

This Data Processing Addendum (DPA) supplements the existing Agreement between ILIBRIS BVBA (hereafter defined as Skyscrapers) and its customers (hereafter defined as Customer) with regards to the processing of Customer Data under the GDPR. Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in the section Definitions of this DPA.

Skyscrapers and Customer may be referred to individually as a Party and collectively as the Parties.

1. Definitions

Agreement

The combination of the Order Approval, Service Terms & Conditions and any other written or electronic agreements between the Customer and Skyscrapers that define what Services are provided to the Customer by Skyscrapers.

Applicable Law

The relevant European Union or Member State data protection and privacy law applicable to the Processing of Personal Data. This includes, to the extent applicable, any other relevant regulations, binding guidelines, policies, and instructions of any governmental authority and any amendments, replacements, updates or later versions thereof.

Customer Applications

The software that Customer owns and deploys on Cloud Infrastructure managed by Skyscrapers as part of Services.

Cloud Infrastructure

Computing infrastructure (compute, storage, networking, etc) sourced from a third party either directly by the Customer or through Skyscrapers as part of Services, on which Skyscrapers performs Services and may Process Customer Data.

Customer Data

Means the Personal Data of Data Subjects collected by the Customer that is uploaded to and stored on Cloud Infrastructure that, if part of the Agreement, is managed by Skyscrapers. The Customer controls, for example through Customer Applications, the method and location of storage within the limits of provisioned Cloud Infrastructure.

GDPR

“GDPR” means 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). We carry over terms from the GDPR including the meaning given to them there, such as:



- Data Controller
- Data Processing
- Data Processor
- Data Subject
- Local Data Protection Authority
- Personal Data
- Personal Data Breach
- Sub-Processor
- Subject Matter

Personnel

All people on the payroll of Skyscrapers, either through an employee contract or through an independent-contractor contract (self-employed contractors), that act as individually identifiable people within the Skyscrapers team.

Security Incident

Means breach of Cloud Infrastructure and/or any Security Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data (a "Personal Data Breach" as defined by GDPR).

Services

Services provided by Skyscrapers to the Customer as defined in the Agreement. This may include but is not limited to:

- Cloud Infrastructure (if sourced through Skyscrapers)
- Operational management of Cloud Infrastructure
- Specific engineering and manipulation of Cloud Infrastructure per the instructions of the Customer

2. Data processing

2.1. Scope and Roles

This DPA applies when Customer Data is processed by Skyscrapers in the context of an Agreement. In this context, Skyscrapers will act as Data Processor on behalf of the Customer who may act either as Data Controller or Data Processor with respect to Customer Data.

2.2. Details of Data Processing

1. **Subject matter:** The Subject Matter of the Data Processing under this DPA is the Customer Data that Skyscrapers may process during the execution of the Agreement for the benefit of the Customer.
2. **Duration:** The duration of the Data Processing under this DPA is for the duration of the Agreement.
3. **Purpose:** The purpose of the Processing under this DPA is any Processing of Customer Data needed to fulfil the Services.
4. **Nature:** The nature of the Processing is that Skyscrapers will Process Customer Data, typically in



highly automated and bulk form, for the fulfilment of the Services and per the instructions of the Customer. This processing will be performed in the context of systems administration. Some examples: data migration in the context of upgrading/modification of Cloud Infrastructure, troubleshooting of Cloud Infrastructure where access to Customer Data is needed, etc.

5. **Type of personal data:** Customer Data as solely determined by the Customer.
6. **Categories of data subjects:** The Customer explicitly controls the categories. This may include Customer's: customers, employees, suppliers, data of customers, etc.

3. Customer Instructions

1. The parties agree that this DPA and the Agreement constitute Customer's documented instructions regarding Skyscrapers' processing of Customer Data (Documented Instructions).
2. Skyscrapers will process Customer Data only in accordance with Documented Instructions.
3. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Skyscrapers and Customer (including any additional fees), have to be reasonable and not be in conflict with any Applicable Law.

