

PRIVACY AND PERSONAL DATA PROTECTION POLICY



FEB/2021

Approval

Owner – Position / Department	Version	Date
Cleiton dos Santos Garcia	2.0	February 23, 2021

Document code: 01-A-DOC-LGPD-UPFLUX

Notice on this translation. This is an English courtesy translation of the document originally issued in Brazilian Portuguese (“Política de Privacidade e Proteção de Dados Pessoais – UpFlux”, 01-A-DOC-LGPD-UPFLUX, version 2.0). The Brazilian Portuguese version is the official document and shall prevail in the event of any discrepancy, divergence of interpretation or omission. Terminology note: **LGPD** is the Brazilian General Data Protection Law (Law No. 13,709/2018); **ANPD** is the Brazilian National Data Protection Authority; **Controller** and **Processor** render the original terms *Controlador* and *Operador*; **Data Subject** renders *Titular dos dados*. Section numbering has been preserved exactly as in the original.

Table of Contents

1 Introduction

- 1.1 Presentation and Objectives
- 1.2 Related Documents
- 1.3 Relationship with the Information Security Policy
- 1.4 Life Cycle of Physical and Logical Information

2 Scope

3 Data Protection Policy

- 3.1 The General Data Protection Law
- 3.2 Definitions
- 3.3 Principles relating to the processing of personal data
- 3.4 Data collection
 - 3.4.1 When the data subject provides the information
 - 3.4.2 When collection is automatic
 - 3.4.3 When obtained through our clients
 - 3.4.4 When obtained through third parties
- 3.5 Legal basis and purpose of data collection
 - 3.5.1 Consent
 - 3.5.2 Legal or Regulatory Obligation
 - 3.5.3 Execution of Public Policies
 - 3.5.4 Performance of a Contract
 - 3.5.5 Vital Interests of the Data Subject
 - 3.5.6 Legitimate Interests
 - 3.5.7 For the Regular Exercise of Rights
 - 3.5.8 For Credit Protection
 - 3.5.9 Guarantee of Fraud Prevention and Data Subject Security
- 3.6 Processing of personal data
 - 3.6.1 Processing of personal data for supplementary purposes
 - 3.6.2 Processing of data of children and adolescents
 - 3.6.3 Sharing of personal data
- 3.7 Data Protection Officer
 - 3.7.1 Tasks of the DPO

4 Processing Records (data mapping)

5 Rights of the Data Subject

- 5.1 Management of Data Subject requests

6 Data Protection Impact Assessment (DPIA)

- 6.1 Privacy by Design
- 6.2 Contracts Involving the Processing of Personal Data

7 International Transfer

8 Incident Management

9 Driving Compliance with the LGPD

Annex. UpFlux data processing activities

1 Introduction

1.1 Presentation and Objectives

UpFlux is a technology startup that helps companies increase their operational efficiency through Artificial Intelligence and Process Mining techniques. Its purpose is to provide transparency and agility for the understanding and improvement of workflows.

In its day-to-day operations, UpFlux makes use of a variety of data about individuals, including but not limited to:

- Employees and job applicants
- Clients
- Users and/or visitors of the website and system
- Suppliers
- Outsourced service providers

In collecting and using such personal data, the company is subject to a variety of laws that determine how such activities must be carried out and what the consequences are should those requirements not be met.

The purpose of this policy is therefore to set out the relevant legislation and to describe the measures UpFlux is adopting in order to ensure its compliance with the law and to protect all personal data entrusted to it as a result of its activities as a Controller and as a Processor.

1.2 Related Documents

This policy relates to other internal UpFlux rules and procedures, such as:

- Confidentiality Agreement;
- Employee Handbook;
- Information Security Policy.

1.3 Relationship with the Information Security Policy

The guidelines and definitions of this policy must be integrated with all the definitions of the Information Security Policy, such as:

- Information classification;
- Business continuity;
- Senior management commitment;
- Training and periodic assessment;
- Awareness and dissemination of culture;
- Review and updating;
- Internal and external audit;
- Incidents and disciplinary measures.

