Valid from	08/15/2026	**Jurisdiction**	Italy — D.Lgs. 231/2001

Code of Ethics

DEVIBRAIN S.r.l. — IndustryUX · Legislative Decree 231/2001

Codice documento	IUX-EN-36
Versione	1.0
Data	2026-08-10
Set	ANNEXES (EN)
Destinatari	Corporate bodies, employees, collaborators, consultants, partners, suppliers and resellers
Lingua	English (authoritative)
Classificazione	Policy

DEVIBRAIN S.R.L., with registered office at Via Coghetti 6, 24128 Bergamo (BG), Italy, VAT and tax identification number IT04507220160, certified electronic mail address devibrain@pec.it (**Provider (DevIBrain)**, designated as the **Provider** in the IndustryUX contractual documentation and referred to in this Code as the **Company**), owner of the IndustryUX platform and of the registered trade mark INDUSTRYUX®, adopts this Code of Ethics as the statement of the principles of conduct that govern every activity carried out in its name, on its behalf, in its interest or to its advantage.

DevIBrain designs and supplies industrial software: three-dimensional models, dashboards, technical content and artificial-intelligence assistants that its customers embed in machines, plants and control systems. The quality of that software has consequences on plants that other people operate. For this reason the Company treats integrity, technical honesty and respect for the law not as a formality of governance but as an engineering requirement of its own product.

Art. 1 — Purpose, legal framework and nature of this Code

1.1 Purpose

This Code of Ethics states the values, the principles and the rules of conduct that the Addressees defined in Article 2 must observe. Its purpose is to prevent unlawful conduct, to make the conduct expected of each Addressee foreseeable and verifiable, and to protect the reputation, the assets and the intangible rights of the Company and of its customers.

1.2 Legal framework

Legislative Decree no. 231 of 8 June 2001 governs the administrative liability of entities for offences committed in their interest or to their advantage by persons in senior positions or by persons subject to their direction. Under Articles 6 and 7 of that Decree, an entity may be exempted from liability only where it has adopted and effectively implemented an organisation, management and control model that is adequate to prevent offences of the type that occurred, and where an autonomous supervisory body has been entrusted with monitoring that model.

1.3 Nature of this document and its limits

This Code is adopted as an autonomous document. It is not, in itself, an organisation, management and control model within the meaning of Legislative Decree 231/2001, and it does not by itself produce the exempting effect described in clause 1.2, which requires in addition the mapping of the offence risks specific to the Company's activity, the preventive protocols for the sensitive processes, the supervisory body, the information flows and the disciplinary system. The Company states this limit expressly, rather than implying a compliance status it has not yet reached. Where a full model is subsequently adopted, this Code becomes an integral part of it under the conditions of Article 11.

1.4 Binding force

This Code is a unilateral corporate act, approved by the administrative body of DevIBrain. It is binding on the Addressees:

• for corporate bodies and employees, as an instruction on the performance of their duties under Articles 2104 and 2106 of the Italian Civil Code;

• for third parties, where it is incorporated into the relevant agreement in accordance with clause 2.4.

This Code does not create rights in favour of third parties, does not amend the contractual terms agreed with customers, suppliers or partners, and does not limit any obligation imposed by mandatory law.

1.5 Values

The conduct of the Company is founded on five values, which are to be used as the criterion of interpretation of every provision of this Code:

1. **Legality.** No commercial, technical or reputational objective justifies the breach of a rule of law.

2. **Technical honesty.** The capabilities, the performance and the limits of the IndustryUX platform

are described as they are. No demonstration, benchmark, specification or artificial-intelligence output is presented as more reliable than it is.

3. **Respect for the person.** Dignity, safety and equal treatment of the people who work with the Company and of the people who work on the plants where its software runs.

4. **Protection of what is entrusted to the Company.** Customer data, industrial know-how and intellectual property received in the course of a relationship are handled as if they were the Company's own, and are never used outside the purpose for which they were received.

5. **Traceability.** Every relevant decision, expense and communication must remain reconstructible ex post by a person who was not present when it was taken.

Art. 2 — Scope and Addressees

2.1 Addressees

This Code applies to:

• the members of the administrative body and any other corporate body of the Company, and any person exercising, in fact, powers of management or control;

• employees of every level and category, including apprentices, trainees and persons on secondment;

• self-employed collaborators, consultants, professionals, contractors and their personnel, agents, procurement intermediaries and temporary workers;

• resellers, distributors, integrators, technology partners and any person authorised to promote, resell or integrate IndustryUX;

• suppliers of goods and services, including providers of cloud infrastructure, connectivity and software components.

