Data Processing Agreement

{{ dataprocessor }} as Data Processor

**Data Processing Agreement**

{{ datacontroller.name }}

CVR.no: {{ datacontroller.CVR }}

{{ datacontroller.address\_block() }}

(the “Data Controller”)

and

{{ dataprocessor.name }}

CVR.no: {{ dataprocessor.CVR }}

{{ dataprocessor.address\_block() }}

(the “Data Processor”)

(each a “Party” and collectively the “Parties”).

have agreed on the following Data Processing Agreement (the “DPA”) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subjects.

# Contents:

1 Contents: 3

2 Introduction and scope 4

3 The rights and obligations of the Data Controller 4

4 The Data Processor acts according to instructions 5

5 Confidentiality 5

6 Security of processing 5

7 Use of sub-processors 6

8 Transfer of data to third countries or international organisations 7

9 Assistance to the Data Controller 8

10 Notification of personal data breach 9

11 Erasure and return of data 10

12 Audit and inspection 10

13 The Parties’ agreement on other terms 10

14 Commencement and termination 11

15 Signature 12

16 Data Controller and Data Processor contacts/contact points 13

**Appendices:**

Appendix A - Information about the processing

Appendix B - Authorised sub-processors

Appendix C - Instruction pertaining to the use of personal data

Appendix D - The Parties’ terms of agreement on other subjects

# Introduction and scope

This DPA set out the rights and obligations of the Data Controller and the Data Processor, when the Data Processor is processing personal data on behalf of the Data Controller.

The DPA has been designed to ensure the Parties’ compliance with Article 28(3) 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 (General Data Protection Regulation).

In the context of the provision of services under {{ another\_agreement }} (the “Agreement”), the Data Processor will process personal data on behalf of the Data Controller in accordance with the DPA.

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

Four appendices are attached to the DPA and form an integral part of the DPA.

Appendix A (Information about the processing) contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subjects and duration of the processing.

Appendix B (Authorised sub-processors) contains the Data Controller’s conditions for the Data Processor’s use of sub-processors and a list of sub-processors authorised by the Data Controller.

Appendix C (Instruction pertaining to the use of personal data) contains the Data Controller’s instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Data Processor and how audits of the Data Processor and any sub-processors are to be performed.

Appendix D (The Parties’ terms of agreement on other subjects) contains provisions for other conditions which are not covered by the DPA.

The DPA along with appendices shall be retained in writing, including electronically, by both Parties.

The DPA shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.

Any term not defined in the DPA shall have the meaning set out in the GDPR.

# The rights and obligations of the Data Controller

The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the DPA. Any references to “Member States” made throughout the DPA shall be understood as references to EEA member states.

The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

The Data Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

# The Data Processor acts according to instructions

The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the Data Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the DPA.

The Data Processor shall immediately inform the Data Controller if instructions given by the Data Controller, in the opinion of the Data Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

The Data Processor may postpone the execution of the relevant instruction(s) if, in the opinion of the Data Processor, the instructions contravene the GDPR or the applicable EU or Member State data protection provisions until it is confirmed or changed by the Data Controller’s representative.

# Confidentiality

The Data Processor shall only grant access to the personal data being processed on behalf of the Data Controller to persons under the Data Processor’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.

The Data Processor shall at the request of the Data Controller demonstrate that the concerned persons under the Data Processor’s authority are subject to the abovementioned confidentiality.

# Security of processing

Article 32 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 Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The Data Controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

pseudonymisation and encryption of personal data;

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

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

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

According to Article 32 GDPR, the Data Processor shall also – independently from the Data Controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the Data Controller shall provide the Data Processor with all information necessary to identify and evaluate such risks.

Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller’s obligations pursuant to Articles 32 GDPR, by *inter alia* providing the Data Controller with information concerning the technical and organisational measures already implemented by the Data Processor pursuant to Article 32 GDPR along with all other information necessary for the Data Controller to comply with the Data Controller’s obligation under Article 32 GDPR.

If subsequently – in the assessment of the Data Controller – mitigation of the identified risks require further measures to be implemented by the Data Processor, than those already implemented by the Data Processor pursuant to Article 32 GDPR, the Data Controller shall specify these additional measures to be implemented in Appendix C (Instruction pertaining to the use of personal data).

