebooks or programming devices protected by a firewall?	☐	☐	☐
1.2.4. Do staff have to comply with the following password requirements? ☐ Individual computer password for each employee that is to be kept secret ☐ Minimum length, if applicable: Number of characters/complexity: _____ ☐ Cycle change, if applicable; please specify interval: _____ ☐ Automatic screen locking after certain period of time:	☐	☐	☐
1.2.5. Are virus scanners used at the following interfaces to the company network? Yes ☐ No ☐ E-Mail services File services Web services	☐	☐	☐
1.2.6. Is a virus scanner used on all servers? Yes, update procedure and frequency: _____ No, specify operating system and reason: _____ Or not relevant, reason:	☐	☐	☐
1.2.7. Is a virus scanner used on all individual workstation computers, technician notebooks and programming devices? Yes, update procedure and frequency: _____ No, specify operating system and reason: _____ Or not relevant, reason:	☐	☐	☐

1.2.8. Are security-relevant software updates installed for existing software regularly and automatically and documented? How often each year?	☐	☐	☐
1.2.9. Do employees have local administrator rights on the individual workstation computer? Yes / No Administrators ☐ ☐ Developers ☐ ☐ Technicians ☐ ☐ Users ☐ ☐	☐	☐	☐
1.2.10. Are employees authorised to access the Internet? Yes / No If yes: have restrictive browser configurations that cannot be changed by employees been set up? ☐ ☐	☐	☐	☐
1.3. Data access control/privileges	**yes**	**no**	**Not relevant**
1.3.1. Are controls in place to ensure that users only have access to network resources that they have been expressly authorised to use and are necessary for their tasks?	☐	☐	☐
1.3.2. Are wireless networks protected against unauthorised access? If so, how? Authentication Cryptography Configuration	☐	☐	☐
1.3.3. Is a formal registration/deregistration process in place for user access to all information systems and services (e.g., Windows with multiple services)?	☐	☐	☐
1.3.4. Are rights to access the Client's information assets scrutinised regularly?	☐	☐	☐
1.3.5. Is a process in place to ensure that user access rights are deleted when employment or the contract ends or are adjusted when an employee's job changes?	☐	☐	☐
1.3.6. Are measures in place to ensure that data relating to individual customers of the Contractor is logically or physically separated?	☐	☐	☐
1.3.7. Is a password policy in place stipulating the following minimum requirements? At least seven characters, only secure passwords, changed every 90 days, access blocked if <= 10 failed attempts, no shared passwords.	☐	☐	☐
1.3.8. Are permissions concepts in place and are these documented?	☐	☐	☐
1.3.9. Is the system for allocating permissions documented on a name-specific basis (in particular, who may allocate which rights)?	☐	☐	☐
1.3.10. Are permissions allocated following the need-to-know principle, and updated and documented on a name-specific basis?	☐	☐	☐
1.3.11. Are administrators authorised to copy/extract Client databases in full or in large quantities? Number of administrators	☐	☐	☐
1.3.12. Are employees (not administrators!) authorised to copy/extract Client databases in full or in large quantities? Number of employees: _____ Formats in which export can take place (e.g., csv, xlsx):	☐	☐	☐
1.3.13. Have the following components of workstation computers been locked/disabled so that no data exports can be saved externally? ☐ USB-Ports ☐ CD-/DVD burner ☐ Memory card slots ☐ Other mobile data carriers	☐	☐	☐

1.3.14. Is remote maintenance access/remote data access is in place? If so: ☐ For employees ☐ For service providers If remote maintenance access/remote data access is in place, please add the following information: Type of authentication (e.g. password, PIN, Token) _____ In case of passwort authentication, deviations to 1.2.4: _____ Protocols/mechanisms used (e.g., SSH, VPN): _____ Additional measures (e.g., individual session sharing):	☐	☐	☐
1.3.15. Is direct access to the network or networks possible via remote maintenance accesses?	☐	☐	☐
1.3.16. Are rules for mobile working (e.g., working from home) in place at the Contractor so as to ensure the confidentiality, integrity, availability and robustness of data processing? Yes ☐ No ☐ The employees are instructed on how to work mobile, with documentation name-specific base:	☐	☐	☐
1.3.17. Are access and authentication measures in place with respect to employees working at home in order to ensure data security and compliance by employees working outside company premises? yes / no Username ☐ ☐ Password ☐ ☐ Secure hardware token/ one-time password ☐ ☐ Secure software token ☐ ☐ Web-based access ☐ ☐ Citrix ☐ ☐ Windows Remote Desktop ☐ ☐ VPN ☐ ☐ Other	☐	☐	☐

