| Valid from | 08/15/2026 | Jurisdiction | EU — Regulation (EU) 2016/679 |
|---|---|---|---|

# Privacy Policy

IndustryUX Platform — Information on the processing of personal data under Articles 13 and 14 GDPR

| | |
|---|---|
| **Codice documento** | IUX-EN-33 |
| **Versione** | 1.1 |
| **Data** | 2026-08-11 |
| **Set** | ANNEXES (EN) |
| **Destinatari** | Data subjects — customers, authorised users, business contacts, website visitors |
| **Lingua** | English (authoritative) |
| **Classificazione** | Policy |

DEVIBRAIN S.R.L. (the "**Provider (DevIBrain)**", hereinafter the "**Provider**", "we", "us") provides this Privacy Policy under Articles 13 and 14 of Regulation (EU) 2016/679 ("**GDPR**") and under Italian Legislative Decree 196/2003 as amended ("**Italian Privacy Code**"). It explains which personal data we process, why, on which legal basis, with whom we share them, for how long we keep them and how data subjects may exercise their rights, in connection with the website www.industryux.com, the IndustryUX platform and the commercial relationships we establish through our three sales channels.

This Policy is an information notice, not a contract: it is not signed and it creates no obligations for the data subject. It is published in the legal section of www.industryux.com, linked from the sign-up flow and from the first access to the platform and to the DevIBrain Console, and delivered together with commercial proposals to the representatives of business customers.

The English text of this Policy is the authoritative text of the IndustryUX documentation set. Courtesy translations are made available; where a translation and the English text diverge, the reading that provides the data subject with the clearer and more protective information prevails, consistently with the transparency principle of Article 12(1) GDPR.

# Art. 1 — Purpose and scope of this Policy

## 1.1 What this Policy covers

This Policy covers the processing operations for which the Provider determines the purposes and the means, and therefore acts as **data controller**. In particular it covers: browsing of the website www.industryux.com; the creation and management of accounts and subscriptions; the purchase of subscriptions, token packages, one-off content and on-premise licences; billing, accounting and tax compliance; support and incident handling; security, licence verification and abuse prevention; the recording of evidence of acceptance of contractual documents; commercial communications; and the management of business contacts of corporate customers and prospects.

## 1.2 What this Policy does not cover

This Policy does not govern the processing operations in which the Provider acts as **data processor** on behalf of a business customer. Those operations are governed by the Data Processing Agreement (DPA) that forms part of the IndustryUX contractual documentation set, and the information duties towards the data subjects concerned lie with the customer, who is the controller. Art. 3 explains exactly where the boundary lies for each sales channel.

## 1.3 Cookies

The use of cookies and other tracking technologies on www.industryux.com and on the platform interfaces is described in the separate Cookie Policy, published at www.industryux.com/legal/cookie-policy, which forms an integral part of the information provided under Articles 13 and 14 GDPR and is summarised in Art. 10.

# Art. 2 — Controller, contact points and data protection officer

## 2.1 Controller

The controller is **DEVIBRAIN S.R.L.**, with registered office at Via Coghetti 6, 24128 Bergamo (BG), Italy, VAT and tax number IT04507220160, certified electronic mail (PEC) devibrain@pec.it, electronic mail support@devibrain.com.

## 2.2 Privacy contact point

All privacy matters, including requests under Articles 15 to 22 GDPR, are handled through a single dedicated contact point. Data subjects may write to support@devibrain.com or to the certified address devibrain@pec.it, using the subject line "GDPR — data subject request", or send a letter to the registered office indicated in clause 2.1 marked for the attention of the privacy contact point. Requests received through any other channel of the Provider are routed internally to the same contact point and are not rejected for reasons of form.

## 2.3 Data protection officer

The Provider has assessed the conditions of Article 37(1) GDPR and has concluded that none of the mandatory cases applies to its activity: the Provider is not a public authority, its core activities do not consist of processing operations that require regular and systematic monitoring of data subjects on a large scale, and they do not consist of large-scale processing of special categories of data or of data relating to criminal convictions and offences. A data protection officer has therefore not been designated, and the privacy contact point of clause 2.2 performs the internal coordination function. This assessment is reviewed at least once a year and whenever the processing operations change materially; should a data protection officer be designated, the contact details will be published in this Policy and notified to the supervisory authority.

## 2.4 Representative in the Union

The Provider is established in Italy and therefore Article 27 GDPR does not apply: no representative in the Union needs to be designated.

# Art. 3 — Privacy roles: how our role changes with the sales channel

## 3.1 Why this section exists

The Provider sells the IndustryUX suite through three distinct channels, and its role under data protection law is different in each of them, and even different for different categories of data within the same channel. This section makes that allocation explicit, as required by the principles of transparency and accountability of Articles 5(1)(a) and 5(2) GDPR, so that every data subject and every customer can identify who decides on the processing and whom to address.

## 3.2 The three channels

• **Channel 1 — Self-service shop (SaaS)**: purchases made directly on www.industryux.com, including the Free Trial plan, the Base plan and the one-off purchase of digital content such as custom web controls. This is the only channel open to consumers and to individuals acting outside a business activity.

• **Channel 2 — Enterprise Online**: managed dedicated single-tenant environments operated by the Provider for business customers, for the Business and Enterprise Online plans, sold under an order form and governed by the Master Subscription and Licence Terms (IUX-EN-01) and by the Enterprise Schedule (Schedule B, IUX-EN-20). Reserved to business customers holding a VAT number.

• **Channel 3 — On-Premise and managed VPS**: software licensed for installation on infrastructure of the customer or on a virtual private server, with or without a server provided under a loan-for-use arrangement. Reserved to business customers holding a VAT number.

