Data processing agreement

pursuant to Article 28 para. 3 of the General Data Protection Regulation ("GDPR") in relation to the Framework or Individual Contract No. or Purchase Order No.

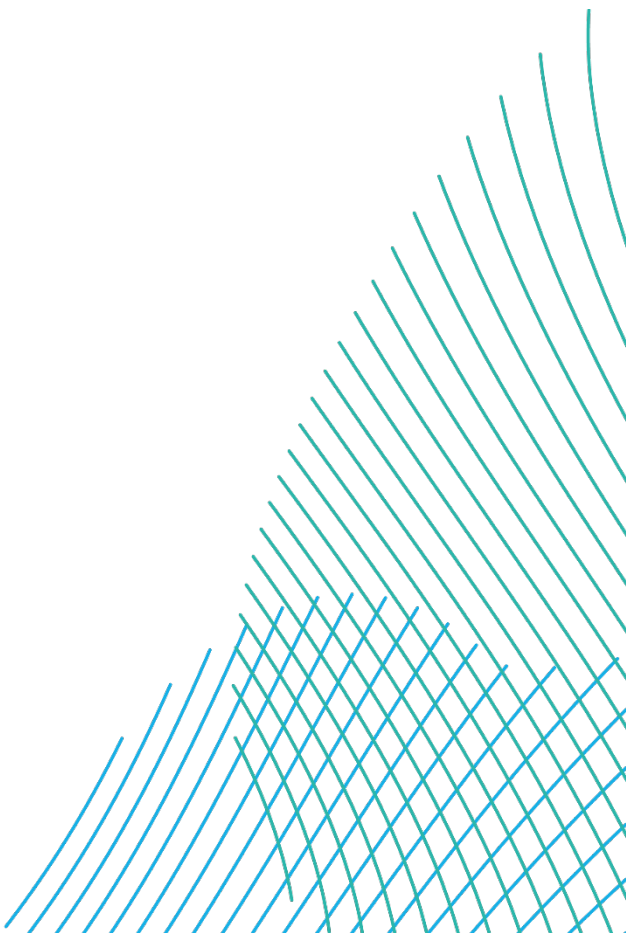
between the

(Controller)

and the

(Processor)

Release: 2025/04



Preamble

The Controller wishes to commission the Processor with the services specified in Chapter 2, section 2.1. Part of the performance of the contract is the processing of personal data on behalf of the Controller. Article 28 GDPR[1] in particular imposes certain requirements on such commissioned processing. 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 affiliates – as defined in Sections 15 et seqq. of the German Stock Corporation Act ("AktG"), the following agreement shall also apply to those companies. Affiliated companies are legally independent companies which, in relation to each other, are majority-owned companies and companies in which a majority interest is held, dependent and controlling companies, group companies, companies with reciprocal interests or parties to an intercompany agreement. Against this background, the following is agreed:

Chapter 1: General information on the company

1.1 Details of the company / Processor

Name

Street, No.

Post code, city

Country

E-mail

Phone

Website

1.2 Details of the Processor's Data Protection Officer

Name

Company[2]

E-mail

Phone

[1] Depending on where the Controller is based and/or whether the processing of personal data is carried out on behalf of the Controller in the course of business activities in these regions, this refers to the EU GDPR and/or the UK GDPR.

[2] If different from the company named under 1.1 (e.g. in the case of an external data protection officer).

1.3 Details of the Processor's Parent Company[3]

Name

Country

☐ If the parent company is established in a third country, it is excluded technically and/or organisationally for personal data to be transferred to the parent company of the processor.

Chapter 2: Information on the processing of personal data

2.1 Scope of services

Please specify the scope of the services provided as commissioned data processing pursuant to Art. 28 GDPR. Define precisely the corresponding purpose and the type of processing of personal data.

2.2 Place of performance

Important: Taking into account any Sub-processors used, cf. Chapter 3.5 and Annex II.

☐ 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 Controller in writing or documented electronic format and may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled.

