Data Processing Agreement (DPA)

pursuant to Article 28 (3) of the General Data Protection Regulation (GDPR) on the framework or individual contract dated

between the

(Principal)

and the

(Contractor)

Preamble

The Principal wishes to commission the Contractor with the services specified in Chapter 2, point 2.1. Part of the performance of the contract is the processing of personal data. In particular, Art. 28 GDPR imposes certain requirements on such processing on behalf. In order to comply with these requirements, the Parties conclude the following Agreement, the performance of which shall not be remunerated separately unless expressly agreed. Insofar as the services are also provided for RWE AG or one of its affiliated companies pursuant to § 15 et seq. of the German Stock Corporation Act (AktG), this agreement shall also apply for the benefit of these companies. Against this background, the following is agreed:

Chapter 1. General information on the company

1.1. Details of the company

Name _____

Street _____ No. _____

City _____ Post-code _____

Country _____

E-mail _____

Phone _____

1.2. Details of the data protection officer

Note: If there is no legal obligation to appoint a company data protection officer, a contact person for data protection must be provided.

Name _____

E-mail _____

Phone _____

Chapter 2. Information on the processing of personal data

2.1. Specify the scope of supplies and services that are provided as processing on behalf (of the Controller) pursuant to Art. 28 of the GDPR. Define precisely the corresponding purpose and the type of processing of personal data.

2.2. Place of performance

Important: Taking into account any subcontractors used, cf. Chapter 4, 4.6.

○ The performance of the contractually agreed service shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation of partial services or the entire service to a third country requires the prior consent of the Principal in writing or in documented electronic format and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

☉ The provision of the contractually agreed service takes place (possibly in part) in a country outside the European Union or another state party to the Agreement on the European Economic Area ("third country"). The adequate level of protection is determined under the additional requirements of the case law of the European Court of Justice ("ECJ"), in particular Case C-311/18 - "Schrems II", and the recommendations of the European Data Protection Board (EDPB),

☐ established in the following countries through standard data protection clauses (Art. 46 (2) (c) and (d) GDPR): [1]

☐ ensured in the following countries by an adequacy decision of the Commission (Art. 45 (3) GDPR):

☐ established in the following countries by approved codes of conduct (Art. 46 (2) (e) in conjunction with 40 GDPR):

☐ established in the following countries through an approved certification mechanism (Art. 46 (2) (f) GDPR):

☐ established in the following countries by the following measures (Art. 46 (2) (a), (3) (a) and (b) GDPR):

2.3. Type of data

Hint: At this point, the personal data processed on behalf of the Principal must be indicated. This explicitly does not include personal data that your company processes in the course of communication with RWE employees or data of the RWE company when initiating the contract as well as data that your company processes internally for invoicing or other internal organisational tasks.

	Data category	Data objects of the data category
☐	Address data	Street, house number, postcode, place of residence, flat number, etc.
☐	Age data	Age, date of birth, place of birth
☐	User data	Login name, passwords, tokens or other credentials, last name and e-mail address, optionally first name, contact details in the company (phone, mobile, fax), departmental affiliation, position in the company, duration of service.
☐	Professional activities	Employer, job title, description of the job, current responsibilities and projects, place of work, working modalities and conditions, etc.

[1] So-called EU Standard Contractual Clauses "Controller to Processor". The conclusion of EU Standard Contractual 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, is the basic requirement of the Principal.