## 3.3 Role map by category of data

In the following table, "**Controller**" means that the Provider determines purposes and means and that this Policy applies; "**Processor**" means that the customer is the controller, that the Provider processes only on the customer's documented instructions and that the DPA applies; "**No processing**" means that the Provider does not access the data at all and therefore holds neither role.

| Category of data | Channel 1 — Self-service shop | Channel 2 — Enterprise Online | Channel 3 — On-Premise and VPS |
|---|---|---|---|
| Registration, identity and account data of the person who subscribes | Controller | Controller | Controller |
| Contact and role data of the business representatives of the customer and of prospects | Controller | Controller | Controller |
| Billing, order, payment and tax data | Controller | Controller | Controller |
| Evidence of acceptance of contractual documents, one-time-password audit trail and files bearing a qualified electronic signature | Controller | Controller | Controller |
| Website browsing data, cookies and marketing preferences | Controller | Controller | Controller |
| Service-level telemetry, licence verification events, entitlement grants, security and access logs | Controller | Controller | Controller |
| Account data of the authorised users created by the customer inside its own environment | Not applicable | Processor | Processor where the Provider administers the environment, otherwise No processing |

| Category of data | Channel 1 — Self-service shop | Channel 2 — Enterprise Online | Channel 3 — On-Premise and VPS |
|---|---|---|---|
| **Customer Data**, as that term is defined in the Master Subscription and Licence Terms (IUX-EN-01): data that the customer or its users upload to or generate in the tools (operator and personnel data, dashboards, alarms, recipes, media, documents, prompts submitted to the artificial-intelligence features) | Processor where the user acts in a professional capacity, otherwise processing on the sole instructions of the user | Processor | No processing, unless remote support or a managed VPS is agreed, in which case Processor |
| Data accessed during a remote support session | Processor | Processor | Processor, limited to the session |
| Aggregated and anonymised statistics that no longer allow the identification of any person | Controller and outside the scope of the GDPR once anonymisation is complete | Controller and outside the scope of the GDPR once anonymisation is complete | Controller and outside the scope of the GDPR once anonymisation is complete |

## 3.4 The decisive criterion for Channel 3

For On-Premise installations the discriminating factor is effective access to the data, not the mere supply of the software. The Data Processing Agreement (IUX-EN-31) is entered into for all delivery variants, including On-Premise and managed VPS; its scope of application to On-Premise installations is the one set out in Article 16 of that document, which makes it operate only where the Provider has actual access to personal data of the customer in intelligible form. Where the Provider performs no remote maintenance and holds no credentials granting such access, the Provider does not process those data and is neither controller nor processor for them: the customer is the sole controller and the DPA, although executed, produces no effect in respect of that data flow. Where the customer requests remote support, receives updates that involve access to data in intelligible form, or purchases a managed VPS, the Provider acts as processor for the duration and within the scope of that activity, and the DPA applies in full. The applicable configuration is recorded in the order form and in the loan-for-use or service agreement.

## 3.5 Independent controllership

In no case does the Provider use Customer Data for its own purposes, and in particular it does not use it to profile data subjects, to build commercial offers or to train models made available to third

parties. Where the Provider acts as processor, any use of the data beyond the customer's instructions would make the Provider a controller under Article 28(10) GDPR, and the Provider undertakes not to make such use.

### 3.6 Referral to the DPA

For everything concerning the processor role — documented instructions, confidentiality of authorised personnel, security measures under Article 32 GDPR, engagement of sub-processors, assistance with data subject requests and with personal data breaches, deletion or return of the data at the end of the relationship, and audit rights — the applicable document is the DPA, which prevails over this Policy within its scope.

## Art. 4 — Categories of personal data we process

### 4.1 Data provided by the data subject

• Identification and contact data: first name, family name, business electronic mail address, telephone number, job title, company name, language and country.

• Account data: user name, credentials in hashed form, security settings, two-factor authentication data, session and device identifiers.

• Order and billing data: billing address, VAT number, tax code, order history, subscriptions, token balances, invoices, means of payment and payment status. The Provider never stores full payment card numbers or card security codes.

• Content of communications: support requests, messages, attachments, recordings of scheduled demonstration sessions where the participants have been informed in advance.

• Preferences: marketing consents and objections, communication settings, cookie preferences.

### 4.2 Data generated by the use of the service

• Service-level usage and telemetry data: features used, volume of processing, number and identifier of the designated machines, token consumption, performance and error data.

• Licence data: entitlement grants signed with an elliptic-curve digital signature and registered on the License Manager, activation codes, machine identifiers, results of the periodic licence verification, grace-period status.

• Security and access logs: date and time, network address, user agent, requested resource, outcome of the operation, authentication and administration events.

• Browsing data on the website, as detailed in the Cookie Policy.

### 4.3 Evidence data

The audit trail generated when a contractual document is accepted: date and time stamp, network address, user agent, account identifier, hash and version of the document accepted, evidence of the separate approval of the clauses requiring specific approval, and, in the enterprise workflow of the European Union, the file bearing the qualified electronic signature of the person empowered to sign, together with its validation report.

## 4.4 Special categories of data

The Provider does not seek and does not require special categories of personal data under Article 9 GDPR, nor data relating to criminal convictions and offences under Article 10 GDPR, for any of the purposes described in this Policy. Data subjects are asked not to include such data in support requests or in free-text fields. Where a customer chooses to process such data through the tools as Customer Data, that processing takes place under the customer's exclusive responsibility as controller and is governed by the DPA.

