Data Processing Agreement.

DPA Hive CPQ.

Hive CPQ | Kleindokkaai 17, Gent, Belgium | info@hivecpq.com | +32 9 277 81 81 | BE0677.439.858

Table of contents.

Data Processing Agreement.

This Data Processing Agreement forms part of the Service Contract between (i) the Company, i.e. the Controller, on the one hand, and (ii) the Service Provider, i.e. the Processor, on the other hand.

1. Definitions and interpretation.

1.1. The terms which follow shall have the following meanings (unless the context otherwise requires), notwithstanding any other meaning given to such terms in the Agreement:

Agreement	means this data processing agreement and its addendum, as in force and amended from time to time.
Applicable Legislation	means all applicable laws and regulations pertaining to the security, confidentiality, protection or privacy of Personal Data, as amended or re-enacted from time to time, including (to the extent applicable) GDPR (as defined below).
Controller	means the entity / person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	means an identified or identifiable natural person.
GDPR	means Regulation (EU) 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).
Personal Data	means any information about an identified or identifiable natural person being processed by a party in the performance of its obligations under the Agreement and this Annex; 'identifiable' means a natural person who can be identified directly or indirectly, namely by means of an identifier such as a name, an identification number, location data, an online identifier or by one or more elements which are characteristic for the physical, physiological, genetic, psychic, economic, cultural or social identity of that natural person.

Processing	means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means the entity / person which processes Personal Data under the Controller's instructions.
Purposes	means the specified, explicit and legitimate Purposes of the Processing.
Security Incident	means any unauthorized or unlawful access, deletion, mutilation, loss or any form of unauthorized or unlawful Processing of the Personal Data, or any other incident which shall lead (or may lead) to the accidental or unlawful deletion, loss, modification, unauthorized disclosure of – or access to – the Personal Data, any Personal Data Breach as defined in the GDPR, or any indication that a breach of that nature shall occur or has occurred.

1.2. In this Agreement (unless the context otherwise requires):

(a) The singular includes the plural and vice versa and any gender includes any other gender.

(b) Terms defined in the Applicable Legislation shall have the same meaning when used in this Annex.

(c) The headings in this document are inserted for convenience and do not affect its construction or interpretation; and

(d) The wording and phrases other, including, and in particular do not limit the generality of any preceding words and the words which follow them shall not be construed as being limited in scope to the same class as the preceding words where a wider construction is possible.

2. Personal data of the controller.

2.1. The Controller and the Processor acknowledge that the Controller owns or has in its possession certain Personal Data or other personal and/or confidential information. The performance of the Services may involve the Processing, transfer and/or storage of such Personal Data by the Processor as "Processor" to the benefit and on behalf of the Controller in its capacity of "Controller".

2.2. The Processor warrants that the Personal Data will only be processed, transferred, and/or stored for the performance of the Services under the Agreement.

2.3. A list of the categories and A list of the categories and types of Personal Data as well as the purposes for which the Personal Data are Processed for the benefit of the Controller, the subject matter and duration of the Processing, the nature of the Processing and the categories of Data Subjects has been included in this Agreement.

3. Compliance with Applicable Legislation.

3.1. The Processor shall comply with all Applicable Legislation in the Processing of the Personal Data.

3.2. The Processor shall Process the Personal Data under the documented instructions of the Controller (including with regard to transfers of Personal Data to a third country or an international organization), unless Processing is required by Applicable Legislation to which the Processor is subject, in which case the Processor shall, to the extent permitted by Applicable Legislation, inform the Controller of that legal requirement before the relevant Processing of that Personal Data.

3.3. The Processor shall not disclose Personal Data directly or indirectly to any person, another controller or governmental entity. If such disclosure is necessary for the proper Processing of Personal Data, this may only occur after prior written permission of the Controller and then only under a full obligation of confidentiality and in accordance with the legal requirements of the GDPR. The Processor may, upon timely prior notification to the Controller, release Personal Data pursuant to an order issued by a court or a competent governmental agency.

3.4. Other Processing activities shall only be performed, when the Processor is explicitly instructed to do so by the Controller or to comply with a legal

requirement, after having notified the Controller. In no case shall the Processor Process Personal Data obtained in the framework of the Agreement for its own purposes nor for the purposes of any third party, unless such is explicitly requested by the Controller.

3.5. The Processor shall take all necessary steps to ensure that any natural person acting under its authority and/or on its behalf does not Process Personal Data in contravention with current provision or the GDPR.

3.6. The Processor shall Process the Personal Data verifiably, properly, and carefully and in accordance with all applicable data protection regulations and shall not, by any act or omission, put the Controller in breach of any data protection regulations in connection with this Annex.