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

2.3 Type of data

Note: The personal data processed on behalf of RWE must be indicated here. This explicitly does not include personal data that you process in the course of communication with RWE employees or data of the RWE company when initiating the contract as well as data you process internally for invoicing or other internal organisational tasks.

[3] If different from 1.1., please enter the contact details of the parent company, if the Processor is a company within a group of companies and the parent company is established outside the EEA.

2.3.1. Categories of data to which the technical and organisational measures "standard" apply

Data category		Data objects of the data category
☐	Age data	Age, date of birth, place of birth
☐	Contact details (business)	Street, building number, postcode, place of residence, flat number, phone number, email address etc.
☐	Contact details (private)	Street, building number, postcode, place of residence, apartment number, phone numbers, email address, social media accounts, fax, etc.
☐	Electronic identification data	IP addresses, cookies, connection times and data, electronic signature, etc.
☐	Employee data	Personnel number, employee ID number
☐	Financial identification data & Assets	Bank identification and bank account number, credit and debit card numbers, pin codes, capital, real estate etc.
☐	Geolocation data	geographical location data or GPS data, i.e. information about whereabouts, distances travelled and geographical information collected and processed by sensors, actuators, protocols and/or functionalities of devices
☐	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.
☐	Name data	First and last name, title, maiden name, other names
☐	Pensions	Retirement date, type of scheme, leaving date, details of payments received and made, options, beneficiaries, etc.

Data category		Data objects of the data category
☐	Professional activities	Employer, job title, description of the position, current responsibilities and projects, place of work, working modalities and conditions, etc.
☐	Public identification data	National (tax) identification number, identity card number, passport registration number, social security card number, motor vehicle registration number, 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 logs, system logs, communication links, etc.
☐	User data in a system or application	Login name, passwords, tokens or other credentials, surname and e-mail address, optionally first name, business contact details (telephone, mobile, fax), departmental affiliation, position in the company, duration of employment, seniority
☐	Other	

2.3.2. Categories of data to which the technical and organisational measures "Extended" apply

Data category		Data objects of the data category
☐	Biometric identification data	Fingerprints, voice recognition, iris scanning, facial recognition, finger or hand vein authentication, signature dynamics, etc.
☐	Data on criminal convictions and offences	Certificate of good conduct, data on misconduct and criminal offences, penalty notices, etc.

Data category		Data objects of the data category
☐	Ethnic data	Information on origin, ancestry, compatriots' associations, etc.
☐	Genetic data	Data in the context of a detection, examination of heredity, DNA, etc.
☐	Health data	Medical records or reports on physical or mental health, diagnosis, treatment, examination result, disability or infirmity, diet, stress level; other special health requirements for treatment, travel or accommodation, etc.
☐	Political opinions, philosophical or religious beliefs	Information on philosophical, militant or religious beliefs, memberships in such associations, party membership, positions and functions, membership fees and contributions made, etc.
☐	Sexuality	Information on sexual behaviour, gender, gender transition, etc.
☐	Trade union membership	Information on trade union membership, such as the name of the trade union, date of joining, trade union positions held, duration, trade union preferences and politics, etc.
☐	Other	

2.3.3. Activation of the technical and organisational measures "Extended

☐ Irrespective of the selection of data categories made above, the Processor warrants to comply with all technical and organisational measures listed in Annex I Sections 1 and 2.

2.3.4. The following technical and organisational measures cannot, or can only partially, be fulfilled

Please indicate here with the corresponding number from Annex I (e.g. "1.5.3") which technical and organisational measures cannot, or can only partially, be fulfilled. Please explain why.

2.4 Categories of data subjects

☐ Employees[4]

☐ Relatives of employees

☐ Applicants

☐ Customers

☐ Employees of business partners of the RWE Group[5]

☐ External third parties[6]

☐ Other:

Chapter 3: Agreement on the processing of personal data on behalf of Art. 28 para. 3 GDPR

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

The underlying agreement on commissioned data processing is concluded between the commissioning company(ies) of the aforementioned framework or individual agreement and the Processor named in 1.1 Insofar as further affiliated companies of RWE AG, as defined in Sections 15 et seqq. AktG, join the individual or framework agreement, this Data Processing Agreement shall apply to them equally.

