Data Processing Agreement for Public Cloud

between

the entity or person party to the Agreement (“Customer”)

and

Cleura AB (“Cleura”)

each a “party”, together “the parties”,

have agreed on the following data processing agreement in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

Table of Contents

1 Preamble

1.1 The Data Processing Agreement for Public Cloud is comprised of this document with accompanying annexes and addendums (jointly the “data processing agreement” or “DPA”). This DPA is applicable when part of an “Agreement” entered into between Customer and Cleura, which references this DPA. Capitalised terms defined in the Agreement shall apply to the DPA as well.

1.2 The DPA is intended to ensure the parties’ compliance with Article 28(3) and/or 28(4) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("GDPR”).

1.3 The terms “personal data”, “data subject”, “processing”, “pseudonymisation”, “controller”, “processor”, “personal data breach”, “supervisory authority” and “international organisation” used in the DPA shall have the meanings given to them in the GDPR.

1.4 In the context of the provision of the Services, Cleura is a processor of personal data in accordance with the DPA. Customer is a controller and/or processor as applicable.[1] The DPA may therefore separately mention Customer and the controller, even though they may be one and the same. If there is more than one controller, references to the controller shall refer to all of them.

1.5 Any processing by Cleura as a controller is not governed by this DPA, but is rather explained in Cleura’s privacy notice.

1.6 The DPA shall take priority over any similar provisions contained in other agreements between the parties.

1.7 Two annexes are attached to the DPA and form an integral part of the DPA.

- Annex A: Processing in the Services for the controller’s purposes.
- Annex B: Processing of Cleura Cloud Management Portal user accounts, API user accounts and support cases for Customer’s purposes.

In addition, Cleura’s services, regions and sub-processors are listed on Cleura’s website.

1.8 The DPA along with annexes, as well as any modifications and addendums, shall be retained in writing, including electronically, by both parties.

1.9 The DPA shall not exempt the parties from obligations to which they are subject pursuant to the GDPR or other legislation. For information on how Cleura handles legal requests for data, see section 8 Legal requests for data.

[1] See e.g. EDPB Guidelines 07/2020 on the concepts of controller and processor, paras 12 and 26.

2 The rights and obligations of Customer

2.1 Customer shall ensure that its responsibilities regarding the processing of personal data are fulfilled in compliance with the GDPR, the applicable EU or Member State[2] data protection provisions and the DPA.

2.2 Customer acknowledges that the controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.3 Customer acknowledges that the controller is responsible for ensuring that the processing of personal data, which Cleura is instructed to perform, has a legal basis.

2.4 Customer warrants on an ongoing basis that the information in Annex A accurately reflects the processing of personal data for Customer's use of the Cleura Public Cloud Service.

2.5 If Customer is a processor:

a) Customer warrants on an ongoing basis that the relevant controller has authorised:

i. the information set out in Annex A,

ii. instructions for processing given by Customer to Cleura, including any instructions regarding transfers to third countries or international organisations and instructions regarding erasure or return of personal data,

iii. Customer's engagement of Cleura as a sub-processor, and

iv. Cleura's engagement of sub-processors as set out on Cleura's website and section 6 Cleura's use of sub-processors.

b) without prejudice to other information Customer shall provide to the controller, Customer shall immediately forward to the relevant controller any information Cleura provides to Customer regarding objections to instructions, personal data breaches and possible personal data breaches, sub-processors, requests from data subjects or communication from supervisory authorities.

3 Cleura acts according to instructions

3.1 As a processor, Cleura shall process personal data only on the documented instructions given by Customer, unless Cleura is required to do so by Union or Member State law to which Cleura is subject. Such instructions are specified in Annex A and Annex B.

3.2 Subsequent instruction requests can be given by Customer throughout the duration of the processing of personal data, but instructions given shall always be documented and kept in writing, including electronically.

3.3 Cleura shall immediately inform Customer if the instructions are unclear, not sufficient, or in the opinion of Cleura, contravene the GDPR or the applicable EU or Member State data protection or privacy provisions.

[2] References to "Member States" in the DPA shall be understood as references to "EEA Member States".