3.7. The Processor shall comply with all reasonable instructions provided by the Controller in relation to the Processing of the Personal Data. The Processor shall immediately notify the Controller if, in its view, any instructions are in conflict with Belgian law or with GDPR.

4. Confidentiality.

4.1. The Processor shall inform any person, including but not limited to employees, civil servants, interim staff or self-employed workers, who has access to the Personal Data of the obligations resting on the Processor with regard to the Controller's Personal Data.

4.2. The Processor shall make sure that all persons involved in the Processing of the Controller's Personal Data are subject to (i) the confidentiality obligations set in article 6.2 of the Agreement and (ii) professional or statutory obligations of confidentiality, with the purpose of safeguarding the confidentiality and integrity of the Controller's Personal Data.

5. Security of processing and Technical and Organizational measures.

5.1. The Processor shall keep the controller's Personal Data (physically and logically) separate from any data belonging to the Processor and/or third parties, ensuring that the Controller's Personal Data is under no circumstances combined or mixed with any other data.

5.2. The Processor shall implement and maintain all adequate and appropriate technical and organizational measures and controls to prevent unauthorized or unlawful Processing of Personal Data and accidental loss, destruction, damage, theft, use or (unauthorized) disclosure of such Personal Data, and shall protect against any anticipated threats or hazards to the security or integrity of the Personal Data, and detect and prevent unlawful or unauthorized Processing of, or unlawful or unauthorized access to, the Personal Data, and such measures shall at a minimum meet the standard required by Applicable Legislation (including but not limited to the standard required by Article 32 of the GDPR, ensuring the protection of the rights of the Data Subject (in particular but in no way limited to Chapter III of the GDPR), even if the Processor is not directly subject to the requirements of the GDPR).

5.3. Such measures shall provide a level of security which could be considered as appropriate considering the technical standards and the kind of Personal Data Processed, taking into account the state of the art, and 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.

5.4. The Parties acknowledge that security requirements are changing continually, and that effective security requires a frequent assessment and regular improvement of security measures. The Processor shall therefore continually assess and tighten, supplement or improve the measures implemented for the continued compliance with its obligations.

5.5. The Processor shall provide the Controller with a full and clear description, in a transparent and understandable manner, of the manner in which the Processor Processes the Controller’s Personal Data.

6. Sub-processing.

6.1. The Processor shall not subcontract the Processing of Personal Data to a sub-processor without prior written consent of the Controller. In the event that the Controller provides its consent, the Processor shall (prior to the sub-processor Processing the Personal Data) enter into an agreement with the sub-processor on terms that provide no less protection for the Personal Data than those set out in this Agreement and shall ensure that the agreement remains in force for the duration of the sub-processor's Processing of Personal Data.

6.2. The Processor shall procure that each sub-processor complies with the provisions of this Agreement. The Processor shall remain fully liable for the acts and omissions of each sub-processor.

7. Data Subject Rights.

7.1. Considering the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, to respond to requests to exercise Data Subject rights under the Applicable Legislation.

7.2. The Processor shall promptly and without undue delay and at least within 72 hours notify the Controller in writing of all Data Subject requests, enquiries or complaints (including any request by a Data Subject to exercise their rights under the Applicable Legislation) it receives. The Processor shall comply with the Controller's instructions with respect to the request or notice and shall not reply to this request or notice without instruction from the Controller.

7.3. Taking into account the nature of the Processing, the Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, and provide its full and timely cooperation to the Controller in order to respond to requests for exercising the Data Subject's rights in accordance with the GDPR, after having obtained the approval from and having been instructed by the Controller.

7.4. The Processor shall notify without undue delay to the Controller any inquiry into or a seizure by government authorities of the Personal Data, or the presumption of such an occurrence, unless that law prohibits such information on important grounds of public interest.

8. Personal Data Breach.

8.1. The Processor shall notify without delay the Controller in writing of each Security Incident of which it becomes aware relating to the Personal Data and shall provide such assistance in relation to each Security Incident as is reasonably requested by the Controller.

8.2. The Processor shall document any Security Incident, comprising the facts relating to the Security Incident, any useful information on the origin, nature,

scope and consequences of the Security Incident, the risk that Personal Data have been or may be unlawfully Processed, the remedial action that have been or shall be taken and all relevant information. The Processor shall share this information with the Controller within 24 hours so that the Controller is in a position to comply with the requirements of the data protection legislation regarding (i) informing of the competent authorities and of the Data Subjects without undue delay taking into account the terms for such notification as set out in the GDPR (72 hours after having become aware of a Personal Data Breach), and (2) the implementation of all necessary remedies.

8.3. The Processor shall without any delay remedy any negative consequences arising from an Incident and/or reduce any further consequences to a minimum.

