

Annex 4: Data Processing Agreement / Annexe 4 : Accord sur le traitement des données

(Version 1.0.1, 16.06.2025)

between

METEOCONTROL as Processor as defined by the GDPR

and

CUSTOMER as Controller as defined by the GDPR

entre

METEOCONTROL en tant que Sous-traitant conformément à la définition du RGPD et

le CLIENT en tant que Responsable du traitement conformément à la définition du RGPD

1.	<u>GENERAL INFORMATION</u>	1
2.	<u>SUBJECT MATTER OF THE DPA</u>	2
3.	<u>RIGHTS AND OBLIGATIONS OF THE CUSTOMER</u>	3
4.	<u>RIGHTS AND OBLIGATIONS OF METEOCONTROL</u>	3
5.	<u>MONITORING AUTHORISATIONS</u>	5
6.	<u>SUBCONTRACTING RELATIONSHIPS</u>	6
7.	<u>CONFIDENTIALITY OBLIGATION</u>	7
8.	<u>SAFEGUARDING THE RIGHTS OF DATA SUBJECTS</u>	8
9.	<u>SECRECY OBLIGATIONS</u>	8
10.	<u>REMUNERATION</u>	8
11.	<u>TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES</u>	8
12.	<u>DURATION OF THE DPA</u>	9
13.	<u>TERMINATION</u>	9
14.	<u>RIGHT OF RETENTION</u>	9
15.	<u>FINAL PROVISIONS</u>	9
	<u>APPENDIX 1 TO ANNEX DPA: SUBCONTRACTORS</u>	10
	<u>APPENDIX 2 TO ANNEX DPA: TECHNICAL AND ORGANISATIONAL MEASURES BY METEOCONTROL</u>	11

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.

1. Informations générales

- 1.1. Les PARTIES ont conclu un accord sur la fourniture de services basés sur le cloud (« CONTRAT »). Conformément au CONTRAT, METEOCONTROL fournit au CLIENT des SERVICES basés sur le cloud pour le traitement des données, y compris des données à caractère personnel.
- 1.2. Le présent accord sur le traitement des données (ci-après dénommé « DPA » pour Data Processing Agreement), tel que défini à l'art. 28 du Règlement général sur la protection des données (RGPD) de l'UE, régit les droits et obligations des PARTIES, dans la mesure où METEOCONTROL traite des données à caractère personnel pour le CLIENT.
- 1.3. Lorsque le DPA utilise les termes « traitement des données » ou « traitement » (des données), il se fonde sur la définition de « traitement » stipulée à l'article 4, paragraphe 2, du RGPD.

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. Objet du DPA

- 2.1. Le CONTRAT du CLIENT avec METEOCONTROL comprend les travaux et/ou services suivants :**
- 2.2. VCOM / mc Assetpilot**
- 2.2.1.** Conformément au CONTRAT actuel entre le CLIENT et METEOCONTROL, l'objet du CONTRAT est la fourniture payante de solutions techniques permettant de gérer les données de mesure d'installations de production d'énergie et de batteries à l'aide d'une surveillance Internet (VCOM) et de surveiller et comparer les installations de production d'énergie et les batteries dans le cadre du calcul de leur performance (financière) (mc Assetpilot). Cela comprend l'utilisation contractuelle des logiciels, l'assistance technique, les actions de formation et les services de conseil.
- 2.2.2.** Cela englobe toutes les modifications et tous les services supplémentaires qui seront appliqués à l'avenir dans le cadre du CONTRAT.
- 2.2.3.** METEOCONTROL assure les services de traitement suivants pour le compte du CLIENT :
- 2.2.3.1.** Dans la PLATFORME fournie, METEOCONTROL obtient un accès via un utilisateur. Le CLIENT a la possibilité de créer ses propres utilisateurs en saisissant les données personnelles nécessaires à l'enregistrement de nouveaux utilisateurs. Cela est nécessaire pour pouvoir effectuer les travaux d'assistance et fournir les services requis. À cet égard, METEOCONTROL a la possibilité de consulter ou de modifier des données dans le cadre de la configuration du CLIENT.
- 2.2.3.2.** Hébergement : METEOCONTROL enregistre les données personnelles du CLIENT sur ses systèmes afin de les stocker pour le CLIENT et de les mettre à sa disposition.
- 2.2.3.3.** Services d'assistance : en cas de besoin d'assistance, METEOCONTROL peut accéder aux données du CLIENT pour procéder à l'analyse des défauts et aux réparations.
- 2.3. Académie meteocontrol**
- 2.3.1.** METEOCONTROL met à la disposition de ses CLIENTS une plateforme d'apprentissage basée sur un navigateur, sur laquelle le CLIENT peut s'inscrire. Le CLIENT et ses employés ont accès aux vidéos d'apprentissage et autres contenus de formation que METEOCONTROL met à leur disposition.
- 2.3.2.** METEOCONTROL effectue les activités de traitement suivantes pour le CLIENT :
- 2.3.2.1.** Hébergement : METEOCONTROL enregistre les données personnelles du CLIENT sur ses systèmes afin de les stocker pour le CLIENT et de les mettre à sa disposition, et de permettre au CLIENT d'accéder à la plateforme d'apprentissage.
- 2.3.2.2.** Services d'assistance : en cas de besoin d'assistance, METEOCONTROL peut accéder aux données du CLIENT pour procéder à l'analyse des défauts et aux réparations.
- 2.4. Les données des catégories suivantes font régulièrement l'objet d'un traitement :**
- 2.4.1.** Cela s'applique aux catégories suivantes, y compris les données spécifiques :
- 2.4.1.1.** Données de base (prénom, nom, adresse, coordonnées (adresse électronique, numéro de téléphone)), autorisations, données

