Privacy and Data Processing Policy

Guidelines Document

V.5.0

Introduction

upLexis Tecnologia Ltda.("upLexis", "We" or Our")

Calçada do Lírios, nº 220 - Room 3B - Barueri/SP Centro Comercial, CEP 06453-034

CNPJ: 06.242.066/0001-74

This Policy applies to any websites, applications or platforms operated by UpLexis Tecnologia Ltda. ("We", "Our", "Our") or on our behalf ("Our Platforms").

In order to be able to offer You the best results from our products and services, We collect and process Personal Data.

In the paragraphs below, we describe what personal data we collect and process, for what purposes and their respective legal bases.

As a condition of access and use of our products and services, You declare that you have read this Policy completely and carefully, being fully aware, giving your free and express agreement with the terms stipulated herein, including the collection of the Data mentioned herein, as well as its use for the purposes specified below.

If You do not agree with the provisions of this Policy, You must discontinue your access to or use of our website, products and/or services.

1. What information does upLexis collect?

Personal data

Personal Data is information related to an identified or identifiable natural person. This term refers to information that identifies or may identify a particular individual or customer.

Information you provide

Data, Personal or otherwise, may be collected when You submit it or when You interact with Our website or use Our products or services.

What do we collect?	What do we collect for?
Registration data	
Full name CPF/CNPJ Email Birth date contact phone Adresses	(i) Identify and Authenticate You. (ii) Fulfill the obligations arising from the use of our services. (iii) Improve, publicize and promote Our products and services; enrich Your experience with us. (iv) Expand our relationship, inform you about news, features, content, news and other events that we consider relevant to you.

	(v) Operate, maintain, enhance and provide all features of Our services, to provide services and information that You request, to respond to comments and questions and to provide support to You. (vi) Ensure Data portability if requested by You. (vii) Protect You by performing fraud prevention, credit protection and associated risks, in addition to complying with legal and regulatory obligations.
Digital Identification Data	
Source IP Address and Logical Port Device (OS version) Web Browser Information Geolocation Timestamps of every action You take Which screens did you access? session id Cookies	(i) Identify and Authenticate You. (ii) Collect information about your interaction with the email messages we send you, for example, whether you opened, clicked on, or forwarded a message (logs). (iii) Comply with legal record-keeping obligations established by the Civil Rights Framework for the Internet - Law 12,965/2014. (iv) Analyze and understand your usage trends and preferences, to improve Our services and to develop new products, services, features and functionality. (v) Protect You by performing fraud prevention, credit protection and associated risks, in addition to complying with legal and regulatory obligations.
Questionnaire data	
Questionnaire responses and optional surveys	(i) Improve our relationship by preparing analyzes and statistical studies.
upAPI	
API route IP used in the request body of the request response body Request time Request execution time User ID customer ID API key ID used to make the request	(i) To keep track of the most used parameters. (ii) To track whether the API is responding correctly (iii) To execute the route/request that the client requested. (iv) To return the response requested by the customer. (v) For performance/execution monitoring. (vi) For identification of the applicant/customer. (vii) For auditing purposes.

Many of Our services directly depend on some Data reported in the table above, mainly Registration Data. If You choose not to provide some of this Data, we may be unable to provide all or part of our services to You.

You are solely responsible for the accuracy, veracity or lack thereof in relation to the Data you provide or for its outdatedness. Please be aware that it is your responsibility to ensure accuracy or keep them up to date.

You are also responsible for the secrecy of your Personal Data and you must always be aware that sharing passwords and access data violates this Policy and may compromise the security of your Data and Our website and Our products and/or services.

It is very important that You protect Your Data against unauthorized access to Your computer, account or password, in addition to making sure You always click on "exit" when ending your browsing on a shared computer.

It is also very important that You know that we will never send electronic messages requesting confirmation of data or with attachments that can be executed (extensions: .exe, .com, among others) or even links to eventual downloads. All payment transactions, whether by credit card or not, are performed using SSL (secure socket layer) technology, ensuring that all your Data is not unlawfully disclosed. In addition, such technology aims to prevent information from being transmitted or accessed by third parties.

Internally, the Personal Data collected is accessed only by duly authorized professionals, respecting the principles of proportionality, necessity and relevance for the purposes of Our business, in addition to the commitment to confidentiality and preservation of your privacy under the terms of this Policy.

Information about "Cookies"

When you access Our website or use Our services, we may send one or more cookies (small text files containing a string of alphanumeric characters) to your device.

To find out how we use cookies and how to manage them, acess our **Cookie Policy**.

Information from external sources

We may obtain information, including Personal Data, from third parties and other data sources such as public sources, partners and customers. If we combine or associate information from other sources with Personal Data collected through Our services, we will treat the combined information as Personal Data, always in accordance with this Policy.

From which sources does upLexis collect Personal Data?

We use several sources to collect personal data:

The public sources from which we obtain Personal Data may include:

i. Records and public sources of data;

ii. Information from the public sector, federal agencies, and regulatory bodies;

iii. National and international sanctions lists, watch lists and PEP;

iv. Websites available on the Internet;

v. Searches and APIs from Google or another Internet search provider.

Non-public sources from which we may obtain Personal Data may include:

i. The data subject itself, including the information you provide us for access, billing and contact;

ii. Business entities and their customers and suppliers;

iii. National and international data suppliers and partners.

