Valid from	08/15/2026	Jurisdiction	EU — Regulation (EU) 2016/679, art. 28

Data Processing Agreement

Annex to the IndustryUX Master Subscription and Licence Terms — Article 28 GDPR

Codice documento	IUX-EN-31
Versione	1.2
Data	2026-08-11
Set	ANNEXES (EN)
Destinatari	Customers acting as controllers — Shop, Business, Enterprise Online, VPS and On-Premise channels
Lingua	English (authoritative)
Classificazione	Contractual document
Note	Includes Annexes 1 to 5 (processing description, security measures, sub-processors, Standard Contractual Clauses 2021/914, transfer impact assessment)

This Data Processing Agreement (the "DPA") is entered into between **DEVIBRAIN S.R.L.**, a company incorporated under Italian law, with registered office at Via Coghetti 6, 24128 Bergamo (BG), Italy, VAT and tax number IT04507220160, certified electronic mail devibrain@pec.it (the **"Provider (DevIBrain)"**, referred to throughout this DPA as the "Provider" and, where its technical role under the GDPR is concerned, as the "Processor"), and the customer identified in the Order (the "Controller" or the "Customer"), each a "Party" and together the "Parties".

The DPA is concluded pursuant to Article 28(3) of Regulation (EU) 2016/679 (the "GDPR"). It forms an integral and substantial part of the IndustryUX Master Subscription and Licence Terms (the "Master Terms", IUX-EN-01), of the applicable Channel Schedule, namely the Shop Schedule (Schedule A, IUX-EN-10) or the Enterprise Schedule (Schedule B, IUX-EN-20), and of each Order placed under them (together, the "Agreement"), and it governs the processing of personal data carried out by the Provider on behalf of the Customer in the provision of the IndustryUX platform and of its applications (the "Platform").

Where the Agreement is accepted through the self-service flow, this DPA is accepted together with the Master Terms and its acceptance is recorded in the acceptance evidence described in the Master Terms. Where the Agreement is executed through the signature flow, this DPA is signed together with the Master Terms.

Art. 1 — Definitions and interpretation

1.1 Terms defined elsewhere

Capitalised terms not defined in this DPA have the meaning given to them in the Master Terms. The terms "personal data", "special categories of personal data", "processing", "controller", "processor", "sub-processor", "data subject", "personal data breach", "supervisory authority" and "third country" have the meaning given to them in the GDPR.

1.2 Specific definitions

• **"Customer Personal Data"** means the personal data contained in Customer Data that the Provider processes on behalf of the Customer in the provision of the Platform, as described in Annex 1.

• **"Data Protection Law"** means the GDPR, Italian Legislative Decree 196/2003 as amended by Legislative Decree 101/2018, Directive 2002/58/EC as implemented in Italy, and every other data protection provision applicable to the processing described in Annex 1, including the measures of the supervisory authorities.

• **"EEA"** means the European Economic Area.

• **"SCC"** means the standard contractual clauses for the transfer of personal data to third countries set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced.

• **"Sub-processor"** means any third party engaged by the Provider that processes Customer Personal Data on behalf of the Customer.

• **"Sub-processor Page"** means the public page at https://www.industryux.com/legal/sub-processors, which lists the Sub-processors in force and allows subscription to change notifications.

• **"TIA"** means the transfer impact assessment described in Annex 5.

• **"Usage Data"** means technical, licence-verification and telemetry data generated by the operation of the Platform, as described in Article 2 and in the IndustryUX Privacy Policy.

1.3 Interpretation

Headings are for convenience only. "Including" means "including without limitation". References to legislation are to that legislation as amended, replaced or recast from time to time. Annexes 1 to 5 form an integral part of this DPA. Time periods expressed in days are calendar days unless expressly

stated to be working days.

Art. 2 — Scope, roles of the Parties and dual capacity

2.1 The Provider as processor

In respect of Customer Personal Data, the Customer acts as controller and the Provider acts as processor. The Provider processes Customer Personal Data solely to provide, operate, maintain, secure and support the Platform in accordance with the Agreement and with the Customer's documented instructions.

2.2 The Provider as independent controller

The Provider acts as an independent controller, and this DPA does not apply, in respect of: (a) registration, account, contact and billing data of the Customer and of its business representatives; (b) Usage Data and licence-verification telemetry processed for the purposes of licence compliance, fraud prevention, security, capacity planning and product improvement, which the Provider processes in pseudonymised form wherever technically possible; (c) evidence of acceptance of the contractual documents, retained in tamper-evident form for ten years; (d) navigation, cookie and marketing data collected on the public website. Those processing activities are governed by the IndustryUX Privacy Policy and the Cookie Policy, and their lawful basis is the performance of the contract, compliance with legal obligations or the legitimate interest of the Provider, as stated in that Privacy Policy. This Article resolves, in favour of transparency, the dual capacity of the Provider and prevails, in accordance with the order of precedence referred to in Article 3.1, over any contrary reading of the telemetry and audit provisions of the Master Terms.

2.3 Customer acting as processor for a third party

If the Customer is itself a processor acting on behalf of one or more third-party controllers, the Provider acts as sub-processor and this DPA applies mutatis mutandis. The Customer warrants that it holds the authorisations required to engage the Provider and to grant the instructions given under this DPA, and that its own agreement with the third-party controller is consistent with this DPA.

2.4 Consumers and self-service channels

For customers acquiring the Platform through the Shop channel in a purely personal or household capacity, the exemption in Article 2(2)(c) GDPR applies to their own use and this DPA does not apply; the Provider remains controller of the data described in Article 2.2. This DPA applies to Shop and Trial customers only where and to the extent that they use the Platform in a professional capacity and upload personal data relating to third parties.

2.5 Customer warranties

The Customer warrants that: (a) it has an appropriate lawful basis for the processing it instructs; (b) it has provided the information required by Articles 13 and 14 GDPR to the data subjects, the Provider having no direct relationship with them; (c) the Customer Personal Data it uploads is adequate, relevant and limited to what is necessary; and (d) it has assessed the suitability of the Platform's security measures, described in Annex 2, for the risk of its own processing.

Art. 3 — Order of precedence

3.1 Hierarchy

The order of precedence between the documents of the Agreement, including the rank of this DPA on data protection matters, is the single order of precedence set out in Article 2.3 of the Master Terms (IUX-EN-01); it is not restated here and applies to this DPA as it applies to every other document of the Agreement. Where the SCC or any other transfer tool executed by the Parties apply, they prevail over this DPA in the event of conflict, in accordance with Article 11.3 and with Annex 4.

3.2 Mandatory law

Nothing in this DPA limits or excludes an obligation that Data Protection Law imposes on either Party, nor the rights that data subjects derive from it. Any provision that proves incompatible with Data Protection Law is to be read as modified to the minimum extent necessary to make it compatible, the remainder being unaffected.