# Art. 5 — Sources of the data and information under Article 14 GDPR

## 5.1 Data not collected from the data subject

Some personal data reach the Provider from sources other than the data subject. This is the case, in particular, of:

• the contact and role data of the representatives, technical referents and signatories of a business customer or prospect, communicated by the customer itself, by a colleague of the data subject, by a distributor or by a partner;

• the identification data of the authorised users of an Enterprise Online environment, created inside the environment by the customer, in respect of which the Provider processes as controller only the service-level metadata described in clause 3.3;

• the contact data of professional contacts collected at trade fairs, industry events and webinars, or obtained from publicly accessible sources such as business registers, company websites and professional directories;

• data communicated by public authorities, by professional advisers of the parties or by third parties in the context of a claim or of a legal proceeding.

## 5.2 Categories concerned and timing of the information

The categories of data obtained from such sources are limited to identification, contact, role and, where relevant, technical account data. The Provider provides the information required by Article 14 GDPR within a reasonable period and in any case within one month of obtaining the data, or at the time of the first communication with the data subject if that occurs earlier, normally by referring to this Policy in the first electronic mail message sent to the data subject.

## 5.3 Public sources

Where data are obtained from publicly accessible sources, this Policy indicates that circumstance and the data subject may at any time ask which source was used, by writing to the contact point of clause 2.2.

# Art. 6 — Purposes of the processing and legal bases

## 6.1 Table of purposes

| Purpose | Data concerned | Legal basis |
|---|---|---|
| Registration, activation and management of the account and of the subscription; provision of the platform and of the purchased content | Identification, account, order data | Article 6(1)(b) GDPR where the customer is a natural person; Article 6(1)(f) GDPR where the contract is with a legal person and the data subject is its representative or authorised user, our legitimate interest being the performance of that contract |
| Management of orders, payments, invoicing, credit control and accounting | Order, billing, payment data | Article 6(1)(b) and Article 6(1)(c) GDPR, the latter for accounting, tax and electronic invoicing obligations |
| Qualification of the counterparty as a consumer or as a business, verification of the VAT number and of the powers of the signatory | Identification, tax, role data | Article 6(1)(c) GDPR and Article 6(1)(f) GDPR, our legitimate interest being the correct application of the mandatory consumer protection rules and of the segmentation of the sales channels |
| Recording and preservation of the evidence of acceptance of the contractual documents, including the separate approval of the clauses requiring specific approval, and archiving of documents bearing a qualified electronic signature | Evidence data of clause 4.3 | Article 6(1)(c) GDPR for the record-keeping duties imposed by consumer and electronic commerce legislation, and Article 6(1)(f) GDPR, our legitimate interest being the establishment, exercise and defence of legal claims, as further described in Art. 8 |

| Purpose | Data concerned | Legal basis |
|---|---|---|
| Verification of licences and entitlements, enforcement of the agreed usage metrics, reconciliation of token consumption and of the number of designated machines, detection of unauthorised use | Licence, telemetry, machine identifiers | Article 6(1)(f) GDPR, our legitimate interest being the protection of our intellectual property and the correct settlement of the fees due |
| Security of the platform and of the network, prevention of fraud and abuse, logging, backup, business continuity, vulnerability handling | Security logs, account and device data | Article 6(1)(f) GDPR and Article 6(1)(c) GDPR in conjunction with Article 32 GDPR and with the applicable cybersecurity legislation |
| Support, incident management, remote assistance sessions requested by the user | Communications, account, log data | Article 6(1)(b) GDPR and Article 6(1)(f) GDPR for business customers |
| Improvement, sizing and quality assurance of the service through aggregated or pseudonymised usage data | Service-level telemetry | Article 6(1)(f) GDPR, our legitimate interest being the development and stability of the service, with the right to object under Art. 18 |
| Direct marketing by electronic mail of products and services analogous to those already purchased, addressed to existing customers | Electronic mail address, purchase history | Article 130(4) of the Italian Privacy Code and Article 6(1)(f) GDPR, with the possibility to object free of charge at the time of collection and in every message |
| Newsletters, commercial communications and event invitations addressed to prospects and to persons who are not customers | Contact data, preferences | Article 6(1)(a) GDPR, consent, freely given and revocable at any time |
| Management of the professional relationship with the representatives of business customers and prospects | Contact and role data | Article 6(1)(f) GDPR, in line with Recital 47 GDPR, as described in Art. 7 |
| Handling of requests of data subjects and demonstration of compliance | All data strictly necessary | Article 6(1)(c) GDPR in conjunction with Articles 12 and 15 to 22 GDPR |

| Purpose | Data concerned | Legal basis |
|---|---|---|
| Establishment, exercise or defence of legal claims, management of disputes and recovery of receivables | Contract, evidence, communication data | Article 6(1)(f) GDPR |
| Screening required by export control and restrictive-measures legislation before activating a licence or a tenant environment | Identification data of the customer and of its representatives, country of destination | Article 6(1)(c) GDPR in conjunction with Regulation (EU) 2021/821 and with the restrictive measures in force |
| Cookies and similar tracking technologies | As detailed in the Cookie Policy | Article 122 of the Italian Privacy Code: consent, except for technical tools strictly necessary to provide the service |

## 6.2 Balancing test

Every processing operation based on legitimate interest has been assessed through a documented balancing test, which weighs our interest against the rights and freedoms of the data subject and records the safeguards adopted, such as data minimisation, pseudonymisation of the telemetry, restriction of access to authorised personnel and the possibility to object. A summary of the relevant balancing test is provided to any data subject who requests it at the contact point of clause 2.2.