1.4. Separation control	**yes**	**no**	**Not relevant**
1.4.1. Are measures taken to separate Client data? ☐ Network separation by means of the following measures: ☐ Dedicated client, provided especially for the job	☐	☐	☐
1.4.2. Is a permissions concept in place for the clients/network segments specified above, which precludes employees who do not work for the Client from accessing data?	☐	☐	☐
1.4.3. Are employees obligated in writing not to use information from Client databases in other projects/for other purposes?	☐	☐	☐

2. Integrity

2.1. Transfer control	**yes**	**no**	**not relevant**
2.1.1. Is data transferred between the Client and the Contractor using data carriers (e.g., paper documents, hard drive, USB stick, CD)? no / yes / Procedure The data transferred by digital data carriers is encrypted. ☐ ☐ Response to the Client upon receipt or suspected loss: ☐ ☐	☐	☐	☐
2.1.2. Is a special type of encryption used for data exchange/communication between the Client and Contractor if data is transferred electronically? ☐ SFTP ☐ S/MIME ☐ HTTPS (e.g. Web interface, cloud storage): ☐ SSL-VPN oder Citrix: ☐ Other procedures:	☐	☐	☐

2.1.3. Is personal data and information belonging to the Client stored by the Contractor? ☐ unencrypted ☐ Encrypted, procedure:	☐	☐	☐
2.1.4. Is Client data that is included in back-ups protected (e.g., secure safekeeping of back-up media, back-up encryption)? ☐ Encrypted storage ☐ Encrypted transfer	☐	☐	☐
2.1.5. How is Client data deleted (e.g., in accordance with which standards/practices)? Electronic data in systems: ☐ not relevant Electronic data carriers: ☐ not relevant Paper documents: ☐ not relevant When is data deleted or when are data carriers disposed of: ☐ not relevant How is data deletion of disposal of data carriers documented: ☐ not relevant	☐	☐	☐
2.1.6. Are measures in place for protecting Client data (including temporary data) on mobile devices? Mobile workstation computers/data carriers, etc. (e.g., privacy filter on screens, encryption please give details of encryption where applicable): ☐ not relevant Smartphones, tablets, etc. (e.g., mobile device management, encryption; please give details of encryption where applicable): ☐ not relevant	☐	☐	☐
2.1.7. Are your employees allowed to use mobile technologies (such as smartphones) to access systems that store or process RWE data? yes ☐ no ☐ Are all of these technologies owned by the Supplier and under its management?	☐	☐	☐
2.1.8. Are your employees allowed to use mobile technologies (such as smartphones) to access systems that store or process RWE data? (i.e., remote wipe or PIN lock required) Which controls are in place?	☐	☐	☐
2.2. Input control	**yes**	**no**	**not relevant**
2.2.1. In order to trace the deletion or modification of Client data, are log files created for each employee on a name-specific basis?	☐	☐	☐
2.2.2. Is a restrictive access concept in place for the log files mentioned above?	☐	☐	☐
2.3. Operational Security	**yes**	**no**	**not relevant**
2.3.1. Is adequate log management (Syslog) in place and suitable monitoring (SIEM)? yes ☐ no ☐ The audit trail history is kept for at least one year. A period of at least three months is immediately available for analysis. You are able to support longer retention periods if required by law. Logs are (continually) monitored for unauthorised activities. Does the company have access to up-to-date and real-time information on technical vulnerabilities?	☐	☐	☐