☐ Image recording data	Data within the scope of image recordings of any kind, such as films, photographs, video recordings, digital photographs, infrared images, X-ray images, etc.
☐ Biometric identification data	Fingerprints, voice recognition, retinal imaging, recognition of the face, finger or hand shape, signature dynamics, etc.
☐ Data on criminal convictions and offences	Certificate of good conduct, data on misconduct and criminal offences, penalty notices, etc.
☐ Electronic identification data	IP addresses, cookies, connection times and data, electronic signature, etc.
☐ Ethnic data	Information on origin, ancestry, compatriots' associations, etc.
☐ Financial identification data	Bank identification and bank account number, credit and debit card numbers, secret codes, etc.
☐ Genetic data	Data in the context of a detection, examination of heredity, DNA, etc.
☐ Geolocation data	Information about whereabouts, distances travelled and geographical information collected and processed by sensors, actuators, protocols and/or functionalities of devices.
☐ Physical health condition	Medical record, medical report, diagnosis, treatment, examination result, disability or infirmity, diet; other special health requirements for treatment, travel or accommodation, etc.
☐ Medication data	Data on the means and procedures used for the medical or paramedical care of the patients, etc.
☐ Staff data	Personnel number, employee ID number.
☐ Name data	First and last name, title, maiden name, other names
☐ Public identification data	National (tax) identification number, identity card number, passport registration number, social security card number, vehicle registration number, etc.
☐ Philosophical, militant or religious beliefs	Information on philosophical, militant or non-statist religious beliefs, memberships in such associations, positions and functions, membership fees and benefits paid, etc.
☐ Political affiliations	Information on party affiliation, political opinions and preferences, political positions held, etc.
☐ Private contact details	Phone numbers, e-mail address, social media accounts, fax number, etc.
☐ Pensions	Retirement date, scheme type, retirement date, details of payments received and made, options, beneficiaries etc.
☐ Sexual behaviour	Information on sexual behaviour, gender, gender reassignment, etc.
☐ Sound recording data	Data in the context of sound recordings of any kind, such as electronic and magnetic sound recordings, recordings of telephone conversations and video conferences, etc.

☐	Transaction data and log files	Access and access logs, system or access logs, communication links, etc.
☐	Other:	

2.4. Categories of data subjects

☐	Employees	*Definition: Employees of the RWE Group, including temporary agency workers in relation to the hirer; employees employed for their vocational training; rehabilitated persons; volunteers performing a service under the JFDG (Youth Volunteer Service Act) or the BFDG (Federal Volunteer Service Act).*
☐	Relatives of employees	
☐	Applicants	
☐	Customers	
☐	Employees of business partners of the RWE Group	
☐	External third parties	*Definition: External third parties are persons with whom RWE Group companies have no contractual relationship (e. g. police, public order office, mining authority, interested parties or visitors).*
☐	Other:	

2.5. Representative of the Contractor in the European Union pursuant to Art. 27 (1) GDPR

Note: To be completed only if your place of business is outside the EU.

Name			
Street		No.	
City		Post-code	
Country			
E-mail			
Phone			

Chapter 3. Technical and organisational measures

You undertake to comply with the technical and organisational measures set out below. These technical and organisational measures must be defined for the processing commissioned by the Principal. If individual measures are only partially fulfilled or not fulfilled or are not relevant, this must be justified.

3.1. Information on service provision (multiple selection possible)

3.1.1. The provision of the contractual services takes place ...

☐ exclusively with the help of end devices provided by the RWE Group. No end devices of your company are used.

☐ both with end devices provided by the RWE Group and with end devices provided by your company.

☐ exclusively with your company's end devices.

☐ takes place exclusively at locations of the RWE Group. Remote access via untrusted networks does not take place.

☐ both at RWE Group locations and by remote access via untrusted networks.

☐ exclusively by remote access via untrusted networks.

3.1.2. The storage of data and the hosting of applications of any kind takes place ...

☐ exclusively in an infrastructure provided by the Contractor or a commissioned subcontractor (usually software-as-a-service).

☐ both in an infrastructure provided by the Contractor or an appointed subcontractor and an infrastructure provided by the Principal.

☐ exclusively in an infrastructure provided by the Principal (usually on-premise).

3.2. Details of the protective measures implemented by your company and any subcontractors engaged

3.2.1. Joiner-Mover-Leaver process (personnel security)

The processor shall ensure that all persons entrusted with the processing are informed about existing regulations, instructions and procedures on data protection and are obliged to comply with them.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.2. Roles, responsibilities and separation of functions

The processor shall ensure that the tasks and responsibilities in the data protection process are regulated and accessible. The tasks and the roles and functions required for them shall be structured in such a way that incompatible tasks such as operational and control functions are distributed among different persons. A separation of functions shall be defined and documented for incompatible functions. Representatives shall also be subject to segregation of duties.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.3. Allocation of responsibility