3.4 If Cleura has informed Customer that, in the opinion of Cleura, the documented instructions contravene the GDPR or the applicable EU or Member State data protection or privacy provisions, and Customer still demands that Cleura follows these documented instructions, Cleura has the right to stop delivery of the Services under the Agreement until both parties have agreed to new documented instructions. Should the parties not reach such an understanding, Cleura has a right to terminate the Agreement and the associated DPA with thirty (30) days' notice.

4 Confidentiality

4.1 Cleura shall only grant access to the personal data being processed on behalf of the controller to persons under Cleura's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

4.2 Cleura shall at the request of Customer demonstrate that the concerned persons under Cleura's authority are subject to the abovementioned confidentiality.

4.3 Confidentiality shall continue to apply after the DPA is terminated.

5 Security of processing

5.1 Article 32(1) GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. If Customer is a processor, Customer and Cleura shall implement the measures that fall on the processor to implement, as agreed upon in the DPA.

5.2 Customer warrants that it has assessed the technical and organisational measures detailed in the Agreement, including in Annex A of the DPA, which Cleura has implemented by default as well as any further measures which Customer shall apply in each case as appropriate.

5.3 Customer warrants that the measures implemented by Cleura and Customer provide the appropriate level of security required by the controller, the measures including, depending on their relevance:

a) the pseudonymisation and encryption of personal data,

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.4 Cleura may update its security measures provided that such updates do not result in a material reduction of security.

6 Cleura's use of sub-processors

6.1 Cleura shall meet the requirements specified in Articles 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

6.2 Cleura shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the prior general written authorisation of the controller. Customer warrants that Cleura has the general authorisation of the controller for the engagement of sub-processors. The list of sub-processors already authorised by the controller is available on Cleura's website.

6.3 Cleura shall inform Customer of any intended changes concerning the addition, replacement or significant additional tasks of sub-processors at least thirty (30) days in advance. Cleura may inform the Customer of this through updates to Cleura's website. Customer shall without delay inform the controller, thereby giving the controller the opportunity to object to such changes in advance. Customer shall immediately notify Cleura in writing of any such objections.

6.4 Where Cleura engages a sub-processor for carrying out specific processing activities under the DPA, the same data protection obligations as set out in the DPA shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the DPA and the GDPR.

Cleura shall therefore be responsible for requiring that the sub-processor complies with the data protection obligations to which Cleura is subject pursuant to the DPA.

6.5 If Cleura does not fulfil its data protection obligations due to a failure of Cleura's sub-processor to fulfil its data protection obligations, Cleura shall remain liable to Customer. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against Customer, controller, Cleura and the sub-processor.

7 Transfers of personal data to third countries

7.1 Any transfer of personal data to third countries or international organisations by Cleura shall only occur on the basis of documented instructions from Customer and shall always take place in compliance with Chapter V GDPR.

7.2 If transfers to third countries or international organisations, which Cleura has not been instructed to perform by Customer, are required under EU or Member State law to which Cleura is subject, Cleura shall inform Customer or controller of the legal requirement prior to processing unless that EU or Member State law prohibits such information on important grounds of public interest.

7.3 Without documented instructions given by Customer, Cleura therefore cannot within the framework of the DPA:

a) transfer personal data to a controller or a processor in a third country or in an international organisation,

b) transfer the processing of personal data to a sub-processor in a third country, or

c) have the personal data processed by Cleura in a third country.

7.4 Customer is considered to give documented instructions regarding transfers of personal data to third countries, including the applicable transfer tool to be used under Chapter V GDPR, based on which services and regions Customer chooses to use, as well as any other instructions provided.

7.5 The DPA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the DPA cannot by itself be relied upon by the parties as a transfer tool under Chapter V GDPR.

8 Legal requests for data

8.1 Article 32(4) GDPR stipulates that processors shall take steps to ensure that any natural person acting under the authority of the processor who has access to personal data does not process them except on instructions from the controller, unless the person is required to do so by EU or Member State law.

8.2 Cleura can take different steps depending on the services and regions where data is processed.

8.3 Local law applies in each region where data is processed. Cleura may let requirements according to a region's local law take precedence over other laws, regulations, certifications and agreements, such as the Agreement between Customer and Cleura.