# Use of sub-processors

The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

{%p if authorisation\_for\_subprocessers == ‘specific\_written\_authorisation’ %}

The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of the DPA without the prior specific written authorisation of the Data Controller.

The Data Processor shall engage sub-processors solely with the specific prior authorisation of the Data Controller. The Data Processor shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the Data Controller can be found in Appendix B (Authorised sub-processors).

{%p else %}

The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

The data processor has the data controller’s general authorisation for the engagement of sub-processors. The data processor shall inform in writing the da-ta controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

{%p endif %}

Where the Data Processor engages a sub-processor for carrying out specific processing activities on behalf of the Data Controller, 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.

The Data Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the Data Processor is subject pursuant to the DPA and the GDPR.

If the sub-processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the sub-processor.

{%p if dataprocesser\_shall\_give\_copy\_to\_datacontroller %}

A copy of such a sub-processor agreement and subsequent amendments shall – at the Data Controller’s request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the Data Controller.

{%p endif %}

{%p if dataprocesser\_agrees\_to\_tpb\_enforcement %}

The Data Processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the Data Processor – the Data Controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the Data Processor, e.g. enabling the Data Controller to instruct the sub-processor to delete or return the personal data.

{%p endif %}

# Transfer of data to third countries or international organisations

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

In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the DPA:

transfer personal data to a data controller or a data processor in a third country or in an international organization

transfer the processing of personal data to a sub-processor in a third country

have the personal data processed by the Data Processor in a third country

The Data Controller’s instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Article 6 of Appendix C (Instruction pertaining to the use of personal data).

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 be relied upon by the Parties as a transfer tool under Chapter V GDPR.

# Assistance to the Data Controller

Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller’s obligations to respond to requests for exercising the data subjects’ rights laid down in Chapter III GDPR.

This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller’s compliance with:

the right to be informed when collecting personal data from the data subjects

the right to be informed when personal data have not been obtained from the data subjects

the right of access by the data subjects

the right to rectification

the right to erasure (‘the right to be forgotten’)

the right to restriction of processing

notification obligation regarding rectification or erasure of personal data or restriction of processing

the right to data portability

the right to object

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

In addition to the Data Processor’s obligation to assist the Data Controller pursuant to Clause 6.3, the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

The Data Controller’s obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, namely the supervisory authority in the country in which the Data Controller is established, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

the Data Controller’s obligation to without undue delay communicate the personal data breach to the data subjects, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

the Data 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);

the Data Controller’s obligation to consult the competent supervisory authority, namely the supervisory authority in the country in which the Data Controller is established, 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 Data Controller to mitigate the risk.

The Parties shall define in Appendix C (Instruction pertaining to the use of personal data) the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required. This applies to the obligations set out in Clause 9.1 and 9.2.

# Notification of personal data breach

In case of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

The Data Processor’s notification to the Data Controller shall, if possible, take place without undue delay after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the Data Controller’s obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

In accordance with Clause 9.2(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the Data Controller’s notification to the competent supervisory authority:

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;

the likely consequences of the personal data breach;

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.

The Parties shall in Appendix D (The Parties’ terms of agreement on other subjects) define all the elements to be provided by the Data Processor when assisting the Data Controller in the notification of a personal data breach to the competent supervisory authority.

# Erasure and return of data

On termination of the provision of personal data processing services, the Data Processor shall subject to the Data Controller’s instruction be under obligation to either (i) delete all personal data processed on behalf of the Data Controller and certify to the Data Controller that it has done so or (ii) return all the personal data to the Data Controller and delete existing copies, unless Union or Member State law requires storage of the personal data.

# Audit and inspection

The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

Procedures applicable to the Data Controller’s audits, including inspections, of the Data Processor and sub-processors are specified in Article 7 and 8 of Appendix C (Instruction pertaining to the use of personal data).

The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller’s and the Data Processor’s facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor’s physical facilities on presentation of appropriate identification.

