Data Processing Agreement (DPA)

Structure

This DPA is structured as follows:

Section	Content
Section A – Key Terms	The key variables that apply to the DPA are defined in Section A.
Section B – Legal Terms	Sets out the general legal terms applicable to the processing.
Section C – TOMs	The applicable technical and organizational measures.

Section A – Key Terms

Variable	Value
Controller(s)	Customer, as defined in cosmos' General Terms & Conditions
Processor(s)	**cosmos GmbH** Dolivostraße 17, 64293 Darmstadt, Germany (together with the Controller(s) the "**Parties**")
Processing purpose	Processing in the context of the cosmos' General Terms and conditions, signed between the Parties (the "**Base Agreement**")
Duration of processing	As long as required for the Base Agreement
Categories of data subjects	• Consultants • Contractors • Customers • Freelancers • Potential clients • Suppliers
Categories of personal data	• Banking and financial data (credit card number, IBAN) • Contact data (email, phone) • IP address, device type • Name, surname
Place of storage & processing	At the business locations of the Processor and Sub-Processors.
On-premise audits	No
Sub-processors	Sub-processors are listed in the Annex to this DPA.
Transfer outside of EU/EEA/Switzerland	Only allowed to countries where the Processor or an approved Sub-processor is registered.

The variables defined in Section A serve as definitions in Section B.

Section B – Legal Terms

1 Purpose and scope

a) The purpose of this Data Processing Agreement (the "DPA") is to ensure compliance with Article 28(3) and (4) of the EU General Data Protection Regulation ("GDPR"), Article 28 of the UK General Data Protection Regulation ("UK GDPR") and Article 9 of the Swiss Federal Act on Data Protection ("FADP"), with respect to each law only if and to the extent applicable to the respective processing activity.

b) This DPA applies with respect to the processing of personal data as specified in Section A.

2 Interpretation

a) Where this DPA uses the terms defined in the GDPR, UK GDPR or the FADP, as applicable, those terms shall have the same meaning as in that law.

b) This DPA shall be read and interpreted in the light of the provisions of the GDPR, UK GDPR and the FADP, as applicable.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR, UK GDPR or the FADP, as applicable, or prejudices the fundamental rights or freedoms of the data subjects.

3 Hierarchy

In the event of a conflict between this DPA and the provisions of any other agreement between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail, except where explicitly agreed otherwise in text form.

4 Description of processing(s)

The details of the processing operations, and in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the data controller, are specified in Section A.

5 Obligations of the Parties

5.1 General

a) The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union, Member State or Swiss law to which the processor

is subject. Such instructions are specified in Section A. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the data controller throughout the duration of the processing of personal data. Such instructions shall always be documented.

b) The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, infringe applicable Union, Member State or Swiss data protection provisions.

5.2 Purpose limitation

The data processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Section A.

5.3 Erasure or return of data

a) Processing by the data processor shall only take place for the duration specified in Section A.

b) Upon termination of the provision of personal data processing services or termination pursuant to Clause 8, the data processor shall delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so and delete existing copies unless Union, Member State or Swiss law requires storage of the personal data.

5.4 Security of processing

a) The data processor shall implement the technical and organizational measures specified in Section C to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (personal data breach), in accordance with Art. 5, Art. 28, para 3. lit c, and Art. 32 GDPR and Art 8 FADP. In assessing the appropriate level of security, they shall in particular take due account of the risks involved in the processing, the nature of the personal data and the nature, scope, context and purposes of processing.

b) In the event of a personal data breach concerning data processed by the data processor, it shall notify the data controller without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information concerning the personal data breach can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and data records concerned), its likely consequences and the measures taken or proposed to be taken to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all information at the same

time, the initial notification shall contain the information then available and further information shall be provided as it becomes available without undue delay.

c) The data processor shall cooperate in good faith with and assist the data controller in any way necessary to enable the data controller to notify, where relevant, the competent data protection authority and the affected data subjects, taking into account the nature of processing and the information available to the data processor.

d) The data processor shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. The data processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

e) If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (special categories of data), the data processor shall apply specific restrictions and/or additional safeguards as reasonably required by the data controller.

5.5 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with this DPA.

b) The data processor shall deal promptly and properly with all reasonable inquiries from the data controller that relate to the processing under this DPA.

c) The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations set out in this DPA and that are stemming directly from the GDPR or the FADP and at the data controller's request, allow for and contribute to reviews of data files and documentation or of audits of the processing activities covered by these Clauses, in particular if there are indications of non-compliance.

d) The data controller may choose to conduct the audit by itself, to mandate, at its own cost, an independent auditor or to rely on an independent audit mandated by the data processor. Where the data processor mandates an audit, it has to bear the costs of the independent auditor. The data controller's audit, access, and inspection rights under this Clause are limited to the data processor's records only (including inter-alia the registers of personal data processing activities, the registers of recipients of personal data) and does not apply to Processor's physical premises. Any audit and request for information shall be limited to information necessary for the purposes of

this DPA and shall give due regard to the data processor's confidentiality obligations and legitimate interest to protect business secrets.

e) The data processor and data controller shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority on request if and to the extent required by the GDPR or the FADP, as applicable.