For all business processes, applications, IT systems, rooms and buildings as well as communication links, it shall be determined who is responsible for them and their protection.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.4. Protection of sensitive information in the workplace

All employees must be made aware that sensitive information or IT systems must not be freely accessible at unattended workplaces.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.5. Allocation of physical access authorisations

It shall be defined which physical access authorisations are issued to which persons within the scope of their function and which are withdrawn from them. The issuance or revocation of access means used, such as smart cards, shall be documented. If access means have been compromised, they shall be replaced. In case of prolonged absences, authorised persons shall be temporarily blocked.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.6. Allocation of access authorisations

It shall be determined which access authorisations are issued to which persons within the scope of their function and which are withdrawn from them. If access means such as chip cards are used, the issue or withdrawal shall be documented. In case of longer absences, authorised persons shall be temporarily blocked.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.7. Allocation of access rights

It shall be defined which access rights are granted to which persons within the scope of their function and which are withdrawn from them. If smart cards or tokens are used in the context of access control, the issue or withdrawal shall be documented. In case of longer absences, authorised persons shall be temporarily blocked. It shall be ensured by means of an authorisation component that users can only perform actions to which they are authorised. All access to protected content and functions shall be controlled before it is executed. If it is not possible to assign access rights, an additional security product shall be used for this purpose. If the access control is faulty, access shall be denied. Similarly, access to files by users with restrictive file system permissions shall be restricted. Access rights must be assigned restrictively. Each user should ONLY be able to access the files they need to perform their tasks. The access right itself, in turn, shall be limited to the necessary type of access.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.8. Identification and authentication

Access to all IT systems and services shall be secured by appropriate identification and authentication of the accessing users, services or IT systems. Preconfigured authentication means shall be changed before productive use. Identification and authentication mechanisms appropriate to the protection needs shall be used. Passwords used shall be strong. There shall be a password policy for strong passwords. Authentication data shall be protected by the IT system or IT applications against spying, modification and destruction at all times during processing. It shall be ensured that users authenticate themselves appropriately when they want to access protected resources. For this purpose, a suitable authentication method shall be selected and the selection process documented. The component shall enforce users to use strong passwords according to a password policy. Limits for failed login attempts shall be defined. All authentication methods offered shall have the same level of security.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.9. Allocation of tasks and separation of functions

The defined incompatible tasks and functions shall be separated by identity and authorisation management.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.10. Regulation for the establishment, modification and withdrawal of authorisations

User IDs and permissions must ONLY be assigned based on actual need. In the event of staff changes, user IDs and permissions that are no longer required must be removed. If staff members request authorisations that go beyond the standard, these may only be assigned after additional justification.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.11. Documentation of user IDs and rights profiles

It shall be documented which user IDs, created user groups and rights profiles have been authorised and created. The documentation of the authorised users, created user groups and rights profiles shall be checked regularly to ensure that it is up-to-date. The documentation shall be protected against unauthorised access.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.12. Regulation for password-processing applications and IT systems

A password policy shall be established. Changes regarding the password policy shall be implemented uniformly for all devices, IT systems and applications, if possible at the same time. The password policy shall require strong and complex passwords. Purely timed changes must be avoided. Measures must be taken to detect password compromise. Default passwords must be replaced with sufficiently strong passwords and predefined identifiers must be changed. After a password change, at least the last five passwords must not be used. Passwords shall be stored as securely as possible. When authenticating in networked systems, passwords must not be transmitted unencrypted over insecure networks.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.13. Suitable key management for cryptographic procedures

Different keys must be used for encryption and signature formation. If keys are used, the authentic origin and integrity of the key data shall be verified.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.14. Encryption of the communication links

Communication links shall be suitably encrypted. Security requirements for the communication link between devices and systems in trusted and untrusted networks shall be defined. It shall be ensured that the confidentiality, integrity and authenticity of the transmitted data are guaranteed. In addition, the authenticity of the communication partners shall be guaranteed.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.15. Encryption of data and information