Art. 4 — Subject-matter, duration, nature and purpose of the processing

4.1 Description

The subject-matter, duration, nature and purpose of the processing, the types of personal data, the categories of data subjects, the frequency of the processing and the retention periods are described in Annex 1, which satisfies Article 28(3) GDPR and also constitutes Annex I.B of the SCC where the SCC apply.

4.2 Duration

The processing lasts for the term of the Agreement and, thereafter, for the retrieval and deletion periods set out in Article 14. Statutory retention obligations affecting the Provider as controller under Article 2.2 are unaffected.

4.3 Activation of further modules

If the Customer activates a module of the Platform that is not listed in Annex 1, Annex 1 is deemed supplemented by the description of that module published by the Provider and communicated to the Customer at activation, without any reduction in the protections of this DPA.

Art. 5 — Documented instructions

5.1 Processing on instructions only

The Provider processes Customer Personal Data only on the documented instructions of the Customer, including in relation to transfers to a third country. The following constitute documented instructions: the Agreement and this DPA; the Order; the configuration, options and settings selected by the Customer within the Platform; the use of the Platform's functions by the Customer and by its Authorised Users; and any further written instruction given in accordance with Article 5.2.

5.2 Further instructions

Further instructions are given in writing to the contact point in Article 19. The Provider implements instructions that are compatible with the functions of the Platform and with Data Protection Law. Where an instruction requires developments, configurations or activities that exceed the ordinary functions of the Platform, the Provider informs the Customer in advance and may make its execution conditional on the payment of a reasonable charge based on the rates in the Order or, absent those rates, on its standard professional service rates in force.

5.3 Unlawful instructions

The Provider informs the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Law, and may suspend the execution of that instruction until it is confirmed, amended or withdrawn in writing, without such suspension constituting a breach by the Provider. The Provider is not obliged to carry out a legal assessment of the Customer's instructions.

5.4 Processing required by law

If Union or Member State law to which the Provider is subject requires it to process Customer Personal Data otherwise than on the Customer's instructions, the Provider informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5.5 No processing for own purposes

The Provider does not process Customer Personal Data for its own purposes, does not sell it, does not make it available to third parties other than the Sub-processors listed in Annex 3, and does not use it to train, fine-tune or improve models or functions made available to other customers, as further provided in Article 15.

5.6 Special categories and minimisation

The Customer is instructed not to upload to the Platform special categories of personal data within the meaning of Article 9 GDPR or data relating to criminal convictions and offences within the meaning of Article 10 GDPR, unless expressly agreed in writing in the Order together with the

supplementary measures required by the risk. The Platform is not designed to process such data by default, and the Provider does not carry out any prior check on the content uploaded by the Customer.

Art. 6 — Confidentiality and authorised personnel

6.1 Undertakings of the personnel

The Provider ensures that the persons authorised to process Customer Personal Data have undertaken in writing to keep it confidential or are subject to an appropriate statutory obligation of confidentiality, have received instructions and periodic training on data protection, and access Customer Personal Data only to the extent strictly necessary to perform their duties.

6.2 Access management

Access to production environments is nominal, individual, subject to multi-factor authentication, granted according to the least-privilege principle and logged. Support access to a tenant is granted only for the time necessary to handle the request and is revoked when the request is closed. Access rights are reviewed at least every six months and revoked on the same day on which the employment or professional relationship terminates.

6.3 Survival

The confidentiality obligations survive the termination of the Agreement for as long as the information retains its confidential character and, in any event, for five years, without prejudice to the perpetual protection of personal data required by Data Protection Law.

Art. 7 — Security of processing

7.1 Technical and organisational measures

The Provider implements and maintains the technical and organisational measures described in Annex 2, which are appropriate to the risk within the meaning of Article 32 GDPR taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing. Annex 2 is contractually binding and also constitutes Annex II of the SCC where the SCC apply.

7.2 Evolution of the measures

The Provider may update the measures in Annex 2 to keep pace with technical developments, provided that the level of security is not materially reduced. Material updates are notified to the Customer at least thirty days before they take effect.

7.3 Responsibilities of the Customer

The Customer is responsible for the correct configuration of the roles, permissions and options made available by the Platform, for the management and custody of the credentials of its Authorised Users, for the choice of the content it uploads and, in the On-Premise deployment model, for the security of its own network, systems and physical premises. The Provider is not responsible for the consequences of configurations, permissions or uploads decided by the Customer, nor for the security of environments that the Provider does not operate.

7.4 Cooperation on network security and product security

The Parties cooperate in good faith so that each may discharge its obligations under Directive (EU) 2022/2555 (NIS2) as implemented in Italy by Legislative Decree 138/2024 and, for the components qualifying as products with digital elements, under Regulation (EU) 2024/2847 (Cyber Resilience Act), including the reporting of actively exploited vulnerabilities applicable from 11 September 2026. The Provider informs the Customer of vulnerabilities affecting the Platform that require action by the Customer, together with the available mitigations. An addendum on digital operational resilience under Regulation (EU) 2022/2554 (DORA) is made available on request to customers subject to that regulation.

7.5 Certifications

As at the version date the Provider does not hold a certification under Article 42 GDPR and does not adhere to an approved code of conduct under Article 40 GDPR, and makes no representation to the contrary. The Provider makes available to the Customer its security documentation, the answers to its security questionnaire and the evidence described in Article 13.

Art. 8 — Sub-processors

8.1 General authorisation

The Customer grants the Provider a general written authorisation to engage Sub-processors, within the meaning of Article 28(2) GDPR and of Clause 9(a), Option 2 of the SCC, subject to the procedure in this Article.

8.2 List in force

The Sub-processors authorised as at the version date are listed in Annex 3. The updated list is published on the Sub-processor Page, which also allows the Customer to subscribe to change notifications by electronic mail. The Customer undertakes to keep at least one valid electronic mail address subscribed to those notifications.

8.3 Prior notice of changes

The Provider notifies the Customer of the intended addition or replacement of a Sub-processor at least thirty days before that Sub-processor begins to process Customer Personal Data. The notice states the identity of the Sub-processor, the service entrusted to it, the place of processing, the categories of data concerned and, for processing outside the EEA, the transfer tool used.

8.4 Objection and remedies

Within fifteen days of the notice the Customer may object in writing on reasonable grounds relating to the protection of personal data. The Parties then discuss the objection in good faith for a further period of thirty days and the Provider proposes, where available, a reasonable alternative solution. Failing agreement within that period, the Customer may terminate, without penalty and by written notice, the services actually affected by the change, with a pro-rata refund of the fees paid for the unused period and, as regards prepaid balances, with the treatment provided for by the Master Terms and by the applicable channel Schedule: the Prepaid Credits of the account wallet are credited or reimbursed under the Shop Schedule (IUX-EN-10), while the Tokens credited to the wallet of a Designated Machine remain bound to that Machine under the Enterprise Schedule (IUX-EN-20) and are not converted into a credit or into a refund, save for the rights which the applicable law does not permit to be excluded. Pending the discussion, the Provider does not entrust the objecting Customer's Customer Personal Data to the new Sub-processor where technically feasible.