3. Availability and resilience

3.1. Availability control	yes	no	not relevant
3.1.1. Are backups carried out? Which systems are backed uo? Which content is backed up? Backup frequency (interval)? Number of backup generations kept:	☐	☐	☐
3.1.2. Is there a secure storage location for back-up media? Safe External storage ≥5 km away (linear distance)	☐	☐	☐
3.1.3. Are authorisation processes in place for restoring data from back-ups?	☐	☐	☐
3.1.4. Is there a restart time for data centres? Restart time after complete destruction of the data centres in days:	☐	☐	☐
3.1.5. Are contracts in place for the maintenance of IT/ OT systems by third parties? Exclusively in the EU Access from third countries possible	☐	☐	☐
3.1.6. Is there a record of back-up media and information allowing traceability?	☐	☐	☐
3.1.7. Are the back-up process and the physical media used subjected to testing?	☐	☐	☐
3.1.8. Are systems, applications and components hardened before use? (regulations, admin/ rights; user accounts; encryption; ports; vulnerabilities; If so: yes ☐ no ☐ Procedure Do regulations exist, how the hardening should take place? ☐ ☐ Are user and system rights adapted so that unprivileged rights are favoured over privileged rights? ☐ ☐ Are unnecessary user accounts and software components deactivated? ☐ ☐ Are cryptographic procedures checked and introduced for transmission and persistent storage? ☐ ☐ Are unnecessary ports and connections closed? ☐ ☐ Will known vulnerabilities be avoided or eliminated? Is this done continuously? ☐ ☐	☐	☐	☐
3.1.9. Is a proven emergency plan in place?	☐	☐	☐
3.1.10. Is a proven business continuity plan in place?	☐	☐	☐
3.1.11. Do information processing facilities have sufficient redundancy to fulfil the availability requirements of companies?	☐	☐	☐

4. Procedures for regular review, assessment and evaluation

4.1. Order control	yes	no	not relevant
4.1.1. Have the following people signed confidentiality or non-disclosure agreements with respect to the handling of personal data?	☐	☐	☐

		yes	no		
Employees		☐	☐		
Service providers		☐	☐		
Third parties		☐	☐		
4.1.2.	Are employees obligated in writing to maintain secrecy of communications[4]?			☐	☐	☐
4.1.3.	Does the Supplier collect from its employees the following additional declarations in writing (in the context of data privacy and data protection and in the context of mobile working)? Which?			☐	☐	☐
4.1.4.	Have sub-contractors who have access to Client data been engaged?			☐	☐	☐
		yes	no			
	Contracts on commissioned data processing acc. to Article 4, No. 8 and Article 28 of the GDPR, and, if applicable, on security acc. to Article 4 of Directive 2002/58/EC in conjunction with Directive 2009/136/EC are in place with sub-contractors who process Client data:	☐	☐			
	Sub-contractors who are given access to Client data comply with the technical and organisational measures agreed in this checklist in exactly the same way as the Contractor itself, and have contractually agreed to such compliance:	☐	☐			
	Are there sub-contractors outside the EU who have access to Client data?	☐	☐			
	If so, how are appropriate safeguards acc. to Article 46 et seq. GDPR established?	☐ Approved codes of conduct acc. to Article 40 ☐ Approved certification mechanisms acc. to Article 42 ☐ Adequacy decisions acc. to Article 45 ☐ EU contractual clauses acc. to Article 46 ☐ Binding corporate rules acc. to Article 47 ☐ Derogations for specific situations acc. to Article 49 ☐ EU Privacy Shield					
4.1.5.	Are employees trained with respect to data privacy and information security, and is such training documented on a name-specific basis?			☐	☐	☐
4.1.6.	Do all the Contractor's employees and third-party users complete regular training to raise awareness of security, which is appropriate to their role and function within the company?			☐	☐	☐
4.1.7.	Are certificates/data privacy concepts currently in place, which are submitted with this checklist? (please specify title and date): Please specify title and date:			☐	☐	☐
4.1.8.	If the service is provided using Cloud services (cf., 1.1.1, 2.1.2, 4.1.4), is an architecture outline also submitted showing the IT/ OT components used, storage locations and protocols used? Please specify title and date:			☐	☐	☐
4.2.	**Data Protection Management System**			**yes**	**no**	**not relevant**
4.2.1.	Has been a data protection officer appointed?			☐	☐	☐
		yes	no			
	The data protection officer has the necessary expertise for the company.	☐	☐			
	There are no conflicts of interest for the Data Protection Officer.	☐	☐			
	The Data Protection Officer is directly subordinate to the highest level of management and reports directly to it.	☐	☐			
	The Data Protection Officer will be duly and promptly involved in all matters relating to the protection of personal data.	☐	☐			
4.2.2.	A data protection and risk management system is established which meets the requirements of the GDPR.			☐	☐	☐
4.2.3.	The management is sufficiently involved in the data protection organisation and the corresponding communication, escalation and decision-making processes and ensures that the tasks and obligations can be fulfilled to the required extent and quality.			☐	☐	☐
4.2.4.	The Plan-Do-Check-Act cycle is used to ensure that documents are always up to date and processes are continuously improved.			☐	☐	☐

[4] In accordance with the ePrivacy Directive or Regulations as amended, in conjunction with national rules on telecommunications secrecy, e.g., Section 88 of the Telecommunications Act (TKG) (for Germany).