5.6 Use of Sub-processors

a) The data processor has the data controller's general authorization for the engagement of sub-processors. The list of sub-processors the data processor can be found in Section A. The data processor shall inform in text form the data controller of any intended changes of that list through the addition or replacement of sub-processors at least 15 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). Such objection shall not be unreasonable raised. The Parties shall keep the list up to date.

b) Where the data processor engages a sub-processor for carrying out specific processing activities (on behalf of the data controller), it shall do so by way of a contract which imposes on the sub-processor the same obligations as the ones imposed on the data processor under this DPA. The data processor shall ensure that the sub-processor complies with the obligations to which the data processor is subject pursuant to this DPA, Art. 28 para 2-4 of the GDPR and Art. 9 para 3 of the FADP.

c) The data processor shall provide, at the data controller's request, a copy of such a sub-processor agreement and subsequent amendments to the data controller.

d) The data processor shall remain fully responsible to the data controller for the performance of the sub-processor's obligations under its contract with the data processor. The data processor shall notify the data controller of any failure by the sub-processor to fulfil its obligations under that contract.

5.7 International transfers

a) Any transfer of data to a "Third Country" (any country outside of the EU/EEA and Switzerland) or an international organization by the data processor shall be undertaken only if authorized in accordance with Section A and shall take place in compliance with Chapter V of the GDPR and Section 2 of the FADP, as applicable.

b) The data controller agrees that where the data processor engages a sub-processor in accordance with Clause 5.6 for carrying out specific processing activities (on behalf of the data controller) in a Third Country and those processing activities involve transfer of personal data within the meaning

of the GDPR or the FADP, as applicable, the processor and the sub-processor may use standard contractual clauses adopted by the Commission on the basis of Article 46(2) of the GDPR in order to comply with the requirements of Chapter V of the GDPR, provided the conditions for the use of those clauses are met and provided that an internal assessment concluded that such transfer meets the level of data protection of the GDPR and the FADP.

6 Data Subject Rights

a) The data processor shall promptly notify the data controller about any request received directly from the data subject. It shall not respond to that request itself, unless and until it has been authorized to do so by the data controller.

b) The data processor shall assist the data controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights in accordance with Chapter III of the GDPR and Chapter IV of the FADP, namely:

   1) the right to be informed when personal data are collected from the data subject,
   2) the right to be informed when personal data have not been obtained from the data subject,
   3) the right of access by the data subject,
   4) the right to rectification,
   5) the right to erasure ('the right to be forgotten'),
   6) the right to restriction of processing,
   7) the notification obligation rectification or erasure of personal data or restriction of processing,
   8) the right to data portability,
   9) the right to object,
   10) the right not to be subject to a decision based solely on automated processing, including profiling,
   11) the right to withdraw consent.

c) The data processor shall assist the data controller in case a data subject has lodged a complaint to the competent supervisory authority that concerns data processed on the basis of this DPA.

d) In addition to the data processor's obligation to assist the data controller pursuant to Clause 6(b), the data processor shall furthermore assist the data controller in ensuring compliance with the following obligations, taking into account the nature of the processing and the information available to the data processor:

1) The obligation to notify a personal data breach to the competent supervisory authority without undue delay after having become aware of it, (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons), in accordance with Art. 33 of the GDPR and Art. 24 para. 1-3 of the FADP;

2) the obligation to communicate without undue delay 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, in accordance with Art. 34 of the GDPR and Art. 24 para. 3 of the FADP;

3) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in accordance with Art. 35 of the GDPR and Art. 22 of the FADP;

4) the obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk, in accordance with Art. 36 of the GDPR and Art. 23 of the FADP.

e) The Parties shall set out in Section C the appropriate technical and organizational measures by which the data processor is required to assist the data controller in the application of this Clause as well as the scope and the extent of the assistance required.