8.5 Obligations imposed on Sub-processors and liability

The Provider imposes on each Sub-processor, by a written contract, data protection obligations at least equivalent to those of this DPA, including as regards security measures, confidentiality, assistance, audit and international transfers. The Provider remains fully liable to the Customer for the performance of the Sub-processor's obligations in accordance with Article 28(4) GDPR.

8.6 Urgent replacement

Where a Sub-processor must be replaced immediately for security reasons, service continuity or because of its insolvency or non-compliance, the Provider may proceed with the replacement and notifies the Customer as soon as possible and in any event within five working days, the Customer's right of objection and the remedies in Article 8.4 remaining unaffected.

Art. 9 — Assistance with data subject requests

9.1 Functions made available

Taking into account the nature of the processing, the Provider assists the Customer by making available the functions of the Platform that allow the Customer to access, rectify, erase, restrict, export and communicate Customer Personal Data autonomously, so as to enable the Customer to respond to requests under Articles 15 to 22 GDPR.

9.2 Requests received directly

If the Provider receives a request from a data subject relating to Customer Personal Data, it does not respond to it on the merits, informs the requester that the request must be addressed to the Customer where lawful, and forwards the request to the Customer without undue delay and in any event within five working days of receipt.

9.3 Additional assistance

Where the Customer cannot satisfy a request through the functions of the Platform, the Provider provides reasonable additional assistance. Such assistance is included in the fees, save for manifestly excessive or repetitive requests, which the Provider may charge at the rates in the Order or, absent those rates, at its standard professional service rates in force, having given the Customer prior notice of the estimated cost.

Art. 10 — Security incidents, personal data breaches, impact assessments

10.1 Notification to the Customer

The Provider notifies the Customer of any personal data breach affecting Customer Personal Data without undue delay and in any event within forty-eight hours of becoming aware of it. Awareness arises when the Provider has a reasonable degree of certainty that a security incident has occurred that has led to a breach of personal data.

10.2 Content of the notification

The notification contains, to the extent then available: the nature of the breach and, where possible, the categories and approximate number of data subjects and records concerned; the likely consequences; the measures taken or proposed to address the breach and to mitigate its effects; the contact point for further information. Where the information is not available at once, it is provided in phases without further undue delay.

10.3 Cooperation and remediation

The Provider investigates the breach, adopts the measures reasonably necessary to contain and remedy it, preserves the relevant evidence and logs, and cooperates with the Customer so that the Customer may discharge its obligations under Articles 33 and 34 GDPR. The Provider does not notify the supervisory authority or the data subjects on the Customer's behalf unless expressly instructed to do so in writing.

10.4 No admission

The notification of a breach and the cooperation described in this Article do not constitute any admission of fault or liability by the Provider.

10.5 Impact assessments and prior consultation

Taking into account the nature of the processing and the information available to it, the Provider assists the Customer in carrying out data protection impact assessments under Article 35 GDPR and in the prior consultation under Article 36 GDPR, by providing information on the architecture, data

flows, retention periods and security measures of the Platform. The Customer remains responsible for the assessment and for the decisions it takes on its basis.

Art. 11 — Location of the data and international transfers

11.1 Location

Customer Personal Data processed by the Provider in the Business, Enterprise Online and VPS deployment models and in the shared environment of the self-service shop plans is hosted within the EEA, in the primary data centre operated by the Provider in Italy and, for redundancy copies, in facilities located within the EEA. In the On-Premise deployment model Customer Personal Data remains on the Customer's systems, as provided in Article 16.

11.2 Conditions for transfers

The Provider does not transfer Customer Personal Data outside the EEA, and does not allow access to it from outside the EEA, except where one of the following applies: (a) an adequacy decision of the European Commission is in force for the country or the recipient; (b) the SCC in the module applicable to the case have been executed and the TIA described in Annex 5 has been completed with a positive outcome, together with the supplementary measures it identifies; or (c) a derogation under Article 49 GDPR applies on the Customer's prior written instruction and under its responsibility.

11.3 Standard contractual clauses

The SCC are incorporated into this DPA by reference and are completed as set out in Annex 4, which identifies the applicable modules, the options selected and the correspondence between the annexes of the SCC and the annexes of this DPA. Where the SCC apply, they prevail over this DPA in the event of conflict.

11.4 EU-US Data Privacy Framework

The Provider does not rely on the adequacy decision of 10 July 2023 concerning the EU-US Data Privacy Framework as its primary transfer basis, for the reasons set out in Annex 4, and adopts the SCC combined with a TIA as its primary basis for transfers to the United States. Certification of an importer under that framework, where present, is treated as an additional element of assessment and never as a substitute for the SCC and the TIA.

11.5 Onward transfers

The Provider ensures that each Sub-processor established outside the EEA, or making the data accessible from outside the EEA, is bound by the SCC in the applicable module and by the supplementary measures identified in the TIA, and that any onward transfer is subject to the same conditions.

11.6 United Kingdom and Switzerland

Transfers to the United Kingdom take place on the basis of the adequacy decisions renewed by the European Commission on 19 December 2025 and valid until 27 December 2031; no additional transfer tool is required for as long as those decisions remain in force. If a United Kingdom exporter is introduced into the chain, the international data transfer addendum issued by the Information Commissioner's Office is added to the SCC. For transfers subject to the Swiss federal data protection act, the SCC apply with the adaptations recognised by the Swiss federal data protection and information commissioner.

Art. 12 — Requests from public authorities

12.1 Handling of requests

If the Provider or a Sub-processor receives a legally binding request from a public authority, including a judicial authority, for the disclosure of Customer Personal Data, the Provider: (a) notifies the Customer without undue delay, unless prohibited by law, in which case it uses its best efforts to obtain a waiver of the prohibition and documents those efforts; (b) challenges the request where there are reasonable grounds to consider it unlawful under the law of the requesting country or under Union law, including through the available appeals and interim relief; (c) discloses only the minimum amount of data lawfully required; (d) documents the request and the response and makes that documentation available to the Customer and, on request, to the competent supervisory authority.

12.2 No direct or unrestricted access

The Provider does not grant any public authority direct, unrestricted or generalised access to Customer Personal Data, does not create or maintain back doors or equivalent means of access, and does not hold any obligation of that nature towards any public authority. The Provider informs the Customer promptly if it becomes unable to make that statement.

Art. 13 — Audit and demonstration of compliance

13.1 Information

The Provider makes available to the Customer all the information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, including the description of the security measures, the record of processing activities kept under Article 30(2) GDPR for the part concerning the Customer, and the list of Sub-processors.

13.2 Audit procedure

The Customer may carry out an audit on at least thirty days' prior written notice, once every twelve months, during business hours, in a manner that does not disrupt the operation of the Platform. The audit is conducted, as a first step, remotely, by examining documentation, questionnaires and

remote sessions with the personnel responsible; an on-site audit at the Provider's premises may be carried out only where the remote audit has proved objectively insufficient and the reasons are stated in writing.