# The Parties’ agreement on other terms

The Parties may agree other terms concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not directly or indirectly contradict the DPA or prejudice the fundamental rights or freedoms of the data subjects and the protection afforded by the GDPR.

# Commencement and termination

The DPA shall become effective on the date of both Parties’ signature.

Both Parties shall be entitled to require the DPA renegotiated if changes to the law or inexpediency of the DPA should give rise to such renegotiation.

The DPA shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the DPA cannot be terminated unless other terms governing the provision of personal data processing services have been agreed between the Parties.

If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1 and Article 4 of Appendix C (Instruction pertaining to the use of personal data), the DPA may be terminated by written notice by either Party.

# Signature

On behalf of the Data Controller:

|  |  |
| --- | --- |
| Date: |  |
|  |  |
| Name:  Position: |  |

On behalf of the Data Processor:

|  |  |
| --- | --- |
| Date: |  |
|  |  |
| Name:  Position: |  |

# Data Controller and Data Processor contacts/contact points

The Parties may contact each other using the following contacts/contact points:

The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Data Controller contact points:

Name: {{ datacontroller.contact }}

Position: {{ datacontroller.contact.position }}

Telephone: {{ datacontroller.contact.phone\_number }}

E-mail: {{ datacontroller.contact.email }}

Data Processor contact points:

Name: {{ dataprocessor.contact }}

Position: {{ dataprocessor.contact.position }}

Telephone: {{ dataprocessor.contact.phone\_number }}

E-mail: {{ dataprocessor.contact.email }}

In case of a data breach, the following e-mail must be used by the Data Processor:

Name: {{ dataprocessor. databreachcontact }}

Position: {{ dataprocessor. databreachcontact.position }}

Telephone: {{ dataprocessor. databreachcontact.phone\_number }}

E-mail: {{ dataprocessor. databreachcontact.email }}

Appendix A

Information about the processing

**A.1. The purpose of the Data Processor’s processing of personal data on behalf of the Data Controller is:**

{%p for activity in activities %}

**{{ activity.name }}**

{%p if activity.processing\_purpose\_clear %}

The data processor is processing personal data on behalf of the data controller for the purpose of providing the services agreed between the parties under the Agreement.

{%p else %}

{%p for choice, chosen in service\_and\_purpose.items() %}

{% if chosen %}[x] {% else %}[\_] {% endif %} {{ choice }}

{%p if choice == ‘Other purposes’ and chosen %}

{{ activity.other\_purposes }}

{%p endif %}

{%p endfor %}

{%p endif %}

{%p endfor %}

**A.2. The Data Processor’s processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):**

The nature of processing carried out under the Agreement in accordance with this DPA, will involve:

{%p for activity in activities %}

**{{ activity.name }}**

{%p for choice, chosen in activity.processing\_choices.items() %}

{% if chosen %}[x]{% else %}[\_] {% endif %} {{ choice }}

{%p if choice == ‘Other processing types’ and chosen %}

{{ activity.other\_processing\_types }}

{%p endif %}

{%p endfor %}

{%p endfor %}

**A.3. The processing includes the following types of personal data about data subjects:**

The processing will involve processing of the following types of personal data about data subjects:

{%p for activity in activities %}

**{{ activity.name }}**

{%p for choice, chosen in activity.personal\_data\_choices.items() %}

{% if chosen %}[x] {% else %}[\_] {% endif %} {{ choice }}

{%p if choice == ‘Other types of personal data’ and chosen %}

{{ activity.other\_personal\_data\_types }}

{%p endif %}

{%p endfor %}

{%p endfor %}

**A.4. Processing includes the following categories of data subjects:**

The categories of data subjects are the identified or identifiable natural person whose personal data is being processed under the DPA. Personal data about the following categories of data subjects will be processed under the DPA:

{%p for activity in activities %}

**{{ activity.name }}**

{%p for choice, chosen in activity.data\_subjects\_choices.items() %}

{% if chosen %}[x] {% else %}[\_] {% endif %} {{ choice }}

{%p if choice == ‘Other categories’ and chosen %}

{{ activity.other\_categories }}

{%p endif %}

{%p endfor %}

{%p endfor %}

**A.5. The Data Processor’s processing of personal data on behalf of the Data Controller may be performed when the DPA commence. Processing has the following duration:**

The term of this DPA shall continue until the latter of the following; the termination of the Agreement, or the date at which the data processor ceases to process the personal data.