3.1 Subject matter and duration of the contract

3.1.1. Subject matter

The subject matter of this agreement results from the respective individual and/or framework agreements concluded.

3.1.2. Duration of the contract/termination

The duration of this contract (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 Processor fails to comply with its obligations under this agreement or violates other applicable data protection provisions

[4] Definition: Employees of the RWE Group, including temporary agency workers in relation to the hirer; employees employed for their vocational training; rehabilitees; volunteers performing a service under the Youth Volunteer Service Act or the Federal Volunteer Service Act.

[5] This category includes employees of existing business partners as well as employees of companies that are in the process of doing business with the client.

[6] 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).

intentionally or through gross negligence. The same shall apply if the Processor is unable or unwilling to carry out a reasonable instruction of the Controller or if the Processor opposes the control rights of the Controller in a manner contrary to the agreement. In particular, non-compliance with the obligations set out in this Agreement and derived from Art. 28 GDPR constitutes a serious breach.

3.2 Technical and organisational measures

3.2.1. The Processor shall organise its internal company processes in such a way that compliance with the special requirements for the protection of personal data is ensured. It shall take the technical and organisational measures to adequately protect the Controller's personal data from misuse and loss in accordance with the requirements of the applicable data protection law. An overview of the technical and organisational measures is attached to this Agreement as Annex I (Technical & Organisational Measures). Insofar as the Processor additionally processes categories of data pursuant to Chapter 2 Section 2.3.2 of this Agreement, all technical and organisational measures listed in Annex I shall be complied with. Otherwise, the technical and organisational measures listed in Annex I Section 1 shall apply as a minimum standard. The Processor shall regularly monitor compliance with these measures.

3.2.2. Processing of data outside the premises of the Processor (e.g. telework, home office, mobile work) is permitted. The Processor shall ensure compliance with the technical and organisational measures for the processing situation.

3.2.3. The Processor shall establish security in accordance with Art. 28 para. 3 lit. c, Art. 32 GDPR, in particular in connection with Art. 5 paras. 1 and 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 costs of implementation, and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons within the meaning of Article 32 para. 1 GDPR must be taken into account.

3.2.4. The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is obliged to ensure a procedure for the regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of the processing. The Processor 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.

3.3 Rectification, restriction of processing and erasure of data as well as assistance to the processor

3.3.1. The Processor may not correct, delete or restrict the processing of the data processed under this Agreement on its own authority but only in accordance with documented instructions from the Controller, with the exception of the provisions under 3.9 of this Agreement. The Processor shall support the Controller as far as possible with appropriate technical and organisational measures in the fulfilment of the Controller's obligations under Articles 12-22 as well as Articles 32 and 36 of the GDPR. If a data subject contacts the Processor directly in this regard, the Processor shall immediately refer the data subject to the Controller and await the Controller's instructions.

3.3.2. Insofar as included in the scope of services, the authorisation and deletion concept, the right to be forgotten, rectification, data portability and access to information shall be ensured directly by the Processor in accordance with the Controller's documented instructions. The provisions in 3.9 remain unaffected.

3.4 Quality assurance and other obligations of the Processor

In addition to compliance with the provisions of this Agreement, the Processor has statutory obligations pursuant to Articles 28 to 33 GDPR; in this respect, the Processor shall in particular ensure compliance with the following requirements:

3.4.1. The Processor shall inform the Controller of the responsible data protection officer or - if no data protection officer is required - a contact person for data protection (see 1.2). The Controller shall be notified in writing without delay if the data protection officer/contact person changes.

3.4.2. The processor shall also proactively inform the controller of the company name, address, contact person and their name, function, contact details of all sub-processors.