13.3 Auditor

The Customer may appoint a third-party auditor, provided that the auditor is not a competitor of the Provider and is bound by confidentiality obligations at least equivalent to those of the Agreement. The Provider may object, with reasons, to a specific auditor, in which case the Customer appoints a different auditor.

13.4 Costs

Each Party bears its own costs of the audit; the cost of the resources that the Provider devotes to the audit beyond one working day per year is borne by the Customer at the rates in the Order or, absent those rates, at the standard professional service rates in force. By way of exception, the Provider bears the full cost of an audit carried out following a personal data breach attributable to it or ordered by a competent supervisory authority, and of any additional audit made necessary by findings of non-compliance attributable to it.

13.5 Limits

The audit may not extend to the data, systems or information of other customers of the Provider, may not include unsupervised access to production systems, penetration testing or vulnerability scanning without prior written authorisation, and may not extend to the source code, the algorithms or the industrial and trade secrets of the Provider, save to the extent strictly necessary to verify a specific security measure and by means that preserve confidentiality.

13.6 Findings

The findings of the audit are confidential and may be used only to verify compliance with this DPA. The Provider submits a remediation plan for any non-compliance found within thirty days of receipt of the report and implements it within the agreed timeframe.

Art. 14 — Return and deletion of Customer Personal Data

14.1 Choice of the Customer

At the end of the provision of the services relating to processing, the Customer chooses whether the Provider is to return Customer Personal Data or delete it. Absent a choice communicated within the retrieval period, the Provider deletes it in accordance with Article 14.3.

14.2 Retrieval period

For thirty days from the effective date of termination or expiry, the Customer retains access to the export functions of the Platform to retrieve Customer Personal Data and the other Customer Data in structured, commonly used and machine-readable open formats. No switching or exit charge is applied, in accordance with Articles 25 and 29 of Regulation (EU) 2023/2854 (Data Act). Where the Customer requests the assisted transition described in the Master Terms, the transition is completed within thirty days of the request, on notice of commencement of not more than two months.

14.3 Deletion

The Provider deletes Customer Personal Data from the production environments within thirty days of the end of the retrieval period, and from the backup copies at the next rotation cycle of the backups and in any event within sixty days of the end of the retrieval period. Until deletion is complete, the data remains protected by the measures in Annex 2 and is not accessible for any purpose other than restoration.

14.4 Certificate of deletion

On written request from the Customer made within six months of the end of the retrieval period, the Provider issues a written certificate of deletion within fifteen days of the completion of the operations.

14.5 Retention required by law

The Provider retains, in its capacity as controller under Article 2.2, the data required by statutory obligations, in particular accounting and tax documentation and the evidence of acceptance of the contractual documents, for the periods stated in the Privacy Policy. Such retention does not constitute processing on behalf of the Customer and is subject to appropriate security measures and to the restriction of any further processing.

14.6 Termination for non-payment

Deletion under this Article also applies where the Agreement terminates for non-payment; the retrieval period is granted in full and may not be made conditional on payment of the amounts in dispute, without prejudice to the right of the Provider to recover them by the means provided for in the Master Terms.

Art. 15 — Artificial intelligence features, training data and automated decisions

15.1 Local execution by default

The artificial intelligence features of the Platform, including document-based training, the local assistant, the document store, speech transcription, optical character recognition and image analysis, are executed by default within the Customer's tenant or on the infrastructure operated by

the Provider within the EEA, without transmission of content to third-party suppliers.

15.2 No cross-customer training

The Provider does not use Customer Personal Data, nor the content uploaded by the Customer, to train, fine-tune, evaluate or improve models, features or services made available to other customers or used by the Provider for its own purposes. That prohibition may be departed from only on the basis of a separate, specific and revocable consent document, executed by the Customer for that purpose alone, which is the sole vehicle of any such authorisation: neither the acceptance of the Agreement, nor the Order, nor any option within the Platform constitutes that consent, and its revocation takes effect for the future without affecting the lawfulness of the processing already carried out. The models trained on the Customer's content are dedicated to the Customer's tenant and are deleted in accordance with Article 14.

15.3 Remote inference

Where a feature requires a model that exceeds the capacity of the local infrastructure, remote inference is disabled by default and may be enabled only on the express written instruction of the Customer. Enabling is conditional upon: the prior listing of the supplier on the Sub-processor Page with the notice period in Article 8.3; the execution of the SCC in the applicable module and the completion of a TIA where the supplier is established outside the EEA; the contractual undertaking of the supplier not to use the content for its own training purposes and to retain it only for the time strictly necessary to produce the response; and the minimisation of the content transmitted in the prompt.

15.4 Voice recordings

Voice recordings processed by the transcription feature are used solely to produce the corresponding text and are not used to identify a natural person uniquely; they therefore do not constitute biometric data within the meaning of Article 4(14) GDPR. The recordings are deleted once the transcription has been produced and in any event within thirty days.

15.5 Roles under the artificial intelligence regulation

For the purposes of Regulation (EU) 2024/1689, the Provider is the provider of the artificial intelligence features of the Platform within the meaning of Article 3(3) of that regulation and the Customer is the deployer within the meaning of Article 3(4). The Customer is responsible for informing the natural persons who interact with the assistant, and the Provider supplies the corresponding transparency notices from the date of application of Article 50 of Regulation (EU) 2024/1689. The artificial intelligence features are not intended for autonomous safety functions and do not replace the safety, protection and emergency systems of the plant.

15.6 Automated decision-making

The Provider does not carry out, on the Customer's behalf, automated decision-making producing legal effects concerning data subjects or similarly significantly affecting them. Where the Customer

configures the Platform to support decisions of that nature, the Customer is solely responsible for compliance with Article 22 GDPR, including human intervention and the information owed to data subjects.

Art. 16 — On-Premise and VPS deployment models

16.1 Criterion of application

This DPA is entered into for every deployment model, including On-Premise, and this Article is the single source of its scope of application to the On-Premise and VPS deployment models: no other document of the Agreement defines that scope. The application of this DPA to the On-Premise and VPS deployment models depends on a single criterion: whether the Provider has actual access to Customer Personal Data in intelligible form. The mere supply of the software, the issue of licence grants and the verification of their validity do not, of themselves, constitute processing of personal data on behalf of the Customer.

16.2 On-Premise without remote access

Where the Platform is installed on systems of the Customer, or on a server supplied on loan for use located at the Customer's premises, and the Provider has no remote access to the Customer's data and performs no support activity involving access to that data in intelligible form, the Provider is neither processor nor controller of the data processed by the Customer through the Platform and this DPA does not apply. In that configuration the Provider undertakes that: the licence-verification mechanism transmits only the identifiers of the signed grant, of the installation and of the designated asset, and no content data; a grace period of thirty days applies where verification cannot take place; the confidentiality obligations of the Agreement and of the non-disclosure agreement remain fully applicable. The Customer remains solely responsible, as controller, for the data processed on its systems.