1.4 Life Cycle of Physical and Logical Information

For the purposes of this Privacy and Personal Data Protection Policy, physical and logical data are organized according to the following life cycle:

- **Data Collection:** consists of the moment at which the information is obtained from the data subject or from third parties on behalf of the data subject. Within the scope of Law No. 13,709, it covers the following processing operations: collection, production, reception and reproduction;
- **Data Storage:** consists of the physical or logical filing of the information in a UpFlux environment or in a third-party environment acting on behalf of UpFlux. Within the scope of Law No. 13,709, it covers the following processing operations: filing and storage;
- **Data Access:** consists of the use of the data for its processing. Within the scope of Law No. 13,709, it covers the following processing operations: use, access, processing, evaluation or control of information, modification and extraction;
- **Data Sharing:** consists of making data available to processors acting on behalf of UpFlux. Within the scope of Law No. 13,709, it covers the following processing operations: transmission, distribution, communication, transfer and dissemination;
- **Deletion:** consists of the definitive deletion of the data or of its anonymization in such a way that the data no longer allows the identification of a natural person. Within the scope of Law No. 13,709, it covers the following processing operation: deletion.

2 Scope

This policy applies to all personal data processed at UpFlux, both in its capacity as Controller and as Processor.

Controller Activities	Processor Activities
When acting as a Controller, UpFlux processes the personal data of its employees, partners, suppliers, business partners, interns, outsourced service providers, job applicants, volunteers, users and clients. For a more comprehensive overview of UpFlux's data processing activities as a Controller, refer to the Annex and to Supplementary Document B.	When acting as a Processor, UpFlux processes personal data on behalf of its clients, in accordance with their instructions. UpFlux uses Artificial Intelligence and Process Mining techniques to increase operational efficiency and improve workflows. For a more comprehensive overview of UpFlux's data processing activities as a Processor, refer to the Annex.

3 Data Protection Policy

3.1 The General Data Protection Law

The Brazilian General Data Protection Law (LGPD) is one of the most significant laws affecting the way in which UpFlux carries out its personal data processing activities. Significant administrative sanctions and fines are applicable. Accordingly, we have a duty to ensure compliance with the requirements of the LGPD and other relevant legislation, demonstrating at all times, clearly and transparently, that we are in compliance.

3.2 Definitions

The LGPD sets out a number of definitions. However, the most fundamental definitions in relation to this policy are the following:

- ✓ **Personal data:** information relating to an identified or identifiable natural person, that is, any data capable of identifying a person.
- ✓ **Sensitive Personal Data:** personal data concerning racial or ethnic origin, religious belief, political opinion, membership of a trade union or of a religious, philosophical or political organization, data concerning health or sex life, genetic or biometric data, where linked to a natural person.
- ✓ **Data subject:** the natural person to whom the personal data being processed refers.
- ✓ **Data processing:** any operation carried out with personal data, such as those relating to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination or extraction.
- ✓ **Controller:** a natural person or legal entity, governed by public or private law, responsible for the decisions regarding the processing of personal data.
- ✓ **Processor:** a natural person or legal entity, governed by public or private law, that carries out the processing of personal data on behalf of the controller.
- ✓ **Data Protection Officer (DPO):** the person appointed by the controller and the processor to act as a communication channel between the controller, the data subjects and the Brazilian National Data Protection Authority (ANPD).

3.3 Principles relating to the processing of personal data

UpFlux processes personal data in accordance with the principles set out in art. 6 of the LGPD, which are:

- I – **purpose:** carrying out the processing for legitimate, specific and explicit purposes informed to the data subject, with no possibility of subsequent processing in a manner incompatible with those purposes;
- II – **adequacy:** compatibility of the processing with the purposes informed to the data subject, in accordance with the context of the processing;
- III – **necessity:** limitation of the processing to the minimum necessary to achieve its purposes, covering data that is relevant, proportionate and not excessive in relation to the purposes of the data processing;
- IV – **free access:** guarantee to data subjects of facilitated and free consultation on the form and duration of the processing, as well as on the completeness of their personal data;
- V – **data quality:** guarantee to data subjects of accuracy, clarity, relevance and updating of the data, in accordance with the need and for the fulfilment of the purpose of its processing;
- VI – **transparency:** guarantee to data subjects of clear, accurate and easily accessible information on the carrying out of the processing and on the respective processing agents, subject to trade and industrial secrets;
- VII – **security:** use of technical and administrative measures capable of protecting personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;
- VIII – **prevention:** adoption of measures to prevent the occurrence of damage arising from the processing of personal data;
- IX – **non-discrimination:** impossibility of carrying out the processing for unlawful or abusive discriminatory purposes;
- X – **accountability:** demonstration by the agent of the adoption of effective measures capable of proving the observance of and compliance with personal data protection rules and, further, the effectiveness of such measures.