2.4.2.1. Business partners/customers of the CUSTOMER

2.4.2.2. Employees of the CUSTOMER

d'accès. Les données système peuvent également être à caractère personnel dans certaines circonstances.

2.4.1.2. Rapports de modification propres à l'utilisateur.

2.4.1.3. Données système si le système se trouve dans un ménage privé.

2.4.2. Groupe de personnes concernées par le traitement des données :

2.4.2.1. Partenaires commerciaux/clients du CLIENT

2.4.2.2. Employés du CLIENT

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.

3. Droits et obligations du CLIENT

3.1. Le CLIENT est le Responsable du traitement conformément à la définition de l'article 4, paragraphe 7 du RGPD, et en tant que tel est responsable du traitement contractuel des données par METEOCONTROL. L'évaluation de la licéité du traitement des données relève de la seule responsabilité du CLIENT. Conformément à l'article 4.6, METEOCONTROL a le droit d'informer le CLIENT en cas de traitement de données considéré comme illégal.

3.2. En tant que Responsable du traitement, le CLIENT est responsable de la protection des droits des personnes concernées. METEOCONTROL informe le CLIENT dans les meilleurs délais s'il advient que les personnes concernées exercent leurs droits vis-à-vis de METEOCONTROL.

3.3. Avant le début du traitement des données et à intervalles réguliers par la suite, le CLIENT doit s'assurer que les mesures techniques et organisationnelles de sécurité des données appliquées par METEOCONTROL sont respectées. Les mesures techniques et organisationnelles sont indiquées dans l'Annexe 2 du présent DPA. Le CLIENT doit documenter le résultat de manière appropriée.

3.4. Le CLIENT a le droit de donner à tout moment à METEOCONTROL des instructions supplémentaires concernant le type, l'étendue et la procédure du traitement des données. Les instructions peuvent être données par écrit, par courrier électronique ou par fax.

3.5. Le CLIENT doit désigner les personnes habilitées à donner des instructions. En cas de changement au niveau des personnes autorisées au sein de l'organisation du CLIENT, ce dernier en informe METEOCONTROL par écrit ou sous forme de texte.

3.6. Le CLIENT informe METEOCONTROL dans les meilleurs délais s'il constate des erreurs ou des irrégularités dans le cadre du traitement des données à caractère personnel par METEOCONTROL.

3.7. S'il existe une obligation de notification telle que définie aux articles 33 et 34 du RGPD, le CLIENT est responsable du respect de cette 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

4. Droits et obligations de METEOCONTROL

4.1. METEOCONTROL traite les données à caractère personnel exclusivement dans le cadre des accords établis et/ou conformément aux instructions supplémentaires données par le CLIENT. La finalité, le type et l'étendue du traitement de données sont strictement conformes à ce DPA et/ou aux instructions du CLIENT. METEOCONTROL n'est pas autorisée à traiter des données d'une autre manière, à moins que le CLIENT n'y ait

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 by 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

consenti par écrit. METEOCONTROL s'engage à effectuer le traitement des données uniquement dans les États membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE).

4.2. METEOCONTROL a désigné un délégué à la protection des données conformément à l'art. 37 du RGPD :

M. Sven Lenz - Deutsche Datenschutzkanzlei

Téléphone : +49 831 930653-00

E-mail : lenz@deutsche-datenschutzkanzlei.de

Une preuve de qualification doit être fournie au CLIENT sur demande. Le CLIENT doit être informé du changement de délégué à la protection des données sans délai excessif.

Si METEOCONTROL n'a pas désigné de délégué à la protection des données, METEOCONTROL doit fournir au CLIENT un justificatif prouvant qu'elle n'est pas légalement tenue de désigner un délégué à la protection des données et que des règles organisationnelles ont été instaurées pour garantir que les données à caractère personnel sont traitées conformément aux règles légales, aux dispositions du présent contrat et à toute autre instruction données par le CLIENT.

4.3. En ce qui concerne le traitement contractuel convenu des données à caractère personnel, METEOCONTROL assure que toutes les mesures seront appliquées comme convenu contractuellement.

