upLexis Privacy and Data Processing Policy ("Policy")

Introduction

upLexis Tecnologia Ltda. ("upLexis", "We" or Ours")
Avenida Marquês de São Vicente, 1619, 16º andar, Barra Funda, São Paulo/SP
CNPJ (Legal Entity Taxpayer Number): 06.242.066/0001-74

In order to offer the best results from our products and services to You, 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 basis.

As a condition of access and use of our products and services, You declare that You have read this Policy fully and attentively, being fully aware of it, conferring Your free and express agreement with the terms set forth 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 or use of our website, products and/or services.

1. What information does upLexis collect?

Personal Data

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

Information you provide

The Data, Personal or Not, 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	(i) Identify and authenticate You. (ii) Fulfill the obligations arising from the use of our services. (iii) Improve, disclose and promote our products and services; enrich your experience with us.
CPF (Legal Entity Taxpayer Number)	
Email	
Date of birth	

Gender Telephone for contact Addresses:	(iv) Expand our relationship, inform you about news, functionalities, content, news and other events that we consider relevant to you. (v) Operate, maintain, improve and provide all the resources 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 compliance with legal and regulatory obligations.
Digital Identification Data	
IP Address and Logical Port of Origin Device (operating system version) Web Browser Information Geolocation Records of date and time of each action that You perform Which screens have you accessed 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 or forwarded a message (logs). (iii) Comply with legal obligations of record maintenance established by the Civil Landmark of the Internet - Brazilian Law 12.965/2014. (iv) Analyze and understand your usage trends and preferences, to improve our services and to develop new products, services, resources and functionalities. (v) Protect You by performing fraud prevention, credit protection and associated risks, in addition to compliance with legal and regulatory obligations.
Questionnaire data	
Answers to questionnaire and optional surveys	(i) Improve our relationship by developing statistical analysis and studies.

upAPI	
API Route IP used in the request Body of requisition Response body	i. To track the most commonly used parameters. ii. To track whether the API is responding correctly iii. To run the route/requisition that the client requested. iv. To return the response requested by the customer.

Requisition time	v. For performance/execution monitoring.
Requisition runtime	vi. For identification of the requester/customer.
ID do usuário	vii. For audit purposes.
Customer ID	
API key ID used to make request	

Many of our services depend directly on some of the data provided 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 of it in relation to the Data you provide or for its out-date. Be aware that it is your responsibility to ensure accuracy or keep them updated.

You are also responsible for the confidentiality of your Personal Data and should always be aware that sharing passwords and access data violates this Policy. It may compromise the security of your Data and of Our site and Our products and/or services.

It is very important that you protect your Data from unauthorized access to your computer, account or password, and make sure always to click "exit" when you exit from a shared computer.

It is also very important to know that we will never send electronic messages requesting data confirmation or with attachments that can be executed (extensions): .exe, .com, among others) or links for eventual downloads. All payment transactions, credit card or not, are executed with SSL technology (secure socket layer), ensuring that all your Data is not disclosed in illicit form. Furthermore, this technology aims to prevent the information from being transmitted or accessed by third parties.

Internally, the Personal Data collected are only accessed by duly authorized professionals, respecting the principles of proportionality, necessity and relevance to the objectives of Our business, in addition to the commitment to confidentiality and preservation of your privacy under 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, please request our Cookies 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 various sources to collect personal data:

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

i. Records and public data sources;

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

iii. National and international lists of sanctions, observation lists and PEP;

iv. Websites available on the Internet;

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

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

i. The data owner himself, including the information You provide us for access, billing and contact;

ii. Commercial entities and their customers and suppliers;

iii. National and international data suppliers and partners.

2. How does upLexis use the information collected?

We use the information collected in a number of ways to operate our business, including:

Business Management

Compliance & Risk Management

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

i. Identify, check 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 business;

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

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

Marketing Information

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

3. How does upLexis share or disclose information?

Information about our customers is 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 give your 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 to 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 respect the conditions stipulated herein and the standards of information security.

ii. We may provide certain information automatically collected, aggregated or non-personally identifiable to third parties for various purposes, including monitoring network traffic or activity to detect malware, botnets, hackers and other threats to the Internet or to protect You, Us or other persons from unlawful uses or other illegal activities for complying with legal reporting obligations. For the purposes of market intelligence research, dissemination of data to the press and advertising, the data provided by You will be shared anonymously, that is, in a way that does not enable its identification

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

4. How long does upLexis keep the information?

We store Personal Data, including the Reports and Consultations carried out on the Platform, for the period necessary to meet the purposes informed in this Privacy Policy, respecting the period of data retention determined by applicable legislation.

Should you request the deletion of your account, the Personal Data, including the Reports and Queries made on the Platform, provided during your use of Our services will be definitively deleted whenever the legislation so requires.

For auditing, security, fraud control, credit protection, legal or regulatory obligation and preservation of rights, we may remain with the Data registration history for a longer period in the cases that the law or regulatory rule so establishes.

We may retain information that is encrypted or not personally identifiable for backups, archiving, fraud and abuse prevention, analysis, or where we believe we have a legitimate reason to do so.

The Data collected may be stored on servers located in the United States of America, as well as in a resource usage environment or cloud computing server, **which may require an international transfer and/or processing of this Data.**

5. How to control Personal Data?

You may request our Personal Data Officer to confirm the existence of Personal Data treatment, in addition to the display or rectification of Personal Data, through our Service Channel.

By the Service Channel, you may also apply for:

(i) The limitation of the use of Personal Data;

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

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

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

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

Once the maintenance period and the legal need have expired, the Personal Data will be deleted using safe disposal methods, or will be used anonymously for statistical purposes.

6. Contact Information

We consider it important to protect the privacy and confidentiality of personal information and therefore we guarantee appropriate technical and organizational measures to protect personal data from loss, misuse and any form of unlawful processing. Feel free to contact us through the **Service Channel** privacidade@uplexis.com.br or write to us:

upLexis Tecnologia (Brazil Office) - Information Security Area

Av. Marquês de São Vicente, 1619 - 16º andar - São Paulo / SP - CEP: 01139-003
Tel.: 55 (11) 3094-7444

7. 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 of a provision of law or norm that has equivalent legal force. It is your responsibility to check this whenever you access our website or use our products and/or services.

If there are updates to this document that require further collection of consent, You will be notified through the contacts You inform.

Should a Data Authority or court deem any part of this Policy inapplicable, the remaining conditions shall remain in full force and effect.

You acknowledge that any communication made by email (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 matter that refers to the services we provide, your Data, as well as the conditions of its provision or any other subject addressed therein, being the exception only that this Policy provides as such.

In case of dispute or conflict over this Policy, the competent Data Protection Authority and/or the forum of your domicile shall be elected to settle any controversy involving this document, except for specific personal, territorial or functional jurisdiction under applicable law.

Update: Version 3 – February, 1st 2022