8.4. The Processor shall implement without any delay all remedies requested by the Controller or the competent authorities to fix any Security Incident, security breach or any other non-compliance and/or mitigate the risks associated with it. The Processor shall at all times cooperate with the Controller and observe the Controller's instructions, so as to enable the Controller and/or any third party mandated by the Controller to perform a proper inquiry into the Security Incident, formulate a correct response and subsequently take adequate action with respect to the Security Incident.

8.5. If such is deemed necessary by the Controller, the Controller shall inform the Data Subjects and other third parties, including the supervisory authority, about any Security Incidents. It is not permitted for the Processor to provide information about Security Incidents to Data Subjects or other third parties, except if the Processor is obliged by law to do so.

9. Data Protection Impact Assessment and Prior Consultation.

9.1. The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, which the Controller reasonably considers to be required of the Processor by article 35 or 36 of the GDPR or equivalent provisions of any other Applicable Legislation, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

10. Deletion or return of the Processor Personal Data.

10.1. The Processor shall, unless the Applicable Legislation requires storage of Personal Data, (i) securely return to the Controller or (ii) securely destroy (at the Controller's option) all Personal Data, together with all copies in any form and in any media, in the Processor's power, possession or control promptly following the earlier of:

(i) Termination or expiry of the Agreement.

(ii) A request from the Controller; or

(iii) If the Processor no longer needs the Personal Data in connection with the performance of its obligations under the Agreement between the parties.

10.2. At the Controller’s request the Processor shall provide proof of the fact that the Personal Data have been deleted or removed.

10.3. Upon expiry of the Agreement, for whichever reason, the Processor shall notify all third parties involved in the Processing of Personal Data of the termination of this Agreement. The obligations under this clause apply by analogy to these third parties, which the Processor shall ensure and for which the Processor safeguards and holds harmless the Controller. The Processor shall warrant that all third parties involved shall give effect to these and shall indemnify and hold harmless the Controller in this respect.

11. Documentation and audit.

11.1. The Processor shall provide the Controller with all information reasonably requested by the Controller to enable the Controller to verify the Processor's (and each sub-processor's) compliance with this Annex and the Agreement with respect to the Personal Data.

11.2. Without prejudice to the foregoing paragraph, the Controller shall be entitled to inspect, test and audit or appoint representatives to inspect, test and audit, all facilities, premises, equipment, systems, documents and electronic data relating to the Processing of Personal Data by or on behalf of the Processor and the Processor shall assist with each inspection, test and audit. The Controller shall act reasonably in exercising its rights under this Clause, including by providing prior notice of its intention to exercise its rights where appropriate to do so.

12. Transfers of Personal Data to third countries.

12.1. The Processor shall not Process or transfer the Controller's Personal Data or have these Processed by itself or by third parties outside the European Union, except with the Controller´s explicit prior written permission. The Processor shall ensure that no access to the Controller's Personal Data by a third-party result in any manner in the transfer of the Controller's Personal Data outside of the European Union, except with the Controller´s explicit prior written permission.

12.2. If the Controller agrees on a transfer of the Company's Personal Data outside the European Economic Area, and/or subsequently on the Processing by a third party established outside the European Economic Area (permission and instructions are required in accordance with Article 6 of this Agreement), such transfer and Processing may only take place if the third country in question ensures an adequate level of data protection, pursuant to article 45 GDPR, and the Member States' laws are respected prior to such transfer.

12.3. In case the third country does not ensure an adequate level of protection, the Processor and the third party located in a third country will enter into Standard Contractual Clauses adopted by the European Commission or a supervisory authority and approved by the European Commission pursuant to the examination procedure referred to in Article 93 (2) GDPR as per article 45 GDPR. These Standard Contractual Clauses will be attached to this Agreement.

12.4. The Processor will hold harmless the Controller from any responsibility in respect to any transfer to a third country in violation of this Agreement, the Standard Contractual Clauses or the data protection legislation the Controller is subject to.

13. Term and Termination.

13.1. The Controller is entitled to terminate the Services Agreement and this Annex with immediate effect and without prior judicial intervention if it becomes apparent and/or if the Processor states that it cannot, or no longer, meet the requirements which, on the basis of the developments in legislation and/or case law are imposed on the Processing of the Personal Data.

14. Liability.

14.1. The Processor hereby agrees to indemnify, defend and hold harmless the Controller from and against any and all claims, losses, demands, liabilities, costs and expenses (including reasonable attorney's fees and costs and expenses related thereto) fines or penalties (including penalties imposed by any supervisory authority), and other liabilities which are incurred or sustained by the Controller or third party beneficiaries and either directly arise from or occur in connection with a violation of this Agreement by the Processor, its representatives, its employees or agents and/or its Processors in the performance of its obligations and/or any violation by the Processor of the applicable legislation in the field of the Processing of Personal Data, suffered or incurred by the Company as a result of, or in connection with, any third party claims to the extent caused, in whole or in part, by the fraud, gross negligence or willful misconduct of the Processor, its representatives, its employees or agents and/or its Processors in performing the Services.