4.4. METEOCONTROL est tenue de structurer son entreprise et ses procédures opérationnelles de manière à ce que toutes les données qu'elle traite au nom du CLIENT soient sécurisées dans la mesure où cela est nécessaire et protégées contre les accès non autorisés de tiers. METEOCONTROL informe le client (au moins sous forme écrite) des changements pertinents dans l'organisation du traitement des données contractuelles qui sont importants en termes de sécurité des données.

4.5. METEOCONTROL informe le CLIENT dans les plus brefs délais si elle considère qu'une instruction donnée par le CLIENT enfreint le RGPD ou toute autre réglementation relative à la protection des données de l'UE ou de ses États membres. METEOCONTROL a le droit de suspendre l'exécution de l'instruction en question jusqu'à ce qu'elle soit confirmée ou modifiée par le CLIENT. METEOCONTROL est tenue d'informer le CLIENT si elle est soumise à une obligation concernant le traitement des données à caractère personnel allant à l'encontre des instructions du CLIENT.

4.6. METEOCONTROL est tenue d'informer le CLIENT dans les plus brefs délais de toute violation des dispositions relatives à la protection des données ou des accords contractuels et/ou des instructions données par le CLIENT, survenue dans le cadre du traitement des données par METEOCONTROL ou par d'autres personnes impliquées dans le traitement. En outre, METEOCONTROL informera le CLIENT dans les plus brefs délais si une autorité de contrôle prend des mesures à l'encontre de METEOCONTROL conformément à l'article 58 du RGPD, et si cela peut avoir des répercussions sur un audit du traitement effectué par METEOCONTROL pour le compte du CLIENT.

4.7. Si METEOCONTROL découvre, ou si des faits laissent supposer, que des données à caractère personnel traitées par

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
 - Bin Lu, 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

METEOCONTROL pour le compte du CLIENT ont été transmises illégalement ou divulguées d'une autre façon illégalement à des tiers (violation de la protection des données à caractère personnel traitées dans le cadre du contrat), METEOCONTROL doit en informer le CLIENT dans les plus brefs délais et de manière exhaustive. Les informations communiquées au CLIENT doivent comprendre les éléments énumérés à l'article 33 (3) du RGPD, au moins toutefois

- l'heure, la nature et l'étendue de l'incident ou des incidents,
- une explication de la nature de la divulgation illicite,
- une explication des éventuelles conséquences préjudiciables de la divulgation illicite,
- les mesures prises par METEOCONTROL pour empêcher la transmission illicite ou la prise de connaissance non autorisée par des tiers à l'avenir.

METEOCONTROL est consciente que le CLIENT peut être dans l'obligation de signaler un tel incident en vertu de l'article 33 du RGPD, ce qui implique la transmission d'un rapport à l'autorité de contrôle dans les 72 heures après que le CLIENT a eu connaissance de l'incident. METEOCONTROL aidera le CLIENT à s'acquitter de ses obligations en matière de signalement.

- 4.8.** METEOCONTROL est consciente que le CLIENT peut être dans l'obligation de notifier l'autorité de contrôle en vertu de l'article 34 du RGPD. METEOCONTROL aidera le CLIENT dans le cadre de ces notifications.
- 4.9.** METEOCONTROL doit coopérer à la création du registre des activités de traitement par le CLIENT. Elle doit fournir au CLIENT les informations requises de manière appropriée.
- 4.10.** METEOCONTROL doit informer le CLIENT de la (des) personne(s) autorisée(s) à recevoir les instructions du CLIENT. Les personnes autorisées à recevoir des instructions chez METEOCONTROL sont :
- Cheng Liu, Directeur général
 - Stijn Stevens, Directeur financier, Directeur général
 - Bin Lu, Directeur général

En cas de changement au niveau des personnes autorisées à recevoir des instructions chez METEOCONTROL, METEOCONTROL en informera le CLIENT par écrit ou sous forme de texte.

- 4.11.** METEOCONTROL est tenue d'aider le CLIENT à remplir les obligations visées aux articles 32 à 36 du RGPD, en tenant compte de la nature du traitement et des informations dont elle dispose.
- 4.12.** METEOCONTROL est tenue de fournir au CLIENT toutes les informations nécessaires pour démontrer le respect des obligations en vertu de l'article 28 du RGPD.

5. Autorisations dans le cadre du contrôle

- 5.1.** Le CLIENT a le droit de contrôler le respect des dispositions légales en matière de protection des données et/ou le respect des dispositions contractuelles établies entre les PARTIES et/ou le respect par METEOCONTROL des instructions du CLIENT, à tout moment et dans la mesure où cela est nécessaire.
- 5.2.** METEOCONTROL a une obligation de divulgation envers le CLIENT, dans la mesure où cela est nécessaire pour effectuer le

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

contrôle tel que défini dans l'Article 5.1.