16.3 On-Premise with remote support access

Where the Customer requests, authorises or enables remote or on-site support, maintenance, updating, diagnostic or fault-correction activities that involve access to Customer Personal Data in intelligible form, the Provider acts as processor and this DPA applies to those activities alone. In that case: each session is authorised in advance by the Customer and recorded in a support log stating the date, the operator, the purpose and the systems accessed; the Provider accesses only the data strictly necessary; supervised remote sessions are preferred over the extraction of copies; any copy taken for diagnostic purposes is deleted within thirty days of the closure of the intervention and, on request, a certificate of deletion is issued.

16.4 Change of configuration

If the factual circumstances change, and in particular if remote access to data in intelligible form is enabled after activation, Article 16.3 applies automatically from that date, without further formality, and the Parties record the change in the support log. Neither Party may rely on the absence of a

separate agreement to exclude the application of this DPA to processing that has actually taken place.

16.5 VPS deployment model

Where the Platform is provided on a virtual private server operated by the Provider, the Provider acts as processor and this DPA applies in full. The supplier of that infrastructure is a Sub-processor, is identified in the Order before activation and is listed on the Sub-processor Page in accordance with Article 8.3; only suppliers with data centres located within the EEA are used.

16.6 Return of the server supplied on loan

On the return of a server supplied on loan for use, the Provider performs a secure erasure of the storage media, in accordance with a documented procedure, before any reuse, and issues a written record of the erasure. Prior to collection, the Customer is given the opportunity to retrieve its data in accordance with Article 14.2.

Art. 17 — Liability and indemnities

17.1 Liability towards data subjects

Article 82 GDPR governs the liability of the Parties towards data subjects and is not modified by this DPA. No provision of this DPA or of the Agreement limits the rights of data subjects.

17.2 Liability between the Parties

As between the Parties, liability arising from this DPA is subject to the aggregate limitation of liability set out in the Master Terms, equal to the fees paid by the Customer in the twelve months preceding the event giving rise to liability. That limitation does not apply, and may not be relied upon, in cases of wilful misconduct or gross negligence, in accordance with Article 1229 of the Italian Civil Code, nor in respect of the liability referred to in Article 17.1.

17.3 Recourse

Where one Party has paid full compensation for the damage suffered by a data subject, it is entitled to claim back from the other Party that part of the compensation corresponding to that other Party's part of responsibility, in accordance with Article 82(5) GDPR.

17.4 Indemnities

The Customer holds the Provider harmless from the consequences of instructions that infringe Data Protection Law, of the absence of an appropriate lawful basis, of the failure to provide the information owed to data subjects and of the uploading of content in breach of Article 5.6. The Provider holds the Customer harmless from the consequences of processing carried out in breach of this DPA or contrary to the Customer's lawful instructions.

17.5 Administrative fines

Each Party bears the administrative fines imposed upon it for breaches attributable to its own conduct. Where a fine is imposed as a result of conduct attributable to the other Party, the affected Party may claim it back within the limits of Article 17.2.

Art. 18 — Term, amendments, survival, governing law and jurisdiction

18.1 Term

This DPA takes effect on the date of acceptance or signature of the Agreement and remains in force for as long as the Provider processes Customer Personal Data, and in any event until the deletion operations under Article 14 have been completed.

18.2 Amendments

Amendments to this DPA are made in writing. The Provider may update Annexes 2 and 3 unilaterally, in accordance with Articles 7.2 and 8.3, provided that the level of protection is not materially reduced; the Customer's right of objection under Article 8.4 remains unaffected for changes to Annex 3.

18.3 Statutory adaptations

If new standard contractual clauses, new implementing decisions or new binding measures of the supervisory authorities are adopted, the Parties adopt them and adapt the Annexes within the time limits prescribed, and in the absence of a prescribed time limit within ninety days. Where a transfer tool is declared invalid or is withdrawn, the Provider informs the Customer without undue delay, suspends the affected transfers where necessary and proposes an alternative tool.

18.4 Survival

Articles 6, 12, 14 and 17 survive the termination of this DPA, together with any provision which by its nature is intended to survive.

18.5 Governing law and jurisdiction

This DPA is governed by Italian law. For business customers, in every country, the Court of Bergamo has exclusive jurisdiction over any dispute arising out of or in connection with this DPA, in accordance with Article 25 of Regulation (EU) 1215/2012, without prejudice to the right of the Provider to seek interim relief and injunctive orders before any competent court and to the optional arbitration provided for in the Master Terms. The mandatory protections of consumers, including the jurisdiction of the courts of the consumer's place of residence, are unaffected. Where the SCC apply, their governing law and their choice of forum prevail for the matters they govern, and the right of data subjects to bring proceedings under the SCC is unaffected.

18.6 Severability

If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in force and the Parties replace the invalid provision with a valid provision achieving as closely as possible the same economic and legal effect.

Art. 19 — Contact points, notices and records

19.1 Provider contact point

Data protection communications addressed to the Provider are sent to support@devibrain.com with the reference "GDPR" in the subject line, or by certified electronic mail to devibrain@pec.it, or by registered letter to DEVIBRAIN S.R.L., Via Coghetti 6, 24128 Bergamo (BG), Italy. Notifications of personal data breaches and requests from public authorities are also sent to that address and are handled as a priority.

19.2 Data protection officer

As at the version date the Provider has not appointed a data protection officer, the conditions of Article 37(1) GDPR not being met, and designates the contact point in Article 19.1 as the reference point for data protection matters. If those conditions are met, the Provider appoints a data protection officer, publishes the contact details on the Sub-processor Page and communicates them to the Customer.

19.3 Customer contact point

The Customer's contact point is the one stated in the Order or, absent such a statement, the administrator of the Customer's account on the Platform. The Customer keeps that contact point up to date and is responsible for the consequences of an invalid or unmonitored address, including in relation to the notices under Articles 8.3 and 10.1.

19.4 Form of notices

Notices under this DPA are valid if sent by electronic mail to the contact points, with a copy in the Platform's notification area. They take effect on receipt or, if later, on the date they state.

19.5 Records of processing

Each Party keeps the record of processing activities required by Article 30 GDPR. The Provider makes available to the Customer, on request and once per year, the part of its record under Article 30(2) GDPR that concerns the Customer.