7 Notification of personal data breaches

a) In the event of a personal data breach, the data processor shall cooperate in good faith with and assist the data controller in any way necessary for the data controller to comply with its obligations under Articles 33 and 34 of the GDPR and Article 24 of the FADP, as applicable, taking into account the nature of processing and the information available to the processor.

b) The data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, where relevant. The data processor shall be required to assist in obtaining in particular the following information which, pursuant to Article 33(3) of the GDPR or Article 24 para.2 of the FADP, as applicable, shall be stated in the data controller's notification:

1) 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;

2) the likely consequences of the personal data breach;

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

8 Termination

a) Without prejudice to any provisions of the GDPR or the FADP, as applicable, in the event that the data processor is in breach of its obligations under this DPA, the data controller may instruct the data processor to temporarily suspend the processing of personal data until the latter complies with this DPA or the contract is terminated. The data processor shall promptly inform the data controller in case it is unable to comply with this DPA, for whatever reason.

b) The data controller shall be entitled to terminate this DPA where:

1) the processing of personal data by the data processor has been temporarily suspended by the data controller pursuant to point (a), data processor's breach is material, and compliance with this DPA is not restored within a reasonable time and in any event within one month;

2) the data processor is in substantial or persistent breach of this DPA or its obligations under the GDPR or the FADP, as applicable, and such breach cannot be reasonably expected to be remedied;

3) the data processor fails to comply with a binding decision of a competent court or the competent supervisory authority regarding its obligations under this DPA or under the GDPR or the FADP, as applicable.

c) This Agreement shall remain in full force and effect so long as the Base Agreement remains in effect. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Base Agreement in order to protect Personal Data shall remain in full force and effect.

Section C – TOMs

Description of the technical and organizational security measures implemented by the data processor(s):

1 Organizational security measures

1.1 Security Management

a) Security policy and procedures: The data processor has a documented security policy with regard to the processing of personal data.

b) Roles and responsibilities:

   1) Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.

   2) During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand-over procedures is clearly defined.

c) Access Control Policy: Specific access control rights are allocated to each role involved in the processing of personal data, following the need-to-know principle.

d) Resource/asset management: The data processor has a register of the IT resources used for the processing of personal data (hardware, software, and network). A specific person is assigned the task of maintaining and updating the register (e.g. IT officer).

1.2 Incident response and business continuity

a) Incidents handling / Personal data breaches:

   1) An incident response plan is defined to ensure effective and orderly response to incidents pertaining personal data.

   2) The data processor will report without undue delay to the controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any personal data.

b) Business continuity: The data processor has established the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).

1.3 Human resources

a) Confidentiality of personnel: The data processor ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.

b) Training: The data processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.

2 Technical security measures

2.1 Access control and authentication

a) An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing, and deleting user accounts.

b) The use of common user accounts is avoided. In cases where this is necessary, it is ensured that all users of the common account have the same roles and responsibilities.

c) When granting access or assigning user roles, the “need-to-know principle” shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the Processor’s processing purposes.

d) Where authentication mechanisms are based on passwords, the data processor requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability.

e) The authentication credentials (such as user ID and password) shall never be transmitted unprotected over the network.

2.2 Logging and monitoring

Log files are activated for each system/application used for the processing of personal data. They include all types of access to data (view, modification, deletion).

2.3 Security of data at rest

a) Server/Database security

1) Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.

2) Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.

b) Workstation security:

1) Anti-virus applications and detection signatures are configured on a regular basis..

2) Critical security updates released by the operating system developer are installed regularly.

2.4 Network/Communication security

a) Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.

b) Traffic to and from the IT system is monitored and controlled through firewalls and intrusion detection systems.

2.5 Back-ups

a) Backup and data restore procedures are defined, documented, and clearly linked to roles and responsibilities.

b) Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.

c) Execution of backups is monitored to ensure completeness.

2.6 Mobile/Portable devices

a) Mobile and portable device management procedures are defined and documented establishing clear rules for their proper use.

b) Mobile devices that are allowed to access the information system are pre-registered and pre-authorized.

2.7 Application lifecycle security

During the development lifecycle, best practice, state of the art and well acknowledged secure development practices or standards are followed.

2.8 Data deletion/disposal

a) Software-based overwriting will be performed on media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction will be performed.

b) Shredding of paper and portable media used to store personal data is carried out.

2.9 Physical security

The physical perimeter of the IT system infrastructure is not accessible by non-authorized personnel. Appropriate technical measures (e.g. intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g. security guard) shall be set in place to protect security areas and their access points against entry by unauthorized persons.

Annex: List of Sub-Processors

Company	Tool	Purpose	Location
Intercom R&D Unlimited Company	Intercom	Customer support	Ireland (EU)
HubSpot Germany GmbH	Hubspot	E-mail communication	Germany (EU)
Stripe Payments Europe, Limited	Stripe	Payment processing	Germany (EU)
IONOS Cloud Inc.	IONOS Cloud	Cloud and hosting	Germany (EU)