Annex 4: Data Processing Agreement

(Version 1.0, 17.10.2024)

between

METEOCONTROL as Processor as defined by the GDPR

and

CUSTOMER as Controller as defined by the GDPR

1. General information

1.1. The PARTIES have established an agreement on the provision of cloud services ("CONTRACT"). According to the CONTRACT, METEOCONTROL provides the CUSTOMER with cloud-based SERVICES for the processing of data, including personal data.

1.2. This data processing agreement (hereafter DPA) as defined in Art. 28 EU General Data Protection Regulation (GDPR) regulates the rights and obligations of the PARTIES, insofar as METEOCONTROL processes personal data for the CUSTOMER.

1.3. Where the DPA uses the terms "data processing" or "processing" (of data), this is based on the definition of "processing" as per Art. 4 Section 2 GDPR.

2. Subject matter of the DPA

2.1. The CUSTOMER's CONTRACT to METEOCONTROL includes the following work and/or services:

2.2. VCOM / mc Assetpilot

2.2.1. In accordance with the current CONTRACT between CUSTOMER and METEOCONTROL, the scope of the CONTRACT is the fee-based provision of technical solutions which make it possible to manage measurement data of energy production plants and batteries with the aid of internet-supported monitoring (VCOM) and to monitor and compare energy production plants and batteries as part of calculations of their (financial) performance (mc Assetpilot). This includes the contractual use of the software, technical support, training measures and consulting services.

2.2.2. This encompasses all changes and additional services that will be applied in the CONTRACT in the future.

2.2.3. METEOCONTROL shall perform the following processing services for the CUSTOMER:

2.2.3.1. Within the PLATFORM provided, METEOCONTROL receives access via a user. The CUSTOMER has the option of setting up their own users by capturing personal data to enter new users. This is necessary in order to be able to carry out the necessary support and service work. In this respect, METEOCONTROL has the possibility to view or change data within the scope of the CUSTOMER's setup.

2.2.3.2. Hosting: METEOCONTROL saves the CUSTOMER's personal data on their systems to store them for the CUSTOMER and make them available.

2.2.3.3. Support services: Whenever support is required, METEOCONTROL may access the CUSTOMER's data to conduct fault analysis and repair work.

2.3. meteocontrol academy

2.3.1. METEOCONTROL provides their CUSTOMERS with a browser-based learning platform, on which the CUSTOMER can register. The CUSTOMER and their employees are granted access to the learning videos and other training content METEOCONTROL provides there.

2.3.2. METEOCONTROL conducts the following processing activities for the CUSTOMER:

2.3.2.1. Hosting: METEOCONTROL saves the CUSTOMER's personal data on their systems to store them for the CUSTOMER and make them available, and to give the CUSTOMER access to the learning platform.

2.3.2.2. Support services: Whenever support is required, METEOCONTROL may access the CUSTOMER's data to conduct fault analysis and repair work.

2.4. The following data types are regularly processed:

2.4.1. This applies to the following categories including the specific data:

2.4.1.1. Master data (first name, surname, address information, contact data (e-mail address, phone number)), authorisations, access data. System data may also be personal in certain circumstances.

2.4.1.2. User-specific change reports.

2.4.1.3. System data if the system is in a private household.

2.4.2. Group of persons affected by data processing:

2.4.2.1. Business partners/customers of the CUSTOMER

2.4.2.2. Employees of the CUSTOMER

3. Rights and obligations of the CUSTOMER

3.1. The CUSTOMER is the Controller as defined in Art. 4 Section 7 GDPR and as such is responsible for the contract processing of data by METEOCONTROL. The assessment of whether the data processing is permissible is the sole responsibility of the CUSTOMER. According to Section 4.6 METEOCONTROL has the right to advise the CUSTOMER of any data processing they deem unlawful.

3.2. As the Controller, the CUSTOMER is responsible for safeguarding the rights of data subjects. METEOCONTROL shall inform the CUSTOMER without undue delay if data subjects exercise their data subject rights vis-à-vis METEOCONTROL.