3.4.3. The Processor ensures confidentiality pursuant to Art. 28 para. 3 sent. 2 lit. b, Artt. 29 and 32 para. 4 GDPR and/or the statutory secrecy of telecommunications, if applicable, and preserves the confidentiality of electronic communication data. In carrying out the work, the Processor shall only use employees who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have been familiarised in advance with the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data may only process such data in accordance with the Controller's instructions, including the powers granted in this Agreement, unless they are legally obliged to process the data. The resulting confidentiality obligation shall apply beyond the end of the agreement for an indefinite period of time, irrespective of the

regulation on other confidentiality obligations. The same applies to data, that is subject to telecommunications secrecy.

3.4.4. The Processor ensures the implementation of and compliance with all technical and organisational measures required for this contract pursuant to Art. 28 para. 3 S. 2 lit. c, Art. 32 GDPR.

3.4.5. At the request of the supervisory authority, the contracting authority and the Processor shall cooperate in the performance of their duties.

3.4.6. The Processor informs the Controller without delay about control activities and measures of the supervisory authority, insofar as they relate to this contract. This also applies if a competent authority investigates the Processor in the context of administrative offences or criminal proceedings in relation to the commissioned processing of personal data carried out on behalf of the Controller.

3.4.7. To the extent that the Controller is subject 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 commissioned processing at the Processor, the Processor shall support the Controller to the best of its ability.

3.4.8. The Processor shall regularly monitor the internal processes and 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 ensured.

3.4.9. The Processor ensures that the technical and organisational measures taken are verifiable vis-à-vis the Controller within the scope of its control rights pursuant to 3.6 of this Data Processing Agreement.

3.5 Sub-processors

3.5.1. The Controller agrees to the commissioning of the Processor's Sub-processors listed in Annex II, provided that the Processor imposes on these Sub-processors essentially the same contractual obligations with regard to the processing of personal data as those to which the Processor is also bound in the context of this processing. The requirements of Article 28 paras. 2 - 4 GDPR must be complied with in relation to the Sub-processors. In the case of Sub-processors based in a third country, this authorisation shall apply provided that the principles of data transfer pursuant to Art. 44 et seqq. GDPR as well as the requirements of the relevant case-law of the CJEU (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 Sub-processors.

3.5.2. The Processor shall inform the Controller of any future intended changes regarding the addition or replacement of other Sub-processors, thus giving the Controller the

opportunity to object to such changes. The change of existing Sub-processors is permissible against this background, insofar as:

3.5.2.1. the Processor notifies the Controller of such outsourcing to Sub-processors at least 30 working days in advance in writing or in text form; and

3.5.2.2. the Controller does not object to the planned outsourcing in writing or in text form to the Processor by the time the data is handed over and

3.5.2.3. the requirements according to 3.5.1 are met.

3.5.3. The disclosure of personal data of the Controller to the Sub-processor and its initial activity shall only be permitted once all requirements for sub-processing have been met.

3.5.4. Further outsourcing by the Sub-processor (onward transfer) requires the express authorisation by the Controller (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 that further Sub-processor. The Processor must provide the Controller with appropriate proof of this.

3.5.5. At the request of the Controller, the Processor shall provide a copy of the sub-processing agreements concluded by the Processor or by Sub-processors in relation to the processing of personal data under this Agreement, including the information required in Annex II. Section 3.4.2 shall remain unaffected.

3.6 Control rights of the Controller

3.6.1. The Controller has the right to carry out inspections in consultation with the Processor or to have them carried out by another auditor mandated by the Controller to be named in individual cases. The Controller shall have the right to satisfy itself of the Processor's compliance with this Agreement on the Processor’s business premises by means of spot checks, which the Processor must generally be notified of in good time.

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

3.6.3. 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 mechanism pursuant to Art. 42 GDPR, current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors, supervisory authorities) or appropriate certification as the result of an IT security or data protection audit.