- 5.3.** En général, le CLIENT peut mener des activités de contrôle telles que définies à l'Article 2 dans les locaux de METEOCONTROL après notification préalable assortie d'un délai de préavis approprié, à moins qu'un contrôle inopiné ne soit nécessaire en raison de l'objectif du contrôle, qui pourrait être compromis dans le cas contraire. Le CLIENT veille à ce que le contrôle soit limité à l'étendue nécessaire, de manière à ce que les processus opérationnels chez METEOCONTROL ne soient pas excessivement perturbés par le contrôle. METEOCONTROL est tenue de rendre le contrôle possible et d'y contribuer activement. Elle doit permettre au CLIENT d'entrer dans leurs locaux dans le cadre du contrôle.
- 5.4.** METEOCONTROL est tenue, en cas de mesures prises par l'autorité de contrôle à l'encontre du CLIENT conformément à la définition de l'article 58 du RGPD, en particulier en ce qui concerne les obligations de divulgation et de contrôle, de fournir les informations nécessaires au CLIENT et de permettre à l'autorité de contrôle concernée d'effectuer un contrôle sur place. Le CLIENT doit être informé **par METEOCONTROL de ces mesures prévues.**

6. Relations de sous-traitance

- 6.1.** Le CLIENT consent à l'intervention des sous-traitants cités à l'Annexe 2 de la présente ANNEXE DPA pour la fourniture des services indiqués dans cette Annexe.
- 6.2.** METEOCONTROL est autorisée à établir d'autres relations de sous-traitance avec des sous-traitants différents ou supplémentaires dans le cadre de ses obligations contractuelles. Elle informera le CLIENT de tout sous-traitant supplémentaire dans les plus brefs délais.
- 6.3.** Le CLIENT consent à ce que METEOCONTROL fasse appel à des SOCIÉTÉS AFFILIÉES de METEOCONTROL pour fournir les services convenus par contrat. Les dispositions de l'Article 6.1 s'appliquent par analogie.
- 6.4.** METEOCONTROL doit sélectionner avec soin le sous-traitant et vérifier, avant de le mandater, que le sous-traitant peut respecter les accords conclus entre le CLIENT et METEOCONTROL. En particulier, METEOCONTROL doit vérifier au préalable et régulièrement pendant la durée du contrat que le sous-traitant a pris les mesures techniques et organisationnelles pour la protection des données à caractère personnel requises en vertu de l'article 32 du RGPD. METEOCONTROL doit documenter le résultat du contrôle et le fournir au CLIENT sur demande. METEOCONTROL est tenue d'obtenir du sous-traitant la confirmation qu'il a désigné un délégué à la protection des données conformément à l'article 37 du RGPD. Si le sous-traitant n'a pas désigné de délégué à la protection des données, METEOCONTROL doit en informer le CLIENT.
- 6.5.** METEOCONTROL doit s'assurer que les règles convenues dans le présent DPA et toute instruction supplémentaire donnée par le CLIENT s'appliquent également aux sous-traitants. METEOCONTROL doit contrôler régulièrement le respect de ces obligations.
- 6.6.** METEOCONTROL doit établir un accord de traitement avec le

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

sous-traitant répondant aux exigences de l'article 28 du RGPD. Le CLIENT doit recevoir, sur demande, une copie de l'accord de traitement.

- 6.7.** METEOCONTROL est notamment tenue de mettre en place des dispositions contractuelles garantissant que les autorisations dans le cadre du contrôle (Article 5 de l'ANNEXE DPA) du CLIENT et des autorités de contrôle s'appliquent également au sous-traitant et que les droits en matière de contrôle correspondants du CLIENT et des autorités de contrôle sont accordés. En outre, une disposition contractuelle doit stipuler que le sous-traitant doit autoriser ces mesures de contrôle et, le cas échéant, un contrôle sur place.
- 6.8.** Les services que METEOCONTROL obtient de tiers à titre purement complémentaire pour mener à bien ses activités commerciales ne sont pas considérés comme des relations de sous-traitance telles que définies aux Articles 6.1 à 6.5. Il s'agit par exemple de services de nettoyage, de services de télécommunications en relation avec les services que METEOCONTROL fournit au CLIENT, de services postaux et de messagerie, de services de transport et de services de sécurité. METEOCONTROL est néanmoins tenue de s'assurer, également pour ces services complémentaires fournis par des tiers, que des précautions et des mesures techniques et organisationnelles appropriées sont mises en place pour garantir la protection des données à caractère personnel. Les services de maintenance et de test constituent des relations de sous-traitance soumises à approbation dans la mesure où la maintenance et les tests concernent des systèmes informatiques qui sont également utilisés dans le cadre de la prestation de services pour le CLIENT. Les PARTIES conviennent que les services de maintenance et de test susmentionnés constituent un « traitement » au sens de l'article 28 du RGPD.