3.3. Prior to the start of data processing and at regular intervals thereafter, the CUSTOMER must ensure that the technical and organisational data security measures applied by METEOCONTROL are observed. The applied technical and organisational measures are listed in **Annex 2 to this DPA**. The CUSTOMER shall document the result in a suitable manner.

3.4. The CUSTOMER has the right to issue additional instructions to METEOCONTROL regarding the type, scope, and procedure of data processing at any time. Instructions may be issued in writing or via e-mail or fax.

3.5. The CUSTOMER must name persons who are authorised to issue instructions. If those authorised persons in the CUSTOMER's organisation change, the CUSTOMER shall inform METEOCONTROL in writing or in text form.

3.6. The CUSTOMER shall inform METEOCONTROL without undue delay if they determine errors or irregularities in connection with the processing of personal data by METEOCONTROL.

3.7. If there is a notification obligation as defined in Art. 33, 34 GDPR, the CUSTOMER shall be responsible for compliance with this obligation.

4. Rights and obligations of METEOCONTROL

4.1. METEOCONTROL processes personal data exclusively in the context of the established agreements and/or in accordance with any additional instructions issued by the CUSTOMER. The purpose, type and scope of data processing strictly follow these DPA and/or the CUSTOMER's instructions. METEOCONTROL is not permitted to process data in any other manner unless the CUSTOMER has agreed to it in writing. METEOCONTROL undertakes to carry out the processing of data only in member states of the European Union (EU) or the European Economic Area (EEA).

4.2. METEOCONTROL has appointed a data protection officer as per Art. 37 GDPR:

Mr. Sven Lenz – Deutsche Datenschutzkanzlei
Phone: +49 831 930653-00
E-Mail: lenz@deutsche-datenschutzkanzlei.de

Proof of qualification must be provided to the CUSTOMER upon request. The CUSTOMER must be informed without undue delay if the data protection officer changes.

If METEOCONTROL has not appointed a data protection officer, they must provide documentary proof to the CUSTOMER that they are not legally required to appoint a data protection officer, and that organisational regulations are in place to ensure personal data are processed in compliance with legal regulations, the provisions of this contract, and any other instructions issued be the CUSTOMER.

4.3. With regard to the agreed contract processing of personal data, METEOCONTROL assures that all measures shall be applied as contractually agreed.

4.4. METEOCONTROL is obliged to structure their company and their operational procedures in such a way that any data they process on behalf of the CUSTOMER are secured to the required extent and protected from unauthorised access by third parties. METEOCONTROL shall inform the customer (at least in text form) of relevant changes in the organisation of contract data processing that are significant to data security.

4.5. METEOCONTROL shall inform the CUSTOMER without undue delay if they consider an instruction issued by the CUSTOMER to be in violation of the GDPR or any other data protection regulations of the EU or its member states. METEOCONTROL has the right to suspend the execution of the respective instruction until it is either confirmed or changed by the CUSTOMER. METEOCONTROL is required to inform the CUSTOMER if they are under an obligation regarding the processing of personal data counter to the CUSTOMER's instructions.

4.6. METEOCONTROL is obliged to inform the CUSTOMER without undue delay of any violation of data protection regulations or the contractual agreements and/or the instructions issued by the CUSTOMER, which occurred as part of the processing of data by METEOCONTROL or other

persons involved in the processing. Furthermore, METEOCONTROL shall inform the CUSTOMER without undue delay if a supervisory authority takes action against METEOCONTROL as described in Art. 58 GDPR, and if this may affect an audit of the processing METEOCONTROL performs on behalf of the CUSTOMER.