4.2.5. A data protection report on the functioning and effectiveness of the data protection management system, as well as any malfunctions and data protection-related events, shall be compiled at least once a year and made available on request.	☐	☐	☐
4.3. Miscellaneous	**yes**	**no**	**not relevant**
4.3.1. Is one of the following procedures used by the Contractor to regularly review, assess and evaluate the effectiveness of the technical and organisational measures in order to ensure processing is secure acc. to Article 32(1) GDPR? ☐ ISMS, acc. to the following standard (z.B. ISO 27001/2): ☐ Alternative procedure (please specify): ☐ Not applicable, reason:	☐	☐	☐
4.3.2. Is information classified? Is the classification made according to a regulation?	☐	☐	☐
4.3.3. Do regulations exist which prohibit the private use of components of the contractor and the client?	☐	☐	☐
4.3.4. Is information security covered in contracts concluded by the Contractor with suppliers and service providers?	☐	☐	☐
4.3.5. Are the third-party information security systems certified (e.g., ISO 27001, ISO 9001)? When were they certified?	☐	☐	☐
4.3.6. Are suppliers and service providers subject to regular checks and audits?	☐	☐	☐
4.3.7. Are rules in place for handling security incidents?	☐	☐	☐
	yes	no	
Please specify the procedure:	☐	☐	
Do these ensure that the client is notified immediately?	☐	☐	
4.3.8. Does performance under this contract also include the provision of services or the development of software (e.g., Software as a Service)? Rules are in place:	☐	☐	☐
	yes	no	
on 'data protection by design', to take into account the right to data privacy when developing and designing products, services and applications (e.g., through measures such as pseudonymisation):	☐	☐	
on the use of personal data in software development:	☐	☐	
4.3.9. Are dedicated systems or applications developed (internally or contracted externally) for processing or storing RWE data?	☐	☐	☐
	yes	no	
Do you verify that your code is secure using industry standards?	☐	☐	
Is a controlled change management process in place?	☐	☐	
Is a separate development, testing and operating environment used?	☐	☐	
If development is outsourced, is an escrow agreement in place?	☐	☐	
If systems or applications are developed, are they subjected to security testing as part of the development process?	☐	☐	
Is test data carefully selected, protected and controlled (no production data or anonymised)?	☐	☐	
4.3.10. Is a documented incident management process in place?	☐	☐	☐
	yes	no	
Is an incident response process in place, which reflects the categorisation and severity of incidents in terms of information security?	☐	☐	
In the event of an incident, is data collected in such a way, in terms of information security, that it can be used as evidence?	☐	☐	
4.3.11. Are managers instructed to regularly check that directives and procedures are being followed within their area of responsibility?	☐	☐	☐

Chapter 4: Data processing agreement pursuant to art. 28 (3) GDPR

The Processing of personal data takes place as processor in the sense of art. 4 no. 8 in conjunction with 28 EU-GDPR.

The underlying data processing agreement is signed between the controller, RWE AG, and its affiliated companies in accordance with Secs. 15 et seq. of the German Stock Corporation Act (AktG) and the processor named in Section 1.

1. Object and duration of the order

1.1. Object of the order
The object of the contract is determined by the individual and/or framework contracts concluded.

1.2. Duration of the order
The duration of this contract (term) corresponds to the term of the individual and/or framework contracts. A premature termination of the term without period of notice shall be admissible in case of violation of legal or contractual data protection provisions. The same shall also apply if the Supplier does not want to or cannot execute a reasonable instruction of the Client.

2. Specification of the order content

2.1. Nature and purpose of the planned Processing of data
The nature and purpose of the Processing of personal data by the Supplier for the Client are concretely described under chapter 2, number 2.