2.2 Territorial and operational scope

This Code applies to all activities of the Company, wherever carried out, including work performed remotely, activities carried out inside customer premises and activities performed on cloud environments and dedicated tenants operated for customers. Where the law of a country in which an activity is carried out imposes a stricter standard, that stricter standard prevails; where it imposes a laxer one, this Code continues to apply.

2.3 Duty to know, comply and report

Each Addressee must know the contents of this Code, comply with it, refrain from any conduct that may cause the Company to breach it, and report to the channels of Article 9 any conduct which the Addressee reasonably believes to be in breach of it. Ignorance of this Code is not an excuse; the

Company bears the burden of making it available and comprehensible under Article 11.

2.4 Additional duties of persons with responsibility

Persons who direct the work of others, who represent the Company towards third parties or who hold spending powers must in addition: set an example in their own conduct, ensure that the people they direct know this Code, refrain from giving instructions that conflict with it, and not tolerate a breach of it because it appears convenient or urgent. No instruction, target or deadline, from whatever level of the organisation, may derogate from this Code; an Addressee who receives such an instruction must refuse to execute it and report it under Article 9, and such refusal may never be a ground for any unfavourable measure.

2.5 Incorporation into contracts with third parties

The Company includes in its contracts with consultants, suppliers, partners and resellers a clause by which the counterparty declares that it has received this Code, undertakes to comply with it in the performance of the contract and acknowledges that a serious breach of it entitles the Company to terminate the contract with immediate effect under Article 1456 of the Italian Civil Code. Annex 1 contains the acknowledgement form used for this purpose.

Art. 3 — General principles of conduct

3.1 Legality

Addressees comply with the laws and regulations in force in every country where the Company operates, including those of criminal, corporate, tax, employment, health-and-safety, environmental, data-protection, export-control and sanctions law. Where a conduct is lawful but incompatible with the values of clause 1.5, it is nevertheless prohibited by this Code.

3.2 Honesty, good faith and no conflict of interest

Addressees act in good faith, keep the commitments they take, and do not exploit the ignorance, the urgency or the inexperience of a counterparty. They do not pursue, directly or through others, a personal interest in conflict with the interest of the Company, and they disclose any situation capable of generating such a conflict in accordance with clause 5.4.

3.3 Impartiality and non-discrimination

The Company does not discriminate on grounds of sex, gender identity, sexual orientation, age, ethnic or national origin, citizenship, language, disability, health condition, religion, political opinion, trade-union membership or personal and social conditions, in recruitment, remuneration, task assignment, training, promotion, discipline or termination, and applies the same rule to the selection of suppliers and partners.

3.4 Protection of the person

The Company protects the physical and moral integrity of the persons who work for it. Harassment, including sexual harassment, mobbing, intimidation, isolation of a colleague and any conduct that offends the dignity of a person, are prohibited and constitute a serious disciplinary offence. Working under the effect of substances that impair the ability to perform safety-relevant duties is prohibited.

3.5 Transparency and completeness of information

Information given to colleagues, corporate bodies, customers, authorities and the public must be truthful, complete, timely and not misleading by omission. Every entry in the accounts, in a timesheet, in an expense report, in a licence register or in a customer-facing report must correspond to a real, documented and verifiable event.

3.6 Protection of company assets and of the assets entrusted by others

Corporate assets, including hardware, credentials, cryptographic keys, source code, documentation and cloud resources, are used for corporate purposes only, protected against loss, misuse and unauthorised access, and never diverted for private benefit. The same protection applies to assets, data and know-how of customers and third parties held by the Company.

3.7 Fair competition

The Company competes on the merits of its products. Agreements or concerted practices with competitors on prices, markets, customers or tenders, the acquisition of competitors' confidential information by unlawful means, the denigration of competitors and any conduct capable of constituting an offence against industry and commerce are prohibited.

3.8 Areas of particular exposure

Without limiting the generality of this Code, the following areas are those in which the activity of the Company is most exposed to the offences relevant under Legislative Decree 231/2001, and are governed by the articles indicated.