Art. 20 — Specific approval of clauses

20.1 Clauses subject to specific approval

Pursuant to Articles 1341 and 1342 of the Italian Civil Code, the Customer declares that it has read and specifically approves the following provisions of this DPA: Article 5.2 (charges for further instructions), Article 5.3 (suspension of instructions considered unlawful), Article 7.2 (unilateral updating of the security measures), Article 7.3 (responsibilities of the Customer), Articles 8.1, 8.3, 8.4 and 8.6 (general authorisation, unilateral change and urgent replacement of Sub-processors), Article 9.3 (charges for additional assistance), Articles 13.2, 13.4 and 13.5 (procedure, costs and limits of the audit), Article 14.3 (deletion periods), Article 17.2 (limitation of liability between the Parties), Article 17.4 (indemnities), Article 18.2 (unilateral amendment of the Annexes) and Article 18.5 (governing law, exclusive jurisdiction and reservation of arbitration).

20.2 Digital acceptance

Where this DPA is accepted through the self-service flow, the specific approval under Article 20.1 is given in a separate step, distinct from the acceptance of the document as a whole, confirmed by a one-time code sent to the electronic mail address of the person accepting and recorded in the acceptance evidence together with the timestamp, the internet protocol address, the user agent, the account and the hash and version of the document.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

Ai sensi e per gli effetti degli artt. 1341 e 1342 c.c., il Cliente dichiara di avere letto e di approvare specificamente le clausole richiamate nel presente blocco.

Luogo e data: _____

DEVIBRAIN S.R.L.	IL CLIENTE
_____	_____

Annex 1 — Description of the processing

This Annex satisfies Article 28(3) GDPR and constitutes Annex I.B of the SCC where the SCC apply.

A1.1 Subject-matter, nature and purpose

The subject-matter of the processing is the personal data contained in the content that the Customer and its Authorised Users enter, upload or generate through the Platform. The nature of the processing consists of collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, restriction and erasure, carried out by automated means, together with hosting, backup, security monitoring, technical support and, where activated, local artificial intelligence inference and per-tenant training. The purpose of the processing is the provision, operation, maintenance, security and support of the Platform on behalf of the Customer, in accordance with the Agreement and with the Customer's documented instructions, and for no other purpose.

A1.2 Categories of data subjects

• Authorised Users of the Customer, including engineers, plant operators, maintenance technicians, quality personnel and system administrators.

• Employees, collaborators, agency workers and contractors of the Customer whose data appears in dashboards, alarms, recipes, work instructions, shift assignments, audit trails or media managed through the Platform.

• Employees and representatives of the Customer's suppliers, system integrators and customers, where their data appears in the content uploaded by the Customer.

• Any other natural person whose data the Customer decides to include in the content it uploads, including data appearing in documents processed by the document-based training and document store features.

A1.3 Categories of personal data

Category	Examples of data	Source
Identification data	first name, surname, employee or badge number, personnel code	account creation and content uploaded by the Customer
Contact data	business electronic mail address, telephone number, department, site	account creation and content uploaded by the Customer
Account and authentication data	user name, salted hash of the password, role and permissions, multi-factor authentication factors, session identifiers	use of the Platform

Category	Examples of data	Source
Professional data	job title, qualification, shift, plant, line, competence for a given operation	content uploaded by the Customer
Activity data within the tenant	log-in and log-out records, actions performed, timestamps, internet protocol address, device and browser used, audit trail of changes	use of the Platform
Content data	documents, drawings, images, videos, audio recordings, recipes, alarm texts, annotations and free-text fields uploaded or generated by the Customer	content uploaded by the Customer
Technical and diagnostic data attributable to a person	application logs, error reports and support tickets where they contain the data of an identified or identifiable person	use of the Platform and support

A1.4 Special categories of personal data

None. The Customer is instructed under Article 5.6 not to upload special categories of personal data or data relating to criminal convictions and offences, save where expressly agreed in writing in the Order together with the supplementary measures required by the risk. Voice recordings processed by the transcription feature are not used for the unique identification of a natural person and therefore do not constitute biometric data.

A1.5 Processing operations by module

Module	Processing operations	Personal data typically involved
3D Builder	creation, storage and export of three-dimensional models, properties, diagnostics and viewpoints bound to a designated asset	identification and professional data of the operators shown in diagnostics and audit trails
Chart Builder	creation, storage and export of charts and traces	data of the operators associated with the recorded events

Module	Processing operations	Personal data typically involved
Tool Builder	management of documents, media, recipes and alarms	identification and contact data present in documents, media and alarm texts
Smart Process	conversion and analysis of plant diagrams and drawings	data of the persons named in the drawings and in the accompanying documentation
UI Designer	design and storage of dashboards and interfaces	data of the operators shown in the interfaces
Artificial intelligence assistant, document store, transcription and optical character recognition	indexing, transcription, extraction and per-tenant training on the content uploaded by the Customer	any personal data contained in the content uploaded by the Customer
Console and licence manager	management of Authorised Users, roles, signed licence grants and provisioning of the tenant	identification, contact and account data of the Authorised Users
Technical support	handling of tickets, diagnostics and supervised remote sessions	data present in the systems accessed during the intervention

A1.6 Frequency and duration

The processing is continuous for the hosted deployment models and occasional for support interventions in the On-Premise deployment model. The duration is the term of the Agreement, plus a retrieval period of thirty days, deletion from production environments within a further thirty days and purging of the backup copies at the next rotation cycle and in any event within sixty days from the end of the retrieval period.

A1.7 Retention within the Platform

Content data is retained for as long as the Customer keeps it in its tenant and is deleted when the Customer deletes it or when the periods in Article 14 expire. Application and access logs are retained for twelve months and then deleted or aggregated in a form that does not permit identification.

Backup copies are retained for thirty days on a rolling basis. Voice recordings are deleted once the transcription has been produced and in any event within thirty days.

A1.8 Transfers to Sub-processors

The subject-matter, nature and duration of the processing carried out by the Sub-processors are those stated in Annex 3 for each of them and are limited to what is necessary for the service entrusted to them.

Annex 2 — Technical and organisational security measures

This Annex describes the measures implemented under Article 32 GDPR and constitutes Annex II of the SCC where the SCC apply. The measures are binding on the Provider and may be updated only in accordance with Article 7.2.

A2.1 Pseudonymisation and encryption

Data in transit is protected by transport layer security version 1.2 or higher, with certificates managed automatically and renewed before expiry, on every public interface and between the components exposed outside the host. The production hosts use full-disk encryption of the volumes containing the data. Backup copies are encrypted with the advanced encryption standard using a key length of 256 bits, and the keys are kept separately from the backups. Passwords are stored only as salted one-way hashes. Licence grants are signed with elliptic curve cryptography on the P-256 curve; the private signing key is held solely in the management console, never in the tenant environments, and is never included in the images distributed to customers. Usage Data and telemetry are pseudonymised wherever technically possible.

A2.2 Confidentiality and access control

Access is by individual, nominal credentials, with role-based permissions and the least-privilege principle. Multi-factor authentication is required for administrative access to the console and to the infrastructure. Sessions expire after a period of inactivity. Administrative permissions are reviewed at least every six months and revoked on the day the relationship terminates. Access to production is granted only for the time necessary to handle a request and is logged. Secrets and credentials are not stored in source code repositories.