Appendix B

Authorised sub-processors

**B.1. Approved sub-processors**

On commencement of the DPA, the Data Controller authorises the engagement of the following sub-processors:

{%p if subprocessors | length <= 1 %}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **CVR/Company ID.** | **Address** | **Description of Processing** | **Transfer Outside EU/EEA** | **Certification (E.G. ISO27001)** |
| {%tr for item in subprocessors %} |  |  |  |  |  |
| {{ item.name }} | {{ item.cvr }} | {{ item.address }} | {{ item.processing\_description }} | {{ yesno(item.transfer).capitalize() }} | {{ item.certification }} |
| {%tr endfor %} |  |  |  |  |  |

{%p endif %}

{%p if subprocessors | length > 1 %}

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Name** | **CVR/Company ID.** | **Address** | **Description of Processing** | **Transfer Outside EU/EEA** | **Certification (E.G. ISO27001)** | **Processing Activity** |
| {%tr for item in subprocessors %} |  |  |  |  |  |  |
| {{ item.name }} | {{ item.cvr }} | {{ item.address }} | {{ item.processing\_description }} | {{ yesno(item.transfer).capitalize() }} | {{ item.certification }} | {{ item. processing\_activity }} |
| {%tr endfor %} |  |  |  |  |  |  |

{%p endif %}

The Data Controller shall on the commencement of the DPA authorise the use of the abovementioned sub-processors for the processing described for that Party. The Data Processor shall not be entitled – without the Data Controller’s written authorisation in accordance with Clause 7 – to engage a sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing.

**B.2. Prior notice for the authorisation of sub-processors**

If the Data Controller has reasonable grounds to object to the Data Processor’s use of a new sub-processor then the Data Controller shall promptly, but in no case later than fourteen (14) days following the Data Processor’s notification pursuant to Clause 7, provide notice to the Data Processor explaining its objections to the new sub-processor. Should the Data Processor choose to retain the objected-to sub-processor, the Data Processor will notify the Data Controller at least fourteen (14) days before authorising the sub-processor to process personal data and then the Data Controller may upon a ten (10) days’ notice terminate the services affected by the use of the sub-processor and the relevant portion(s) of the Agreement. Upon any termination by the Data Controller pursuant to this Article B.2, the Data Processor shall refund the Data Controller any prepaid fees for the terminated portion(s) of the Agreement that were to be provided after the effective date of termination. This shall be the Data Controller’s sole and exclusive remedy under this Article B.2.

Appendix C

Instruction pertaining to the use of personal data

**C.1. The subject of/instruction for the processing**

The Data Processor’s processing of personal data on behalf of the Data Controller shall be carried out as specifically set out under the Agreement and as a part of providing the agreed services, as specified in Appendix A.

**C.2. Security of processing**

The level of security shall take into account:

Taking into account the nature, scope, context and purposes of processing as set out above, as well as the risks for the rights and freedoms of the data subjects, the following elements have been taken into account when assessing the security of processing:

{%p for activity in activities %}

**{{ activity.name }}**

{%p for choice, chosen in activity.risk\_assessment\_choices.items() %}

{% if chosen %}[x]{% else %}[\_]{% endif %} {{ choice }}

{%p endfor %}

{%p endfor %}

The Data Processor shall as a minimum implement the following measures that have been agreed with the data controller and taking the types of processing with its inherent risks into account:

***Organisational security***

* *The Data Processor has a documented information security policy that addresses how information security is ensured in the Data Processor’s organisation.*
* *The Data Processor maintains and enforces policies on handling data securely and to ensure personal data is processed in accordance with applicable law. The Data Processor takes appropriate steps to ensure that such policies are known to all employees through regular awareness training.*
* *The Data Processor ensures that third party service providers adhere to a minimum set of controls prescribed by the Data Processor and are made subject to confidentiality obligations prior to engagement.*
* *The Data Processor regularly audits third party services and sub-processors based on risk in the processing of personal data.*
* *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing the Data Processor will implement and adhere to the data protection by design principles in all phases of the data and system life-cycle.*