3.4 Data collection

UpFlux collects personal data only where it needs the data for a legitimate purpose. Such data is collected, but not limited to, as follows:

- a) the data subject itself provides the information;
- b) collection is automatic;
- c) obtained through our clients;
- d) obtained through third parties.

Set out below is a description of the various scenarios falling within each of these four categories and of the information collected in each of them.

3.4.1 When the data subject provides the information

Some of the personal information collected by UpFlux is provided by the data subject. This occurs when the individual:

- ✓ Fills in forms made available on the website
- ✓ Sends a CV to apply for a job vacancy
- ✓ Is hired by the company
- ✓ Supplies something to the company
- ✓ Becomes a client
- ✓ Contacts the company by telephone, messaging application, e-mail or in person
- ✓ Creates a login and password to access the system
- ✓ Downloads our files

- ✓ LinkedIn

3.4.2 When collection is automatic

Some personal data is collected automatically when the individual visits our website or accesses our system or application. Such collected data originates from:

Browsers, devices and servers:

- ✓ Internet protocol address
- ✓ Browser type
- ✓ Time zone
- ✓ Referring URL
- ✓ Date and time of access
- ✓ Language preference
- ✓ Operating system

Application logs and mobile analytics, cookies and tracking technology:

- ✓ Clicks
- ✓ Scrolling
- ✓ Features accessed
- ✓ Time and frequency of access
- ✓ Errors generated
- ✓ Performance data
- ✓ Location
- ✓ Browsing performance

3.4.3 When obtained through our clients

The largest database containing personal information held by UpFlux is supplied by our clients. With regard to such data, UpFlux acts solely as the data Processor. For this personal data, UpFlux has no decision-making power, the processing being carried out in accordance with the instructions of the client, which is the data Controller.

Where UpFlux collects data in the capacity of Processor, it must observe the following guidelines:

- In collection situations in which UpFlux receives the data from another company and not directly from the data subject, a contract must be established with the data Controller.
- The contract with the data Controller must hold the Controller responsible for the sharing of such data.
- The contract with the data Controller must define the processing purposes permitted to UpFlux.
- The data Controller must provide guidance on the appropriate handling by UpFlux of the information provided.

3.4.4 When obtained through third parties

Some of the personal data collected and processed by UpFlux is received from third parties. Such data originates from, but is not limited to:

- ✓ Interaction on UpFlux's social media channels
- ✓ Referrals
- ✓ Cookies

3.5 Legal basis and purpose of data collection

There are several alternatives for carrying out data processing lawfully, as provided for in the LGPD. It is UpFlux's practice to identify the appropriate legal basis for carrying out the processing. The available legal bases are briefly described in the topics below.

3.5.1 Consent

UpFlux obtains the explicit consent of a Data Subject in order to collect and process their data, save for the exceptions provided for in the LGPD.

3.5.2 Legal or Regulatory Obligation

Where the data is necessary in order to comply with a legal obligation, explicit consent will not be required. In this case, the processing is justified by the requirements of other laws or decrees in force.

3.5.3 Execution of Public Policies

Where UpFlux performs a task in the public interest or an official duty, the consent of the Data Subject will not be requested. The assessment of the public interest or of the official duty will be documented and made available as evidence when necessary.

3.5.4 Performance of a Contract

Where the personal data collected and processed is necessary in order to perform a contract with the Data Subject, explicit consent will not be required. There are two situations in which UpFlux may process data relying on this legal basis: a) for contractual obligations to be performed; b) where it relates to preliminary acts of the contract, that is, the pre-contractual phase.

3.5.5 Vital Interests of the Data Subject

In cases where personal data is necessary in order to protect the vital interests of the Data Subject, this basis will be used as the legal basis for the processing. UpFlux will maintain sufficient documented evidence of such situations.