4. Confidentiality

1. Skyscrapers will not access or use, or disclose to any third party, any Customer Data, except as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body.
2. If a government body sends Skyscrapers a demand for Customer Data, Skyscrapers will attempt to redirect the governmental body to request that data directly from Customer. The latter implies sharing the contact details of the Customer to the governmental body. If compelled to disclose Customer Data to a government body and Skyscrapers is not legally prohibited to do so then Skyscrapers will give Customer reasonable notice of the demand.
3. Skyscrapers will restrict its Personnel from processing Customer Data without authorisation by Skyscrapers and only for the purposes of performing activities related to fulfilling the Services.
4. Skyscrapers imposes appropriate contractual obligations upon its Personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Security of Data Processing

5.1. Skyscrapers security measures

1. Skyscrapers has implemented, will maintain and continuously evolve the technical and organisational measures to maximise the security of the Processing of Customer Data while performing the duties part of Services within the scope of the Agreement.
2. Skyscrapers has implemented and will maintain technical and organisational measures as described in the Skyscrapers Security Policy. Skyscrapers determines the relevant measures taking into account the current state of the art, the cost of implementation and the nature of the Services provided. In particular this includes:
 - a. All remote management, either manual or automated, is done over encrypted channels



- b. All access control and authentication rely on 2 factor authentication, if supported by the underlying systems
 - c. Secure transfer and management of credentials
3. Customer agrees that the technical and organisational measures described in the Skyscraper Security Policy provide an appropriate level of security.

5.2. Customer controlled security measures

1. Customer may elect and is encouraged to implement specific technical and organisational security measures on the Cloud Infrastructure in relation to Customer Data. This may include but is not limited to the following:
 - a. the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - b. the ability to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident;
 - c. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. If within the context of the Agreement Skyscrapers may be asked to advise on technical and organisational security measures. These can be implemented by Skyscrapers. Skyscrapers cannot be held liable should any of the measures fail.

6. Sub-processing

1. Authorisation: Customer authorises Skyscrapers to use any existing sub-processors to fulfill its contractual obligations under this DPA or to provide certain services in order to fulfil Services as per the Agreement. Customer furthermore provides Skyscrapers with a general authorization to rely on self-employed contractors for the provision of the Services.
2. Skyscrapers will inform Customer of any intended changes concerning the addition or replacement of any sub-processors (with the exception of self-employed contractors, as per [article 6.1: authorisation](#)), thereby giving Customer the opportunity to object to such changes. In any case, Skyscrapers will not change any sub-processors that form any or all parts of the Cloud Infrastructure without prior agreement of the Customer.
 - a. Skyscrapers will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services;
 - b. Skyscrapers will enter into an agreement with the sub-processor and Skyscrapers will impose on the sub-processor the same contractual obligations that Skyscrapers has under this DPA; and
 - c. Skyscrapers will remain responsible for the sub-processor's compliance with the obligations of this DPA.

7. Data transfer

1. Skyscrapers will not transfer Customer Data outside of the European Economic Area except in these cases:
 - a. towards sub-processors or self-employed contractors both as described in this section 6;



- b. Customer instructed to do so through the Documented Instructions; or
 - c. Customer provides written instruction or approval to do so;
2. With regard to the self-employed contractors based outside of the European Economic Area (if any) , the Customer authorises Skyscrapers to enter into an unaltered version of the EU Model Clauses (controller to processor) in the name and on behalf of the Customer.

8. Data Subject Rights

1. Customer remains responsible for complying with its obligations towards Data Subjects. Taking into account the nature of the Services the Customer may choose to implement the necessary controls as part of Services to comply with its obligations towards Data Subjects.
2. Skyscrapers will assist the Customer in those cases where the Customer's implemented controls are insufficient to meet its obligations towards Data Subjects. In these cases additional fees may be charged.
3. Should a Data Subject contact Skyscrapers with regard to exercising its rights, Skyscrapers will use commercially reasonable efforts to forward such requests to Customer.

9. Security Breach Notification

1. Skyscrapers will notify Customer of Security Incident without undue delay after becoming aware of the Security Incident.
2. Skyscrapers will take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident.
3. To assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, Skyscrapers will provide all relevant and information available to Skyscrapers about the nature of the Security Incident, the scope of the Security Incident, it's known consequences and the proposed and/or taken measures to mitigate the effects and limit damage.
4. Skyscrapers obligations described in this section are not and will not be construed as an acknowledgement by Skyscrapers of any fault or liability of Skyscrapers with respect to the Security Incident.
5. Notification(s) of Security Incidents, if any, will be delivered to one or more Customer's contacts, assigned as part of the Agreement, through any means Skyscrapers deems suitable for the situation at hand, including email. It is the Customer's responsibility to keep the Agreement updated with accurate and up to date contact information.
6. In case Skyscrapers becomes aware of events or information, relating to the Cloud Infrastructure, Services or Customer Applications, that in the opinion of Skyscrapers introduces a risk of leading to a Security Incident, Skyscrapers will inform Customer. Customer agrees to take the necessary actions to mitigate the stated risk.
7. When a Security Incident has occurred the Customer is responsible to take the following actions:
 - a. Customer takes all adequate measures to remedy and limit the consequences, and avoid recurrence;
 - b. Customer informs the Local Data Protection Authority no later than 72 hours after having becoming aware of it.