Area of exposure	Rules of this Code
Relations with public authorities, tenders, grants, inspections	Article 4
Bribery in private-sector relations, gifts, conflicts of interest	Article 5
Computer crimes, unauthorised access, circumvention of licences	Article 6
Copyright and third-party software licences	Article 6
Protection of personal data and of customer information	Article 6

Area of exposure	Rules of this Code
Corporate communications, accounting and tax obligations	Article 7
Money laundering, self-laundering, payment flows	Articles 5 and 7
Health and safety at work, irregular employment	Article 8
Environmental obligations	Article 8
Export control, sanctions and embargoes	Articles 4 and 5

Art. 4 — Relations with the Public Administration

4.1 General rule

Relations with public administrations, public officials, persons in charge of a public service, public undertakings, supervisory and regulatory authorities and European Union institutions are conducted exclusively by persons expressly authorised by the administrative body, in writing, and are documented so that the content of each contact remains reconstructible. Addressees who are not so authorised do not enter into negotiations, do not make commitments and do not provide declarations on behalf of the Company.

4.2 Public tenders, grants and subsidised funding

In public tendering procedures and in applications for public funding, Addressees ensure that every declaration, certification, technical specification and reference submitted is truthful and complete, and that documents produced by third parties are verified before being submitted. Agreements with other participants aimed at altering the outcome of a procedure, the presentation of complacent offers and the misrepresentation of the Company's technical requirements are prohibited. Public funds and subsidised funding obtained are used exclusively for the purpose for which they were granted, and their use is separately documented.

4.3 Inspections, audits and proceedings

The Company cooperates with inspections, investigations and requests of the competent authorities. Addressees do not conceal, alter, destroy or make unavailable documents, data, log files or backups relevant to an inspection or a proceeding, do not induce any person to make false statements or to remain silent before a judicial authority, and do not hinder the exercise of the functions of supervisory authorities. Any request received from an authority is transmitted without delay to the administrative body.

4.4 Export control, licences and customs declarations

Software supplied outside the European Union may be subject to export-control legislation, in particular Regulation (EU) 2021/821 on dual-use items as amended, and to restrictive measures adopted by the European Union. Addressees do not submit false or incomplete statements to customs or licensing authorities, do not classify a product otherwise than in accordance with the classification formally adopted by the Company, and do not proceed with a supply for which an authorisation is required and has not been obtained. Any doubt as to classification or licensing is escalated before, and not after, the supply.

4.5 Prohibition of undue payments

It is prohibited to offer, promise, give, request or accept, directly or through an intermediary, money, goods, services, benefits, employment opportunities, charitable donations or any other utility, to or from a public official or a person in charge of a public service, in order to obtain or reward an act, an omission or an advantage. The prohibition applies irrespective of the value involved and irrespective of local practice; payments intended to accelerate a routine administrative action are equally prohibited. It is likewise prohibited to offer employment, internships or consultancy assignments to a public official, or to a relative of one, in a context capable of being related to a decision affecting the Company.

4.6 Gifts and hospitality towards public officials

Gifts and hospitality towards public officials are prohibited, with the sole exception of promotional items bearing the corporate or product mark whose unit value does not exceed EUR 50, offered transparently, never in cash or in a form convertible into cash, authorised in advance in writing by the administrative body and recorded in the register kept under clause 5.3. Travel, accommodation and entertainment expenses for public officials may only be borne where they relate to a documented technical event, are proportionate and are authorised in advance in writing.

Art. 5 — Relations with customers, suppliers, partners and resellers

5.1 Contractual transparency and correctness of commercial information

Contractual terms are presented in a complete and comprehensible manner before the contract is concluded, including terms concerning duration, renewal, price adjustments, licence metrics, service levels, limitations of liability and the consequences of termination. Commercial materials, demonstrations, benchmarks and proofs of concept describe the platform as it actually performs in the configuration offered; the use of results obtained in a different configuration, of unrepresentative data or of functions not yet available, without saying so clearly, is prohibited. Statements concerning certifications, compliance status or third-party approvals may only be made where the Company holds the corresponding evidence.

5.2 Prohibition of bribery in the private sector

It is prohibited to offer, promise, give, request or accept money or any other utility, directly or through an intermediary, to or from directors, managers, employees, collaborators or agents of a customer, supplier, partner or competitor, in order to induce or reward an act or omission in breach of their duties of office or of loyalty, or to obtain an undue advantage. Conduct of this kind is a criminal offence under Article 2635 of the Italian Civil Code and a ground for immediate termination of any contract with the Company.