In the event of an increased need for protection, the data and information of the responsible party should be encrypted with a product or procedure that is considered secure. This should also apply to virtual machines with productive data. Not only a TPM alone should serve as key protection. The recovery password should be stored in a suitable secure location. For very high requirements, e. g. for confidentiality, full volume or full disk encryption should be used.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.16. Secure deletion and destruction of cryptographic keys

Keys and certificates that are no longer needed must be securely deleted or destroyed.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.17. Data backup according to the minimum backup concept

The processor shall create a minimum data protection concept for data protection. This shall specify the minimum data backup requirements to be met and who is responsible for them. The minimum backup policy shall contain at least a brief description of which IT systems and which data on them are backed up by which backup, how the backups can be created and restored, which parameters are to be selected and which hardware and software are used. The processor shall create regular data backups in accordance with the (minimum) data backup concept. The created data backups shall be appropriately protected from access by third parties. Regular tests shall be carried out to check whether the data backup works as desired, especially whether backed up data can be restored without problems and in a reasonable time.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.18. Virus protection programmes for terminals, gateways and IT systems

Depending on the operating system used, other existing protection mechanisms, as well as the availability of suitable virus protection programmes, an appropriate protection programme must be selected and installed for the specific purpose. only products for the enterprise sector may be used. Products for home users only or products without manufacturer support must not be used in professional operations. only cloud functions of such products may be used for which there are no serious, verifiable data protection or confidentiality aspects that speak against this.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.19. Restrictive configuration of the firewall

All communication between the networks involved shall be routed through the firewall. It must be ensured that no unauthorised connections can be established from outside into the protected network. Likewise, no unauthorised connections must be established from the protected network. Clear rules shall be defined for the firewall that determine which communication connections and data streams are allowed. All other connections shall be prevented by the firewall (whitelist approach). The communication relationships with connected service servers (e. g. e-mail servers, web servers) that are routed through the firewall shall be included in the rules. IT systems must not access the internal network from outside via the firewall. Responsible persons shall be appointed to design, implement and test filter rules. In addition, it must be clarified who is allowed to change filter rules. The decisions taken as well as the relevant information and reasons for decisions shall be documented.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.20. Network separation

The network shall be physically separated into at least three security zones: internal network, demilitarised zone (DMZ) and external connections (including internet connection as well as connection to other untrusted networks). Zone transitions shall be secured by a firewall. This control shall follow the principle of local communication, so that only permitted communication is forwarded by firewalls (whitelisting). Untrusted networks (e.g. Internet) and trusted networks shall be separated by a two-tier firewall structure. At least one stateful packet filter shall be used to network-separate Internet and external DMZ. All incoming and outgoing data traffic shall be controlled and filtered by the external packet filter and the internal packet filter, respectively.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.21. Connection of apps with backend systems

The connection between the app and backend systems shall be secured by cryptographic measures. Here it shall be checked whether the methods offered by the operating system are sufficiently secure for the app or whether own methods may have to be implemented at app level. If an app accesses backend systems via a user account, a dedicated service account shall be used for this purpose.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.22. Patch, change and update management

If IT components, software or configuration data are to be changed, there shall be specifications for this that also take security aspects into account. All patches and changes shall be appropriately planned, approved and documented. When patches are installed and changes are made, fallback solutions shall be in place. Major changes must involve the Data Protection Officer. Overall, it shall be ensured that the targeted level of security is maintained during and after the changes.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.23. Remote maintenance

If clients are accessed remotely, this access must be initiated by the user of the IT system. The user of the remotely administered client shall explicitly agree to the remote access. The possible access and communication interfaces for establishing a connection shall be limited to what is necessary. Likewise, all remote maintenance connections shall be disconnected after remote access. It shall be ensured that remote maintenance software is only installed on systems where it is needed. Remote maintenance connections via untrusted networks shall be encrypted. The selection of the authentication method and the reasons leading to the selection shall be documented. Remote maintenance access shall be considered in identity and authorisation management.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.24. Secure configuration of a VPN

A secure configuration shall be defined for all VPN components. Authentication and encryption methods that are considered secure and have sufficient key length shall be used. The responsible administrator shall also regularly check whether the configuration is still secure and adjust it for all IT systems if necessary.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.25. Controlled integration of data and content in web applications and apps