A2.3 Integrity and separation of processing

Each tenant runs in a dedicated container group with its own database and its own network, without shared application state between tenants. Segregation between development, test and production environments is enforced; production data is not used for development or testing, and where a copy is strictly necessary it is anonymised beforehand. Changes to the software follow a documented

process with version control, peer review and end-to-end tests before release. Administrative actions are recorded in a tamper-evident audit trail. Evidence of acceptance of the contractual documents is stored in tamper-evident form and retained for ten years.

A2.4 Network and application security

The infrastructure is exposed through a single hardened edge component; the application ports are not published directly. The internal networks are segmented by function and by tenant. The application front ends do not load fonts, scripts, style sheets or other resources from external content delivery networks at runtime, all static resources being hosted locally; this constraint, adopted for air-gapped industrial environments, also prevents unintended transfers of network identifiers to third parties. Content security policies restrict the sources permitted to the browser. Dependencies are monitored and updated; security corrections are applied within the periods graduated by common vulnerability scoring system severity set out in Article 7.3 of the Service Level Agreement (IUX-EN-30), which is the single source of those periods and which this Annex does not reduce.

A2.5 Availability, backup and continuity

Backups are performed daily, retained for thirty days on a rolling basis and stored separately from the production systems within the EEA. Restore tests are carried out at least twice a year and the results are documented. The recovery objectives and the availability levels are those stated in the Service Level Agreement (IUX-EN-30). The infrastructure is protected against power failures and monitored for saturation of storage and computing resources.

A2.6 Incident management

A documented incident management procedure is in place, defining classification, escalation, containment, eradication, restoration and post-incident review, together with the notification to the Customer within forty-eight hours provided for in Article 10.1. A single point of contact is designated for security incidents. Logs and evidence relevant to an incident are preserved for the time necessary for the investigation and for the exercise of rights.

A2.7 Personnel measures

Personnel are bound by written confidentiality undertakings, receive data protection and information security training on recruitment and periodically thereafter, and are subject to a documented offboarding procedure providing for the immediate revocation of accesses and the return of equipment. Access to Customer Personal Data is granted only on a need-to-know basis.

A2.8 Supplier management

Sub-processors are selected on the basis of documented due diligence covering security, location of processing and transfer safeguards, are bound by written contracts under Article 28(4) GDPR and are reassessed at least once a year. Suppliers with processing located within the EEA are preferred, and a supplier established outside the EEA is engaged only after the execution of the SCC and a TIA with a positive outcome.

A2.9 Physical security

The systems are housed in premises with controlled access, in rooms reserved for information technology equipment, with access limited to authorised personnel and recorded. Storage media that reach end of life are erased in accordance with a documented procedure or physically destroyed, with a written record.

A2.10 Data minimisation, quality and portability

The Platform allows the Customer to configure the fields collected, to correct and delete data and to export it in structured, commonly used and machine-readable open formats, including the formats used for models, charts, documents and images managed by the applications. Deletion functions operate on the production environment immediately and on the backup copies through the rotation described in Article 14.3.

A2.11 Governance and accountability

The Provider maintains the record of processing activities required by Article 30(2) GDPR, a register of security incidents, a register of the sub-processing relationships and the TIA documentation described in Annex 5. The measures in this Annex are reviewed at least once a year and following any significant incident or any material change to the architecture.

Annex 3 — Sub-processors

A3.1 Published list

The list of Sub-processors in force is published on the Sub-processor Page at https://www.industryux.com/legal/sub-processors, which states for each of them the identity, the registered office, the service entrusted, the place of processing, the categories of data concerned and the transfer tool where applicable, together with the date of the last update. The page allows subscription to change notifications by electronic mail. Changes are governed by Article 8.

A3.2 Sub-processors authorised as at the version date

As at the date of this Annex no external sub-processor is active. Customer Personal Data is processed exclusively by the internal operations function of the Provider, described in the table below. The engagement of any external Sub-processor is subject to the thirty days' prior notice under Article 8.3 and to the Customer's right of objection under Article 8.4, and the Sub-processor is

named — with its identity, registered office, service entrusted, place of processing, categories of data concerned and transfer tool — in that notice and on the Sub-processor Page before it begins to process Customer Personal Data.

Sub-processor	Service entrusted	Place of processing	Categories of data	Transfer tool
DEVIBRAIN S.R.L. — internal operations function	hosting, backup, monitoring, second-level support of the Enterprise Online environments on infrastructure operated directly by the Provider	Bergamo, Italy (EEA)	all the data described in Annex 1	not applicable, no transfer

A3.3 Statements

As at the version date no third party has access to Customer Personal Data. Remote inference is disabled by default and no Customer Personal Data is transmitted to a supplier outside the EEA in the absence of the express instruction and the safeguards provided for in Article 15.3; a supplier of remote inference becomes a Sub-processor only once it has been named in accordance with Article A3.2. Where the VPS deployment model is activated, the supplier of the infrastructure is engaged as a Sub-processor in accordance with Articles 8.3 and 16.5. In the On-Premise deployment model no Sub-processor is engaged, the data remaining on the Customer's systems.

A3.4 Suppliers of the Provider as controller

The following suppliers are not Sub-processors within the meaning of this DPA, since they process data in respect of which the Provider acts as controller under Article 2.2. They are listed here for transparency and are described in the Privacy Policy.

Supplier	Service	Place of processing	Role
Nexi Payments S.p.A.	acceptance and processing of card payments for self-service subscriptions	Italy (EEA)	independent controller for the payment transaction, processor for the data transmitted by the Provider

Annex 4 — Standard contractual clauses 2021/914

A4.1 Incorporation

Where a transfer of Customer Personal Data to a third country not covered by an adequacy decision takes place, the Parties execute the SCC, which are incorporated into this DPA by reference and completed as set out in this Annex. The Parties are deemed to have signed the SCC on the date of

acceptance or signature of the Agreement, for the modules applicable to their relationship. In the event of conflict, the SCC prevail over this DPA.

