Standard Contract Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) for the processing of personal data by the processor

between

Customer
(as specified in the Main Agreement)

(the data controller)

and

Supplier
(as specified in the Main Agreement)

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject

Table of contents

2 Preambel

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have 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).

3. In the context of the provision of a unified standard B2B e-commerce platform as described in the agreement between the parties (the "Main Agreement"), the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B 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.

8. Appendix C 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.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

    The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3 Rights and obligations of the data controller

1. 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[1] data protection provisions and the Clauses.

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

[1] References to "Member State" in these provisions shall be construed as references to "EEA Member States"

3. 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.

4 The data processor acts according to instructions

1. 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 Clauses.

2. 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.

5 Confidentiality

1. 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.

2. 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.

6 Security of processing

1. 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:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure 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;

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

2. 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.

3. 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.

4. If subsequently – in the assessment of the data controller – mitigation of the identified risks requires 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.

7 Use of sub-processor

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

2. 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.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 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.

4. 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 Clauses 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 Clauses 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 Clauses and the GDPR.

5. 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.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards 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.

8 Transfer of data to third countries or international organisations

1. 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.

2. 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.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization
    b. transfer the processing of personal data to a sub-processor in a third country
    c. have the personal data processed in by the data processor in a third country

4. 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 Appendix C.6.

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

9 Assistance to the data controller

1. 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 subject's 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:

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

2. 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:

   a. 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, at the place of the data controller's venue, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data 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 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);

   d. the data controller's obligation to consult the competent supervisory authority, at the place of the data controller's venue, 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.

3. The parties shall define in Appendix C 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 foreseen in Clause 9.1. and 9.2.

10 Notification of personal data breach

1. 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.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours 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.

3. 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:

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;

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.

4. The parties shall define in Appendix C 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.

11 Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

   The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

12 Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and 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.

13 The parties' agreement on other terms

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

14 Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

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

3. The Clauses 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 Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. 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 Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature:

   These Clauses shall be considered as an integrated part of the Main Agreement between the parties and is attached to the Main Agreement as an appendix.

   These Clauses shall therefore be considered as entered when entering into the Main Agreement.

15 Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points.

   The parties'contact/contact points are stated in the Main Agreement.

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

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:

The parties have agreed that the data processor shall provide one or more of the following services as further described in the Main Agreement.

The purpose of the processing is to provide a SaaS based unified standard B2B e-commerce platform solution and related services as further described in the Main Agreement.

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 tasks are ordered and defined by the data controller, and the data processor is involved to the extent necessary to ensure correct task definition.

The data processor processes personal data in connection with the provision of SaaS services and implementation services related thereto, as further defined in the parties' Main Agreement.

In specific cases, the processing may include organisation, systematisation, facilitation, temporary storage, filtering, troubleshooting, adaptation or alteration, retrieval, search, use, collation, combination, restriction or erasure of personal data, when necessary, in connection with the performance of the data processor's provision of the services described in the Main Agreement or when necessary to comply with a specific request from the data controller.

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

The data processor shall process the types of personal data that the data controller directly or indirectly gives the data processor access to, which typically includes:

Ordinary categories of personal data cf. article 6 of the General Data Protection, incl. the following types of personal data:

- Personal information (name, job title, e-mail address, phone number, address, login information, user ID, activity logs)
- Commercial information (financial information, sales information, customer information, purchase behaviour)

Special categories of personal data cf. article 9 of the General Data Protection Regulation, incl. the following types of personal data:

- None

Personal data relating to criminal convictions or offences cf. article 10 of the General Data Protection regulation.

- None

National identification numbers cf. article 87 of the General Data Protection Regulation:

- None

A.4. Processing includes the following categories of data subject:

The data processor shall process personal data about the categories of data subjects that the data controller directly or indirectly gives the data processor access to, which typically includes:

- Customers (B2B buyers)
- Employees of customers
- Supplier representatives
- Website users
- Administrators
- End users of the platform
- Prospects / leads
- Company employees (name, email, phone number, login information)