## 6.3 Further purposes

Should the Provider intend to process personal data for a purpose other than that for which they were collected, it will first provide the information required by Articles 13(3) and 14(4) GDPR and, where necessary, obtain consent.

# Art. 7 — Business representatives and contacts of corporate customers and prospects

## 7.1 Who is concerned

This article concerns natural persons whose data we process because of their professional role: employees, collaborators, directors and technical or administrative referents of a customer, of a prospect, of a distributor, of a partner or of a supplier. In these cases the contractual counterparty is the organisation, not the individual, and the data processed are limited to business contact data.

## 7.2 Legal basis and legitimate interest pursued

The legal basis is our legitimate interest under Article 6(1)(f) GDPR. Recital 47 GDPR expressly recognises that the processing of personal data may be based on a legitimate interest where a relevant and appropriate relationship exists between the data subject and the controller, which is the case where the data subject is a client or is in the service of the controller's counterparty, and that data subjects may reasonably expect such processing at the time and in the context of the collection. The legitimate interests pursued are: managing the negotiation and the performance of the contract with the organisation, identifying the persons entitled to place orders, to sign documents and to receive technical or administrative notices, ensuring the traceability of the instructions received, and addressing business-to-business commercial communications that are pertinent to the professional role of the data subject.

## 7.3 Data minimisation and safeguards

Only data relating to the professional sphere are processed: name, business electronic mail address, business telephone number, role and organisation. No data of the private sphere are requested and none are inferred. Business contact data are not enriched with information purchased from data brokers and are not transferred to third parties for their own marketing purposes.

## 7.4 Right to object

The data subject may object at any time to the processing based on legitimate interest, including business-to-business commercial communications, by writing to the contact point of clause 2.2 or by using the unsubscribe link contained in every message. In case of objection to direct marketing, the processing for that purpose ceases immediately and unconditionally. In case of objection to other processing based on legitimate interest, the processing ceases unless the Provider demonstrates compelling legitimate grounds that override the interests, rights and freedoms of the data subject, or the need to establish, exercise or defend legal claims.

## 7.5 Change of role

Where the data subject informs us that he or she no longer holds the role for which the data were provided, the contact data are deleted or replaced with those of the new referent indicated by the organisation, save for the evidence data that must be retained under Art. 8.

# Art. 8 — Evidence of acceptance, electronic signatures and licence grants

## 8.1 Why we keep this evidence

The IndustryUX contractual documentation set is accepted through channel-specific mechanisms: a one-time password sent to the electronic mail address of the data subject, together with a complete audit trail, for the self-service channel and for non-European enterprise customers; the download, qualified electronic signature and re-upload of the document for enterprise customers established

in the European Union. Clauses requiring specific approval are always accepted in a separate second step. In order for these mechanisms to produce the intended legal effect, the evidence that a specific person accepted a specific version of a specific document at a specific moment must be preserved in a tamper-evident manner.

## 8.2 Data retained as evidence

The data listed in clause 4.3 are retained: date and time stamp, network address, user agent, account identifier, hash and version identifier of the accepted document, the result of the verification of the one-time password, the record of the separate approval step and, where applicable, the signed file with its signature validation report.

## 8.3 Legal basis and retention period

The processing is based on Article 6(1)(f) GDPR, our legitimate interest being the establishment, exercise and defence of legal claims and the ability to prove the content and the acceptance of the contract in the event of a dispute, and, for the elements that consumer and electronic commerce legislation requires us to record, on Article 6(1)(c) GDPR. The retention period is **ten years** from the termination of the contract to which the evidence relates, which corresponds to the ordinary limitation period for contractual claims under Article 2946 of the Italian Civil Code. Where a dispute, an audit or an inspection is pending or reasonably foreseeable at the end of that period, the evidence relating to that matter is retained until the matter is definitively closed.

## 8.4 Restricted access

Evidence data are stored in a dedicated repository with integrity controls, are accessible only to a restricted number of authorised persons for the purposes of contract management, dispute handling and compliance verification, and are never used for marketing, profiling or service improvement purposes.

## 8.5 Licence grants

Entitlement grants signed with an elliptic-curve digital signature, issued by the DevIBrain Console and registered on the License Manager, contain identifiers of the customer, of the environment and of the designated machines, and the record of the verification events. They constitute the technical evidence used for settlement and audit purposes and are retained as indicated in Art. 14. They contain no data other than those necessary to identify the entitlement and its holder organisation.

# Art. 9 — Commercial communications and consent management

## 9.1 Communications to existing customers

Where a data subject has provided an electronic mail address in the context of the purchase of a product or of a service, the Provider may use that address to send commercial communications concerning products and services analogous to those purchased, under Article 130(4) of the Italian Privacy Code. The data subject is informed of this possibility at the time of collection and may object, free of charge and in a simple manner, both at that time and in every subsequent message.

## 9.2 Communications requiring consent

Newsletters, invitations to events and commercial communications addressed to persons who are not customers, as well as communications concerning products that are not analogous to those purchased, are sent only with the prior, specific and freely given consent of the data subject. Consent is never a condition for the provision of the service, for the activation of a trial or for the purchase of a subscription.

## 9.3 Withdrawal of consent

Consent may be withdrawn at any time, with the same ease with which it was given, through the unsubscribe link in every message or through the contact point of clause 2.2. Withdrawal does not affect the lawfulness of the processing carried out before the withdrawal. Once withdrawal or objection has been recorded, the electronic mail address is kept in a suppression record for the sole purpose of ensuring that no further communications are sent.

## 9.4 No transfer for third-party marketing

Personal data are never sold, rented or otherwise transferred to third parties so that they may use them for their own marketing purposes.