***Physical Security***

* *Sites, including data centres, offices and off-site storage facilities, or locations from where the Data Controller’s data can potentially be accessed, have appropriate physical security controls to protect against unauthorised access.*
* *The data processor ensures secure disposal of data, media, equipment and paper containing personal data in accordance with recognised industry standards.*

***System and Network Security***

* *Networks and devices on which personal data are processed, are protected from unauthorised access or infiltration, both internally and externally.*
* *Network security is maintained by the use of commercially available equipment and industry standard techniques, including conducting periodic external vulnerability scanning and maintaining perimeter defences such as firewalls and intrusion prevention/detection systems.*
* *The infrastructure must be segmented to at least separate production systems from test and development environments.*
* *Anti-virus and anti-malware systems are used on operating systems together with secure configuration. Vendor recommended security patches are applied in a timely fashion for both applications and operating systems.*
* *Updated malware protection must be installed and maintained on all systems that are exposed to malware.*
* *Encryption is used on laptop hard drives, devices and portable media, as required to protect the personal data. All personal data transmitted by the Data Processor must be encrypted while in transit.*
* *Risk assessments are performed and documented using industry accepted methodologies such as Cloud Security Alliance or equivalent, SSAE16, ISO 27001 or other independent framework.*
* *Mobile device management software are used to administer security controls on both corporate supplier and employees’ own devices, which are used for business purposes.*

***Access Management***

* *The Data Processor ensures that the Data Controller’s personal data is only accessed by authorised persons, through the means of access management procedures that ensure access on a least privilege basis and that access is terminated where and when it is appropriate.*
* *The Data Processor must have user administration procedures in place, which define user roles and their privileges and how access is granted, changed and terminated.*
* *The Data Processor must perform regular controls of the assigned rights. The controls must be documented and the documentation must be provided to the Data Controller upon request.*
* *Systems used to process the Data Controller’s personal data is further secured through multiple factor authentication and remote access to data, applications and infrastructure must require two-factor authentication.*

***Logging***

* *All login attempts must be logged in order to detect unauthorized access to personal data.*
* *All access to personal data must be logged and the access log must include the date and time of access, the UserID and the type of access (read, edit, delete, search criteria etc.).*
* *Security logging must be enabled on all network equipment, servers and on all applications including databases and on IT system administrators.*
* *Logs of access to personal data and the use of personal data must be monitored and regularly reviewed by the Data Processor in order to detect unauthorized access to personal data.*
* *The Data Processor must have a documented procedure for how often log files are reviewed and who has performed the control. Documentation must be made available to the Data Controller on request.*

***Back-up***

* *The Data Processor must perform back-up of the personal data processed on behalf of the Data Controller and must have procedures in place to ensure the re-establishing of backed-up data in a timely manner to ensure the availability and access to personal data.*
* *The Data Processor must have a documented procedure for performing backup. Such procedure must identify data retention and data deletion requirements.*
* *The Data Processor must implement procedures to verify backups by successfully re-establishing backed-up data, software and systems at least every 6 months.*
* *Backups must be protected from unauthorized access including destruction and must be encrypted if the back-up contains any personal data where encryption based on a risk assessment is required.*

***Availability***

* *The Data Processor must implement procedures for effective detection, analysis and handling of security events to ensure the availability of personal data.*
* *The Data Processor must implement a documented and tested disaster recovery plan and business continuity strategy covering systems used to process personal data.*
* *Disaster recovery plans and business continuity strategies must be tested and updated regularly, and at least annually, to ensure that they are up to date and effective. Documentation must be made available to the Data Controller upon request.*

**C.3. Assistance to the Data Controller**

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clause 9.1 and 9.2 by implementing the following technical and organisational measures:

The Data Processor has in place policies and procedures to ensure that appropriate aspects of good security practices are enforced so that the Data Processor is able to assist the Data Controller in a timely fashion, including in ensuring that the data subjects’ rights are met.