4.7. In the event that METEOCONTROL discovers, or facts give rise to the assumption that personal data processed by METEOCONTROL for the CUSTOMER have been unlawfully transmitted or otherwise unlawfully disclosed to third parties (violation of protection of personal data processed under contract), METEOCONTROL must inform the CUSTOMER without undue delay and in full. The information to the CUSTOMER must include the contents listed in Art. 33 (3) GDPR, but at least

- The time, nature, and scope of the incident/s
- Explanation of the nature of unlawful disclosure
- Explanation of possible detrimental consequences of the unlawful disclosure
- What measures were taken by METEOCONTROL to prevent the unlawful transmission or unauthorised awareness by third parties in the future.

METEOCONTROL is aware that the CUSTOMER may be under obligation to report any such incident as per Art. 33 GDPR, which requires a report to the supervisory authority within 72 hours after the incident becomes known. METEOCONTROL shall support the CUSTOMER with such reporting obligations.

4.8. METEOCONTROL is aware that the CUSTOMER may be under obligation to notify the supervisory authority as per Art. 34 GDPR. METEOCONTROL shall support the CUSTOMER with such notifications.

4.9. METEOCONTROL must cooperate in the creation of the record of processing activities by the CUSTOMER. They must provide the CUSTOMER the respective required information in a suitable manner.

4.10. METEOCONTROL must inform the CUSTOMER of the person(s) who are authorised to receive instructions from the CUSTOMER. Persons authorised to receive instructions at METEOCONTROL are:

- Cheng Liu, Managing Director
- Stijn Stevens, CFO, Managing Director

If the persons authorised to receive instructions at METEOCONTROL change, METEOCONTROL shall inform the CUSTOMER in writing or in text form.

4.11. METEOCONTROL is obliged to support the CUSTOMER with fulfilling the obligations named in Articles 32 to 36 GDPR, taking into consideration the nature of the processing and the information available to them.

4.12. METEOCONTROL is obliged to provide the CUSTOMER with all necessary information to demonstrate compliance with the obligations as per Art. 28 GDPR.

5. Monitoring authorisations

5.1. The CUSTOMER has the right to monitor compliance of the legal data protection regulations and/or compliance of the contractual regulations established between the PARTIES and/or METEOCONTROL's compliance with the CUSTOMER's instructions at any time to the necessary extent.

5.2. METEOCONTROL has a disclosure obligation to the CUSTOMER, to the extent this is necessary to conduct the monitoring as defined in Section 5.1.

5.3. In general, the CUSTOMER may conduct monitoring activities as defined in Section 2 at METEOCONTROL's premises after prior notification with an appropriate notice period, unless unannounced monitoring is required because the purpose of the monitoring would otherwise be jeopardised. The CUSTOMER shall ensure that the monitoring is limited to the necessary extent, so that operational processes at METEOCONTROL are not excessively disturbed by the monitoring. METEOCONTROL is obliged to make the monitoring possible and actively contribute to it. They must allow the CUSTOMER to enter their premises as part of the monitoring.

5.4. METEOCONTROL is obliged, in the event of measures by the supervisory authority against the CUSTOMER as defined in Art. 58 GDPR, in particular with regard to disclosure and monitoring obligations, to provide the necessary information to the CUSTOMER and to allow the respective supervisory authority to carry out on-site monitoring. The CUSTOMER must be informed by METEOCONTROL of such planned measures.

6. Subcontracting relationships

6.1. The CUSTOMER consents to the involvement of the subcontractors listed in **Appendix 2 of this ANNEX DPA** for the provision of the services listed in that Appendix.

6.2. METEOCONTROL is authorised to establish further subcontracting relationships with different or further subcontractors as part of their contractual obligations. They shall inform the CUSTOMER of any further subcontractors without undue delay.

6.3. The CUSTOMER consents to METEOCONTROL involving AFFILIATED COMPANIES of METEOCONTROL to provide their contractually agreed services. The provisions of Section 6.1 apply analogously.