# Art. 10 — Cookies and similar technologies

## 10.1 Referral to the Cookie Policy

The complete list of cookies and similar tracking technologies used on www.industryux.com and on the platform interfaces, together with their purpose, duration, nature and the identity of any third parties involved, is set out in the Cookie Policy published at www.industryux.com/legal/cookie-policy.

## 10.2 Consent and preferences

Tools that are not strictly necessary to provide the service requested by the user are installed only after the user has given consent through the banner. The banner offers, at the first level and with equal prominence, the commands to accept all tools, to reject all tools and to manage preferences; rejecting requires the same number of actions as accepting; the mere continuation of browsing or the scrolling of the page does not constitute consent; access to the website and to the service is not conditional upon consent to tracking. Recorded preferences are valid for six months, after which the banner is presented again. Preferences may be changed at any time from the link available in the footer of every page.

### 10.3 No external delivery of static assets

Fonts, icons, scripts and the consent management component used on our public interfaces are served from our own infrastructure and not from external content delivery networks, so that browsing our pages does not by itself cause the network address of the user to be communicated to third parties.

## Art. 11 — Automated decision-making, profiling and artificial-intelligence features

### 11.1 No automated decisions producing legal effects

The Provider does not take decisions based solely on automated processing, including profiling, that produce legal effects concerning the data subject or that similarly significantly affect the data subject, within the meaning of Article 22(1) GDPR. Automated controls exist for anti-fraud, anti-abuse and licence verification purposes, and they may flag an account or an environment for review; the suspension or the termination of a service is never the result of the automated control alone, but always of an assessment carried out by a member of our staff, and the customer is informed and may present its position.

### 11.2 No profiling of data subjects for commercial purposes

Usage and telemetry data are used at the level of the account, of the environment and of the designated machines for technical, licensing and statistical purposes. They are not used to build behavioural profiles of individual persons, nor to differentiate prices or commercial conditions on the basis of individual behaviour.

### 11.3 Artificial-intelligence features

The suite includes features that use artificial-intelligence models, such as the assistant, the analysis of process documents and the generation of content. Where those features are used, the input submitted by the user is processed for the sole purpose of returning the requested output. Inference is performed by default on models hosted on the Provider's infrastructure located in the European Union. Where a specific feature requires a model that can only be executed by an external provider, that provider acts as a processor or sub-processor, is listed in the sub-processor list referred to in Art. 12, and the activation of the remote path is disclosed in the applicable order form and in the DPA. Data submitted to the artificial-intelligence features are not used to train models made available to third parties.

### 11.4 Transparency of interaction with the artificial-intelligence system

Users are informed, in a clear and distinguishable manner and at the moment of the first interaction, that they are interacting with an artificial-intelligence system, and content generated or substantially modified by the system is identified as such, in line with the transparency duties of

Article 50 of Regulation (EU) 2024/1689. Users may at any time request the intervention of a member of our staff instead of the automated assistant.

# Art. 12 — Recipients of the data, processors and sub-processors

## 12.1 Categories of recipients

Personal data may be disclosed to the following categories of recipients, always within the limits of what is necessary:

• providers of hosting, colocation, connectivity and infrastructure maintenance services for the platform and for the tenant environments, established in the European Union;

• providers of transactional electronic mail and messaging services, used in particular to deliver one-time passwords, service notices and invoices;

• payment service providers, in particular Nexi Payments S.p.A. for the acceptance of card payments and of the recurring payment mandates: with regard to the payment transaction and to the obligations imposed on payment institutions by payment services and anti-money-laundering legislation, the payment service provider acts as an independent controller and applies its own privacy information notice;

• providers of specialised software and technical services used to operate the platform, including monitoring, backup and security tools operated within our infrastructure;

• accountants, tax advisers, auditors, lawyers, notaries, debt collection agencies, insurers and technical experts, who act either as processors or as independent controllers depending on their statutory position;

• the Italian Revenue Agency and its Interchange System for the transmission of electronic invoices, and other public authorities, judicial authorities and supervisory authorities where disclosure is required by law or by a valid order;

• purchasers or counterparties in a corporate transaction concerning the Provider or a business unit thereof, subject to confidentiality undertakings and to the information duties of Articles 13 and 14 GDPR.

## 12.2 Authorised personnel

Within the Provider's organisation, access is restricted to persons who need it in order to perform their duties, who have been designated as authorised persons under Article 29 GDPR and Article 2-quaterdecies of the Italian Privacy Code, who have received specific instructions and training and who are bound by confidentiality obligations that survive the end of their relationship with the Provider.

## 12.3 Processors

Third parties who process personal data on our behalf are appointed as processors under Article 28 GDPR by means of a written agreement that specifies the subject matter, the duration, the nature and the purpose of the processing, the categories of data and of data subjects, the security measures and the conditions for engaging further sub-processors, and that does not merely restate the text of the regulation but describes concretely how each obligation is met.

## 12.4 Sub-processors and general authorisation

Where the Provider acts as processor for a business customer, sub-processors are engaged under the general written authorisation provided for in Article 28(2) GDPR. The updated list of sub-processors, with the name, the location and the service provided by each of them, is published at www.industryux.com/legal/sub-processors. Customers are informed of any intended addition or replacement of a sub-processor at least thirty days before the change becomes effective and may object on reasoned data protection grounds within fifteen days of the notice; if the objection cannot be resolved, the customer may terminate the affected services without penalty, in accordance with the DPA.

## 12.5 No sale of data

Personal data are never sold and are never made available to third parties for purposes other than those described in this Policy.