5.3 Gifts, hospitality and sponsorships in private-sector relations

Gifts and hospitality in private-sector relations are permitted only where they are of modest value, consistent with normal business courtesy, transparent, never in cash and never capable of influencing, or of appearing to influence, a decision. The internal threshold of modest value is EUR 150 per beneficiary per calendar year, considering all items cumulatively; above that threshold, prior written authorisation of the administrative body is required. Gifts given and received above EUR 50, and all authorisations granted under this clause and under clause 4.6, are recorded in a gift register kept by the function designated under Article 11. Sponsorships and donations are permitted only towards identified beneficiaries, on the basis of a written agreement, with traceable payment, and never where a beneficiary is designated by a counterparty in the context of a pending negotiation, tender or dispute.

5.4 Conflicts of interest

An Addressee is in a conflict of interest where a personal, family, financial or professional interest may influence, or reasonably appear to influence, the impartiality of a decision taken for the Company, including where the Addressee, a relative or a person with whom the Addressee cohabits holds an interest in a customer, supplier, partner or competitor, or performs activities for one of them. The Addressee must disclose the situation in writing to the administrative body as soon as it arises and in any event within five working days from becoming aware of it, must abstain from taking or influencing the relevant decision until a written instruction is given, and must comply with that instruction. Disclosures and instructions are recorded in a conflicts register kept by the function designated under Article 11. Failure to disclose is a disciplinary offence irrespective of whether any damage results.

5.5 Selection of suppliers, partners and resellers

Suppliers, partners and resellers are selected on objective and documented criteria of technical capacity, quality, security, reliability, service levels and price, with no preferential treatment based on personal relations. Before appointment, the Company verifies the existence and the regular standing of the counterparty, its position with respect to European Union restrictive measures, and, where the counterparty processes personal data or operates infrastructure on behalf of the Company or of its customers, its security and data-protection measures. The appointment of a supplier who processes customer personal data is subject to the rules applicable to sub-processors under the data processing agreement in force with the customer concerned.

5.6 Payments and prevention of money laundering

Payments are made and received only to and from bank accounts held in the name of the contractual counterparty, in the country in which that counterparty is established or in which the service is performed, against a regularly issued invoice or accounting document. Payments to third parties, to accounts in the name of individuals connected with the counterparty, or through structures whose purpose is not economically justified, are prohibited. Cash is not used for payments to or from counterparties, save for petty expenses duly documented and not exceeding EUR 100, and in any event within the limits set by anti-money-laundering legislation as in force from time to time. Any request to alter payment instructions received during a relationship is verified through a channel other than the one from which the request came, before any payment is made.

5.7 Sanctions, embargoes and restrictions along the commercial chain

The Company does not supply its products or services, directly or indirectly, to persons, entities or countries subject to restrictive measures which prohibit that supply, and screens customers, resellers and suppliers against the applicable lists of designated persons before entering into a relationship and, thereafter, on renewal. In supplies to counterparties established outside the European Union and not established in a partner country listed by the applicable sanctions legislation, the Company includes a contractual prohibition of re-export to, or use in, the Russian Federation and Belarus. Any circumvention of these rules, including through intermediaries, is prohibited and constitutes a ground for immediate termination.

Art. 6 — Data protection, intellectual property and information systems

6.1 Personal data

Personal data are processed lawfully, fairly and transparently, only for the purposes for which they were collected, only by persons authorised and instructed for that purpose, and only to the extent necessary. Addressees do not access customer environments, tenant data, mailboxes or log files except where necessary for the performance of a documented task, do not extract or copy personal data outside the authorised systems, and do not use personal data received in the course of a customer relationship for the Company's own purposes. The processing carried out on behalf of a customer is governed by the data processing agreement in force with that customer; personal data of a customer are not used to train, tune or evaluate artificial-intelligence models except where the customer has given a documented instruction to that effect.

6.2 Confidentiality and trade secrets

Information relating to the Company, its customers, its suppliers and its partners which is not public is confidential, whether or not it is marked as such, and is disclosed only to persons who need it for a legitimate purpose and are bound by equivalent obligations. Confidentiality obligations continue after the end of the employment or of the contractual relationship, in accordance with the terms of the applicable agreement, and, for information protected as a trade secret, for as long as it retains that character.