The Data Processor has established and will maintain procedures and technical features in the IT systems used in the provision of the services that will allow the data processor, upon request from the Data Controller, to (i) identify personal data related to data subjects in order for the Data Controller to accommodate data subject access requests, (ii) rectify or delete personal data recorded and (iii) restrict further processing of personal data.

**C.4. Storage period/erasure procedures**

Personal data is stored for the period of time agreed in the Agreement or as instructed by the Data Controller from time to time after which the personal data is automatically erased by the Data Processor.

Until termination of the Agreement, the Data Controller shall implement, operate and maintain compliant erasure procedures into the services delivered by the Data Processor unless the Data Processor is instructed otherwise in writing and subject to separate payment.

Upon termination of the Agreement, the Data Controller may request retrieval of its personal data from the Data Processor (exclusive of back-ups, if any) during a period of thirty (30) days (“Data Retrieval Period”) following the termination of the Agreement. The Data Processor will provide reasonable assistance for retrieval of the personal data in a readily accessible and commercially reasonable file format. Following the Data Retrieval Period, the Data Processor may delete the personal data without notice.

**C.5. Processing location**

Processing of the personal data under the DPA cannot be performed outside the EU/EEA without the data controller’s prior written authorisation. Currently the processing is performed at the locations specified in Appendix B*.*

**C.6. Instruction on the transfer of personal data to third countries**

The Data Processor and its sub-processor(s) (if any) may transfer personal data processed on behalf of the Data Controller out of the EU/EEA upon a thirty (30) days’ prior written notice to the Data Controller, to the extent the Data Controller does not object to the transfer in writing within such notice period. The Data Processor will comply with any requirements established by any supervisory authority or other government authorities necessary for the granting of approval by such authorities for the transfer of personal data outside of the EU/EEA.

The Data Processor shall ensure the legal basis for the transfer of personal data either by way of (a) the third country being a jurisdiction on the list of the European Commission with jurisdictions that provide an adequate level of data protection, (b) the third country being a party to a certification scheme approved by the European Commission as providing the adequate level of data protection (such as the EU-U.S. and EU-Swiss Privacy Shield) or (c) procuring that the sub-processor enters into the European Commission’s Standard Contractual Clauses for the transfer of personal data to the sub-processor established in third countries. The Data Processor and its sub-processor(s) (if any) will not be entitled to require any amendments to the Commission’s Standard Contractual Clauses. The Data Controller authorises the Data Processor to execute the European Commission’s Standard Contractual Clauses for the transfer of personal data to sub-processors established in third countries on behalf of the Data Controller.

In the event that a legal basis for transfer of personal data as set out in this Article C.6 is found non-compliant with the applicable data protection legislation and is replaced or otherwise no longer considered to be the foundation for a valid legal basis for the transfer of personal data outside of the EU/EEA the Parties will together without undue delay find and execute another legal basis for the transfer of personal data out of the EU/EEA.

**C.7. Procedures for the Data Controller’s audits, including inspections, of the processing of personal data being performed by the Data Processor**

The Data Processor shall keep documentation of the types of personal data and the processing hereof. The documentation shall be available to the Data Controller upon thirty (30) days written notice.

Upon the Data Controller’s written request, the Data Processor will either provide to the Data Controller an audit report covering control of the technical and organisational security measures implemented by the Data Processor which will be prepared by a reputable independent third party that attests to the compliance of the applicable security controls, or complete a security questionnaire submitted by the Data Controller to the Data Processor.

{%p if activity.dataprocessor\_audit == ‘low\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

In addition to the above, the Data Controller or the Data Controller’s representative shall upon at least fourteen (14) days’ notice be entitled to perform a physical inspection of the places, where the processing of personal data is carried out by the Data Processor, including physical facilities as well as systems used for and related to the processing to ascertain the Data Processor’s compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

On entering Data Processors physical premises, including physical facilities as well as systems used for and related to the processing, both Data Controller and the Data Controller’s representative must accept being bound by confidentiality as laid out in Data Processors non-disclosure agreement.

In addition to the planned inspection, the Data Controller may perform an inspection of the Data Processor when the Data Controller deems it required.