The processor shall ensure that web applications and apps only embed and deliver intended data and content to the user. If web applications and apps offer a file upload function, this function shall be restricted as much as possible by the processor. Access and execution rights shall also be set restrictively in this case. In addition, it shall be ensured that a user can only save files in the specified path. The developers shall ensure that the user cannot influence the location of the uploads. The targets of the forwarding function of a web application shall be sufficiently restricted so that users are only forwarded to trusted websites.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.26. Configuration of logging at system and network level

All security-relevant events of IT systems and applications shall be logged. If the IT systems and applications defined as relevant in the logging policy have a logging function, it shall be used. When logging is set up, it shall follow the manufacturer's specifications for the respective IT systems or applications. Spot checks must be made at appropriate intervals to ensure that logging is still functioning correctly. The intervals shall be defined in the logging policy. If operationally and safety relevant events cannot be logged on an IT system, other IT systems shall be integrated for logging (e. g. of events on network level).

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.27. Minimisation and control of permissions

Before an IT system, application or app is introduced, it shall be ensured that it only receives the minimum required permissions for its function. Authorisations that are not absolutely necessary shall be questioned and, if necessary, prevented. Security-relevant authorisation settings shall be fixed in such a way that they cannot be changed by the user or IT system, application or app. Where this is not technically possible, the authorisation settings shall be regularly checked and reset.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.28. Deletion and destruction of information

It shall be regulated how the deletion and destruction of information takes place. It shall be regulated which information and resources may be deleted and disposed of under which conditions. It shall also be determined in which spatial areas disposal and destruction facilities are to be set up. Before already used data carriers are passed on or used again, all data on them shall be securely deleted. Appropriate procedures shall be available to staff for this purpose.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.29. Archiving information

It shall be defined which goals are to be achieved with archiving. In particular, it shall be taken into account which regulations are to be observed, which employees are responsible and which functional and performance scope is aimed for. The results shall be recorded in an archiving concept. The archiving concept shall be regularly adapted to the current circumstances. All accesses to electronic archives shall be logged. For this purpose, the date, time, user, client system and the actions performed as well as error messages shall be recorded.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.30. Regulated decommissioning of IT systems and data carriers

It shall be regulated and documented how IT systems and data carriers are to be decommissioned. It shall be ensured that all information stored on an IT system or data carrier is securely deleted prior to decommissioning.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.31. Client separation in the case of outsourcing

A suitable client separation concept shall ensure that application and data contexts of different clients are cleanly separated.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.32. Safety-relevant events

Appropriate reporting and alerting channels shall be established and documented. It shall be clearly defined what a data protection incident is. A data protection incident shall be demarcated as far as possible from disruptions in day-to-day operations. Contact information shall always be up-to-date and easily accessible. In order to successfully resolve a security incident, the processor shall first isolate the problem and find the root cause. Then it shall select the necessary measures to fix the problem. A release shall be issued before the measures are implemented. Afterwards, the cause shall be eliminated and a secure state shall be established.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.33. Protection against SQL injection

If data is passed to a database system, developers must use stored procedures or prepared SQL statements if supported by the deployment environment. If neither stored procedures nor prepared SQL statements can be used, the SQL queries must be secured separately.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.34. Hardening of system, applications and devices

A strategy shall be developed on how systems, applications and devices are hardened prior to deployment in the infrastructure. The strategy shall at least include the assessment of necessary ports, communication protocols and functions. The hardening of systems, applications and devices shall take into account the requirement of "data protection through privacy-friendly default settings". only necessary personal data shall be processed and necessary functionalities released. All unneeded services and applications must be disabled or uninstalled, especially network services. All unneeded functions in the firmware must also be disabled. Unnecessary user IDs must either be deleted or at least deactivated in such a way that no logins to the system are possible under these IDs. Existing default identifiers shall be changed or deactivated as far as possible. Preset passwords of default identifiers shall be changed.