8.4 If authorities in a region where Cleura processes personal data require Cleura to give access to or otherwise process that data, Cleura may comply if the requirement is valid under local law. Cleura will inform Customer or controller of such a requirement when permitted by law. Accordingly, if U.S. authorities require Cleura to give access to data in a region in the USA and this is valid under U.S. law, Cleura may comply.

8.5 Cleura will not comply with an extraterritorial requirement to give access to or otherwise process data in an EU region, unless the requirement is based on an international agreement such as a mutual legal assistance treaty in force between the requesting country and the country of the region, or unless the requirement is otherwise valid under the region's local law. An extraterritorial requirement comes from authorities in a country different from the region where the data is processed.

8.6 Accordingly, if U.S. authorities require Cleura to give access to data in a region in the EU, Cleura will not comply unless the requirement is based on an international agreement such as a mutual legal assistance treaty in force between the country making the requirement and the country where the data is processed, or unless the request is otherwise valid under local law in the region where the data is. For the avoidance of doubt, an adequacy decision is not an international agreement which allows for extraterritorial requests for data in the EU to become valid.

9 Assistance to Customer

9.1 Taking into account the nature of the Services and the processing, Cleura shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that Cleura shall, insofar as this is possible, assist Customer in the controller's compliance with:

a) the right to be informed when collecting personal data from the data subject,

b) the right to be informed when personal data have not been obtained from the data subject,

c) the right of access by the data subject,

d) the right to rectification,

e) the right to erasure ('the right to be forgotten'),

f) the right to restriction of processing,

g) notification obligation regarding rectification or erasure of personal data or restriction of processing,

h) the right to data portability,

i) the right to object, and

j) the right not to be subject to a decision based solely on automated processing, including profiling.

9.2 Customer acknowledges that when the Services involve the infrastructure or platform layer, Customer's visibility into the day-to-day processing may be at a better level than Cleura's. Customer may thus be better positioned to assist the controller in fulfilling data subject rights. For measures that may be required at the level of the Services, such as deletion of a virtual machine, Customer shall familiarise itself with the tools provided by Cleura as part of the Services to determine if and how they can be used to fulfil data subject rights, and make manual requests for assistance if these tools are insufficient.

9.3 Cleura shall, taking into account the nature of the processing and the information available to Cleura, assist Customer in ensuring the controller's compliance with:

a) the controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons,

b) the controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons,

c) the controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment), and

d) the controller’s obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

10 Notification of personal data breach

10.1 In case of any personal data breach, Cleura shall, without undue delay after having become aware of it, notify the controller of the personal data breach.

10.2 In accordance with section 9.3, Cleura shall assist the controller in notifying the personal data breach to the competent supervisory authority. Cleura shall, taking into account the nature of the Services and processing and the knowledge available to Cleura, assist the controller in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the controller’s notification to the competent supervisory authority:

a) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

b) the likely consequences of the personal data breach, and

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.3 Cleura shall at Customer’s or controller’s request provide assistance to investigate suspicions of possible unauthorised processing and/or access to personal data.

10.4 Customer has the right to request a report prepared in connection with a personal data breach.

11 Erasure and return of personal data

11.1 On termination of the provision of the Services involving processing of personal data, Cleura shall, depending on the instructions given by Customer:

a) delete all personal data processed on behalf of the controller and certify to Customer that it has done so, unless Union or Member State law requires further processing of the personal data, or

b) make the personal data available to the controller and delete existing copies, unless Union or Member State law requires further processing of the personal data.

11.2 Customer is responsible for downloading and/or deleting the personal data well before access to the Services is terminated, and Customer’s use of these options shall constitute instructions given to Cleura. Customer shall immediately notify Cleura if Customer is unable to download or delete the data. If Customer does not use these options, Customer instructs Cleura to delete the personal data when the relevant Services involving processing of personal data are deactivated.

12 Audit and inspection

12.1 Taking into account the nature of the Services and processing, Cleura shall provide assistance by making available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and the DPA and when necessary by allowing for and contributing to audits, including inspections, conducted by the controller or another auditor mandated by the controller (however, never a competitor to Cleura).