10. Inspections, Assessments and Adjustment

1. Taking into account the nature of the Services and the information available to Skyscrapers, Skyscrapers will assist Customer in complying with Customer's obligations in respect of data protection impact assessments.
2. Customer can perform an audit on all technological and organisational measures referred to in this DPA in the scope of all Services and Cloud Infrastructure covered by Agreement and to ensure Customer meets their Article 28 obligations set forth in the GDPR. This audit can be done once a year or, if the Customer sees the necessity to do so, following a Security Incident.
3. Customer agrees to bear all costs, as communicated by Skyscrapers, the articles in this section may introduce unless otherwise agreed on in the Agreement.
4. Skyscrapers will provide all information requested in the scope of this article within a reasonable time period providing it does not violate any other confidentiality agreements it may have around that information, for example with other Data Subjects, Personnel or other Customers, in which case Skyscrapers reserves the right to withhold this information.
5. Parties acknowledge that security requirements, state of the art around technological and organisational measures, and regulatory requirements evolve over time. Both parties will support each other in ensuring this DPA and the Skyscrapers Security Policy evolve along with those evolutions.
6. Skyscrapers will promptly inform the Customer if Customer provides instructions to Skyscrapers that, in Skyscraper's opinion, are in violation with Applicable Law or the GDPR.

11. Return and/or Deletion of Customer Data

1. After termination of the Agreement and this DPA, Skyscrapers will immediately cease and desist all Processing of Customer Data with regard to its Services including deleting all Customer Data, either immediately or within an agreed upon period after Termination.
2. At least 30 days before termination of the Agreement Customer can request Skyscrapers to provide all Customer Data that may exist on the Cloud Infrastructure. Customer agrees to bear any additional costs, as communicated by Skyscrapers, this may introduce outside of the Agreement.

12. Liability and claims

1. Customer warrants that if a Data Subject invokes any rights according to the Applicable Law and/or claims compensation for damages under this DPA, Skyscrapers cannot be held responsible, except for breaches solely caused by Skyscrapers.
2. Parties agree that if one Party is held liable for a violation of the clauses of this DPA committed by the other Party, the latter will, to the extent to which it is liable, indemnify the first Party for any cost, charge, damages, expenses or loss it has incurred.
3. In all cases described in this article penalties that Skyscrapers may pay out are limited to the amount set forth in the Agreement or, in absence of that, limited to the total revenue generated by Services over the last 12 months, excluding the costs of Cloud Infrastructure.
4. Indemnification is contingent upon



- a. the Customer promptly notifying Skyscrapers of a claim; and
- b. Customer giving Skyscrapers the possibility to cooperate with the Customer in the defence and settlement of the claim.

13. Duration and termination

1. This DPA enters into force after the date that Skyscrapers provides Services in a fully delivered state, as will be described in the Agreement, to the Customer.
2. This DPA shall remain in force and effect until the Agreement is terminated or expired, unless Parties agree that earlier termination is required.
3. Any obligation arising from this DPA that by nature has post-contractual effect shall continue to be in effect after termination of this DPA for a maximum of 12 months.
4. Either Party shall be entitled, without prejudice to the provisions for this purpose in the Agreement, to suspend implementation of the DPA and the Agreement linked to it, or to terminate the Agreement without any repercussions with immediate effect if:
 - a. the other Party is dissolved, declared bankrupt or otherwise ceases to exist; and
 - b. the other Party culpably fails to fulfil the obligations arising out of the present Data Processing Addendum and these serious shortcomings are not resolved within 30 days after a written notification to this this effect;

14. Final provisions

1. This DPA together with the Agreement constitutes the entire agreement and understanding between the Parties with respect to its Subject matter and replaces all previous agreements between, or understandings by, the Parties with respect to such Subject matter.
2. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Agreement and this DPA, the terms of this DPA will control.
3. Any conflicts shall be discussed first with both Parties trying to resolve them in close consultation with each other.
4. In the event that one or more provisions in this DPA turn out not to be legally valid or not enforceable, the specific provision(s) will modified to the minimum extent necessary to make the provision(s) valid, legal and enforceable. Parties will negotiate in good faith to amend the provision so that it, to the greatest extent possible, achieves the intended commercial result of the original provision. If such modification is not possible, the relevant (part of the) provision shall be deemed deleted. Any modification or (partial) deletion of a provision shall not affect the validity and enforceability of this DPA.
5. Parties acknowledge that this DPA is governed by Belgian law. Any disputes arising within the scope of this DPA may only be brought before the competent courts of the judicial district of Antwerp.