3.5.6 Legitimate Interests

Where the processing of personal data occurs by reason of UpFlux's legitimate interest, and it is verified that it does not significantly affect the

rights and freedoms of the data subject, the processing will be safeguarded as lawful. In order to rely on this legal basis, UpFlux will carry out an applicability assessment.

3.5.7 For the Regular Exercise of Rights

Where personal data is necessary in order to exercise a constitutional principle such as bringing judicial, administrative or arbitration proceedings, the explicit consent of the data subject will not be required.

3.5.8 For Credit Protection

This is a legal basis that dispenses with the consent of the data subject. It is provided for in strict cases of credit protection. Simultaneous compliance with the relevant legislation is expressly required.

3.5.9 Guarantee of Fraud Prevention and Data Subject Security

This legal basis is applicable to the processing of sensitive personal data in order to ensure the identification and authentication of the data subject for the authentication of registration in electronic systems, with a view to the prevention of fraud and the guarantee of the data subject's security.

In order to fall within this legal basis, UpFlux will assess whether there is no other means of identifying the data subject without the need to process sensitive data. This legal basis refers, for example, to the possibility of using biometrics for identification and authentication in electronic systems. It should be noted that this legal basis may not be relied upon where the fundamental rights and freedoms of the data subject requiring the protection of personal data prevail.

3.6 Processing of personal data

When acting as a Controller, UpFlux will comply with the law as set out in this chapter; the largest volume of personal data processing will, however, occur under the following conditions:

Controller Activities	
Purpose	Legal Basis
Processing of personal data for government bodies and tax authorities.	Legal obligation
Processing of personal data for the performance of employment, client, supplier, outsourced service provider or partner contracts.	Performance of a contract
Processing of personal data in order to: personalize proposals, better meet the expectations of the data subject, enhance the business, attract clients and assess the performance of the team and of the services provided.	Legitimate Interest
Processing of personal data in order to record evidence of the unequivocal choice of the data subject.	Consent

When acting as a Processor, UpFlux will only process personal data under the following conditions:

Processor Activities	
Purpose	Legal Basis
When acting as a Processor, UpFlux must strictly comply with the instructions of the Controller, in particular with regard to the purpose of the processing of personal data. In other words, it must comply with the provisions established in the contract and/or in the terms of service.	The legal basis is an obligation of the Controller; UpFlux will therefore not assume responsibility for determining the legal basis on behalf of the Controller, nor the appropriate technical and organizational measures to be implemented in order to deploy the consent mechanism.

3.6.1 Processing of personal data for supplementary purposes

Where UpFlux considers processing personal data for purposes other than the initial purpose for which the data was collected (that is, supplementary purposes), and the data subjects have not given consent, UpFlux will first assess whether the supplementary purpose is compatible with the initial purpose. This assessment must consider:

- Whether there is any link between the initial purpose and the supplementary purpose;
- The context of the initial purpose, including the relationship between UpFlux and the data subject;
- The nature of the personal data, including whether it contains special categories;
- The potential consequences that the supplementary processing may have for the data subjects; and
- The existence of appropriate safeguards (such as encryption or pseudonymization).

If the processing is not compatible with the initial purpose and is not for the purposes of archiving in the public interest, scientific research purposes or statistical purposes, then the processing must not be carried out.

3.6.2 Processing of data of children and adolescents

The services provided by UpFlux are not directed at individuals under 18 years of age. As a Controller, UpFlux does not intentionally collect personal information of children and adolescents, except where necessary in order to comply with a legal obligation.

Should there be an exceptional need to collect data of persons under 18 years of age, the processing of the data will take place subject to the specific consent of their legal guardians.

As a Processor, however, UpFlux receives information of children and adolescents and processes such data in accordance with the terms stipulated by the data Controller. UpFlux therefore has no decision-making power over such data, and it is for the Controller to hold the legal basis and the consent management for the collection and processing of such data.

3.6.3 Sharing of personal data

UpFlux will use Processors that are committed to the privacy and security of information. Data must be shared only with service providers related to UpFlux's operations.