7. Obligation de confidentialité

- 7.1.** Lors du traitement des données pour le CLIENT, METEOCONTROL est tenue de respecter la confidentialité des données qu'elle reçoit ou dont elle prend connaissance dans le cadre du contrat. METEOCONTROL s'engage à respecter les mêmes règles de protection des secrets que celles qui s'appliquent au CLIENT. Le CLIENT est tenu d'informer METEOCONTROL de toute règle particulière en matière de secret.
- 7.2.** METEOCONTROL confirme qu'elle a pris connaissance des dispositions applicables en matière de protection des données et qu'elle est au fait de leur application. METEOCONTROL s'assure que les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont soumises à des obligations légales de confidentialité adéquates et que ces personnes connaissent les règles de protection des données qui leur sont applicables. L'engagement de ces personnes doit être démontré au CLIENT sur demande. Si METEOCONTROL participe à la fourniture de services commerciaux de télécommunications dans le cadre des services fournis au CLIENT, elle est tenue d'obtenir de la part des employés concernés un engagement écrit à respecter le secret

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

des télécommunications conformément à l'article 3 de la TDDDG [loi allemande sur la protection des données dans les services numériques et les télécommunications].

8. Protection des droits des personnes concernées

- 8.1.** Le CLIENT est seul responsable de la protection des droits des personnes concernées définis au chapitre III du RGPD.
- 8.2.** En ce qui concerne le type de traitement, METEOCONTROL aide le CLIENT, dans la mesure du possible, par des mesures techniques et organisationnelles appropriées, à s'acquitter de son obligation de répondre aux demandes d'exercice des droits des personnes concernées mentionnées au chapitre III.
- 8.3.** Les dispositions relatives à la rémunération éventuelle des efforts supplémentaires déployés par METEOCONTROL dans le cadre de services de coopération en rapport avec l'exercice des droits des personnes concernées à l'encontre du CLIENT restent inchangées.

9. Obligations de secret

- 9.1.** Les deux PARTIES s'engagent à préserver le caractère confidentiel de toutes les informations qu'elles reçoivent dans le cadre de l'exécution du présent Contrat pour une durée indéterminée et à ne les utiliser que pour l'exécution du Contrat. Aucune des PARTIES n'est autorisée à utiliser ces informations, en totalité ou en partie, à d'autres fins que celles susmentionnées, ni à les rendre accessibles à des tiers.
- 9.2.** L'obligation susmentionnée ne s'applique pas aux informations que l'une des PARTIES a manifestement reçues de tiers sans être tenue à la confidentialité, ni aux informations qui sont de notoriété publique.

10. Rémunération

- 10.1.** La rémunération de METEOCONTROL est convenue dans le CONTRAT.
- 10.2.** S'il n'existe pas de réglementation relative à l'engagement de frais dans le cadre des obligations de contrôle et si l'effort dépasse un montant raisonnable pour METEOCONTROL, METEOCONTROL facturera un forfait horaire de 150 euros net.

11. Mesures techniques et organisationnelles de sécurité des données

- 11.1.** METEOCONTROL est tenue de prendre toutes les mesures requises conformément à l'article 32 du RGPD dans le cadre de ses activités de traitement. Il en va de même lorsque METEOCONTROL autorise le traitement à distance.
- 11.2.** L'état de l'art en matière de mesures techniques et organisationnelles au moment de l'établissement du contrat est fourni en Annexe 2 de la présente ANNEXE DPA.
- 11.3.** METEOCONTROL est tenue de contrôler et d'adapter les mesures techniques et organisationnelles qu'elle prend, sur une base régulière et en fonction des événements, en ce qui concerne leur efficacité et leur nécessité conformément à l'article 32 du RGPD. METEOCONTROL est tenue d'adapter les mesures techniques et organisationnelles indiquées à l'Annexe 2.

- 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.

METEOCONTROL est tenue d'informer sans délai le CLIENT de la version adaptée et mise à jour des mesures techniques et organisationnelles et de fournir ces mesures au CLIENT.

- 11.4.** METEOCONTROL fournira au CLIENT une documentation appropriée sur les mesures techniques et organisationnelles qu'elle a prises pour garantir le niveau de protection conformément à l'article 32 du RGPD et au présent DPA.

12. Durée du DPA

- 12.1.** La durée contractuelle du DPA est égale à celle du CONTRAT.
- 12.2.** Le CLIENT peut résilier le contrat à tout moment sans délai de préavis en cas de violation grave par METEOCONTROL des dispositions applicables en matière de protection des données ou des obligations découlant du présent DPA, si METEOCONTROL, en violation du contrat, ne peut pas ou refuse de se conformer à une instruction du CLIENT, ou si METEOCONTROL, en violation du contrat, refuse l'accès au CLIENT ou à l'autorité de contrôle compétente.