6.3 Intellectual property of the Company

The source code, the architecture, the algorithms, the documentation, the design, the trade marks and the licensing infrastructure of IndustryUX are the exclusive property of the Company. Addressees do not copy, disclose, publish or reuse them outside their duties, do not upload them to third-party services not approved by the Company, including public artificial-intelligence services, and do not retain copies after the end of the relationship. The private cryptographic keys used to sign licence grants are handled exclusively by the persons expressly designated, are never exported from the systems in which they reside, are never copied to a customer environment and are never transmitted outside those systems; any suspicion of compromise is reported immediately under clause 6.7. Works created by employees and collaborators in the performance of their duties belong to the Company in accordance with the applicable law and contract.

6.4 Intellectual property of third parties and open-source components

The Company respects the intellectual property of others. It is prohibited to install or use software without a valid licence, to exceed the scope of a licence held, to reproduce protected content without authorisation and to incorporate third-party or open-source components into IndustryUX without verifying and recording the applicable licence terms. Components subject to reciprocal licence conditions may not be combined with proprietary code in a manner capable of triggering an obligation to disclose or to license the Company's source code. The inventory of third-party components and of their licences is kept up to date and is a condition of every release.

6.5 Information systems and computer crimes

Addressees use corporate information systems in accordance with the security rules issued by the Company. It is prohibited to access without authorisation an information system of the Company, of a customer or of a third party, to exceed the limits of an authorisation granted, to intercept or interrupt communications, to introduce or spread malicious software, to hold or use tools designed to circumvent technical protection or licensing measures, to share individual credentials and to disable security controls. Credentials, tokens and interface keys are personal, are protected and are never transmitted through insecure channels. Testing activities against systems of third parties are permitted only on the basis of a prior written authorisation of the system owner.

6.6 Artificial intelligence

Where the Company supplies or operates artificial-intelligence functions, it makes their nature evident to the persons who interact with them, does not present their output as a verified engineering assessment, and maintains human review over decisions capable of affecting the safety of persons or plants. Addressees do not use artificial-intelligence tools in a manner that involves the transmission of confidential information, personal data or source code to services not approved by the Company, and remain personally responsible for the content they produce with the aid of such tools.

6.7 Reporting of incidents and vulnerabilities

Any security incident, loss or unauthorised disclosure of data, suspected compromise of credentials or keys, and any vulnerability of the platform of which an Addressee becomes aware, must be reported to the administrative body immediately upon becoming aware of it, and in any event without any delay capable of prejudicing the notification obligations of the Company or of its customers. Concealing an incident, or delaying its reporting in order to avoid a personal consequence, is a serious disciplinary offence.

Art. 7 — Corporate records, accounting, tax and financial integrity

7.1 Truthfulness and completeness of the accounts

Every operation is recorded accurately, completely, promptly and in a manner that permits its reconstruction, and is supported by adequate documentation. It is prohibited to make or to cause to be made an entry that does not correspond to reality, to omit an entry that is due, to create funds or reserves not recorded in the accounts, to issue or receive invoices for transactions that did not occur and to alter the accounting or supporting documentation.

7.2 Corporate communications and controls

Financial statements, reports and communications required by law and directed to shareholders, to the public and to supervisory authorities present the economic and financial situation of the Company faithfully. It is prohibited to conceal information or documents from persons entrusted with control functions, to hinder the performance of those functions, to distribute profits or reserves in breach of the law, and to influence the formation of a resolution of a corporate body by simulated or fraudulent means.

7.3 Tax obligations

The Company fulfils its tax obligations correctly and on time. Structures whose predominant purpose is to obtain an undue tax advantage, the use or issue of documentation relating to transactions that did not occur, and the concealment or destruction of accounting records are prohibited.

7.4 Use of corporate resources and expense reporting

Expenses are incurred in the interest of the Company, within the powers granted, and are reported truthfully and with adequate supporting documents. The use of corporate resources, including cloud resources and licences, for personal purposes or for the benefit of third parties is prohibited unless expressly authorised.