Sharing must observe the following guidelines:

- Every data sharing operation must generate a record of that sharing operation, by physical or logical means in accordance with each specific process.
- In addition to the purpose map, the data sharing entities must be listed where applicable to a given purpose (Supplementary Document C).
- Where the purpose involves sharing with another controller, such circumstance must be prominently stated in the purpose map.
- The correction of data internal to UpFlux must be passed on to all sharing entities, in a recorded and formal manner.
- The deletion of data internal to UpFlux must be passed on to all sharing entities, in a recorded and formal manner.

Note: *The communication or shared use, between controllers, of sensitive personal data concerning health for the purpose of obtaining an economic advantage is prohibited, save in the situations relating to the provision of health services, pharmaceutical assistance and healthcare assistance, provided that paragraph 5 of that article is observed, including ancillary diagnostic and therapeutic services, for the benefit of the interests of the data subjects (LGPD, art. 11, II, g, § 4).*

3.7 Data Protection Officer

The LGPD requires that an officer in charge of the company's personal data be appointed. This officer, also known by the acronym DPO (Data Protection Officer), will act as a communication channel between the controller, the data subjects and the Brazilian National Data Protection Authority (ANPD).

The DPO must oversee the privacy, data protection and data security policies in order to ensure the operationalization of those policies across all organizational units, so as to ensure that the company processes personal data in a compliant manner. The DPO must operate independently, with the full support of senior management and of the board, and must have access to all the resources necessary to perform the work in accordance with best practices.

The appointment of UpFlux's DPO must be recorded in the minutes of a meeting of the board of directors.

3.7.1 Tasks of the DPO

The main tasks of a DPO are:

- To inform and advise the company and its employees on how to comply with the LGPD;
- To manage internal policies;
- To promote awareness and provide training for all employees involved in personal data processing activities;
- To provide advice on the data protection impact assessment and to monitor its performance;
- To give advice and recommendations to the company on the interpretation or application of data protection rules;
- To handle complaints or requests from institutions, from the data controller and from data subjects;
- To monitor compliance with the LGPD or with other data protection law;
- To identify and assess the company's data processing activities;
- To cooperate with the supervisory authority;
- To maintain the records of processing operations.

UpFlux, through its Information Security and Privacy Committee, must provide all the tools, resources and personnel necessary to enable the DPO to perform these tasks. Responsibility for compliance with the law rests exclusively with the company, the DPO being merely a facilitator.

4 Processing Records (data mapping)

UpFlux will keep a record of any and all processing of personal data when acting as a Controller and as a Processor.

Controller Activities	Processor Activities
When acting as a Controller, UpFlux must keep a processing record containing, but not limited to, the following information: ✓ Name of the person responsible for the record; ✓ The purposes of the processing and the legal basis; ✓ Description of the categories of Data Subjects and of the personal data; ✓ Identification of third parties to whom personal data has been or will be disclosed, including those located outside Brazil; ✓ Data storage location; ✓ Data retention; ✓ Security measures adopted. For further information, refer to the Annex and to Supplementary Document B.	UpFlux will only act as a Processor after establishing a contract with the data Controller. When acting as a Processor, UpFlux must keep a record of all the processing activities carried out on behalf of the Controllers, including, but not limited to, the following information: ✓ User identification; ✓ The categories of processing carried out on behalf of the Controller; ✓ Where applicable, transfers of personal data to other countries; ✓ Data storage location; ✓ Security measures adopted; ✓ Wherever possible, a general description of the technical and organizational measures implemented. For further information, refer to the Annex.

5 Rights of the Data Subject

The data subject holds the rights provided for in the LGPD. These consist of:

- Right to information on the existence of the data
- Right of access to the data
- Right to information on sharing
- Right to request proof of consent
- Right to review of automated decisions
- Right to correct and update their information
- Right to anonymization, blocking or deletion
- Right to data portability
- Right to be informed of the negative consequences of withholding consent
- Right to withdraw consent
- Right to have their data deleted after the end of the contract

UpFlux is aware that the Data Subject may object to a type of processing carried out that dispenses with consent (Art. 18, IX, § 2 of the LGPD). UpFlux may, however: i) accept the objection with no negative consequences for the data subject; ii) accept the objection and inform the data subject of the negative consequences; iii) deny the objection, where the processing is indispensable for achieving the objective.