13. Résiliation

- 13.1.** Après avoir mis fin à la prestation de services de traitement, METEOCONTROL doit, à la discrétion du CLIENT, soit supprimer, soit restituer au CLIENT l'ensemble des documents, données et résultats de traitement ou d'utilisation préparés en rapport avec la relation contractuelle et contenant des données à caractère personnel dont elle a pris possession. Dans le cadre de ce processus, METEOCONTROL s'assure que la suppression rend impossible l'accès (ultérieur) aux informations personnelles contenues dans les données à supprimer, moyennant un effort raisonnable, ou leur traitement d'une manière significative.
- 13.2.** Cette obligation s'applique également aux copies. Les supports de données de METEOCONTROL doivent ensuite être supprimés. Ceci inclut également les sauvegardes effectuées par METEOCONTROL. La suppression doit être documentée de manière appropriée. Les matériaux et déchets de test doivent être détruits ou supprimés physiquement sans délai.
- 13.3.** Le CLIENT a le droit de contrôler que les données sont restituées et supprimées de manière complète et contractuelle par METEOCONTROL.

14. Droit de rétention

- 14.1.** Les PARTIES conviennent que l'exercice par METEOCONTROL d'un droit de rétention au sens de l'article 273 du code civil allemand portant sur les données traitées et les supports de données correspondants est exclu.

15. Dispositions finales

- 15.1.** Si la propriété du CLIENT chez METEOCONTROL est menacée en raison de mesures prises par des tiers (telles que la saisie ou la confiscation), en raison d'une procédure d'insolvabilité ou de tout autre événement, METEOCONTROL doit en informer le CLIENT dans les plus brefs délais. METEOCONTROL informera sans délai les créanciers du fait que les données sont traitées

- 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.
- 15.4.** The CONTRACT language is English. The French translation is solely for the purpose of better understanding and is not binding, particularly in the event of deviations from the English version. The contract in English is authoritative.

dans le cadre d'un contrat.

- 15.2.** Les accords annexes doivent être rédigés sous forme écrite.
- 15.3.** La nullité de certaines parties du présent DPA n'affecte en rien la validité des autres dispositions du DPA.
- 15.4.** La langue du CONTRAT est l'anglais. La traduction française sert uniquement à une meilleure compréhension et n'est pas contraignante, notamment en cas de divergences par rapport à la version anglaise. Le contrat en anglais fait foi.

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.

Annexe 1 de l'ANNEXE DPA : Sous-traitants

Pour le traitement des données au nom du CLIENT, METEOCONTROL utilise des services fournis par des tiers, qui traitent les données en son nom.

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

Sous-traitant	Finalité du traitement	Garanties appropriées si des données sont traitées dans un pays tiers
meteocontrol Italia s.r.l.	Services d'assistance	UE, DPA consigné
meteocontrol France SAS	Services d'assistance	UE, DPA consigné
meteocontrol Ibérica SL	Services d'assistance	UE, DPA consigné
Raising Power GmbH	Services d'assistance	UE, DPA consigné
mc Beteiligungs GmbH	Services d'assistance	UE, DPA consigné
meteocontrol Romania SRL.	Services d'assistance	UE, DPA consigné
meteocontrol North America Inc.	Services d'assistance	CCT établies
meteocontrol Japan Corporation	Services d'assistance	Décision d'adéquation consignée ; DPA consigné
meteocontrol Chile SpA	Services d'assistance	CCT établies
meteocontrol AMEA DMCC	Services d'assistance	CCT établies
meteocontrol Taiwan Inc.	Services d'assistance	CCT établies
Functional Software, Inc.	Utilisation du service Sentry.io pour contrôler les performances de la base de données et pour l'analyse des erreurs ; stockage des adresses IP dans le cadre de la transmission des erreurs.	Des CCT (processeur à processeur) ont été établies
Eurekos Systems ApS	Mise à disposition d'une plateforme pour l'académie meteocontrol	UE, DPA consigné

Infrared Power Techsol Pvt. Ltd.	Prestation de services d'assistance, hors UE	CCT et DPA établis
-------------------------------------	---	--------------------

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.

Annexe 2 de l'ANNEXE DPA : Mesures techniques et organisationnelles mises en place par METEOCONTROL

Partie A : Garantir la confidentialité des données personnelles (art. 32 (1) b RGPD)

1. Contrôle d'accès physique

1.1. Le contrôle d'accès physique englobe les mesures visant à empêcher les personnes non autorisées d'accéder aux systèmes de traitement des données qui traitent ou utilisent des données à caractère personnel.

1.2. Mesures

- L'administration se situe sur un site accessible au public. L'accès au site avec le centre informatique qui exploite les services cloud est restreint.
- Une description/documentation de toutes les mesures de contrôle d'accès utilisées sur le site est consignée.
- Des systèmes de contrôle d'accès mécaniques sont installés dans les bâtiments.
- Les serveurs de l'entreprise sont installés dans une salle fermée à clé et dont l'accès est contrôlé.