3.7 Notification of breaches by the Processor

The Processor shall assist the Controller in complying with the obligations pursuant to Articles 32 to 36 of the GDPR in relation to the security of personal data, data breach notification requirements, data protection impact assessments and prior consultations. These include, among others:

3.7.1. 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 possible infringement of rights due to a breach of security and enable relevant incidents to be detected without delay;

3.7.2. the obligation to report any breaches (including cases of loss or unlawful transmission or knowledge) of the Controller's personal data without undue delay and in any event within 48 hours, regardless of the cause, and to provide the Controller, in this context, with all relevant information in its possession or control;

3.7.3. the obligation to support the Controller in the context of his duty to inform the data subject and to provide the Controller with all relevant information in this context without delay;

3.7.4. supporting the Controller in its data protection impact assessment.

3.7.5. assisting the Controller in prior consultations with the supervisory authority.

3.8 Authority of the Controller to issue instructions

3.8.1. The Processor may only collect, use or otherwise process data within the framework of the individual or framework agreement and in accordance with the Controller's instructions. The Controller's instructions shall initially be determined by this Agreement and may thereafter be amended, supplemented or replaced by individual instructions by the Controller in accordance with 3.8.2. The Controller shall be entitled to issue corresponding instructions at any time. This also includes instructions with regard to the rectification, deletion and blocking of data.

3.8.2. The Controller shall always issue instructions in writing, at least in text form. If an instruction from the Controller is only given verbally, the Processor shall request confirmation from the Controller at least in text form. All instructions issued shall be documented by both the Controller and the Processor and shall be kept for the duration of their validity and subsequently for three further full calendar years. The Processor shall also inform the Controller if the Processor is unable to comply with an instruction.

3.8.3. Persons authorised to give instructions on behalf of the Controller, who also act as contact persons for data protection questions arising within the framework of the Agreement and, if necessary, establish contact with the Controller's data protection

officer, are the respective signatories of the respective individual and/or framework agreements. They are authorised to issue instructions individually.

3.8.4. The Processor shall inform the Controller without delay if it is of the opinion that an instruction violates data protection laws. The Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.

3.9 Use and deletion of data and return of data carriers

3.9.1 The Processor shall not use the personal 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 Controller'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.

3.9.2 After completion of the contractual work or earlier upon request of the Controller - but no later than when the service agreement ends - the Processor shall, at the choice of the Controller delete all documents that have come into its possession, processing and usage results created, test and reject material, as well as personal data related to the contract, and certify to the Controller that this has been done, or the Processor shall return all personal data to the Controller and delete existing copies, provided that there are no legal obligations of the Processor to store the personal data.

3.9.3 The Processor warrants continued compliance with these clauses until the personal data is deleted or returned. The log of the deletion/destruction must be submitted to the Controller without solicitation.

3.9.4 The Processor shall store documentation which serves as proof of proper and contractually compliant data processing in accordance with the respective retention periods beyond the end of the agreement. The Processor may hand them over the documentation to the Controller at the end of the agreement for its own discharge.

3.10 Liability

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

3.10.2. The Processor shall be liable in accordance with the statutory provisions for all other damage incurred by the Controller as a result of non-compliance with a given instruction.

3.11 Precedence

3.11.1. In the event of conflicting clauses between the main contract and this data processing agreement, the data processing agreement shall take precedence in this respect.

3.11.2. The business relationship between the Controller and the Processor shall be governed exclusively by this Data Processing Agreement. Deviating data processing agreements of the processor will not be recognised unless the controller expressly agrees to their validity.

3.12 Final provisions

3.12.1. The Processor shall not withhold any personal data and acknowledges that it is required to provide all personal data and the associated data carriers in a timely manner, regardless of any claim for set-off or other legal right.

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

3.12.3. If any provision of this Agreement is or becomes invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected thereby.

Signatures

SIGNED FOR AND ON BEHALF of the Parties, by their duly authorised representatives:

For the Controller:	**For the Processor:**
Place, date	Place, date
Signature	Signature
Name (Title)	Name (Title)
Place, date	Place, date
Signature	Signature
Name (Title)	Name (Title)

I. Annex 1 : Technical and organisational measures

1. Technical and organisational measures "Standard" (RWE DPA)

1.1 Physical access control

Physical access to the building and rooms is adequately regulated and documented.

1.2 Data access control

1.2.1 When using multi-client systems, sufficient client separation is ensured. Data of the different clients cannot be viewed or changed among each other.