A4.2 Applicable modules

Module	Configuration	Application to the IndustryUX relationship
Module 1 — controller to controller	exporter controller, importer controller	residual; applies only to exchanges of business contact data with partners established outside the EEA acting as independent controllers
Module 2 — controller to processor	exporter controller, importer processor	applies where the Provider acts as controller under Article 2.2 and entrusts a processing operation to a supplier established outside the EEA
Module 3 — processor to processor	exporter processor, importer sub-processor	applies where the Provider, as processor for the Customer, engages a Sub-processor established outside the EEA, in particular a supplier of artificial intelligence inference or of cloud capacity; no such Sub-processor is engaged as at the version date
Module 4 — processor to controller	exporter processor established in the EEA, importer controller established outside the EEA	applies where the Customer is a controller established outside the EEA and the Provider, established in Italy, makes Customer Personal Data available to it or returns it to it

A4.3 Options selected

Clause	Option selected
Clause 7 — docking clause	included; further parties may accede with the agreement of the existing parties

Clause	Option selected
Clause 9 — use of sub-processors, Modules 2 and 3	Option 2, general written authorisation, with a notice period of thirty days as provided in Article 8.3
Clause 11 — redress	the optional paragraph on the independent dispute resolution body is not selected
Clause 13 — supervision	the competent supervisory authority is the Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Rome, Italy, the exporter being established in Italy; where the exporter is the Customer established in another Member State, the supervisory authority of that Member State is competent
Clause 17 — governing law	Option 1, Italian law
Clause 18 — choice of forum and jurisdiction	the courts of Italy, without prejudice to the right of data subjects to bring proceedings before the courts of their habitual residence

A4.4 Correspondence of the annexes

Annex of the SCC	Content	Source
Annex I.A — list of the parties	identity, address, contact point, activities and role of the parties	the identification details in the preamble of this DPA and in the Order for the Customer; for the importer, the details published on the Sub-processor Page and stated in the notice under Article 8.3
Annex I.B — description of the transfer	categories of data subjects and of data, frequency, nature, purposes, retention, sub-processing	Annex 1 of this DPA

Annex of the SCC	Content	Source
Annex I.C — competent supervisory authority	identification of the authority	Clause 13 as completed in Article A4.3
Annex II — technical and organisational measures	security measures of the importer	Annex 2 of this DPA and the measures of the importer stated in the notice under Article 8.3
Annex III — list of sub-processors, Module 3	identity and description of the processing	Annex 3 of this DPA and the Sub-processor Page

A4.5 EU-US Data Privacy Framework

The adequacy decision of 10 July 2023 concerning the EU-US Data Privacy Framework is in force but is not adopted as the primary transfer basis for the relationship governed by this DPA. The reasons are the following, assessed as at the version date: the judgment of the Supreme Court of the United States of 29 June 2026 in Trump v. Slaughter, which removed the protection against removal without cause of the members of the Federal Trade Commission, the authority on which the enforcement and redress mechanisms of that framework rest; the loss of quorum of the Privacy and Civil Liberties Oversight Board since January 2025, which prevents the annual reviews of the redress mechanism; and the appeal brought on 31 October 2025 before the Court of Justice of the European Union against the judgment of the General Court of 3 September 2025 in the Latombe case, still pending, which makes a further annulment of the adequacy decision a realistic prospect. Consequently the Provider adopts the SCC combined with the TIA in Annex 5 as its primary basis for transfers to the United States, and treats certification under that framework as an additional element of assessment. If the adequacy decision is annulled or withdrawn, the transfers already covered by the SCC and by the TIA continue without interruption.

A4.6 Supplementary measures

The supplementary measures adopted for transfers based on the SCC are, as a minimum: encryption in transit and at rest with keys held within the EEA and inaccessible to the importer; minimisation of the data transmitted, in particular in the prompts sent to remote inference

suppliers; a contractual prohibition on the importer using the data for its own purposes or retaining it beyond the time necessary; the transparency and challenge obligations set out in Article 12; and the periodic review of the TIA under Annex 5.

Annex 5 — Transfer impact assessment

A5.1 Purpose and method

Before any transfer based on the SCC, and periodically thereafter, the Provider carries out and documents a transfer impact assessment following the six-step method of Recommendations 01/2020 of the European Data Protection Board on measures supplementing transfer tools. The TIA is a document of internal accountability under Articles 5(2) and 24 GDPR; it is not published, but it is made available to the Customer on request under Article 13.1 and to the competent supervisory authority on request.

A5.2 The six steps and the content of the record

Step	Question to be answered	Content the record must state
1. Map the transfer	which data goes where, to whom and for what purpose	identification of the exporter and of the importer, the module of the SCC used, the categories of data and of data subjects, the volumes, the frequency, the technical route of the data, the onward transfers and any remote access from a third country
2. Identify the transfer tool	which instrument in Chapter V GDPR is relied upon	the module of the SCC executed, the date of execution, any adequacy decision relied upon as an additional element and the reasons why it is not adopted as the primary basis
3. Assess the law and practice of the third country	whether the law of the destination country compromises the effectiveness of the tool	analysis of the surveillance legislation applicable to the importer, in particular the provisions on access by public authorities for national security purposes and on extraterritorial production orders, the remedies available to non-nationals, the actual practice documented by public sources and the statements obtained from the importer, together with a reasoned conclusion on the level of risk

Step	Question to be answered	Content the record must state
4. Identify supplementary measures	which technical, contractual and organisational measures reduce the residual risk	the technical measures such as strong encryption with keys held in the EEA, pseudonymisation and minimisation of the content transmitted; the contractual measures such as transparency, challenge, notification and audit obligations; the organisational measures such as internal policies, training and periodic review; and the assessment of whether they are sufficient
5. Adopt the measures and formalise them	which procedural steps have been completed	the amendments made to the contract with the importer, the technical configurations activated, the date of adoption, the internal owner of the measure and the evidence of implementation
6. Re-evaluate at appropriate intervals	when the assessment is to be reviewed	the review date, at least annually, and the triggers for immediate review, namely a legislative change in the third country, an incident, a request from a public authority, a change of importer or a decision of a court or of a supervisory authority affecting the transfer tool

A5.3 Outcome and consequences

The record concludes with one of three outcomes: transfer permitted with the ordinary measures; transfer permitted subject to the additional measures identified, which are to be implemented before the transfer begins; transfer not permitted, in which case the transfer is not started or, if already begun, is suspended and the Customer is informed without undue delay in accordance with Article 18.3. The conclusion is dated, attributed to a named person responsible and approved by the legal representative of the Provider.

A5.4 Retention and updating

The TIA records, and their successive versions, are retained for the entire duration of the transfer and for five years after it ends. The register of the TIAs in force, indicating for each of them the importer, the country, the date of the last review and the outcome, forms part of the accountability documentation referred to in Article A2.11.

Validation note

This document is a release candidate version 1.2 of the IndustryUX contractual corpus, prepared on the basis of the legislation, case law and measures of the supervisory authorities in force on 10

August 2026. It is not a legal opinion. Before being used with real customers it must be validated by a qualified lawyer and, for the parts concerning the protection of personal data, by a qualified data protection professional, who is to verify in particular the correspondence between the measures described in Annex 2 and those actually implemented, the completeness of the list in Annex 3 with reference to the infrastructure in production, and the currency of the assessment in Article A4.5 concerning transfers to the United States, which depends on developments that are still in progress.

Changelog

Version	Date	Changes
1.0	2026-08-10	First release candidate
1.1	2026-08-11	Gate decisions: machine-bound Tokens, 24-month Prepaid Credit validity, On-Premise service-fee model
1.2	2026-08-11	Plan matrix 2026-08-11: the Pro plan is renamed Business and Enterprise Cloud is renamed Enterprise Online; channel references updated accordingly

IUX-EN-31 · v1.2 · 2026-08-11 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.