The Data Controller’s costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection.

{%p endfor %}

{%p endif %}

{%p if activity.dataprocessor\_audit == ‘medium\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

The Data Processor shall yearly at Data Processor’s expense obtain an ISAE 3000 audit report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The ISAE 3000 audit report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

The Data Controller or the Data Controller’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the Data Processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Data Controller deems it required. The Data Processor is required to set aside necessary resources (mainly time) to assist with the inspection.

On entering Data Processors physical premises, including physical facilities as well as systems used for and related to the processing, both Data Controller and the Data Controller’s representative must accept being bound by confidentiality as laid out in Data Processors non-disclosure agreement.

The Data Controller’s costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection.

{%p endfor %}

{%p endif %}

{%p if activity.dataprocessor\_audit == ‘high\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

The Data Processor shall yearly at Data Processor’s expense obtain an ISAE 3000 audit report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The ISAE 3000 audit report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

To the extent the ISAE 3000 report does not comprise all data processing activities performed by the Data Processor, contain any deviations or is with reservations, the Data Controller is entitled to require an ISRS 4400 report regarding related services, which covers the missing data processing activities, deviations or reservations in the ISAE 3000 report. The Data Processor is responsible for the expenses for obtaining the ISRS 4400 report.

Based on the results of such an audit/inspection, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA

The Data Controller or the Data Controller’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the Data Processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Data Controller deems it required. The Data Processor is required to set aside necessary resources (mainly time) to assist with the inspection.

On entering Data Processors physical premises, including physical facilities as well as systems used for and related to the processing, both Data Controller and the Data Controller’s representative must accept being bound by confidentiality as laid out in Data Processors non-disclosure agreement.

The Data Controller’s costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection.

{%p endfor %}

{%p endif %}

**C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors**

Upon the Data Controller’s written request, the Data Processor will have the sub-processor complete a security questionnaire submitted by the Data Controller to the Data Processor.

{%p if activity.subprocessor\_audit == ‘low\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

In addition to the above, the Data Processor or the Data processor’s representative shall upon at least fourteen (14) days’ notice be entitled to perform a physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processors compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The Data Processor’s and the sub-processor´s costs, if applicable, relating to physical inspection shall not concern the Data Controller - irrespective of whether the Data Controller has initiated and participated in such inspection. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Processor to be able to perform the inspection.

The Data Processor’s and the sub-processor’s costs related to physical supervision/inspection at the sub-processor’s facilities shall not concern the Data Controller – irrespective of whether the Data Controller has initiated and participated in such inspection.

{%p endfor %}

{%p endif %}

{%p if activity.subprocessor\_audit == ‘medium\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

The Data Processor shall yearly at the Data Processor’s expense obtain an ISAE 3000 report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The Data Processor shall make an assessment of the ISAE 3000 report and inform the Data Controller about any deviations, reservations or other conditions which may be of relevance to the protection of the Data Controller’s personal data. The Data Processor shall document its assessment and upon request provide documentation hereof to the Data Controller.

The ISAE 3000 report shall without undue delay be submitted to the Data Controller for information.

Based on the results of such an audit report, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The Data Processor or the Data Processor’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Data Processor (or the Data Controller) deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

The Data Processor’s and the sub-processor’s costs related to physical supervision/inspection at the sub-processor’s facilities shall not concern the Data Controller – irrespective of whether the Data Controller has initiated and participated in such inspection.

{%p endfor %}

{%p endif %}

{%p if activity.subprocessor\_audit == ‘high\_risk’ %}

{%p for activity in activities %}

**{{ activity.name }}**

The Data Processor shall yearly at Data Processor’s expense obtain an ISAE 3000 report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The ISAE 3000 audit report shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

To the extent the ISAE 3000 report does not comprise all data processing activities performed by the Data Processer and sub-processor, contain any deviations or is with reservations, the Data Controller is entitled to require an ISRS 4400 report regarding related services, which covers the missing data processing activities, deviations or reservations in the ISAE 3000 report. The Data Processor is responsible for the expenses for obtaining the ISRS 4400 report.