1.2.2 All persons entrusted with the processing of personal data shall be informed about existing regulations, instructions and procedures on data protection and shall be obliged to comply with them. All persons involved in the processing must be trained in the requirements of the applicable data protection laws and information security before taking up the activity subject to this DPA, and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. There are explicit regulations for the treatment of employees who leave the company.

1.2.3 It must be determined which access rights are issued to which persons within the scope of their function and which are withdrawn. The issuance/withdrawal of smart cards, tokens or certificates must be documented. Access to files by users is limited by restrictive file system rights. Each user must only be able to access the files s/he needs to perform the tasks.

1.2.4 Access to all IT systems and services shall be secured by appropriate identification and authentication of the accessing users, services or IT systems. An identification and authentication mechanism appropriate to the need for protection shall be used. Strong passwords shall be used. Authentication data shall be protected against spying, alteration and destruction at all times during processing by the IT system or IT applications. Appropriate authentication procedures have been chosen.

1.2.5 Regulations on granting, modifying and withdrawing authorisations are in place. User IDs and authorisations may only be issued according to actual need. In the event of personnel changes, user IDs and authorisations that are no longer required shall be removed.

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

1.2.7 In the case of increased need for protection, the data and information shall be encrypted according to the standard that corresponds to the "state of the art". In the case

of very high requirements, e.g. for confidentiality, full-volume or full-disk encryption, and appropriate transport encryption shall be used.

1.3 Input control

All security-relevant events of IT systems and applications must be logged. If relevant IT systems and applications have a logging function, this shall be used. If operational and security-relevant events cannot be logged on an IT system, other IT systems must be used for logging (e.g. of events at network level).

1.4 Availability control

1.4.1 There must be a minimum backup concept for data backup. This must define the minimum requirements for data backup and specify who is responsible for it. There must be a brief description of which IT systems and which data on those systems are backed up, by which data backup, and how the data backups can be created and restored. The data backups must be protected in an appropriate manner from access by third parties.

1.4.2 When archiving, it must be determined which employees are responsible and what scope of functions and services is sought. The results must be recorded in an archiving concept. The archiving concept must be adapted to current circumstances regularly. Access to electronic archives must be logged and access to them strictly limited.

1.4.3 There must be rules on how to handle and document security-relevant events, how to select necessary measures to remedy the problem, how to eliminate causes and how to restore a safe state.

1.5 System access control

1.5.1 Hardware and software products come only from known and reputable sources. Reliable technical support is ensured. The supply chain is traceable.

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

1.5.3 All employees must be made aware that neither sensitive information nor IT systems may be freely accessible at unsupervised workplaces.

1.5.4 A malware protection solution is installed on the systems on which RWE information is processed, including on the connected systems (e.g. servers, gateways, clients as well as computer devices, mobile devices, etc.). Malware protection software is distributed automatically and within defined time periods. Regular checks take place to determine that malware and anti-virus software has not been deactivated or restricted in function, the configuration is correct and updates and patterns are applied correctly within defined time periods.

1.5.5 Cloud functions of such products may only be used if no serious, verifiable data protection or confidentiality aspects speak against it.

1.5.6 All communication between the networks involved must be routed through the firewall. It must be ensured that no unauthorised connections to the protected network can be established from outside. Likewise, no unauthorised connections may be established from the protected network. Rules have been defined that specify which communication connections and data streams are permitted.

1.5.7 Different networks must be adequately physically separated (at least e.g. into an internal network, a demilitarised zone (DMZ) and e.g. the internet). The transitions between different networks must be secured by firewalls. Untrusted networks (e.g. Internet) and trusted networks must be separated by a corresponding two-tier firewall structure. A multi-level IT architecture exists for applications that are accessible via the Internet. Network segments are separated from each other according to their protection needs in order to prevent data traffic between segments with different needs for protection.

1.5.8 The connection between the app and the backend systems must be secured by cryptographic measures. If an app accesses backend systems via a user account, a dedicated service account must be used for this purpose.