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

These Clauses shall be effective for the duration of the provision of the services in accordance with the Main Agreement and shall terminate automatically when the data processor no longer processes personal data on behalf of the data controller as part of the services.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	Reg. No.	ADRESS	DESCRIPTION OF PROCESSING	TRANSFER TO THIRD COUNTRIES AND LEGAL BASIS	PROVISION OF SERVICES ON STANDARD TERMS AND CONDITIONS
Microsoft Ireland Operations Ltd. (Microsoft Azure)	IE8256796U	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	Cloud infrastructure hosting, stoage, backup and related support services. Customer data is hosted in EU data centres.	No transfer to third countries for primary hosting. Any incidental transfers (e.g., support) subject to EU-U.S. Data Privacy Framework (DPF) and/or Standard Contractual Clauses (SCCs) where applicable.	https://www.microsoft.com/licensing/terms/productoffering/MicrosoftAzure https://aka.ms/DPA
KeyCDN (proinity LLC)	CHE-245.534.798	Rebgasse 28, 4058 Basel, Switzerland	Content Delivery Network (CDN), caching and global edge delivery of static assets	Yes – global edge delivery may involve transfers outside the EU/EEA. Transfer basis: applicable safeguards under GDPR (including SCCs where required).	Yes – https://www.keycdn.com/terms
Twilio SendGrid, Inc.	46-2846492	1801 California Street, Suite 500, Denver, CO 80202, USA	Transactional email delivery and related analytics	Yes. Transfer basis: EU-U.S. Data Privacy Framework (DPF) and/or Standard Contractual Clauses (SCCs)	Yes – https://www.twilio.com/en-us/legal/tos

The data controller shall on the commencement of the Clauses 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 explicit written authorisation – 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

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than 30 days before the addition or replacement is to take effect, in so far this is possible. If the data controller has any objections to such changes, the data controller shall notify the data processor thereof without undue delay before such change is to take effect. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such refusal.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice or immediately. In such situations, the data processor will notify the data controller of such change as soon as possible.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed services. Such non-performance cannot be ascribed to the data

processor's breach. The data processor will maintain its claim for payment for such services, regardless of if they cannot be provided to the data controller.

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 in accordance with the Main Agreement between the data controller and the data processor.

The data processor's processing of personal data on behalf of the data controller is carried out by the data processor performing the following:

Provision of services in accordance with the Main Agreement entered into between the parties.

C.2. Security of processing

The level of security must reflect the specific services agreed in the Main Agreement.

The data processor is then entitled and obliged to make decisions on which technical and organisational security measures to implement in order to establish the necessary (and agreed) security level.

The data processor shall implement appropriate security measures to protect the personal data provided against accidental or unlawful destruction, loss, alteration, unavailability, unauthorised disclosure of or access to the personal data. The data processor may change the implemented security measures on an ongoing basis, however, changes in security measures must never lead to a deterioration of the agreed security level.

In assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

C.2.1. Organizational security

The data processor has a documented information security policy that addresses how information security is embedded and implemented in the data processor's organization.

The data processor maintains and enforces policies for the secure handling of information and for ensuring that 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 by conducting regular training.

The data processor ensures that third party service providers comply with a minimum set of controls prescribed by the data processor and are subject to confidentiality obligations prior to their use.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing in question, the data processor will implement and observe the principles of data protection by design at all stages of the data and system life cycle.

C.2.2. Physical security

The data processor primarily hosts and processes personal data in secure cloud environments provided by its authorized sub-processors (e.g., Microsoft Azure), which are responsible for the physical security of the data centers in accordance with recognized industry standards.

Access by the data processor's personnel to systems containing personal data is performed remotely via secured network connections, including the use of corporate VPN and authenticated access controls. The data processor maintains policies and procedures designed to limit access to authorized personnel on a need-to-know basis.

The data processor implements reasonable organizational and technical safeguards appropriate to its operating model to reduce the risk of unauthorized access, loss, or disclosure of personal data.

C.2.3. System and network security

The data processor shall ensure that networks and devices on which personal data are processed are protected against unauthorized access or infiltration, both internally and externally.

Network security is maintained through the use of commercially available equipment and industry standard techniques, including performing periodic external vulnerability scanning and maintaining perimeter defences such as firewalls and intrusion protection and detection systems.

The data processor ensures that the infrastructure is at least segmented into separate production systems and away from test and development environments.

The data processor maintains security measures appropriate to its cloud-native architecture. Container images and underlying infrastructure components are regularly updated with security patches in a timely manner.

The data processor utilizes vulnerability and malware protection mechanisms provided by the cloud environment and container ecosystem where applicable and ensures that supported soft-ware components are kept up to date based on vendor security recommendations.

Risk assessments are performed on a periodic basis using industry-recognised risk management practices appropriate to the nature and scale of the services.

C.2.4. Access management

The data processor shall ensure that the data controller's personal data is accessed only by authorised persons using access management procedures that ensure access on a least privilege basis and that access is terminated where and when appropriate.

The data processor must have user management procedures in place that define user roles and their privileges and how access is granted, modified, and terminated.

Systems used to process the data controller's personal data shall be further secured through multi-factor authentication and remote access to data, programmes and infrastructure shall have at least two-factor authentication.