14.2. Any failure of the Processor in the fulfillment of its obligations under this Agreement shall, however, not be liable to the extent that such breach results from an act or omission of the Company, its employees, suppliers, agents or third parties not mandated by the Service Provider.

14.3. No Party shall be liable for any indirect damages, such as loss of customer, loss of reputation or business interruption.

15. General.

15.1. If any provision of this Agreement is held to be illegal, invalid or unenforceable in whole or part, that provision shall to that extent be deemed not to form part of this Agreement and the legality, validity and enforceability of the remainder of this Agreement shall be unaffected.

15.2. The termination of this Agreement shall not affect the coming into force or the continuation in force of any of its provisions which expressly or by implication are intended to come into force or continue in force on or after termination.

15.3. This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the governing law of Belgium.

16. Signature.

This Agreement has been executed in two (2) originals, each Party acknowledging receipt of one signed and initialed original.

For the Processor	For the Processor
_____	_____
Name:	Name:
Function:	Function:

Addendum 1.

Details of processing of Personal Data.

1. The project.

This partnership is based on Hive CPQ consultancy services either development or business application specialist areas.

Hive CPQ allows the customer to make the marketing, quotation and order process with their distributor network seamless.

Hive CPQ will hold personal data of the users connecting to the system. Hive CPQ will also hold data about contacts of customers.

This data is used to display on commercial documents like quotations and order confirmations. The data will be accessible to the customer via the Hive CPQ API to allow integration with their various systems.

2. Data subjects.

The personal data processed concern the following categories of data subjects:

- Customer employees.
- Customer distributor users.
- Distributors final customers data.

3. Categories of Personal Data.

The personal data processed concern the following categories of personal data:

- Customer employees and Customer distributor users.
    - Name
    - Address
    - Email address
    - Phone number and other basic information
    - Country
    - Profile picture
    - Login information
        - First logged in
        - Last logged in
        - Last IP logged in
        - Login counts

        - Location last logged in (for security reasons)
        - Country
        - Web browser
        - Optional: Social media connector used to login
        - Used devices
        - Timezone
        - Total number of logins
        - Email verified true/false
        - Given consent true/false
- Distributors final customers data
    - Only basic information: Name, email, function name, phone, fax & address.

4. Purpose of the Personal Data Processing.

Supplier is mainly used as experts consultants within the area of develop and implementation of the Hive CPQ system. All actions are based on the customers' requests.

5. Processing operations.

The personal data processed will be subject to the following basic processing activities:

- Creation and following up of opportunities/deals.
- Creation, placing and following up of orders.

6. Duration of processing.

The personal data will be processed with the following duration:

Interaction from the Supplier is mainly related to business support, implementation system setup, handling reported incidents and change requests from internal key users or Business Process Owners of the Hive CPQ system.

7. Security measures.

Description of the technical and organizational security measures implemented by the Supplier:[1] Following security guidelines and signed NDA document.

[1] GDPR, art 32

Addendum 2.

Authorization for the Transfer of Personal Data outside the EEA and the Use of a Subprocessor.

Pursuant to Article 12 of the Agreement, the Controller hereby grants authorization to the Processor to transfer Personal Data outside of the European Economic Area, namely to

xxx

Pursuant to Article 6 of the Agreement, the Controller hereby grants authorization to the Processor to use

xxx

as Sub-processor.

The abovementioned authorizations are strictly conditional upon:

- the Processor and the Sub-processor entering into legally compliant Standard Contractual Clauses adopted by the European Commission or a supervisory authority and approved by the European Commission pursuant to the examination procedure referred to in Article 93 (2) GDPR as per article 45 GDPR. These Standard Contractual Clauses will be attached to this Addendum 2. In case the Standard Contractual Clauses entered into by the Processor and the Sub-processor are invalidated for any reason, the Processor undertakes to enter into new legally compliant Standard Contractual Clauses.

- the Processor and the Sub-processor entering into a processing agreement which contains the same data protection obligations as set out in this Agreement or other legal act between the Controller and the Processor as referred to in paragraph 3 of Article 28 GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR. Where the Sub-processor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of Sub-processor's obligations.

For the Processor

For the Controller

_____

Name:

Function:

_____

Name:

Function:

Addendum 3.

Technical and organizational measures for the Processing of Personal Data.

The Processor commits to being ISO 27001 certified during the entire duration of this Agreement.