☐ The requirement is fulfilled. ☐ Not relevant.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

3.2.35. Operation and maintenance of a data protection management system

The Processor shall appoint a Personal Data Protection Officer if there is a legal obligation to do so. In any case, the Processor shall appoint a competent contact person for data protection. Both the Data Protection Officer and the contact person shall have the necessary expertise for the company and report directly to the highest level of management. There shall be no conflicts of interest in the performance of their duties. The processor shall establish a data protection and risk management system that complies with the requirements of the GDPR. There shall be adequate, meaningful documentation for processing operations. The documentation shall also provide for the concrete implementation and execution of technical and organisational measures. The Plan-Do-Check-Act cycle shall be used to ensure permanent up-to-dateness of documentation as well as continuous improvement of processes. A data protection report on the functioning and effectiveness of the data protection management system as well as any malfunctions and data protection-relevant events shall be prepared at least once a year and made available upon request.

☐ The requirement is fulfilled.

☐ The requirement is partially fulfilled.

☐ The requirement is not fulfilled.

Chapter 4. Data Processing Agreement pursuant to Article 28 (3) GDPR

The processing of personal data is carried out on behalf of the Controller (Principal) within the meaning of Art. 4 No. 8 in conjunction with Art. 28 GDPR.

The underlying Data Processing Agreement is concluded between the commissioning company(ies) of the aforementioned framework or individual agreement and the Processor (Contractor) named in 1.1. Insofar as further affiliated companies pursuant to §§ 15 et seq. AktG of RWE AG join the individual or framework agreement, this Data Processing Agreement shall also apply to them.

4.1. Subject and duration of the Order

4.1.1. Subject of the Order
The subject of the Order results from the respective individual and/or framework agreements concluded.

4.1.2. Duration of the Order/termination
The duration of this Order (term) corresponds to the term of the service agreement. Premature termination of the term of the individual or framework agreement by termination without notice is permissible if the Contractor fails to comply with his obligations under this agreement or violates other applicable data protection provisions intentionally or through gross negligence. The same shall apply if the Contractor is unable or unwilling to carry out a justified instruction of the Principal or if the Contractor opposes the control rights of the Principal in a manner contrary to the agreement. In particular, non-compliance with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a serious breach.

4.2. Specification of the Order content

4.2.1. Nature and purpose of the intended processing of data
The nature and purpose of the processing of personal data by the Contractor for the Principal are set out in 2.1.

4.2.2. Place of performance
The places for the provision of the contractually agreed service as well as any necessary guarantees to ensure an adequate level of data protection in third countries are set out in 2.2. Any relocation to a third country requires the prior consent of the Principal and may only take place if the special requirements of Art. 44 et seq. GDPR and the requirements of the relevant case law of the ECJ (in particular Case C-311/18 - "Schrems II") and the recommendations of the European Data Protection Board (EDPB) are met. The Contractor shall be required to demonstrate the fulfilment of the special requirements of Art. 44 et seq. GDPR to the Principal in an appropriate manner.

4.2.3. Nature of the data
The subject of the processing of personal data are the types/categories of data mentioned in 2.3.

4.2.4. Categories of data subjects
The categories of data subjects concerned by the processing include the categories of persons mentioned in 2.4.

4.3. Technical and organisational measures

4.3.1. The Contractor shall document the implementation of the required technical and organisational measures outlined in advance of the Order placement and before the start of the processing, in particular with regard to the specific execution of the Order, and shall hand them over to the Principal for inspection. Unless the Principal objects, the documented measures shall become the basis of the order. Insofar as the examination/audit of the Principal reveals a need for adaptation, this shall be implemented by mutual agreement.

4.3.2. The Contractor shall establish security pursuant to Art. 28 (3) lit. c, 32 GDPR, in particular in connection with Art. 5 (1), (2) GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be taken into account.

4.3.3. The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes shall be agreed in writing.

4.4. Rectification, restriction of processing and deletion of data and assistance by the processor

4.4.1. The Contractor may not rectify, delete or restrict the processing of data processed under the order on its own authority but only in accordance with documented instructions from the Principal, with the exception of the provisions under 4.10 of this Agreement. The Contractor shall support the Principal as far as possible with suitable technical and organisational measures in the fulfilment of the Principal's obligations under Articles 12-22 as well as 32 and 36 of the GDPR. If a data subject contacts the Contractor directly in this regard, the Contractor shall immediately refer the data subject to the Principal and await the Principal's instructions.