2. How does upLexis use the collected information?

We use collected information in a variety of ways to operate Our business, including:

Business management

Risk and Compliance Management (Compliance & Risk Management)

We support various organizations in compliance and risk management activities, processing and providing information that may contain Personal Data, either within a full dossier or information reports to assist organizations in making the following decisions:

i. Identify, verify and/or select potential business partners, customers and suppliers (KYP, KYC, KYS);

ii. Decide whether or not to enter, continue and/or terminate commercial transactions and deals;

iii. Establish the commercial terms under which these transactions take place, including the granting of credit or the provision of (commercial) credit;

iv. Determine (future) debt collection opportunities and/or creditworthiness determination.

Marketing Information

We help organizations by processing and providing business information, which may contain personal data, for marketing activities and prospecting for new business.

3. How does upLexis share or disclose information?

Information about Our customers is considered an important part of our business, therefore, We do not sell Personal Data to third parties for promotional or marketing use.

We may share information with third parties if You consent to do so, as well as in the following circumstances:

i. We work with third-party service providers who provide website, application development, maintenance, storage, transmission, data processing and other services for Us. These third parties may have access to or process your information as part of providing these services. However, we limit the information provided to these service providers to what is strictly necessary for them to perform their functions. In addition, third parties will obligatorily respect the conditions stipulated herein and the information security standards.

ii. We may make certain automatically collected, aggregated, or non-personally identifiable information available to third parties for various purposes, including monitoring traffic or network activity to detect malware, botnets, hackers, and other Internet threats, or to protect You, Us, or others from misuse. illicit activities or other illegal activities, to comply with legal reporting obligations. For the purposes of market intelligence research, disclosing data to the press and carrying out advertisements, the data provided by You will be shared anonymously, that is, in a way that does not allow your identification.

iii. We may share your information with the competent judicial, administrative or governmental authorities, whenever there is a legal determination, requirement, request or specific court order to do so.

4. How long does upLexis keep the information?

The Personal Data collected and activity records are stored in a secure and controlled environment for a minimum period, as shown in the table below:

STORAGE TERM	LEGAL BASIS
Registration data	
5 years after the end of the relationship	Art. 12 and 34 of the Consumer Protection Code
digital identification data	
6 months	Art. 15, Marco Civil da Internet
Reports and Queries carried out on the Platform	
Your consultations are stored for 3 months (90 days), unless a longer period of stay is negotiated in the contract.	Art. 9, Item II of the General Law for the Protection of Personal Data
Other data	
As long as the relationship lasts and there is no request for deletion or revocation of consent	Art. 9, Item II of the General Law for the Protection of Personal Data

For purposes of auditing, security, fraud control, credit protection, legal or regulatory obligation and preservation of rights, we may keep the Data registration history for a longer period in the cases established by law or regulatory rule.

We may retain encrypted or non-personally identifiable information for backups, archiving, fraud and abuse prevention, analysis, or where we believe we have a legitimate reason to do so.

International Transfer

The Data collected may be stored on servers located in the United States of America, as well as in an environment using resources or servers in the cloud (cloud computing), which may require an international transfer and/or processing of this Data.

5. How to control Personal Data?

You may ask Our Personal Data Officer to confirm the existence of Personal Data processing, in addition to displaying or rectifying Personal Data, through our Service Channel.

Through the Service Channel, you can also request:

(i) Limiting the use of Personal Data;

(ii) Express your opposition and/or revoke consent to the use of Personal Data; or

(iii) Request deletion of Personal Data that has been collected by Us.

If You withdraw Your consent for purposes fundamental to the regular functioning of Our Environments and services, such environments and services may become unavailable to You.

If You request the deletion of Your Personal Data, it may occur that the Data need to be kept for a period longer than the deletion request, pursuant to article 16 of the General Law for the Protection of Personal Data, for (i) compliance with a legal or regulatory obligation , (ii) study by a research body, and (iii) transfer to a third party (respecting the data processing requirements set forth in the same Law). In all cases, through the anonymization of Personal Data, whenever possible.

At the end of the maintenance period and the legal necessity, Personal Data will be deleted using safe disposal methods, or used in anonymized form for statistical purposes.

6. What are the Responsibilities?

We are committed to keeping this Policy up to date, adhering to the legislation, and ensuring its compliance.

In addition, we are committed to seeking technical and organizational conditions that are safely able to protect the entire data processing process.

7. Contact Information

We consider it important to protect the privacy and confidentiality of personal information and therefore ensure appropriate technical and organizational measures to protect personal data against loss, misuse and any form of illegal processing. Feel free to contact us through Service Channels or email: privacidade@uplexis.com.br or dpo@uplexis.com.br.

8. General Provisions

You acknowledge Our right to change the content of this Policy at any time, according to the purpose or need, such as for adequacy and legal compliance with a provision of law or rule that has equivalent legal force, it being up to You to verify it whenever you carry out the access to our website or use our products and/or services.

In the event of updates to this document that require a new collection of consent, You will be notified through the contacts You provide.

If any point of this Policy is considered inapplicable by the Data Authority or court, the other conditions will remain in full force and effect.

You acknowledge that all communication made by e-mail (to the addresses informed in your registration), SMS, instant communication applications or any other digital form, are also valid, effective and sufficient for the disclosure of any subject that refers to the services that we provide, to your Data, as well as to the conditions of its provision or to any other subject addressed therein, the exception being only what this Policy provides as such.

In the event of a dispute or conflict regarding this Policy, the competent Data Protection Authority and/or the court of your domicile are elected to resolve any controversy involving this document, unless there is a specific exception of personal, territorial or functional competence under the applicable legislation.

Update: Version 5 – March, 23th 2023.