In order to ensure transparency and to demonstrate UpFlux's diligence in the event of an objection to the processing on the part of the Data Subject, the justification and legal basis will be presented as set out in our policies, processes, terms and contracts.

These rights are upheld by UpFlux by means of appropriate procedures which allow the necessary action to be taken within the following deadlines:

Data Subject Request	Deadline
The right to confirmation of the existence of processing	Immediately
The right of access	15 days
The right to rectification	15 days
The right to deletion	Immediately, unless there is a justification and legal basis
The right to restrict processing	Immediately, unless there is a justification and legal basis
The right to data portability	15 days
Rights in relation to automated decision-making and profiling	30 days

5.1 Management of Data Subject requests

Controller Activities	Processor Activities
As a Controller, UpFlux has made available the contact address dpo@upflux.net so that the Data Subject may contact the data protection officer (DPO) and thereby exercise the rights provided for in the LGPD.	When acting as a Processor, UpFlux shall be under the obligation to observe the instructions of the Controller in relation to data processing and will promptly attend to the Controller's request where it concerns any request for the due fulfilment of a response to the exercise of a Data Subject's right. All guidance on procedures must be detailed in the terms of use and/or in contractual clauses. UpFlux must promptly forward to the Controller any Data Subject request that it receives, unless otherwise agreed between the parties in the services agreement.

6 Data Protection Impact Assessment (DPIA)

In accordance with the LGPD, controllers must carry out a data protection impact assessment (DPIA) for processing that has a strong impact on the rights and freedoms of individuals, especially where it is based on legitimate interest.

The preparation of the report starts from the detailing of all the processing operations that personal data undergoes throughout its life cycle in the operations carried out by UpFlux, as well as of the necessary legal bases and the security measures adopted. This information will be identified in the data mapping and, following analysis, will make it possible to identify the points of fragility in the operation that may represent a risk to the rights of the data subjects. Once the risk assessment has been carried out, the measures necessary for their mitigation will be identified, and these must then be implemented and tested.

UpFlux uses the DPIA to better visualize and understand its operation, so as to avoid excesses and to adopt the most appropriate solutions and measures in the context of privacy and data protection. Preparing it concurrently with the structuring of the operation, or even before it, will ensure from an early stage that all legal requirements are being met, which contributes to the fulfilment of an important duty established by the LGPD: the adoption of measures to protect the privacy and security of data from the design of the product or service onwards, a concept known as privacy by design.

6.1 Privacy by Design

UpFlux adopts the principles of Privacy by Design, which consist of the protection of privacy and of personal data, in all projects developed. No project, product or service may be developed without privacy protection being at the centre of that development, including the carrying out of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for which purposes;
- Assessment of whether the proposed processing of personal data is necessary and proportionate to the purpose(s);
- Assessment of the risks to individuals in the processing of personal data;
- Identification of the controls necessary to address the risks identified and to demonstrate compliance with the legislation.

6.2 Contracts Involving the Processing of Personal Data

UpFlux will ensure that all business partnerships involving the processing of personal data are subject to a contract or documented agreement that includes the specific information and terms required by the LGPD. For further information, refer to the Controller-Processor Contract Policy.

7 International Transfer

Transfers of personal data outside Brazil will be carefully assessed in order to ensure that they fall within the limits imposed by the LGPD.

In international contracts involving the transfer of personal data, jurisdictional rules must be observed, so that UpFlux is able to claim its rights. The possible situations of international data transfer at UpFlux are listed in Supplementary Document C.

Where the transfer of personal data occurs on the part of UpFlux's Processors, such operation must be set out in a contract and duly recorded.

8 Incident Management

UpFlux will act fairly and proportionately in considering the actions to be taken in order to inform the affected parties in relation to personal data breaches.

In line with the LGPD, in the event of verification of the occurrence of a breach that may result in a risk to the rights and freedoms of individuals, the supervisory authority will be informed as soon as possible. This will be managed in accordance with our Information Security Incident Response Procedure, which defines the process for handling information security incidents.