Art. 8 — Health, safety, employment and environment

8.1 Health and safety at work

The Company complies with the legislation on health and safety at work and considers safety a non-negotiable objective. Addressees comply with the prevention measures adopted, use the equipment and the protective devices provided, do not remove or disable safety measures, report risk situations and near misses, and observe the safety rules of the customer premises in which they work. No production or commercial urgency may justify the omission of a safety measure, and reporting a safety risk may never expose the reporting person to any unfavourable consequence.

8.2 Regular employment and protection of working conditions

The Company employs personnel exclusively on the basis of regular contracts, complies with the applicable collective bargaining and social-security obligations, does not employ persons who are not entitled to work, does not resort to labour intermediation outside the cases permitted by law and does not tolerate conditions of exploitation. The Company requires the same standards from contractors and suppliers operating on its behalf, and verifies their compliance where their personnel operate on the Company's or on a customer's premises.

8.3 Environmental responsibility

The Company complies with environmental legislation, in particular as regards the management and disposal of electrical and electronic equipment and of the waste it produces, and manages the energy consumption of the infrastructure it operates with attention to efficiency. Conduct capable of constituting an environmental offence, including irregular disposal, is prohibited.

Art. 9 — Reporting of breaches and protection of the reporting person

9.1 What may be reported

Any Addressee, and any person who becomes aware of relevant information in a work-related context, including candidates, former collaborators, trainees and personnel of suppliers and partners, may report conduct which they reasonably believe to constitute a breach of this Code, of the law, including offences relevant under Legislative Decree 231/2001, or of European Union law in the areas covered by Legislative Decree no. 24 of 10 March 2023. A report may concern a breach that has occurred, that is in progress or that, on the basis of concrete elements, is likely to occur.

9.2 Internal reporting channel

The Company makes available an internal reporting channel consisting of:

• a written channel by electronic mail to the address whistleblowing@devibrain.com, which is accessible exclusively to the person designated as Reporting Manager and is segregated from ordinary corporate mailboxes;

• a written channel by post, in a double sealed envelope marked as personal and confidential, addressed to the Reporting Manager at the registered office of the Company;

• an oral channel, by means of a direct meeting requested through either of the above channels and held, at the choice of the reporting person in person or by remote connection, within fifteen days of the request; the meeting is documented, with the consent of the reporting person, by recording or by minutes submitted to that person for verification.

Reports may be made anonymously and are handled in the same manner, to the extent that the information provided allows an assessment.

9.3 Handling of reports

The Reporting Manager is designated in writing by the administrative body, acts autonomously and is bound to confidentiality. The Reporting Manager acknowledges receipt of the report to the reporting person within seven days of receipt, carries out the necessary enquiries, requests further information where needed, and provides feedback on the action taken or planned within three months of the acknowledgement of receipt or, absent an acknowledgement, within three months of the expiry of the seven-day period. Where the report concerns the Reporting Manager, a member of the administrative body or a person to whom the Reporting Manager reports, the report is handled by an independent external professional designated in advance by the administrative body for that purpose, and the reporting person may in any case use the external channel referred to in clause 9.6.

9.4 Confidentiality and protection of personal data

The identity of the reporting person, of the persons involved and of any person mentioned in the report, together with the content of the report and the related documentation, is kept confidential and may not be disclosed without the express consent of the reporting person, save where disclosure is compulsory by law in the context of proceedings and within the limits there provided. Access to the channel and to the file is restricted to the persons designated under clause 9.3. Reports and the related documentation are retained for the time necessary to their handling and in any event for no longer than five years from the communication of the final outcome. Personal data manifestly not useful to the handling of the report are not collected or, if collected, are deleted without delay.

9.5 Prohibition of retaliation

Any retaliation against a person who has made a report, assisted a reporting person, or is connected to one, is prohibited. Retaliation includes dismissal, suspension, demotion, non-promotion, change of duties or place of work, reduction of remuneration, exclusion from training, negative evaluation, disciplinary measures, coercion, ostracism, early termination or non-renewal of a contract for the supply of goods or services, and any other unfavourable measure adopted by reason of the report. Any measure taken against a reporting person after a report is presumed, in the terms provided by law, to be retaliatory unless the Company proves that it is founded on reasons unconnected with the report. Persons who make a report benefit from the protective measures provided by Legislative Decree 24/2023, including limitations of liability in the cases there provided, and may report retaliation to the National Anti-Corruption Authority, which may impose administrative fines of up to EUR 50.000 for retaliation, for obstruction of a report or for failure to establish or properly manage the reporting channels.