4.4.2. Insofar as included in the scope of services, the deletion concept, the right to be forgotten, rectification, data portability and information shall be ensured directly by the Contractor in accordance with the Principal's documented instructions. The provisions in 4.10 remain unaffected.

4.5. Quality assurance and other obligations of the Contractor

4.5.1. In addition to compliance with the provisions of this Order, the Contractor shall have statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

4.5.1.1. The Contractor shall name to the Principal the responsible Data Protection Officer or - if no Data Protection Officer is required - a contact person for data protection (see 1.2). A change of the Data Protection Officer/contact person shall be notified to the Principal in writing without delay.

4.5.1.2. If the Contractor has its registered office outside the European Union, it shall appoint a representative in the European Union in accordance with Article 27 (1) of the GDPR (see 2.5).

4.5.1.3. Maintaining confidentiality pursuant to Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR and/or the secrecy of telecommunications, if any, as well as maintaining the confidentiality of electronic communication data. When carrying out the work, the Contractor shall only use employees who have been obliged to confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process such data exclusively in accordance with the Principal's instructions, including the powers granted in this Agreement, unless they are legally obliged to process it. The resulting confidentiality obligation shall apply beyond the end of the term of theAgreement for an indefinite period of time, irrespective of the provision on other confidentiality obligations. The same applies to data subject to telecommunications secrecy.

4.5.1.4. The implementation of and compliance with all technical and organisational measures required for this assignment pursuant to Art. 28 (3) sentence 2 lit. c, 32 GDPR.

4.5.1.5. At the request of the supervisory authority, the Principal and the Contractor shall co-operate in the performance of their duties.

4.5.1.6. The immediate information of the Principal about control actions and measures of the supervisory authority, insofar as they relate to this Order. This also applies insofar as a competent authority is investigating the Contractor in the context of administrative offence or criminal proceedings with regard to the processing of personal data during the processing on behalf.

4.5.1.7. Insofar as the Principal, for its part, is exposed to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing on behalf by the Contractor, the Contractor shall support it to the best of its ability.

4.5.1.8. The Contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

4.5.1.9. Verifiability of the technical and organisational measures taken vis-à-vis the Principal within the scope of its supervisory powers pursuant to 4.7 of this Data Processing Agreement.

4.6. Subcontracting relationships

4.6.1. The Principal agrees to the commissioning of subcontractors by the Contractor, provided that the Contractor imposes on these subcontractors essentially the same contractual obligations with regard to the processing of personal data to which the Processor is also bound in the context of this processing on behalf. The provision of Article 28 (2-4) of the GDPR shall be complied with in relation to the subcontractors. In the case of subcontractors based in a third country, this consent shall apply provided that the principles of data transfer pursuant to Art. 44 et seq. GDPR and the requirements of the relevant case law of the ECJ (in particular Case C-311/18 - "Schrems II") and the recommendations of the European Data Protection Board (EDPB) are also complied with in relation to the subcontractors.

4.6.2. The Contractor shall inform the Principal of any future intended changes regarding the addition or replacement of other subcontractors, thus giving the Principal the opportunity to object to such changes. In this light, the change of existing subcontractors is permissible, insofar as:

4.6.2.1. the Contractor gives the principal reasonable advance notice in writing or text form of such outsourcing to subcontractors; and

4.6.2.2. the Principal does not object to the planned outsourcing in writing or in text form to the Contractor by the time the data is handed over, and

4.6.2.3. otherwise the requirements according to 4.6.1 are met.

4.6.3. The transfer of personal data of the Principal to the subcontractor and its first activity shall only be permitted once all requirements for subcontracting have been met.

4.6.4. Further outsourcing by the subcontractor requires the express consent of the principal (at least in text form), the granting of which is subject to the minimum requirement that all contractual provisions in the contractual chain are also imposed on the further subcontractor. The Contractor must provide the principal with appropriate proof of this.