C.2.5. Backup

The data processor shall perform backups of the personal data processed on behalf of the data controller and shall have procedures in place to ensure the restoration of backed-up data in a timely manner to ensure availability and access to personal data.

Backups must be protected against unauthorised access, including destruction, and must be encrypted if the backup contains personal data where encryption based on a risk assessment is required.

C.2.6. Accessibility

The data processor shall implement procedures to effectively detect, analyze and manage security incidents to ensure the availability of personal data.

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:

At the specific request of the data controller, the data processor shall, taking into account the nature of the processing, assist the data controller as far as possible by appropriate technical and organizational measures in compliance with the data controller's obligation to respond to requests for data subjects' rights as stated in the data protection regulation.

If a data subject submits a request for the exercise of his or her rights to the data processor, the data processor shall notify the data controller hereof without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor shall, upon specific request, assist the data controller in ensuring compliance with the data controller's obligations in relation to:

- Implementation of appropriate technical and organizational measures.
- Notification of personal data breach to the supervisory authority.
- Notification of personal data breach to the data subject.
- Conducting impact assessments.
- Prior consultations with the supervisory authority.

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1.

C.5. Processing location

The processing of personal data takes place at the data processors and sub-processor's current and any future locations, including locations under their and their employees' control. In addition, the processing of personal data may take place from the data controller's locations or at a location designated by the data controller.

Sub-processor means current sub-processors and any additions or replacements, considering the conditions for the data controller's authorisation of the sub-processor as set out in Clause 7 and Annex B of the Clauses.

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

The data processor shall only transfer personal data to countries outside the EU or EEA (a "Third Country") or international organization as described below.

C.6.1. General approval of transfer of personal data to secure Third Countries
With the Clauses, the data controller provides a general and prior approval (instruction) for the data processor to transfer personal data to Third Countries if the European Commission has determined that the Third Country, the relevant area, or the relevant sector has a sufficient level of protection.

The data controller also gives by the Clauses its general and prior authorisation (instruction) for the data processor to transfer personal data to organisations in the United States, that are certified under the EU-U.S. Data Privacy Framework ("DPF").

C.6.2. Approval of transfer to specific recipients of personal data in Third Countries subject to appropriate safeguards
The data controller instructs the data processor to transfer personal data to Third Countries, when necessary, in order for the data processor to deliver the service in accordance with the Main Agreement, including by using the listed sub-processors transferring personal data to Third Countries as described in the Main Agreement cf. Appendix B.1. Furthermore, the data processor shall be entitled to transfer personal data to Third Countries if the data controller's acts result in such a transfer.

The data processor is entitled to secure the necessary transfer basis, for example by using the Standard Contractual Clauses and thereby enter into the Standard Contractual Clauses with the relevant sub-processor. The data controller shall in so far as necessary assist the data processor on securing the transfer basis, including for example the Standard Contractual Clauses.

In case the European Commission completes new Standard Contractual Clauses subsequent to the formation of the original Standard Contractual Clauses, the data processor is authorized to renew, update and/or use the Standard Contractual Clauses in force from time to time.

The content of these Clauses shall not be deemed to change the content of such safeguards, incl. the Standard Contractual Clauses.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a Third Country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

In accordance with Article 24 and 28, the data controller has the right and the obligation to carry out audits with the data processor's processing of personal data on behalf of the data controller. The data controller's implementation of supervision of the data processor can be done by the data controller performing one of the following actions:

C.7.1. Self-auditing

The data controller may ask questions to the data processor and, upon request, gain access to a number of documents for the purpose of conducting self-monitoring, including

- Description of physical and organisational security at the data processor.
- Risk assessment - of shared infrastructure (firewall, backup, etc.).
- IT security policy.
- Contingency plans at the data processor.

C.7.2. Written supervision and physical inspection
Audits shall primarily be conducted through written reviews and remote assessments.

Given the cloud-native and remote operating model of the data processor, physical inspections shall be limited to situations where the data controller demonstrates a reasonable and substanti-ated need, and where such inspection is relevant to the processing of personal data.

The data processor may satisfy audit requirements by providing relevant third-party certifications, audit reports, and security documentation relating to its cloud service providers and infrastructure.

Any audit shall be conducted in a manner that does not unreasonably interfere with the data pro-cessor's business operations or compromise the security or confidentiality of other customers
Procedure and reporting for written supervision or physical inspection:

- The data controller shall contact the data processor by e-mail to the data processor's contact person with a request to carry out an audit and/or inspection.
- In the case of written audits, the data controller shall inform the data processor of this without undue delay.
- In the case of physical audits and/or inspections, the data controller shall agree the date of the audit and/or inspection in advance with the data processor.
- The data processor shall confirm receipt and provide the final date for the realisation of the audit and/or inspection.
- The performance of the audit and/or inspection takes place.
- The data controller prepares a report, which is subsequently forwarded to the data processor.
- The data processor reviews the draft report and comments on any observations made by the data controller (may be repeated several times).
- The final report is concluded by the data controller.
- The audit is finalised.