12.2 Audits shall to the greatest extent possible take into account confidentiality undertakings Cleura has under contract law or vis-à-vis third parties and inspections shall to the greatest extent possible be carried out under normal working hours.

12.3 Cleura shall when necessary provide the supervisory authorities, which pursuant to applicable legislation have access to the controller's, Customer's and/or Cleura's facilities, or representatives acting on behalf of such supervisory authorities, with access to Cleura's physical facilities on presentation of appropriate identification.

13 Liability

13.1 If the parties have agreed on a limitation of liability in the Agreement, such liability provisions shall also apply to this DPA. If the parties have not agreed on a limitation of liability, a party's liability due to this DPA or as a consequence of the processing of personal data covered by the DPA shall be limited to a total amount of two (2) price base amounts, as stipulated in the Swedish Social Insurance Code (2010:110).

13.2 The limitations of a party's liability in this section 13 Liability, do not apply in cases of intent or gross negligence. Both parties are further aware that the limitations of liability do not apply to action for damages from data subjects.

13.3 If either party becomes aware of circumstances which may result in a loss for the other party, the first party shall without delay inform the other party of this and actively work with the other party to prevent and minimise such loss.

14 Compensation

14.1 Cleura is entitled to additional compensation from Customer for assistance Cleura gives as a processor under the DPA and the GDPR due to Customer's engagement of Cleura as a processor. This shall include, inter alia, assistance given as a response to service requests, assistance Cleura may be required to provide directly to Customer or the controller including in connection with audits, as well as work reasonably needed to answer questions from or engage in investigations by supervisory authorities, unless the reason for the inquiry is that Cleura has not met its data protection obligations. Compensation shall be paid in accordance with the most recent price list for consulting services.

14.2 Cleura is in any case not entitled to additional compensation for:

a) the establishment of its information security management system certified in accordance with ISO 27001, as well as internal policies and documentation, and

b) initial reporting of a personal data breach at Cleura or at a sub-processor engaged by Cleura, unless the sub-processor has been instructed on behalf of the controller without Cleura's involvement, in which case Cleura is entitled to compensation according to the most recent price list for consulting services.

14.3 If, pursuant to this DPA, Cleura incurs increased costs as a result of new or changed legislation, EDPB or supervisory authority regulations, guidelines, recommendations or other circumstances beyond its control, Cleura will have the right to call for negotiations regarding adjustment of the compensation. The parties will participate in such price negotiations in a good and constructive spirit.

15 Assignment

15.1 Neither party is entitled to assign, in whole or in part, its rights or obligations under the DPA without the other party's written approval. However, Cleura may assign all or part of its rights and obligations, or the DPA, to a company within the same company group as Cleura.

15.2 In addition, if Customer is a processor and has ceased to exist in fact or in law or has become insolvent, the controller shall have the right to give instructions to Cleura, for example, to erase or return the personal data and to terminate Cleura as a processor.

16 Governing law and jurisdiction

16.1 If the parties have agreed on governing law, jurisdiction and/or dispute resolution mechanisms in the Agreement (e.g. in Cleura's Terms of Service), such provisions shall apply to the DPA.

16.2 To the extent the parties have not agreed on such overriding provisions in the Agreement, or if the parties have not concluded such an agreement, the following shall apply:

Any dispute, controversy or claim arising out of or in connection with the Agreement, or the breach, termination or invalidity thereof shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce. The rules for expedited arbitrations shall apply, unless the Stockholm Chamber of Commerce in its discretion determines, taking into account the complexity of the case, the amount in dispute and other circumstances, that the arbitration rules shall apply. In the latter case, the Stockholm Chamber of Commerce shall also decide whether the arbitral tribunal shall be composed of one or three arbitrators. The seat of arbitration shall be Stockholm, Sweden and the language to be used in the arbitral proceedings shall be English.

However, if Customer is a Swedish public authority or equated with a public authority according to Chapter 2 of the Public Access to Information and Secrecy Act (2 kap. offentlighets- och sekretesslagen), and unless the Parties have agreed otherwise, any dispute, controversy or claim arising out of or in connection with the Agreement, or the breach, termination or invalidity thereof shall instead be finally settled by the general courts of Sweden, with Stockholm District Court as the court of first instance, and the language to be used in the proceedings shall be Swedish.