# Art. 13 — Transfers of personal data outside the European Economic Area

## 13.1 Default location of the data

The platform, the Enterprise Online tenant environments and the related backups are hosted in data centres located in the European Union, with the primary infrastructure located in Italy. Each Enterprise Online customer is provided with a dedicated environment and a separate database, logically segregated from those of other customers.

## 13.2 When a transfer may occur

A transfer of personal data to a third country may occur only where a specific service requires it, in particular in the case of an external provider of artificial-intelligence inference activated for a specific feature, of a support tool of a non-European vendor, or of the disclosure of data to a business customer established outside the European Economic Area in respect of the data of its own environment.

## 13.3 Transfer instruments

Transfers take place only where one of the conditions of Chapter V of the GDPR is met, and in the following order of preference:

1. an adequacy decision of the European Commission under Article 45 GDPR. Among the relevant decisions, the two decisions concerning the United Kingdom were renewed on 19 December 2025 and are valid until 27 December 2031, so that data may circulate freely between the European Union and the United Kingdom;

2. the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, in the module appropriate to the specific scenario: Module Two for a transfer from the Provider as controller to a processor established in a third country; Module Three for a transfer from the Provider as processor to a sub-processor established in a third country; Module Four for the transfer of data to a customer established in a third country that acts as controller. The clauses are accompanied by the annexes describing the transfer and the security measures;

3. exceptionally, and never on a systematic or repetitive basis, a derogation under Article 49 GDPR, in particular where the transfer is necessary for the performance of a contract concluded in the interest of the data subject or for the establishment, exercise or defence of legal claims.

## 13.4 Transfer impact assessment and supplementary measures

Whenever the Standard Contractual Clauses are used, the Provider carries out and documents a transfer impact assessment, following the six-step methodology of the recommendations of the European Data Protection Board on measures that supplement transfer tools, and adopts the supplementary measures that the assessment identifies as necessary. These measures typically include encryption in transit and at rest with keys held within the European Union, pseudonymisation of the data transmitted, strict limitation of the categories of data involved, contractual commitments to notify and to challenge unlawful access requests, and periodic re-assessment.

## 13.5 Transfers to the United States

For importers established in the United States, the Provider does not rely solely on the adequacy decision concerning the EU-US Data Privacy Framework. The Standard Contractual Clauses together with the transfer impact assessment are maintained as the primary transfer instrument, so that the protection afforded to data subjects does not depend on the continued validity of that decision, which is the subject of pending judicial challenges. Where an importer is certified under that framework, its certification is treated as an additional safeguard and not as a substitute for the clauses.

## 13.6 Right to obtain a copy

Data subjects may obtain information on the transfers that concern them and a copy of the safeguards adopted, redacted where necessary to protect trade secrets and the security of the infrastructure, by writing to the contact point of clause 2.2.

# Art. 14 — Retention periods

## 14.1 General criterion

Personal data are retained only for as long as is necessary for the purposes for which they were collected, in accordance with the storage limitation principle of Article 5(1)(e) GDPR. At the end of the applicable period the data are deleted or irreversibly anonymised. Where a legal obligation, a pending dispute or an inspection requires a longer retention, the data concerned are retained only for that purpose and with restricted access.

## 14.2 Table of retention periods

| Data or processing | Retention period |
|---|---|
| Account and profile data of an active customer | For the whole life of the account |
| Accounts without an active subscription, including expired trials | Twelve months from the last access, then deletion or anonymisation, following a reminder sent thirty days in advance |
| Contract, order and channel documentation | Ten years from the termination of the contract, corresponding to the ordinary limitation period under Article 2946 of the Italian Civil Code |
| Evidence of acceptance, one-time-password audit trail, documents bearing a qualified electronic signature and their validation reports | Ten years from the termination of the contract, as explained in Art. 8 |
| Accounting, tax and electronic invoicing records | Ten years, under Article 2220 of the Italian Civil Code and under tax legislation |
| Payment and transaction data | Within the accounting records, ten years; authorisation and dispute data, thirteen months from the transaction for the management of chargebacks |
| Application and security logs | Twelve months, then deletion or anonymisation |

| Data or processing | Retention period |
|---|---|
| Aggregated product metrics derived from service-level telemetry, for as long as they still allow indirect identification | Twenty-four months, then deletion or irreversible anonymisation, in line with Article 7.6 of the Master Subscription and Licence Terms (IUX-EN-01) |
| Access logs of system administrators | Twelve months, in any event not less than the six months required by the general measure of the Italian supervisory authority of 27 November 2008 |
| Entitlement grants, activation records and licence verification events | For the term of the licence and for five years thereafter, for settlement and audit purposes |
| Support requests, correspondence and remote assistance records | Twenty-four months from the closure of the request, extended where necessary to establish, exercise or defend a legal claim |
| Marketing consents and commercial communications | Until withdrawal of consent or objection, with a review after twenty-four months of inactivity; records of withdrawal and objection are kept for the time necessary to guarantee that they are honoured and in any event no longer than ten years |
| Business contact data of prospects and professional contacts | Twenty-four months from the last meaningful interaction |
| Cookie preferences | Six months, then the banner is presented again |
| Evidence of the cookie consent given or refused | Twenty-four months after the end of the six-month validity of the choice, as evidence of compliance with Articles 5(2) and 7(1) GDPR, in accordance with the Cookie Policy (IUX-EN-34) |
| Backups | Rolling cycle of thirty days; a deletion request is propagated to the backup copies at the following cycle and in any event within sixty days |
| Job applications received spontaneously or in response to a call | Twelve months from receipt, then deletion |

| Data or processing | Retention period |
| --- | --- |
| Customer Data in an Enterprise Online environment, where the Provider acts as processor | For the term of the agreement, plus a retrieval window of thirty days after its end; deletion within thirty days from the expiry of that window, save for retention required by law, in accordance with the DPA |

### 14.3 Anonymisation

Aggregated statistics on the use of the service, produced from data that no longer allow any person to be identified, may be retained without a time limit, since they are no longer personal data.