9.6 External channel and public disclosure

The reporting person may use the external channel of the National Anti-Corruption Authority where the internal channel is not active or does not comply with the law, where an internal report has not been followed up, where there are reasonable grounds to believe that an internal report would not be effectively followed up or would expose the reporting person to a risk of retaliation, or where the breach may constitute an imminent or manifest danger to the public interest. Public disclosure is protected in the cases and within the limits provided by law. The use of the internal channel is encouraged but is not a condition of protection where those conditions are met.

9.7 Prohibition of abuse of the channel

Making a report which the reporting person knows to be false, or made for the purpose of harming a person, is prohibited and constitutes a disciplinary offence, without prejudice to any liability provided by law. The mere fact that a report is not confirmed after enquiry never constitutes an abuse, and never exposes the reporting person to any consequence, where the report was made on the basis of a reasonable belief.

9.8 Development of the channel

The Company applies the standards of this Article on a voluntary basis, in the awareness that the obligation to establish an internal reporting channel arises by law where the Company employs on average at least fifty subordinate workers in the preceding year, or where it adopts an organisation, management and control model under Legislative Decree 231/2001. Upon the occurrence of either condition, and in any event where the volume of reports so requires, the channel described in clause 9.2 is migrated to a dedicated platform providing encryption, segregation of access, management of anonymous dialogue and a complete audit trail, and the migration is notified to the Addressees under Article 11.

Art. 10 — Disciplinary and contractual consequences

10.1 Principles

The breach of this Code is sanctioned irrespective of whether it results in damage to the Company and irrespective of whether it constitutes a criminal offence. Sanctions are proportionate to the gravity of the conduct, to the degree of fault, to the position of the person and to any repetition, and are applied following a procedure that guarantees the prior communication of the facts and the right of the person concerned to be heard and to present a defence within the time provided by the applicable law and collective agreement.

10.2 Employees

For employees, the breach of this Code constitutes a breach of the obligations of Articles 2104 and 2105 of the Italian Civil Code and is sanctioned, in accordance with Article 7 of Law no. 300 of 20 May 1970 and with the national collective bargaining agreement applicable to the employment relationship, by one of the following measures according to gravity: verbal warning, written warning, fine not exceeding four hours of pay, suspension from work and from pay for up to ten days, dismissal for justified subjective reason or for just cause in the most serious cases, in particular where the conduct is capable of exposing the Company to liability under Legislative Decree 231/2001, involves the deliberate falsification of documents or accounts, the disclosure or misappropriation of confidential information or source code, the compromise of licensing keys, an act of retaliation against a reporting person, or a conduct that endangers the safety of persons.

10.3 Persons with management functions

For managers and for persons who direct the work of others, the sanctions of clause 10.2 apply with the additional consideration of the greater duty of example and of supervision. The failure to supervise, where it has made possible a breach by a subordinate, is itself sanctionable.

10.4 Members of the corporate bodies

Where a breach is attributable to a member of the administrative body or of another corporate body, the person handling the matter informs the shareholders' meeting, which adopts the appropriate measures, including revocation of the appointment, revocation of powers granted and the exercise of the liability action, without prejudice to any other remedy available to the Company.

10.5 Third parties

Where a breach is attributable to a consultant, contractor, supplier, agent, partner or reseller, the Company may, according to the gravity of the conduct, request its immediate cessation, suspend the performance of the contract, refuse the renewal of the contract, terminate the contract with immediate effect under the express termination clause referred to in clause 2.5 and claim compensation for the damage suffered, including reputational damage.

10.6 Relationship with the protection of the reporting person

No measure provided by this Article may be adopted against a person by reason of a report made in accordance with Article 9. The adoption of a disciplinary measure in breach of this clause is itself a serious disciplinary offence for the person who adopted it.

Art. 11 — Governance, dissemination, training and updating

11.1 Ownership and interpretation

This Code is approved, amended and interpreted by the administrative body of DevIBrain, which designates in writing the function responsible for its application, for the keeping of the gift and conflicts registers and for the handling of reports under Article 9. Until an organisation, management and control model with an autonomous supervisory body is adopted, the monitoring functions described in this Code are performed by the administrative body, which reports on them at least once a year.