16.3 The Agreement shall be governed by the substantive laws of Sweden.

17 Commencement, changes and termination

17.1 The DPA shall become effective when the Agreement becomes effective, or at the latest when Customer starts processing personal data according to Annex A.

17.2 Cleura may change the DPA if the change is necessary to comply with applicable law, is specifically permitted by the DPA, or fulfills the following criteria:

a) is commercially reasonable,

b) does not result in a material reduction of the security of the Services, and

c) does not have a material adverse impact on Customer’s rights under the DPA.

Material changes to the DPA will become effective 30 days after the changed DPA is published on Cleura’s website or Customer is otherwise notified (whichever comes first). However, changes required under applicable law will be effective immediately. Customer’s continued use of the Services after a change to the DPA constitutes Customer’s agreement to be bound by the changes.

17.3 The DPA shall apply for the duration of the provision of the Services where Cleura is a processor of personal data.

17.4 If the provision of the Services where Cleura is a processor of personal data is terminated, and the personal data is deleted or returned to Customer, the DPA may be terminated by written notice by either party.

18 Data protection contact points

18.1 The parties shall appoint contact points for the Agreement and those contact points may be used to communicate regarding data protection, unless the parties have agreed in writing to appoint other contact points regarding data protection. The parties shall continuously update each other of changes to the contact points.

18.2 At Cleura’s request, Customer shall without delay provide Cleura with up to date details for a contact point of the controller regarding the processing related to the Services. The contact point shall if possible be a non-personal contact point appropriate for communication regarding data protection.

Annex A

Processing in the Services for the controller’s purposes

A.1 Controllership

This Annex A concerns the processing of personal data for the purposes that the Services are used for.

For the processing described in this annex, Cleura is a processor of personal data on behalf of the controller. The controller is the entity which determines the purposes and means of the processing.

If Customer determines the purposes and means of the processing, then Customer is the controller engaging Cleura as a processor of personal data on the controller's behalf.

If Customer is itself a processor engaged by a controller, or by a processor in a chain of processors between the controller and Cleura, then Customer is a processor engaging Cleura as another processor (sub-processor) of personal data on the controller's behalf. If so, Customer warrants that it has the controller's authorisation regarding the information set out in this Annex A.

Customer warrants on an ongoing basis that the information in this Annex A accurately reflects the processing of personal data for the purposes that the Services are used for.

A.2 Systems processing personal data

Customer shall maintain an updated a list of the systems/servers used to process personal data based on the Services, including a general description of their nature and indicate if each system/server is used for special categories (art. 9), criminal convictions and offences (art. 10) or otherwise privacy sensitive processing.

For a safer processing of personal data and a speedier investigation of personal data breaches, Customer shall at Cleura's request without undue delay provide Cleura with the list.

A.3 The controller's purposes for processing personal data:

Cleura will process personal data for the purposes of delivering the Services to Customer in accordance with this DPA.

A.4 Cleura's processing of personal data on behalf of the controller shall mainly pertain to (the nature of the processing):

Cleura will process personal data on the controller's behalf as necessary to fulfil the Agreement and deliver the Services.

A.5 The processing includes the following types of personal data about data subjects:

Information relating to individuals provided to Cleura via the Services, by (or at the direction of) Customer or the controller or by those directly or indirectly allowed to do so by Customer or the controller, such as end-users of a SaaS solution.

A.6 Processing includes the following categories of data subject:

Individuals about whom information is provided to Cleura via the Services by (or at the direction of) Customer or the controller or by those directly or indirectly allowed to do so by Customer or the controller, such as end-users of a SaaS solution.

A.7 Cleura’s processing of this personal data on behalf of the controller may be performed when the DPA commences. The processing has the following duration:

Customer is responsible for implementing controller’s decisions on retention terms and deletion. Customer shall be able to use tools provided as part of the Services to delete personal data, e.g. virtual objects containing personal data. Cleura will delete personal data according to section 11 Erasure and return of personal data.