1.5.9 It is ensured that technical vulnerabilities are remedied. If IT components, software or configuration data are changed, patches are only obtained from authorised sources and security aspects are taken into account. Overall, it must be ensured that the targeted security level is maintained during and after the changes.

1.5.10 The possible accesses and communication interfaces for establishing connections for remote maintenance must be limited to what is necessary. All remote maintenance connections must be disconnected again after remote access. Remote maintenance software should only be installed on systems where it is needed.

1.5.11 A secure configuration must be defined for all VPN components. Authentication and encryption methods that are considered secure and have a sufficient key length must be used.

1.5.12 Before an IT system, application or app is introduced, it must be ensured that it only receives the minimum authorisations necessary for its function. Authorisations that are not absolutely necessary must be questioned and, if necessary, prevented.

1.5.13 The deletion and destruction of information is carried out according to the specifications of the commissioned data processing.

1.5.14 There are clear instructions for handling data carriers that are no longer needed. This also includes the handling of written or printed paper. It must also be regulated and documented how IT systems and data carriers are decommissioned and disposed of in a data protection-compliant manner.

1.5.15 Information on mobile data carriers and devices is sufficiently protected against unauthorised reading.

1.5.16 If data is forwarded to a database system, secure protection against SQL injections must be set up.

1.5.17 Systems, applications and devices must be adequately hardened before they are deployed. This includes at least evaluating the necessary ports, communication protocols and functions. When hardening systems, applications and devices, the requirement for "data protection through data protection-friendly default settings" must be taken into account. Only necessary personal data may be processed and the required functionalities enabled. All services and applications that are not required must be deactivated or uninstalled, especially network services. All functions in the firmware that are not required must be deactivated. Unnecessary user IDs must be deleted or at least deactivated in such a way that no logins to the system are possible under these IDs.

1.5.18 Existing default identifiers must be changed or deactivated as far as possible. Preset passwords of default identifiers must be changed.

1.5.19 Change control processes were defined, documented, specified and enforced to govern the entire life cycle of information systems.

1.5.20 The principles of secure coding apply to software development.

1.6 Transfer control

1.6.1 The transfer of data to third parties (e.g. in the case of databases or data sets with restricted access), is only implemented with appropriate data minimisation measures.

1.6.2 The communication links must be adequately encrypted. It must be ensured that the confidentiality, integrity and authenticity of the transmitted data is guaranteed. The authenticity of the communication partners must be guaranteed.

1.6.3 When passing on data, the company makes use of the possibilities of anonymisation and pseudonymisation.

1.7 Order control

1.7.1 Personal data shall be stored exclusively in an infrastructure of the RWE Group (usually on-premise) or on the Supplier's own systems and, in the case of an infrastructure provided by the Sub-processor (usually software-as-a-service), only with corresponding data protection agreements.

1.7.2 Prior to the introduction of new or changes to existing IT environments in which personal data of RWE are processed within the scope of commissioned processing, associated relevant information security risks are identified, assessed, dealt with, monitored and kept within acceptable limits.

1.7.3 There must be regulations for dealing with external service providers (e.g. in the case of contracts for work, craftsmen, maintenance of systems) as well as corresponding declarations of confidentiality, personal escort in security zones or the logging of external service providers' visit and actions.

1.7.4 The processor must ensure that web applications and apps integrate and deliver only the intended data and content to the user. If web applications and apps offer an upload function for files, this function must be restricted as much as possible by the responsible company. In this case, access and execution rights must also be set restrictively.

1.7.5 For the outsourcing of data processing, only data centres are used for which qualified certificates appropriate to the risk of the processing are available.

1.7.6 A data protection management system (DPMS) has been established that meets the requirements of the GDPR/the applicable data protection law.

1.7.7 The processor shall ensure that all personnel involved in the processing of personal data are aware of and adhere to the policies established under the DPMS.

1.8 Segregation

1.8.1 Development, test and production systems are operated in (at least logically) clearly segregated network segments. Only test data is used for testing and development purposes. Test data based on real data is anonymised or pseudonymised.