11.2 Dissemination

This Code is published on the corporate website and made permanently available to employees and collaborators, is delivered to every new employee, collaborator and consultant at the beginning of the relationship, and is annexed to contracts with suppliers, partners and resellers under clause 2.5. Where the Company adopts a new version, the Addressees are informed and the new version is made available in the same manner.

11.3 Training

The Company provides training on the contents of this Code to every employee and collaborator within thirty days of the beginning of the relationship, and refresher training at least every twenty-four months and whenever a significant amendment is adopted. Training is documented and the records are retained. Persons operating in the areas of exposure listed in clause 3.8 receive training specific to those areas.

11.4 Requests for clarification

Any Addressee who has a doubt as to the application of this Code to a concrete situation may address a request for clarification to the function designated under clause 11.1, and must do so before acting where the doubt concerns a conduct capable of constituting a breach. A request for clarification made in good faith never exposes the person who makes it to any unfavourable consequence.

11.5 Review

This Code is reviewed at least every twenty-four months and whenever changes in legislation, in the organisation or in the activity of the Company so require, in particular upon the adoption of an organisation, management and control model, upon the establishment of a supervisory body, upon reaching the employment threshold referred to in clause 9.8 and upon a significant change in the products supplied. Each version bears a version number and a date; the version in force is the most recent one published under clause 11.2.

Art. 12 — Final provisions

12.1 Entry into force

This Code, in version 1.0, enters into force on 10 August 2026 and replaces any previous statement of ethical principles of the Company.

12.2 Governing law and language

This Code is governed by Italian law. The English text is the authoritative text; any translation is provided for convenience only and, in the event of a discrepancy, the English text prevails.

12.3 Relationship with contracts and with the law

This Code does not amend, and is not to be interpreted as amending, the contractual terms agreed between the Company and its customers, suppliers or partners, nor does it limit any obligation imposed by mandatory law. Where a provision of this Code is or becomes invalid or unenforceable, the remaining provisions continue to apply, and the invalid provision is replaced by the lawful provision closest to the intention it expressed.

12.4 Contacts

Requests for clarification, communications relating to this Code and reports other than those governed by Article 9 may be addressed to DEVIBRAIN S.R.L., Via Coghetti 6, 24128 Bergamo (BG), Italy, certified electronic mail devibrain@pec.it, electronic mail support@devibrain.com. Reports under Article 9 are addressed exclusively to the channels indicated in clause 9.2.

Annex 1 — Acknowledgement and undertaking by third parties

The undersigned counterparty, in connection with the contractual relationship in place with DEVIBRAIN S.R.L., declares:

1. to have received and read the Code of Ethics of DEVIBRAIN S.R.L., code IUX-EN-36, version 1.0 of 10 August 2026;

2. to undertake to comply with it, and to procure that its directors, employees, collaborators and sub-contractors engaged in the performance of the contract comply with it, in the performance of the contractual relationship;

3. to acknowledge that a serious breach of that Code entitles DEVIBRAIN S.R.L. to terminate the contract with immediate effect under Article 1456 of the Italian Civil Code, without prejudice to compensation for damage;

4. to have been informed of the reporting channels referred to in Article 9 of that Code and to undertake not to adopt any retaliatory measure against a person who makes a report through those channels;

5. that no situation of conflict of interest exists with respect to DEVIBRAIN S.R.L. other than those disclosed in writing before the signature of this acknowledgement.

Luogo e data: ____________________________

DEVIBRAIN S.R.L.	IL CLIENTE
____________________________	____________________________

Validation note

This text is a release candidate, version 1.0, of the Code of Ethics of DEVIBRAIN S.R.L. It has been prepared on the basis of the legislation and of the case law identified as being in force on 10 August 2026 and of the internal decisions recorded on the same date. It does not constitute legal advice and does not replace the professional assessment of a qualified lawyer or, as regards the provisions on personal data and on the reporting channel, of a data protection officer. Adoption of this text towards employees, collaborators and third parties requires its prior validation by a qualified professional, verification of the consistency of the values it states with the organisational reality of the Company at the time of adoption, and formal approval by the administrative body.

IUX-EN-36 · v1.0 · 2026-08-10 · IndustryUX® è un marchio registrato di DEVIBRAIN S.r.l.

IUX-ETHICS · v1.1 · en_US
Frozen copy — the authoritative record is the version stored in the IndustryUX legal registry.