6.4. METEOCONTROL must carefully select the subcontractor and check before commissioning that the subcontractor can fulfil the agreements made between the CUSTOMER and METEOCONTROL. In particular, METEOCONTROL must check in advance and regularly during the contract term that the subcontractor has taken the technical and organisational measures for the protection of personal data required under Art. 32 GDPR. METEOCONTROL must document the result of the check and provide it to the CUSTOMER upon request. METEOCONTROL is obliged to obtain confirmation from the subcontractor that they have

designated a data protection officer as defined by Art. 37 GDPR. If the subcontractor does not have a designated data protection officer, METEOCONTROL must inform the CUSTOMER of that fact.

6.5. METEOCONTROL must ensure that the regulations agreed in this DPA, and any additional instructions issued by the CUSTOMER also apply to the subcontractors. METEOCONTROL must monitor compliance with these obligations regularly.

6.6. METEOCONTROL must establish a processing agreement with the subcontractor that satisfies the requirements of Art. 28 GDPR. The CUSTOMER must be provided with a copy of the processing agreement upon request.

6.7. METEOCONTROL is obliged, in particular, to establish contractual provisions to ensure that the monitoring authorisations (Section 5 of ANNEX DPA) of the CUSTOMER and of supervisory authorities also apply to the subcontractor and corresponding monitoring rights of CUSTOMERS and supervisory authorities are agreed. Furthermore, there must be a contractual provision stating that the subcontractor must permit these monitoring measures and possibly on-site monitoring.

6.8. Services which METEOCONTROL obtains from third parties purely as additional services in order to conduct their business activities are not to be considered subcontracting relationships as defined in Section 6.1 to 6.5. This includes for example cleaning services, telecommunications services without relation to services which METEOCONTROL provides to the CUSTOMER, postal and courier services, transport services, and security services. METEOCONTROL is nevertheless obliged to ensure, also for such additional services provided by third parties, that appropriate precautions and technical and organisational measures are applied to ensure the protection of personal data. Maintenance and testing services constitute subcontracting relationships subject to approval insofar as the maintenance and testing relates to IT systems that are also used in connection with the provision of services for the CUSTOMER. The PARTIES agree that the above-mentioned maintenance and testing services constitute “processing” as defined in Art. 28 GDPR.

7. Confidentiality obligation

7.1. When processing data for the CUSTOMER, METEOCONTROL is obliged to maintain confidentiality about data which they receive or of which they become aware in connection with the contract. METEOCONTROL undertakes to observe the same rules for protection of secrets that apply to the CUSTOMER. The CUSTOMER is obliged to inform METEOCONTROL of any special rules of secrecy.

7.2. METEOCONTROL confirms that they are aware of the applicable data protection regulations and familiar with their application. METEOCONTROL ensures that the persons authorised to process personal data have committed to maintaining confidentiality or are subject to adequate legal confidentiality obligations and that these persons are familiar with the data protection

regulations that apply to them. The commitment of these persons must be demonstrated to the CUSTOMER upon request. If METEOCONTROL participates in providing commercial telecommunications services in connection with services for the CUSTOMER, they are obliged to obtain written commitments from the employees involved to adhere to the secrecy of telecommunications as defined in Section 3 TDDDG [German Telecommunications Digital Services Data Protection ACT].

8. Safeguarding the rights of data subjects

8.1. The CUSTOMER is solely responsible for safeguarding the rights of data subjects defined in Chapter III of the GDPR.

8.2. Regarding the type of processing, METEOCONTROL shall support the CUSTOMER as much as possible with suitable technical and organisational measures in their effort to fulfil their obligation to respond to requests for exercising the rights of data subjects named in Chapter III.

8.3. Regulations about possible remuneration of extra effort incurred by METEOCONTROL due to cooperative services in connection with the assertion of data subjects' rights against the CUSTOMER remain unaffected.

9. Secrecy obligations

9.1. Both PARTIES undertake to keep all information they receive in connection with fulfilling this Contract confidential indefinitely, and to only use it to fulfil the Contract. Neither PARTY is authorised to use this information in its entirety or in part for any but the aforementioned purposes or to make this information accessible to third parties.