A.8 The subject of/instructions for the processing:

Cleura’s processing of personal data on behalf of the controller shall be carried out by Cleura performing the following:

Through the Cleura Cloud Management Portal user accounts and API user accounts, Cleura will give Customer the ability to create, manage and delete virtual objects, and to use virtual objects to process personal data. For personal data processed through these virtual objects, Cleura will be a processor on the controller’s behalf.

Virtual objects are data files that contain the necessary format and information to act as a digital representation of a physical server, switch, firewall, load balancer, router, storage volume, container, or database instance. When a virtual object is deployed through a hypervisor, the virtual object will provide the same functionality as the corresponding physical appliance. The virtual objects will be deployed through Cleura’s cloud infrastructure in the services and regions selected by Customer.

By default, Customer is always responsible for the configuration and management of all virtual objects inside Customer’s domain.

Customer can use virtual objects to process personal data. The following virtual objects allow for persistent storage of personal data:

- Servers
- Containers
- Object storage buckets
- Storage volumes
- Database instances

When Customer uses the Cleura Cloud Management Portal user accounts, API user accounts or API endpoints to perform actions affecting virtual objects, Customer is giving instructions which Cleura immediately and automatically executes in its cloud.

Customer instructs Cleura not to interact directly with data inside virtual objects unless specifically instructed to do so and both parties have agreed to this in writing. Unless such an agreement has been made, Cleura will have no knowledge of the information inside the virtual objects. Cleura will still handle them as if they may contain personal data. Due to the nature of this processing and because Cleura is not meant to know the specific personal data being processed, Customer acknowledges that it has a high level of responsibility to make sure the processing is in accordance with this annex.

Customer can manually request assistance from Cleura in the form of service requests to Cleura's customer support, where Customer requests Cleura to perform processing or actions that result in processing. Customer acknowledges that Cleura may not be able to fulfil all manual requests or instructions, and that Cleura shall perform the processing which the parties agree to in writing.

Customer can add custom information to metadata for virtual objects such as object names, notes and tags through the interfaces Cleura provides. Customer acknowledges that these fields are not intended for personal data and that Customer shall not enter personal data into these fields.

Cleura is not obliged to follow instructions that would lead to processing that violates applicable law, including the GDPR and rules in the area of ePrivacy.

A.9 Security of processing

Security of and inside virtual objects

Cleura manages the technical and organisational security measures up to the hypervisor layer. Cleura is thus responsible for the security of the outside of the virtual objects. The specific technical and organisational security measures Cleura applies are listed in the statement of applicability for Cleura's information security management system.

Customer must ensure appropriate technical and organisational security measures are applied inside the virtual objects, regardless of service and region chosen. Customer is responsible for configurations made inside the virtual objects. The nature of the Services provided by Cleura is not intended for Cleura to interact directly with data inside virtual objects, and Cleura is not intended to be responsible for configuring security measures inside virtual objects.

Cleura offers different regions where Customer can deploy virtual objects. Regions are listed on Cleura's website.

Different regions may have different security controls, implementation and assurance levels. The different levels may make the regions suitable for different types of processing. Customer should select appropriate regions based on, inter alia, the types and amounts of personal data intended to be processed, the regulatory requirements applicable and the level of security required by the controller. Customer may use the suggestions below as a starting point when considering the available regions.

Customer shall on an ongoing basis carefully consider its current and potential use of Cleura Public Cloud and assess whether the security of Cleura Compliant Cloud is more appropriate for Customer's use case and situation.

Customer warrants that the measures implemented by Cleura and Customer provide the appropriate level of security required by the controller.

Regions that may be appropriate for small amounts of data

The following regions may be appropriate for processing small amounts of personal data. Examples are single user account information or processing of single e-mail addresses for marketing communication. The data should not be sensitive or special categories of personal data. These regions are not appropriate for massive aggregated quantities of personal data such as databases or archives.

- FRA1 (Public Cloud)
- KNA1 (Public Cloud)
- STO2 (Public Cloud)

And, depending on the applicable regulatory requirements:

- BUF1 (Public Cloud)
- DX1 (Public Cloud)
- TKY1 (Public Cloud)

Regions that may be appropriate for sensitive or large amounts of personal data

The following regions may be appropriate for processing sensitive personal data or large amounts of personal data. For processing of special categories of personal data, Customer should enable additional safeguards. Cleura offers Customer tools for enabling additional encryption of virtual objects. Customer can, of course, add additional encryption of data inside the virtual objects.