2. Contrôle d'accès

2.1. Mesures visant à empêcher les personnes non autorisées d'utiliser les systèmes de traitement des données.

2.2. Mesures

- Pour tous les services et systèmes d'information, il existe un processus officiel d'inscription et de désinscription des utilisateurs permettant de délivrer et de révoquer les autorisations d'accès.
- Le Wi-Fi est protégé contre les accès non autorisés.
- Il est garanti que seules les personnes autorisées ont un accès logique aux composants du réseau.
- Il existe un processus d'activation officiel auquel les systèmes et les applications contenant des données à caractère personnel doivent être soumis avant de pouvoir accéder au réseau.
- Il est garanti que seuls les appareils autorisés des personnes privées ou des visiteurs bénéficient d'un accès logique au réseau de l'organisation.
- Des mesures ont été mises en place pour identifier et authentifier le personnel de maintenance externe.
- Lors des travaux de maintenance locaux effectués par des entreprises externes, il est garanti qu'aucun équipement ne peut quitter la zone informatique sans faire l'objet d'un contrôle.
- Des autorisations d'accès différenciées et à plusieurs niveaux ont été instaurées.
- Des politiques en matière de pare-feu, de réseau et de mot de passe ont été instaurées.
- Des pare-feu et des systèmes de détection d'intrusion efficaces sont utilisés.
- L'accès aux systèmes administratifs centraux ne peut se

faire que par l'intermédiaire d'un VPN.

- Les réseaux sont séparés logiquement (VLAN).

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.

3. Contrôle d'accès électronique

3.1 Mesures visant à garantir que les personnes autorisées à utiliser un système de traitement des données ne peuvent accéder qu'aux données qui relèvent de leurs droits d'accès et que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées au cours du traitement, de l'utilisation et après avoir été sauvegardées.

3.2 Mesures

- Les utilisateurs veillent à ce que leur équipement de traitement des données soit suffisamment protégé lorsqu'il n'est pas sous surveillance.
- Les principes de « clean desk » consistant à maintenir un bureau propre et un écran vierge sont appliqués (Clean Desk Policy).
- Un logiciel de sécurité spécial est utilisé pour garantir la sécurité des données et le contrôle d'accès électronique.
- Il existe des instructions sur la manière de traiter les supports de données (y compris le papier manuscrit ou imprimé) qui ne sont plus nécessaires.
- Il existe des règles régissant l'élimination ou l'utilisation ultérieure des appareils contenant des supports de stockage.
- Il existe un règlement régissant l'accès administratif externe.
- Il est garanti que les personnes autorisées à utiliser un système de traitement des données n'ont accès qu'aux données qui relèvent de leurs droits d'accès. Ceci est garanti grâce aux mesures suivantes :
 - Vérification automatique des droits d'accès au moyen d'un mot de passe
 - Navigation dans les menus uniquement en fonction des droits d'accès respectifs
 - Droits d'accès différenciés aux programmes d'application
 - Options de traitement différenciées (lecture/modification/suppression)

4. Contrôle de séparation

4.1. Mesures visant à garantir que les données collectées pour des raisons différentes peuvent être traitées séparément.

4.2. Mesures

- Les données à caractère personnel contenues dans les systèmes sont logiquement séparées les unes des autres (les différents ensembles de données d'une base de données uniforme sont marqués en fonction de leur finalité (séparabilité en termes de logiciels)).
- Les environnements de test et de production sont des systèmes distincts.

5. Pseudonymisation

5.1. Les données ne sont pas pseudonymisées.

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.

Sección B: Salvaguarda de la integridad de los datos personales (art. 32, punto 1., letra b) del RGPD)

6. Contrôle des transferts

6.1. Mesures visant à garantir que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou effacées sans autorisation pendant leur transmission électronique, leur transport ou leur enregistrement sur un support de données, et qu'il est possible de vérifier et de déterminer les cas où un transfert de données à caractère personnel par le biais de systèmes de transfert de données est prévu.

6.2. Mesures

- Tous les nouveaux employés reçoivent des informations sur la protection des données lorsqu'ils sont soumis à une obligation de confidentialité.
- Les employés qui traitent/utilisent des données à caractère personnel sont formés à un comportement conforme à la protection des données sur le lieu de travail par le biais d'une formation sur la protection des données. Il est garanti que les données sont transmises uniquement aux destinataires spécifiés par le CLIENT ou aux destinataires appropriés selon la finalité poursuivie.
- Il existe une procédure pour les employés qui quittent l'entreprise, en particulier ceux qui ont été licenciés.
- Il existe un système de classification des données à l'échelle de l'entreprise.
- Il existe une politique de cryptographie régissant le cryptage des transferts de données.

7. Contrôle de saisie

7.1. Mesures visant à garantir qu'il est possible de vérifier et de déterminer ultérieurement si et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement de données.

7.2. Mesures

- Des contrôles aléatoires sont effectués par le délégué à la protection des données (également en ce qui concerne le respect des délais d'effacement).
- Les données enregistrées sont protégées contre toute consultation ou manipulation non autorisée.
- Un responsable de la sécurité informatique a été nommé.