## Art. 15 — Security of the processing and personal data breaches

### 15.1 Technical and organisational measures

The Provider implements appropriate technical and organisational measures under 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, as well as the risks for the rights and freedoms of natural persons. The measures include: encryption of data in transit and at rest; segregation of environments and of networks; role-based access control with the principle of least privilege and multi-factor authentication for administrative access; hardening and patching of systems; logging and monitoring; encrypted and tested backups; secure development practices, code review and vulnerability management; business continuity and restore procedures; training and confidentiality undertakings of authorised personnel; procedures for the management of security incidents. The detailed description of the measures applicable to the processor role is set out in Annex 2 to the DPA (IUX-EN-31).

### 15.2 Personal data breaches

Where a personal data breach occurs in respect of a processing operation for which the Provider is controller, the Provider notifies the competent supervisory authority without undue delay and, where feasible, within seventy-two hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons, and communicates the breach to the data subjects where it is likely to result in a high risk, in accordance with Articles 33 and 34 GDPR. Where the breach concerns a processing operation for which the Provider is processor, the Provider informs the customer without undue delay and provides the information and the assistance necessary for the customer to comply with its own obligations, in accordance with the DPA. All breaches are recorded in an internal register.

### 15.3 Reporting a vulnerability

Security researchers and users may report a suspected vulnerability or incident to support@devibrain.com. Reports are handled confidentially and, where the reporter so requests, without disclosure of his or her identity.

# Art. 16 — Nature of the provision of the data and consequences of refusal

## 16.1 Necessary data

The provision of the identification, contact, account and billing data marked as required in the forms is necessary to conclude and perform the contract and to comply with legal obligations. Refusal to provide those data makes it impossible to create the account, to activate the subscription or the licence, and to issue the invoice.

## 16.2 Evidence data

The generation of the audit trail of acceptance is an inherent consequence of the use of the acceptance mechanism and cannot be deactivated separately, since without it the acceptance of the contractual documents could not be proved. Business customers of the enterprise channel (Business, Enterprise Online, On-Premise and VPS) established in the European Union conclude the contract through the signed-document workflow of Art. 8, which produces a different, but equally retained, set of evidence; for the self-service shop the one-time-password acceptance given at registration is the only mechanism available.

## 16.3 Optional data

The provision of data for marketing purposes, of optional profile information and of the content of free-text fields is optional; refusal has no consequence on the provision of the service.

# Art. 17 — Minors

## 17.1 Age requirement

The IndustryUX platform is a professional tool and is not directed to minors. The self-service purchase of subscriptions and of digital content is reserved to persons who have reached the age of eighteen years and who have full legal capacity; the Enterprise Online, On-Premise and VPS channels are reserved to business customers.

## 17.2 Data of minors

The Provider does not knowingly collect personal data of minors. Where the Provider becomes aware that an account has been created by a minor, the account is suspended and the related personal data are deleted without undue delay, save for what must be retained in order to prove that the account was closed. Anyone who believes that a minor has provided personal data may notify the contact point of clause 2.2.

# Art. 18 — Rights of the data subject and how to exercise them

## 18.1 The rights

Data subjects have the following rights, within the limits and under the conditions set out in the GDPR:

• **Access** (Article 15 GDPR): to obtain confirmation as to whether personal data concerning them are being processed and, if so, access to those data and to the information listed in that article, together with a copy of the data.

• **Rectification** (Article 16 GDPR): to obtain the correction of inaccurate data and the completion of incomplete data.

• **Erasure** (Article 17 GDPR): to obtain the deletion of the data where one of the grounds of that article applies, in particular where the data are no longer necessary, where consent is withdrawn and no other basis applies, or where the data subject objects and no overriding legitimate ground exists. The right does not apply where the processing is necessary to comply with a legal obligation or to establish, exercise or defend legal claims, which is the case for the evidence data of Art. 8 and for the accounting records.

• **Restriction** (Article 18 GDPR): to obtain the restriction of the processing in the cases listed in that article, in particular while the accuracy of the data or the outcome of an objection is being verified.

• **Portability** (Article 20 GDPR): to receive the data provided to us, processed by automated means on the basis of consent or of a contract, in a structured, commonly used and machine-readable format, and to transmit them to another controller, including directly where technically feasible.

• **Objection** (Article 21 GDPR): to object at any time, on grounds relating to the particular situation of the data subject, to processing based on legitimate interest, and to object at any time and without any need for justification to processing for direct marketing purposes.

• **Withdrawal of consent** (Article 7(3) GDPR): to withdraw consent at any time, without affecting the lawfulness of the processing carried out before the withdrawal.

• **Not to be subject to automated decisions** (Article 22 GDPR), it being understood that no such decisions are taken, as stated in Art. 11.

## 18.2 How to exercise the rights

Requests are addressed to the contact point of clause 2.2. The request should indicate the right invoked and the elements necessary to identify the data concerned. The Provider may ask for additional information where it has reasonable doubts as to the identity of the applicant, and uses that information only for the purpose of that verification.

## 18.3 Time limits and costs

The Provider replies without undue delay and in any case within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and the number of the requests, in which case the data subject is informed of the extension and of the reasons for it within the first month. The exercise of the rights is free of charge; a reasonable fee may be charged, or the request refused, only where it is manifestly unfounded or excessive, in particular because of its repetitive character, and the Provider bears the burden of demonstrating that character.