2.2. Place of performance
The locations for the provision of the contractually agreed service, as well as the guarantees that may be required to ensure an adequate level of data protection in third countries, are set out in Chapter 2, paragraph 3. Any relocation to a third country requires the prior consent of the Client and may only take place if the special conditions of art. 44 et seq. GDPR are fulfilled. The Supplier must ensure that the special requirements of art. 44 et seq. GDPR are proven to the principal in a suitable manner.

2.3. Data categories
The subject of processing of personal data shall be the types/categories of data listed in Chapter 2, paragraph 4.

2.4. Data subjects
The categories of data subjects affected by the processing shall include the categories of data subjects listed in Chapter 2, paragraph 5.

3. Technical and organizational measures

Before the commencement of Processing, the Supplier shall document the execution of the necessary technical and organizational measures and, where applicable, operating security in accordance with Article 4 Directive 2002/58/EU and Directive 2009/136/EU, set out in advance of the order, specifically with regard to the detailed execution of the contract, and prior to the Processing, and shall present these documented measures to the Client for inspection. If the Client does not object, the documented measures become the foundation of the order. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

The contractor must provide the security in accordance with art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure an appropriate level of protection for the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of data subjects in terms of Article 32 (1) DS-GVO must be taken into account.

Supplier undertakes to comply with the technical and organisational measures set out in Chapter 3 and, if applicable, the operational safety in accordance with Article 4 of Directive 2002/58/EC in conjunction with RiLi 2009/136/EC. These technical and organizational measures are defined as compulsory for the contractor. The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. The security level of the defined measures may not be undercut. Essential changes must be agreed in writing.

4. Correction, restriction of processing and deletion of data

Any data processed under the contract may not be corrected, deleted or restricted by the Supplier on his own authority, but only according to documented instructions from the Client, with the exception of the provisions under paragraph 11 of these Additional Conditions. Insofar as a data subject directly contacts the Supplier in this matter, the Supplier shall immediately forward this request to the Client.

To the extent covered by the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the Supplier in accordance with the documented instructions of the Client.

5. Quality assurance and other duties of the Supplier

In addition to complying with the provisions of this contract, the supplier has statutory obligations pursuant to art. 28 to 33 GDPR; in this respect, the supplier guarantees in particular compliance with the following requirements:

5.1. The Supplier shall provide the Client with the name of the competent data protection officer or - if no data protection officer is required - a contact person for data protection (see Chapter 1; Details of the Data Protection Officer). The Client must be informed immediately in writing of any change of the data protection officer/contact person.

5.2. If the Supplier is based outside the Union, Supplier shall appoint a representative in the Union in accordance with art. 27 para. 1 GDPR (see Chapter 2, paragraph 6).

5.3. Confidentiality in accordance with art. 28 para. 3 Sentence 2 Point b, Articles 29 and 32 para. 4 GDPR and, if applicable, also the privacy of telecommunications as well as confidentiality about electronic communication data. The Supplier entrusts only such employees with the Data Processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not Process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law. The resulting secrecy obligation shall apply beyond the end of the contract for an undetermined period of time regardless of the provision on other secrecy obligations. The same applies to data which are subject to the privacy of telecommunications.

5.4. Implementation of and compliance with all technical and organizational measures necessary for this Order or Contract in accordance with art. 28 para. 3 Sentence 2 Point c, Article 32 GDPR and, where applicable, operating security in accordance with Article 4 Directive 2002/58/EG and Directive 2009/136/EG.

5.5. Upon the request of the supervisory authority, the Client and the Supplier shall cooperate in the performance of its tasks.

5.6. The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the Processing of personal data in connection with the Processing of this Order or Contract.

5.7. Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a

third party or any other claim in connection with the Order or Contract Data Processing by the Supplier, the Supplier shall make every effort to support the Client.

5.8. The Supplier will regularly review the internal processes as well as the technical and organisational measures to ensure that the processing in his area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the rights of the data subject are protected.

5.9. Evidence of the technical and organisational measures that have been taken can be demonstrated to the customer within the scope of his powers of control in accordance with paragraph 8 of this Data Processing Agreement.

5.10. Notification of the Client by the Supplier about the existence of rules and regulations for the Supplier´s employees and agents about "mobile working", e.g. about being able to work outside of commercial units of the Supplier or subcontractor (according to Section 6 of this DPA).
Obtaining of the approval of the Client for the Processing of data of the Client out of commercial units of the Supplier or subcontractor.
Any Processing of data for the Client outside the commercial units of the Supplier/subcontractor shall only be admissible with the approval of the Client in individual cases.