9 Driving Compliance with the LGPD

The following actions are taken in order to ensure that UpFlux complies with its responsibilities, as required by the LGPD:

- The legal basis for the processing of personal data is clear and explicit;
- A data protection officer is appointed with specific responsibility for the organization's data protection;
- All employees involved in the processing of personal data understand what their responsibilities are in order to follow good data protection practice;
- Training and information on data protection have been provided to all employees;
- Wherever consent is required, it will be requested;
- Means are available for data subjects to make contact;
- Regular reviews of procedures involving personal data are carried out;
- Privacy by Design is adopted for all new or altered systems and processes.

These actions are reviewed regularly as part of the management process relating to data protection.

Annex. UpFlux data processing activities

When UpFlux acts as a Controller

Personal Data of Employees

These rules cover the personal data of UpFlux's employees and partners, interns and third parties providing services to UpFlux, as well as job applicants. Employee personal data may include, without being limited to:

- ✓ Contact information, such as name, date of birth, sex, age, address, telephone numbers, e-mail address, number of children, citizenship, identification documents, visas, work authorization, emergency contacts, information on dependants, marital status, life insurance beneficiaries, photographs or images;
- ✓ Financial information relating to remuneration, benefits and retirement plans, such as salary, bank account, tax rates, travel expenses;
- ✓ Recruitment information such as CV, application form, interview notes, applicant references, qualifications, test results;
- ✓ Administrative employment information such as employment and career history, appraisals, managers, information on the employment contract, absence records, safety records, pre-employment and exit medical examinations, personal development reviews, skills records, official identification numbers;
- ✓ Information on professional experience, such as CV, qualifications, information on projects on which the employee has worked, training history; and
- ✓ Information on the employee's location based on access records.

UpFlux processes employees' personal data exclusively for work-related purposes, which include, but are not limited to, the following activities:

- ✓ Recruitment;
- ✓ Performance appraisal and training;
- ✓ Payroll and other work-related benefits;
- ✓ Day-to-day management activities, such as project deployment, promotion, disciplinary activities, conflict resolution;
- ✓ Benefits administration;
- ✓ Compliance with health and safety rules and with other legal obligations imposed on UpFlux as an employer;
- ✓ IT, security, cybersecurity and access control;
- ✓ Human resources management and mobility;
- ✓ Internal and external communication;
- ✓ Disaster recovery planning and crisis management;
- ✓ Management of company resources;
- ✓ Audits and statistics.

Business contacts

A business contact refers to a supplier, subcontractor, client or partner of UpFlux, whether in an ongoing commercial relationship, a former business contact or a potential client of UpFlux. The personal data that may be held regarding the personnel of its business contacts may include, without being limited to:

- ✓ Contact information such as name, position, employer, address, telephone numbers, e-mail address, messaging application numbers;
- ✓ Financial information relating to invoicing and payment, such as bank account;
- ✓ Relevant experience and/or qualifications (regarding subcontractors' personnel);
- ✓ Information on commercial opinions and interests (such as database information).

UpFlux processes the personal data of business contacts exclusively for work-related purposes. Such purposes include, but are not limited to, the following activities:

- ✓ Entering into and performing contracts with clients, suppliers, subcontractors or partners;
- ✓ Administering accounts and records;
- ✓ Advertising, marketing and public relations;
- ✓ Communicating with business contacts;
- ✓ Market research;
- ✓ Health, safety, environment and quality;
- ✓ Compliance with legal and regulatory obligations;
- ✓ Maintenance of certifications;
- ✓ Audits and statistics.

As a general rule, UpFlux, in its capacity as Controller, neither collects nor processes special categories of personal data. It may, however, process special categories of personal data where this is necessary in order for UpFlux to exercise its rights and/or to comply with its legal obligations as an employer.

When UpFlux acts as a Processor

UpFlux carries out the processing of an extensive variety of personal data covered within the context of the provision of services to its clients. The services provided use Artificial Intelligence and Process Mining techniques to increase operational efficiency and improve workflows. Such processing occurs in accordance with the client's instructions, and the personal data covered also includes special categories of personal data.

The personal data involved in the context of the services provided by UpFlux is contained in, but not limited to, documents such as:

- purchase and sales orders;
- invoices;
- appointment schedules;

- medical records;
- clinical and imaging examinations;
- requests for examinations, procedures and hospital admission;
- medication prescriptions;
- monitoring and vital signs records;
- health plan authorization forms;
- identification and supporting documents.