- FRA1 (Public Cloud)
- STO2 (Public Cloud)

Regions that may be appropriate for larger amounts of special categories of personal data

In addition to its Public Cloud Service, Cleura has a Compliant Cloud Service which is governed by different terms than the Public Cloud Service. The following regions, in the Compliant Cloud Service, may be appropriate for processing larger amounts of special categories of personal data, or other privacy sensitive data. For an even higher level of security Cleura recommends that Customer enables additional safeguards such as encryption of virtual objects or encryption inside the virtual objects.

- STO1HS (Compliant Cloud)
- STO2HS (Compliant Cloud)

Annex B

Processing of Cleura Cloud Management Portal user accounts, API user accounts and support cases for Customer’s purposes

B.1 Controllership

When the Services allow Customer to use Cleura Cloud Management Portal, API user accounts and to make support cases, Customer is a controller and Cleura is a processor for the processing of personal data described in this Annex B.

The processing described in this annex does not encompass the processing of personal data in virtual objects resulting from the instructions Customer gives *through* the Management Portal and API user accounts. That processing is covered by Annex A.

Furthermore, the processing described in this annex does not encompass the processing of personal data related to Cleura's logging of Customer's use of the Management Portal, API user accounts and API endpoints. That processing is described in Cleura's privacy notice.

B.2 Customer's purposes for processing personal data:

By setting up individual Cleura Cloud Management Portal and API user accounts, Customer can effectively manage its use of the Services by appropriately assigning work and roles to Customer's staff across different user accounts.

At the same time, Customer can trace which staff members have done what when using the Services, which helps Customer ensure accountability and that the correct actions were performed.

Regarding support cases, the purpose is to receive support and assistance from Cleura regarding the Services, and to request execution of manual instructions.

B.3 Cleura's processing of personal data on behalf of the controller shall mainly pertain to (the nature of the processing):

Cleura will give Customer the ability to create, manage, use and delete Cleura Cloud Management Portal user accounts, as well as the API user accounts. Cleura will provide this ability through a web portal with a login interface, from which it is also possible to reset and change passwords.

Regarding support cases, processing is managed through a service portal where Customer can create support cases which Cleura will process and respond to.

B.4 The processing includes the following types of personal data about data subjects:

For Cleura Cloud Management Portal user accounts in the Cleura Cloud management portal:

- User account user name.
- User account user-id.
- User account user e-mail address, used for password resets.
- Password and hashed password.

For Cleura Cloud API accounts:

- API account user name.
- API account user-id.

For support cases:

- Support system account user name.
- Name of each person with a user account.
- Password and hashed password.
- Which Customer each account belongs to, through an account user-id tied to Cleura's back-end system.
- Time each message is sent.
- Contents of support messages sent and received.
- Unique string assigned to each support case.
- Classification of cases into levels of urgency.
- Classification of cases into subject matter.

B.5 Processing includes the following categories of data subject:

Customer's staff, which may include employees, consultants, interns and trainees.

B.6 Cleura's processing of this personal data on behalf of the controller may be performed when the DPA commences. The processing has the following duration:

Customer decides when to create and delete the user accounts. In line with the principle of storage minimisation, Customer shall delete a user account if there is no longer a need to keep it.

For support cases, communication is stored at least for the duration of the Agreement.

In any case, Customer instructs Cleura to delete any remaining user and support accounts after the Services are deactivated, when Cleura does not have its own purpose for keeping them.

B.7 The subject of/instructions for the processing:

Cleura shall provide Customer with access to a web based platform with a self-service interface where Customer can create, manage, use and delete the Management Portal and API user accounts.

Cleura shall provide Customer with access to a web based support platform with a self-service interface where Customer can communicate with Cleura regarding support cases. Cleura shall investigate received cases and respond to them through the support platform in order to help Customer.

Cleura shall secure the processing of the personal data according to its information security management system and associated controls.