6. Subcontractual relations

6.1. For the purposes of this provision, subcontractual relationships are understood to be those services which are directly related to the provision of the main service. This does not include auxiliary services which the Supplier uses as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Supplier undertakes to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Customer's data even in the case of outsourced auxiliary services.

6.2. The Supplier may only commission subcontractors (further processors) with the prior express written or documented consent of the Client. The Client agrees to the assignment of the subcontractors mentioned in Chapter 2, paragraph 7 under the condition of a contractual agreement in accordance with art. 28 para. 2-4 GDPR.

6.3. Outsourcing to subcontractors and/or changing existing subcontractors shall be permitted, provided that:

- the Supplier notifies the Client of such outsourcing to subcontractors in writing or in text form within a reasonable period of time in advance and
- the Client does not object to the planned outsourcing in writing or in text form to the Supplier prior to the time of transfer of the data, and
- is based on a contractual agreement in accordance with art. 28 para. 2-4 GDPR.

The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data Processing in the cases of Point a) or Point b) shall only be undertaken after compliance with all requirements has been achieved.

6.4. Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form); the granting of approval is at minimum dependent on the fact that all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor. The Supplier has to prove this to the main Client in an adequate form.

6.5. If a subcontractor renders the agreed service outside the EU/EEA, the Contractor shall ensure compliance with data protection law by taking appropriate measures. Any further outsourcing by a possible subcontractor requires the express written or documented consent of the customer. All contractual regulations in the contract chain must also be imposed on the further subcontractor.

7. Persons authorized to give instructions on Client side

Persons on the client's side who are authorised to issue instructions, who also act as contact persons for data protection issues arising within the framework of the contract and who, if necessary, establish contact with the client's data protection officer, are the respective signing persons of the respective individual and/or framework contracts. They are individually authorized to issue instructions. The Customer shall inform the Contractor in writing without delay of any change in the person(s) authorised to issue instructions.

8. Supervisory powers of the Client

8.1. The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

8.2. The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

8.3. Evidence of such measures, which concern not only the specific Order or Contract, may be provided by compliance with approved Codes of Conduct pursuant to art. 40 GDPR, certification according to an approved certification procedure in accordance with Article 42 GDPR, current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor) or a suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification e.g. ISO/IEC 27001).

9. Notification in case of violations of the Supplier

9.1. The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

- Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
- The obligation to report a personal data breach immediately to the Client regardless of who caused the data breach (including cases of loss of or unlawful transfer of or unlawfully gaining knowledge of personal data).
- The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
- Supporting the Client with its data protection impact assessment.
- Supporting the Client with regard to prior consultation of the supervisory authority.

10. Authority of the Client to issue instructions

10.1. The Client in principle issues instructions in writing (at the minimum in text form). In case as an instruction by the Client is issued only orally, the Supplier shall request confirmation of the instruction at the minimum in text form from the Client.

10.2. Chapter 5, paragraph 5.3. sentence 3 of this Data Processing Agreement applies.

10.3. The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

11. Deletion of data and return of data carriers

11.1. The Supplier shall not Process the data for any other purposes and is in no way entitled to transfer the data to third parties. Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly Data Processing, as well as data required to meet regulatory requirements to retain data.

11.2. After the completion of the contractual works or earlier upon request by the Client – at the latest at the end of the Service Agreement – the Supplier shall return any documents received, prepared Processing and use results as well as data inventories related to the contractual relation to the Client or destroy them in accordance with data protection provisions with the Client's approval. The same shall apply for test and rejected materials. The deletion log shall be submitted to the Client on demand.

11.3. Documentation serving for the evidence of the Data Processing in accordance with the order and proper Data Processing shall be kept by the Supplier in accordance with the respective storage periods even beyond the end of the contract. The Supplier may hand this over to the Client at the end of the order for the purpose of exoneration to relieve the Supplier of this contractual obligation.

Signature

We assure you that the information provided here corresponds to the current status of the technical and organisational measures implemented by us with regard to data protection, data security and information security. Deviations from the information provided here must be reported immediately to the client of the framework agreement.

Name and surname of the person responsible for completing the checklist (block capitals)

Place, date

Signature Supplier