9.2. The above obligation does not apply to information that one of the PARTIES demonstrably received from third parties without being obliged to maintain confidentiality, or to information that is public knowledge.

10. Remuneration

10.1. The remuneration of METEOCONTROL is agreed in the CONTRACT.

10.2. If no regulation exists on the incurrence of costs as part of the monitoring obligations and the effort exceeds an amount that is reasonable for METEOCONTROL, METEOCONTROL shall charge an hourly rate of € 150 net.

11. Technical and organisational data security measures

11.1. METEOCONTROL is obliged to take all measures required according to Art. 32 GDPR as part of their processing activities. This also applies in cases where METEOCONTROL permits the processing to be done via remote work.

11.2. The state of the art of the technical and organisational measures at the time of establishing the

contract is enclosed as **Appendix 2 to this ANNEX DPA**.

11.3. METEOCONTROL is obliged to monitor and adapt the technical and organisational measures they take regularly and also event-based with regard to their effectiveness and their necessity according to Art. 32 GDPR. METEOCONTROL is obliged to adapt the technical and organisational measures listed in Appendix 2. METEOCONTROL is obliged to inform the CUSTOMER about the adapted and updated version of the technical and organisational measures without delay and to provide these measures to the CUSTOMER.

11.4. METEOCONTROL shall provide the CUSTOMER with suitable documentation of the technical and organisational measures they have taken to guarantee the level of protection according to Art. 32 GDPR and this DPA.

12. Duration of the DPA

12.1. The contractual term of the DPA equals that of the CONTRACT.

12.2. The CUSTOMER may terminate the contract at any time without notice period in the event of a severe violation by METEOCONTROL of the applicable data protection regulations or the obligations under this DPA, if METEOCONTROL, in violation of the contract, cannot or refuses to comply with an instruction by the CUSTOMER, or if METEOCONTROL, in violation of the contract, refuses access to the CUSTOMER or the responsible supervisory authority.

13. Termination

13.1. After terminating the provision of processing services, METEOCONTROL must, at the CUSTOMER's discretion, either delete or return to the CUSTOMER all documents, data and prepared processing or usage results related to the contract relationship and containing personal data of which they have gained possession. In this process, METEOCONTROL ensures that the deletion makes it impossible for the personal information contained in the data to be deleted to be (further) accessed with reasonable effort or otherwise processed in any meaningful way.

13.2. This obligation also applies to any copies. The data media of METEOCONTROL must be deleted afterwards. This also includes any backups made by METEOCONTROL. The deletion must be documented in a suitable manner. Test materials and rejects must be destroyed or physically deleted without delay.

13.3. The CUSTOMER has the right to monitor the complete and contractual return and deletion of data by METEOCONTROL.

14. Right of retention

14.1. The PARTIES agree that the plea of right of retention by METEOCONTROL as defined by Section 273 BGB (German Civil Code) regarding the processed data and corresponding data media is excluded out.

15. Final provisions

15.1. If the CUSTOMER's property at METEOCONTROL is jeopardised due to measures by third parties (such as seizure or confiscation), due to insolvency proceedings or any other events, METEOCONTROL must inform the CUSTOMER without undue delay. METEOCONTROL shall inform creditors without delay of the fact that the data are being processed on contract.

15.2. Ancillary agreements hereto must be made in text form.

15.3. If individual parts of this DPA should prove to be invalid, this does not affect the validity of the remaining provisions of the DPA.

Appendix 1 to ANNEX DPA: Subcontractors

For the processing of data on behalf of the CUSTOMER, METEOCONTROL uses services provided by third parties, who process data on their behalf.