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

The data processor regularly audits its sub-processors using a risk-based approach based on the best practices for such audits generally applied from time to time. Such may include review of audit reports, use of questionnaires and other appropriate means.

Appendix D The parties' terms of agreement on other subjects

D.1. In general

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the regulation of other matters and special regulation as specified in this Appendix D.

In the event of any discrepancy between the Clauses and Appendix D, Appendix D shall prevail.

The Clauses shall take precedence over any corresponding regulation in service agreements between the parties regarding the part of the data processor's activities and responsibilities relating to data processing in the Clauses. The performance of all other activities relating to the provision of agreed services is subject to the other parts of the Main Agreement.

D.2. Consequences of the data controller's unlawful instructions

The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller.

If the data controller's instruction is considered as unlawful according to the data processor's reasonable evaluation the data processor is able to end further processing than storage until the data controller gives supplementary instruction on whether the processed personal data once again can be processed legally or if the personal data shall be handed over or deleted. The data processor's end of processing in such situations cannot lead to breach of these Clauses or the parties Main Agreement.

The data processor is not liable for any claims arising from the data processor's acts or omissions to the extent such acts or omissions are a direct data processing activity exercised in accordance with the data controller's instructions and if the data processor is held liable or sanctioned the data controller shall hold the data processor harmless.

D.3. Implementation of other security measures

The data processor is entitled to implement and maintain other security measures than what has been specified in the Clauses and Appendix C.2, however, provided that such other security measures as a minimum provide the same level of security as the described security measures.

D.4. Use of sub-processors supplying on standard terms

Regardless of Clause 7 it is emphasized that if the data processor uses a sub-processor, who provides services on its own terms, which the data processor cannot deviate from, the sub-processor's terms for such processing performed by such sub-processor will apply. If processing is subject to a sub-processor's terms, this will be specified via the list of sub-processors set out in the Appendix B.1, and such standard terms will be forwarded to the data controller at the data controller's request.

With these Clauses, the data controller accepts and instructs that such specific processing activities are based on the sub-processor's terms.

D.5. Compensation for the data processor's assistance and services

The data processor is entitled to receive reasonable payment for time spent as well as other direct costs incurred by the data processor relating to assistance and services provided by the data processor to the data controller. Such assistance and services may include but is not limited to assistance and service described in Clause 9, 10, 12, C.3 and C.7, changes to the instruction, cooperation with supervisory authorities etc. The data processor will without payment and within reasonable limits, answer specific supervisory questions that specifically relate to the processing carried out by the data processor.

The compensation is calculated on the basis of the time spent and the agreed hourly rates in the Main Agreement regarding the data processor's provision of services to the data controller, and if no hourly rates have been agreed on, the data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

If the data processor's assistance and/or service leads to claims for increased security measures to be observed in relation to agreement regarding the data processor's provision of services to the data controller and Appendix C, the data processor will, as far as possible, implement such additional security measures pursuant to further agreement with the data controller, provided that the data processor receives payment for such work. The data processor shall furthermore be entitled to receive payment for the implementation of other security measures if the data processor's ongoing evaluations leads to increased requirements for such security measures compared to the Clauses regarding the data processor's provision of services to the data controller. The data processor will introduce and implement such additional security measures pursuant to further agreement with the data controller.

Regardless of the above a party does not have the right to claim compensation for assistance, service or implementation of changes to the extent where such assistance or changes are a direct consequence of the party's own breach of these Clauses.

D.6. Limitation of liability

The limitation of liability in the Main Agreement applies to the data processor's processing of the personal data under these Clauses, including with regard to art. 82 of the General Data Protection Regulation.

D.7. Claims from data subjects

Each party is responsible and liable for claims arising from the data subjects in accordance with article 82 of the General Data Protection Regulation. In relation to claims between the data controller and the data processor in consequence of claims from the data subjects the limitation of liability in the Main Agreement shall apply as described in section D.7. A data controller's claim against the data processor cannot exceed the cap in the Main Agreement.

Furthermore, the data controller shall hold the data processor harmless for claims from the data controller's data subjects, which may be made towards the data processor but exceeds the cap just like allocation of responsibility and liability between the parties in general takes places in accordance with article 82 of the General Data Protection Regulation as described above.