4.6.5. Upon request of the Principal, the Contractor shall provide a copy of the subcontracting data processing agreements concluded by it or by subcontractors under this Agreement.

4.7. Control rights of the Principal

4.7.1. The Principal has the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. It shall have the right

to convince itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time.

4.7.2. The Contractor shall ensure that the Principal can convince itself of the Contractor's compliance with its obligations pursuant to Art. 28 of the GDPR. The Contractor undertakes to provide the Principal with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

4.7.3. Evidence of such measures, which do not only concern the specific Order, can be provided by compliance with approved codes of conduct pursuant to Art. 40 GDPR, certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR, current test certificates, reports or report extracts from independent bodies (e. g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors) or suitable certification by IT security or data protection audit.

4.8. Notification of infringements by the Contractor

4.8.1. The Contractor shall assist the Principal in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This shall include, but not be limited to:

4.8.1.1. ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for the immediate detection of relevant breach events;

4.8.1.2. the obligation to report breaches (including cases of loss or unlawful transmission or obtaining of knowledge) of personal data of the Principal to the Principal without delay, regardless of causation;

4.8.1.3. the obligation to assist the principal in the context of his duty to inform the data subject and, in this context, to provide him with all relevant information without delay;

4.8.1.4. the support of the Principal for its data protection impact assessment.

4.8.1.5. the support of the principal in the context of prior consultations with the supervisory authority.

4.9. Authority of the principal to issue instructions

4.9.1. The Contractor may only collect, use or otherwise process data within the scope of the individual or framework agreement and in accordance with the Principal's instructions. The Principal's instructions shall initially be determined by this Agreement and may thereafter be amended, supplemented or replaced by the Principal by individual instructions in accordance with 4.9.2. The Principal is entitled to issue corresponding instructions at any time. This also includes instructions with regard to the rectification, deletion and restriction of processing of data.

4.9.2. The Principal shall always issue instructions in writing, at least in text form. If an instruction from the Principal is only given verbally, the Contractor shall request confirmation from the Principal at least in text form. All instructions issued shall be documented by both the Principal and the Contractor and shall be kept for the duration of their validity and subsequently for further three full calendar years.

4.9.3. Persons authorised to give instructions on the part of the Principal, who also act as contact persons for data protection questions arising within the framework of the Agreement and, if necessary, establish contact with the Principal's data protection officer, are the respective signatories of the respective individual and/or framework agreements. They are individually authorised to issue instructions. The Principal shall notify the Contractor without delay of any change in the person(s) authorised to issue instructions (at least in text form).

4.9.4. The Contractor shall inform the Principal without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Principal.

4.10. Deletion of data and return of data carriers

4.10.1. The Contractor shall not use the data for any other purposes and shall in particular not be entitled to pass them on to third parties. Copies and duplicates of the data shall not be made without the Principal's knowledge. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

4.10.2. After completion of the contractual work or earlier upon request by the Principal - but at the latest upon termination of the service agreement - the Contractor shall hand over to the Principal or, after prior consent, destroy in accordance with data protection law all documents, processing and utilisation results produced and data files which have come into its possession and which are connected with the contractual relationship. The same applies to test and reject material. The protocol of the deletion/destruction shall be submitted to the Principal without being requested to do so.

4.10.3. Documentation which serves as proof of the orderly and proper data processing shall be kept by the Contractor beyond the end of the contract in accordance with the respective retention periods. It may hand them over to the Principal for it discharge at the end of the term of the Agreement.

4.11. Liability

4.11.1. If a data subject successfully claims damages against one of the contractual partners due to a breach of the provisions of the GDPR, Art. 82 GDPR shall apply.

4.11.2. The Contractor shall be liable in accordance with the statutory provisions for all other damage incurred by the Principal as a result of non-compliance with an instruction issued.

4.12. Final provisions

4.12.1. The Parties agree that the defence of the right of retention by the Contractor within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the data to be processed and the associated data carriers.

4.12.2. Amendments and supplements to this agreement must be made in writing or text form. This also applies to the waiver of these formal requirements.

4.12.3. Should individual provisions of this agreement be or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions in each case.

Signature/s

Place, date	Signature/s Contractor