Partie C : Garantir la disponibilité des données à caractère personnel (art. 32 (1) b RGPD)

8. Contrôle de la disponibilité

8.1. Mesures visant à garantir que les données à caractère personnel sont protégées contre toute destruction ou perte involontaire et qu'elles peuvent être restaurées rapidement en cas d'incident physique ou technique.

8.2. Mesures

- Les systèmes sont protégés contre les pannes.
- Des sauvegardes sont effectuées régulièrement.
- Un logiciel antivirus est utilisé.
- Des systèmes UPS suffisamment puissants sont utilisés.
- Des contrôles réguliers sont effectués pour vérifier

- 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.

sil'alimentation au niveau des lignes de données, de l'électricité et de l'air conditionné est toujours adéquate.

- Les lignes d'alimentation sont souterraines.
- Il n'y a pas de conduites d'eau dans les salles de serveurs.
- La (les) tension(s) de sortie est (sont) constamment contrôlée(s).
- Des équipements de protection contre la foudre et les surtensions sont installés.
- Il n'y a pas d'éléments inflammables dans la zone des serveurs.
- Un système d'alerte précoce avec des alarmes incendie automatiques est installé.
- Il y a suffisamment d'extincteurs adaptés et le matériel d'extinction adéquat est présent ; l'uniformité est assurée. Dans certaines zones, des systèmes d'extinction automatiques sont utilisés.
- Il existe un manuel d'urgence, qui est constamment mis à jour.
- Il existe un document écrit pour le redémarrage du traitement des données (composition et tâches du comité de gestion des sinistres).
- Il existe un concept d'urgence pour le réseau.
- Les exigences de la sauvegarde sont documentées dans un concept de sauvegarde.
- Les sauvegardes sont protégées contre le vol et la destruction.
- Des processus de sauvegarde ont été établis et documentés dans des instructions de travail.
- Des contrôles réguliers sont effectués pour vérifier si la sauvegarde est utilisable.
- La température de l'air est contrôlée.
- Il existe un centre informatique alternatif.
- Il existe des systèmes de contrôle externes indépendants du système global.
- La redondance matérielle est assurée.

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

9. Processus d'évaluations et de contrôle réguliers (art. 32 (1) d, art. 25 (1) RGPD)

9.1. Critères de sécurité organisationnelle

9.1.1. La sécurité organisationnelle décrit toutes les mesures organisationnelles (instructions de travail, processus, etc.) visant à garantir et à améliorer la sécurité

9.1.2 Mesures

- Un système de gestion de la protection des données (DSMS) a été mis en place.
- Un système de gestion des réponses aux incidents a été mis en place.
- Les employés et les dirigeants sont régulièrement informés et sensibilisés.
- Des audits de sécurité informatique sont régulièrement effectués.
- Des audits de sécurité informatique sont réalisés chaque année.

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.

9.2. Gestion de la réponse aux incidents

9.2.1. Les incidents sont traités à l'aide du système de gestion des incidents (description dans le document principal). Une liste des mesures en découlant ainsi qu'une liste de tous les incidents relevant de la protection des données sont intégrées dans le DSMS.

9.3. Préréglages favorisant la protection des données (art. 25 (2) RGPD)

9.3.1. En règle générale, seules sont collectées et traitées les données qui sont utiles et nécessaires aux fins de l'activité de l'entreprise. Les processus de collecte et de traitement automatisés des données sont conçus de manière à ce que seules les données nécessaires puissent être collectées. Les données des personnes concernées sont stockées sous forme partiellement cryptée. Le délégué à la protection des données est informé des changements et des modifications apportés aux systèmes, conformément au processus de changement (défini dans le document principal). Des audits réalisés à intervalles irréguliers sont également prévus dans le cadre du cycle d'audit PDCA du délégué à la protection des données.

9.4. Contrôle dans le cadre contractuel

9.4.1. Mesures visant à garantir que les données à caractère personnel traitées dans le cadre d'un contrat ne peuvent être traitées que selon les instructions du CLIENT.

9.4.2. Les employés qui ont un accès administratif aux systèmes ont tous reçu une formation sur la protection des données, se sont engagés à respecter la confidentialité et ont accepté des accords de confidentialité et de secret dans le cadre de leur contrat de travail.

9.4.3. Si METEOCONTROL fait appel à des sous-traitants pour le traitement des données, certaines exigences s'appliquent. Ceci inclut la garantie du respect des mesures techniques et organisationnelles de METEOCONTROL telles que définies dans l'article 28 du RGPD et dans l'article 32 (1) du RGPD.

9.4.4. Tout contrat de traitement de données doit toujours reposer sur une base juridique. Dans le cadre de l'exécution des contrats de traitement de données tels que définis à l'article 28 (3) du RGPD, toutes les mesures et exigences requises doivent être respectées.