## 18.4 Requests concerning data processed as processor

Where a request concerns data processed by the Provider on behalf of a business customer, the Provider is not entitled to reply directly. The request is forwarded to the customer, as controller, without undue delay, and the Provider provides the customer with the assistance required by Article 28(3)(e) GDPR. The data subject is informed of the transmission and of the identity of the controller to be addressed.

## 18.5 Relationship with the contractual export rights

The right to portability is separate from, and additional to, the contractual rights of export, retrieval and switching provided for in the IndustryUX contractual documentation set, which allow the customer to obtain its own data and content within the periods indicated in Art. 14 and free of switching charges. Exercising one does not preclude exercising the other.

# Art. 19 — Complaints and judicial remedies

## 19.1 Complaint to the supervisory authority

Every data subject has the right to lodge a complaint with a supervisory authority under Article 77 GDPR, in particular with the authority of the Member State of his or her habitual residence, of his or her place of work or of the place of the alleged infringement. The competent authority for the Provider is the **Garante per la protezione dei dati personali**, Piazza Venezia 11, 00187 Rome, Italy, telephone +39 06 696771, electronic mail garante@gpdp.it, certified electronic mail protocollo@pec.gpdp.it, website www.garanteprivacy.it.

## 19.2 Judicial remedy

Independently of the complaint, the data subject may bring proceedings before the competent judicial authority under Article 79 GDPR and Article 152 of the Italian Privacy Code. The two remedies may not be pursued simultaneously in respect of the same matter, in accordance with Article 140-bis of the Italian Privacy Code.

## 19.3 Prior contact

Data subjects are invited, but in no way obliged, to contact the point indicated in clause 2.2 before lodging a complaint, so that the matter may be resolved directly and rapidly.

# Art. 20 — Relationship with the DPA and with the contractual documentation set

## 20.1 Two distinct instruments

This Policy and the DPA are distinct instruments with distinct addressees. This Policy is addressed to data subjects and describes the processing operations for which the Provider is controller. The DPA is addressed to the business customer, is part of the contract, and governs the processing operations for which the customer is controller and the Provider is processor. Neither instrument replaces the other and, within their respective scopes, neither may be invoked to derogate from the other.

## 20.2 Order of precedence

Within the scope of the processor role, the DPA prevails over this Policy. Within the scope of the controller role, this Policy prevails over any commercial or technical description of the processing contained in other documents. The commercial and contractual terms of the relationship remain governed by the Master Subscription and Licence Terms (IUX-EN-01), by the applicable Channel Schedule — the Shop Schedule (Schedule A, IUX-EN-10) or the Enterprise Schedule (Schedule B, IUX-EN-20) — and by the order form, in the order of precedence set out in Article 2.3 of the Master Subscription and Licence Terms; none of those documents may reduce the level of protection afforded to data subjects by data protection legislation.

## 20.3 Customer obligations

Where a customer uses the platform to process personal data of its own employees, collaborators, customers or third parties, the customer is responsible for identifying an appropriate legal basis, for informing the data subjects and for defining retention periods within the tools. The Provider provides the technical means to configure deletion and export but does not decide on their use.

# Art. 21 — Changes to this Policy

## 21.1 How changes are made

This Policy may be updated to reflect changes in the processing operations, in the infrastructure, in the legislation or in the guidance of the supervisory authorities. Every version carries a version number and a date, and the superseded versions are archived and made available on request.

## 21.2 Notice of material changes

Where a change materially affects the processing of personal data of existing customers or users, in particular where it introduces a new purpose, a new category of recipients or a longer retention period, the Provider informs the data subjects concerned in advance, by electronic mail or through a notice displayed in the platform, at least thirty days before the change takes effect. Where the change requires consent, the change takes effect only in respect of data subjects who have given it.

## 21.3 Current version

The version in force is the one published at www.industryux.com in the legal section, and it is the version that applies to the processing operations carried out from its date of entry into force.

# Art. 22 — Version, status and validation note

## 22.1 Version

This Policy was issued as version 1.0, dated 10 August 2026, as the first version of the document in the restructured IndustryUX documentation set. It supersedes, for the processing operations described herein, the previous privacy information notices circulated within the Italian and worldwide documentation sets, whose content has been reviewed, corrected and completed. Version 1.1, dated 11 August 2026, renames the "Enterprise Cloud" channel as "Enterprise Online" following the adoption of the definitive plan matrix; the processing operations described are unchanged.

## 22.2 Validation note

This text is a release candidate at version 1.1, prepared on the basis of the legislation, the case law and the guidance of the supervisory authorities in force on 11 August 2026. It does not constitute legal advice and it does not replace the professional assessment of the specific situation of DEVIBRAIN S.R.L. Before this Policy is published or relied upon in relations with actual data subjects, customers or supervisory authorities, it must be reviewed and validated by a qualified lawyer and by the data protection professional appointed by DEVIBRAIN S.R.L. The validation must in particular verify: the factual accuracy of the descriptions of the infrastructure, of the recipients, of the sub-processors and of the retention periods, against the record of processing activities kept under Article 30 GDPR; the conclusion reached in clause 2.3 on the designation of a data protection officer; the completeness of the list of sub-processors and of the transfer impact assessments referred to in Art. 13; and the consistency of this Policy with the version of the Data Processing Agreement and of the Cookie Policy in force at the time of publication. DEVIBRAIN S.R.L. remains responsible for the accuracy of the factual elements described in this Policy and for keeping them up to date.

*IUX-EN-33 · v1.1 · 2026-08-11 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.*