Subcontractor	**Purpose of processing**	**Suitable guarantees if data are processed in a third country**
meteocontrol Italia s.r.l.	Support services	EU, DPA on file
meteocontrol France SAS	Support services	EU, DPA on file
meteocontrol Ibérica SL	Support services	EU, DPA on file
Raising Power GmbH	Support services	EU, DPA on file
mc Beteiligungs GmbH	Support services	EU, DPA on file
meteocontrol Romania SRL.	Support services	EU, DPA on file
meteocontrol North America Inc.	Support services	SCC established
meteocontrol Japan Corporation	Support services	Adequacy decision on file; DPA on file
meteocontrol Chile SpA	Support services	SCC established
meteocontrol AMEA DMCC	Support services	SCC established
meteocontrol Taiwan Inc.	Support services	SCC established
Functional Software, Inc.	Use of the service Sentry.io to monitor data base performance and for error analysis; storage of IP addresses as part of error transmission.	SCC (Processor to Processor) were established
Eurekos Systems ApS	Provision of platform for meteocontrol academy	EU, DPA on file
Infrared Power Techsol Pvt. Ltd.	Provision support services, non-EU area	SCC, DPA established

Appendix 2 to ANNEX DPA: Technical and organisational measures by METEOCONTROL

Section A: Safeguarding the confidentiality of personal data (Art. 32 (1) b GDPR)

1. Physical access control

1.1. Physical access control encompasses measures to prevent unauthorised persons from accessing data processing systems that process or use personal data.

1.2. **Measures**

- The administration is located on a publicly accessible property. Access to the property with the computing centre operating the cloud services is restricted.
- A description/documentation of all access control measures used at the location is on file.
- There are mechanical access control systems installed in the buildings.
- The company servers are operated in a locked and access-controlled room.

2. Access control

2.1. Measures to prevent unauthorised persons from using data processing systems.

2.2. **Measures**

- For all information systems and services there is a formal user registration and deregistration process for issuing and revoking access authorisations.
- The Wi-Fi is secured against unauthorised access.
- It is ensured that only authorised persons have logical access to the network components.
- There is a formal activation process that systems and applications with personal data must be subjected to before they can be given network access.
- It is ensured that only authorised devices of private persons or visitors are given logical access to the organisation’s network.
- There are measures in place to identify and authenticate external maintenance staff.
- During local maintenance work by external companies, it is ensured that no equipment can leave the IT area without being monitored.
- There are differentiated and multi-level access authorisations in place.
- There are firewall, network and password policies in place.
- Effective firewalls and intrusion detection systems are being used.
- Central administrative systems may only be accessed via VPN.
- Networks are logically (VLANs) separated.

3. Electronic access control

3.1. Measures to ensure that persons authorised to use a data processing systems can only access data that falls under their access rights, and that personal data cannot be read, copied, changed or removed during processing, use and after being saved.

3.2. **Measures**

- Users ensure that their data processing equipment is sufficiently protected when not under supervision.
- The principles of clean desks and blank screens are applied (Clean Desk Policy).
- Special security software is used to ensure data security and electronic access control.
- There are instructions on how to handle data media (including handwritten or printed paper) that are no longer needed.
- There are regulations governing the disposal or further use of devices containing storage media.
- There is a regulation governing external administrative access.
- It is ensured that persons authorised to use a data processing system have access to only the data that falls under their access rights. This is guaranteed by means of:
  - Automatic check of access rights by means of a password
  - Menu navigation only according to respective access rights
  - Differentiated access rights to application programmes
  - Differentiated processing options (read/edit/delete)

4. Separation control

4.1. Measures to ensure that data captured for different reasons can be processed separately.

4.2. **Measures**

- Personal data on the systems are logically separated from one another (different data sets in a uniform data base are marked according to purpose (software separability)).
- Testing and productive environments are separate systems.

5. Pseudonymisation

5.1. Data are not pseudonymised.

Section B: Safeguarding the integrity of personal data (Art. 32 (1) b GDPR)

6. Transfer control

6.1. Measures to ensure that personal data cannot be read, copied, changed or deleted without authorisation during electronic transmission or during transport or while being saved to data media, and that it is possible to check and determine where a transfer of personal data through

data transfer systems is intended.