Based on the results of such an audit/inspection, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA

The Data Processor or the Data Processor’s representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the Data Controller deems it required. The Data Processor is required to set aside necessary resources (mainly time) to assist with the inspection.

In addition to the planned inspection, the Data Processor may perform an inspection of the sub-processor when the Data Processor (or the Data Controller) deems it required.

Documentation for such inspections shall without undue delay be submitted to the Data Controller for information. The Data Controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the Data Controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection pro-visions and the DPA.

The Data Controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the Data Controller deems that the Data Processor’s supervision of the sub-processor has not provided the Data Controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the DPA.

The Data Controller’s participation in an inspection of the sub-processor shall not alter the fact that the Data Processor hereafter continues to bear the full responsibility for the sub-processor’s compliance with the GDPR, the applicable EU or Member State data protection provisions and the DPA.

The Data Processor’s and the sub-processor’s costs related to physical supervision/inspection at the sub-processor’s facilities shall not concern the Data Controller – irrespective of whether the Data Controller has initiated and participated in such inspection.

{%p endfor %}

{%p endif %}

Appendix D

The Parties’ terms of agreement on other subjects

**D.1 Additional obligations of the parties**

The Data Controller is responsible for compliance with all applicable data protection regulations laid down in the applicable data protection legislation, and other mandatory regulations in respect of the personal data provided to the Data Processor in connection with the Agreement.

The Data Controller agrees not to upload or otherwise submit any sensitive and/or critical personal data, unless already specified in Appendix A, section A.3, to the Data Processor in connection with the Agreement without the written consent of the Data Processor.

**D.2 Data Breach Notification**

The notification to the Data Controller from the Data Processor of a personal data breach must

* describe the personal data breach including the categories and number of data subjects concerned, date and time of the incident, summary of the incident that caused the personal data breach, the categories and number of data records concerned, and the nature and the content of the personal data concerned;
* describe the circumstances of the personal data breach (e.g. loss, theft, copying);
* communicate the identity and contact details of the Data Processor’s data protection officer or other contact point where more information can be obtained;
* recommend measures to mitigate the possible adverse effects of the personal data breach;
* describe the measures proposed or taken by the Data Processor and/or the sub-processor, as applicable, to address the personal data breach;
* include any other information reasonably requested by the Data Controller in order to comply with the GDPR and applicable national data protection legislation, including duties of notification and disclosure in relation to public authorities.

**D.3. Liability**

The Data Processor’s total liability to the Data Controller for breach of the data protection obligations set out in this DPA is subject to the same limitations of liability as otherwise applicable in the Agreement.

The Data Controller shall hold the Data Processor, fully and effectively indemnified against any and all claims, expenses, losses and damages or liabilities arising out of or incurred in relation to the Data Controller’s violation of the applicable data protection legislation.

**D.4. Additional services and changes in legislation**

If changes in applicable legislation lead to a substantial increase in the Data Processor’s costs including but not limited to an increase in time consumption, and the increase in costs cannot be distributed over several projects throughout the Data Processor’s organization, the Data Processor shall give the Data Controller reasonable notice about such costs before they incur, and the Data Controller shall fully reimburse the Data Processor for such reasonable and documented costs.

If the Data Controller requires additional services, e.g. by requesting the Data Processor to implement new technical and organizational security measures than those applicable under this DPA, the Data Processor shall give the Data Controller reasonable notice about such costs before they incur, and the Data Controller shall reimburse the Data Processor for such reasonable and documented costs.

**D. 5. Assistance to the Data Controller**

The Data Processor’s assistance to the Data Controller as set out in Clause 9 of the DPA shall be subject to separate payment on a time and material basis.

**D.6. Choice of law and venue**

{%p if dpa\_law\_and\_venue == ‘follow\_agreement’ %}

Any dispute or claim arising out of or in connection with this DPA shall be settled at the Courts and be governed by the laws set out in the Agreement.

{%p else %}

Any dispute or claim arising out of or in connection with this DPA shall be settled at the jurisdictional court of {{ dataprocessor.address.country }} and be governed by the laws of {{ dataprocessor.address.country }}.

{%p endif %}