1.8.2 Tasks and responsibilities in the data protection process are regulated and accessible.

1.8.3 Tasks and the roles and functions required for them are structured in such a way that incompatible tasks such as operational and control functions are distributed among different persons. Segregation of functions must be defined and documented for incompatible functions. Representatives must also be subject to the segregation of functions.

2. Technical and organisational measures "Extended" (RWE DPA)

2.1 Physical access control

Code or ID cards issued to persons outside the company have a strictly limited validity, which is determined on the basis of the purpose of the stay. The issuance or withdrawal of visitor and company badges is done in a tamper-proof manner. Visitor passes are withdrawn daily. Personal data of company visitors are recorded in a visitor book / visitor list. A concrete definition and documentation of persons authorised and qualified to access the server rooms was established and is maintained.

2.2 Data access control

2.2.1 Access rights shall be limited to approved system functionality and appropriate segregation of duties shall exist. User IDs and passwords shall not be shared. Administrative access to systems that store or process RWE information is limited to a minimum number of administrators and protected by a multi-factor authentication procedure (or, if multi-factor authentication is not technically possible, by equivalent security measures such as temporarily generated passwords).

2.2.2 Administrative access is always logged in order to be able to detect and investigate unauthorised access to and/or unauthorised manipulation of RWE information.

2.3 Input control

The integrity of personal data has to be ensured through digital signatures.

2.4 Availability control

2.4.1 The Processor ensures that the hardware and software products (assets) are recorded in inventories, protected against unauthorised changes, kept up to date, backed up regularly and contain the required information about the assets and, if applicable, compliance requirements relating to the assets. The assets shall be assigned to an officer who is responsible for the operation of the assets.

2.4.2 A certification, such as IEC/ISO 27001 or equivalent, is available and will be provided by the Provider upon request. The Provider warrants that the processing operations described in the data processing agreement are included in the statement of applicability of the certifications.

2.5 System access control

2.5.1 Authentication data must be protected against spying, alteration and destruction at all times during processing by the IT system or IT applications. Appropriate authentication procedures must be chosen. The component must compel users to use strong passwords according to a password policy. Limits for failed login attempts must be defined. All authentication procedures offered must have the same level of security.

2.5.2 The principles of "least privilege", "need-to-know" and "segregation of duties" must be observed. Role-based authorisation concepts must be applied.

2.5.3 A password policy must be established. Changes regarding the password policy must be implemented uniformly for all devices, IT systems and applications, if possible, simultaneously. The password policy must require secure and complex passwords. Measures must be taken to detect whether passwords have been compromised. Standard passwords must be replaced with sufficiently strong passwords and predefined identifiers must be changed. After a password change, the last five passwords, at the least, must no longer be used. Passwords must be stored as securely as possible. When authenticating in networked systems, passwords must not be transmitted unencrypted over insecure networks.

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

2.5.5 The Processor shall ensure that all systems, networks and end devices that process personal data are secured by measures that prevent data leaks.

2.5.6 There is a formal approval process that systems and applications containing personal data must go through before they are granted access to the network.

II. Annex 2: Sub-processors

Sub-processor (name of the company)[7]	Address incl. country of the sub-processor (company)	Name, position, contact details of contact person	Description of the partial services / data processing[8]	Location of data processing (e.g. server location, location of access, etc.)	Description of safeguards concerning transfers to third countries (Art. 44 et seqq. GDPR)[9]

[7] Only those sub-processors that are directly entrusted with the processing of personal data must be listed in Annex II of the DPA. Sub-processors that only provide technical support or infrastructure without direct access to personal data are excluded from this list.

[8] When describing the subject matter and type, please also pay attention to the clear delimitation of responsibilities if several sub-processors are used.

[9] If personal data is transferred to a third country, please enter here the third country guarantees that the Processor has agreed with the respective Sub-processor, as well as the additional security measures to ensure an adequate level of data protection. If required, please also indicate that a Data Transfer Impact Assessment has been carried out. References to a separately retrievable or provided document are also possible.