6.2. Measures

- All new employees are provided with data protection information when they are obliged to maintain confidentiality.
- Employees who process/use personal data are trained in data protection-compliant behaviour in the workplace through data protection training. It is ensured that data is only transmitted to the recipients specified by the CUSTOMER or to the correct recipients according to the intended purpose.
- There is a process for employees leaving the company, in particular those who were terminated.
- There is a company-wide system for the classification of data.
- There is a Cryptography Policy governing the encryption of data transfers.

7. Entry control

7.1. Measures to ensure that it is possible to check and determine at a later date whether and by whom personal data were entered, changed or deleted in data processing systems.

7.2. Measures

- Random checks by the data protection officer are carried out (also with regard to compliance with deletion periods).
- The logged data are protected against unauthorised viewing or manipulation.
- An IT security officer has been appointed.

Section C: Safeguarding the availability of personal data (Art. 32 (1) b GDPR)

8. Availability control

8.1. Measures to ensure that personal data are protected against inadvertent destruction or loss and can be restored quickly in the event of a physical or technical incident.

8.2. Measures

- The systems are secured against outages.
- Backups are carried out regularly.
- Antivirus software is in use.
- Sufficiently large UPSs are in use.
- Regular checks are carried out whether the supply with data lines, power and air conditioning is still adequate.
- The supply lines are below ground.
- There are no water-bearing pipes in the server rooms.
- The output voltage(s) is(are) constantly monitored.

- There is lightning and surge protection equipment installed.
- There are no flammable items in the server area.
- An early warning system with automatic fire alarms is installed.
- There are sufficient suitable fire extinguishers and the correct extinguishing material; uniformity is ensured. In some areas, automatic extinguishing systems are used.
- There is an emergency handbook, which is constantly updated.
- There is a written document for data processing restart (composition and tasks of the disaster committee).
- There is an emergency concept for the network.
- The requirements of the backup are documented in a backup concept.
- The backups are protected against theft and destruction.
- Processes for backups have been established and documented in work instructions.
- There are regular checks whether the backup is usable.
- The air temperature is monitored.
- There is an alternative computing centre.
- There are external monitoring systems independent of the total system.
- Consistent hardware redundancy is ensured.

9. Processes for regular checks, assessments and evaluations (Art. 32 (1) d, Art. 25 (1) GDPR

9.1. Organisational security criteria

9.1.1. Organisational security describes all organisational measures (work instructions, processes, etc.) to ensure and improve security.

9.1.2. Measures

- A data protection management system (DSMS) has been introduced.
- An incident response management system has been established.
- Employees and managers are regularly instructed and sensitised.
- Regular IT security audits are conducted.
- IT security audits are carried out annually.

9.2. Incident response management

9.2.1. Incidents are processed using the Incident Management system (description in the main document). A list of inferred measures as well as a list of all incidents relevant to data protection are integrated in the DSMS.

9.3. Data protection-friendly pre-settings (Art. 25 (2) GDPR)

9.3.1. As a rule, only those data are collected and processed that are expedient and required for the business purposes. Processes of automated data collection and processing are designed so only the necessary data can be collected. The data of data subjects are stored in partially

encrypted form. The data protection officer is notified of changes and modifications in the systems as defined in the change process (defined in the main document). Irregular audits are also part of the PDCA auditing cycle of the data protection officer.

9.4. Contract control

9.4.1. Measures to ensure that personal data processed on contract may only be processed according to the CUSTOMER's instructions.

9.4.2. Employees who have administrative access to the systems are all instructed regarding data protection, have been committed to maintaining confidentiality, and have accepted confidentiality and secrecy agreements as part of their employment contract.

9.4.3. If METEOCONTROL uses contract data processors for the processing of data, certain requirements are implemented. This includes ensuring the technical-organisational measures of METEOCONTROL as defined in Art. 28 GDPR and Art 32 (1) GDPR.

9.4.4. Any contract for data processing must always have a legal basis. In the fulfilment of contracts for data processing as defined in Art. 28 (3) GDPR, all required measures and requirements must be observed.