keyrus
make data matter

DATA PROTECTION POLICY
CLIENTS AND PROSPECTIVE CLIENTS
Version February 2021

PREAMBLE

The purpose of this data protection policy (hereinafter the 'Policy') is to provide Keyrus's clients and prospective clients with information on how it processes their personal data, as a data controller and as a data processor. Under its contractual and pre-contractual relationships, Keyrus undertakes to comply with the regulations in force applicable to personal data processing, specifically Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'GDPR'), as well as any applicable national regulations (hereinafter the 'Regulations').

DEFINITIONS

BELOW ARE SOME DEFINITIONS TO HELP YOU UNDERSTAND OUR POLICY:

« Client » means any natural or legal person for whom Keyrus provides a service or benefit.

« Recipient » means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

« Personal data » means any information relating to an identified or identifiable natural person (hereinafter the 'Data subject'); an 'identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of said natural person.

« KEYRUS » means any company belonging to the Keyrus Group, either controlled by Keyrus SA pursuant or with whom Keyrus SA has a legal relationship.

« Prospective client » means any natural or legal person who may use services provided by and/or be in contact with Keyrus.

« Data controller » means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing; where the purposes and means of such Processing are determined by Union or Member State law, the Data controller or the specific criteria for its nomination may be provided for by Union or Member State law.

« Data processor » means the natural or legal person, public authority, agency or other body which processes Personal data on behalf of the Data controller.

« Processing » means any operation performed on Personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

« Personal data breach » means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed.

1 KEYRUS DATA CONTROLLER

1.1 PRINCIPLES RELATING TO DATA PROCESSING

As stated in the preamble herein, Keyrus makes every effort to ensure ongoing compliance with the key principles of the GDPR and to assure all its Clients and Prospective clients that any Personal data collected is processed in a legal, fair and transparent manner.

Personal data is collected for specific, express and legitimate purposes and KEYRUS undertakes not to process it for purposes which are incompatible with these objectives.

Keyrus respects the principle of data minimisation, in accordance with Article 5(c) of the GDPR, specifically that the Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes defined below. In this way, Keyrus ensures that 'comment fields' include only relevant and limited information.

1.2 PURPOSES AND LEGAL BASIS FOR DATA PROCESSING

Purpose	Legal basis
Client and Prospective client management	Legitimate interest in ensuring the development of the KEYRUS Group
Management of business development activities (management of technical business development operations, including technical operations such as standardisation, enrichment and data deduplication); tracking of marketing campaigns and selection of individuals to carry out activities relating to loyalty, business development and surveys; carrying out marketing campaigns; newsletters; phone calls	Legitimate interest in ensuring the development of the KEYRUS group In some cases, the Data subject's consent is required when their email address is indicated in an application form
Management of business activities (Client management and keeping track of all interactions with them, from the first call and email exchanges, meetings and presentations, to the signing of the contract); won/lost/ ongoing opportunities; management of activities (appointments, phone calls, etc.); monitoring of telephone customer support; carrying out satisfaction surveys; Client accounts management	Legitimate interest in ensuring the development of the KEYRUS Group

Purpose	Legal basis
Management of marketing activities: Carrying out marketing campaigns; designing loyalty programmes (marketing campaigns, tracking responses to the campaign); management of spams and oppositions to campaigns; generation of internet leads in the database; allocation of marketing relaunch tasks; linking an appointment or opportunity to a marketing activity; identification of duplicate contacts; Processing of hard bounces; testimonials or interviews	Legitimate interest in ensuring the development of the KEYRUS Group
Data collected by cookies on Keyrus websites	Consent of the Data subject or legitimate interest in ensuring the development of the KEYRUS Group when the consent is not necessary
Contact forms on Keyrus websites	Legitimate interest in ensuring the development of the KEYRUS Group
Organisation of contests or promotional campaigns	Legitimate interest in ensuring the development of the KEYRUS Group
Management of unpaid invoices (reminders and final demands)	Necessity to perform a contract
Management of litigation and pre-litigation	Keyrus's legitimate interest in enforcing its rights
Performance monitoring (deliverables, delivery, schedule, revenue, monitoring committees, reports, etc.)	Necessity to perform a contract
Compilation of trade statistics	Legitimate interest in ensuring the development of the KEYRUS Group
Pre-sales management (invitations to tender, start-up committee, etc.)	Legitimate interest in ensuring the development of the KEYRUS Group
Invoice management (invoices, deliverables, accounts, etc.)	Necessity to perform a contract
Management of contract documents (quotations, contracts, orders, etc.)	Necessity to perform a contract
Client audit tracking (auditors, schedule, audit scope, etc.)	Necessity to perform a contract
Management of the Processing activities register	Necessity to comply with a legal obligation
Management of requests to exercise data protection rights (right to access, correct or delete data, or limit or object to Processing, and right to portability of Personal data, where appropriate)	Necessity to comply with a legal obligation

For each specific Processing operation, particularly in relation to security (video surveillance, swipe cards, etc.) or use of an IT resource made available to the Client or Prospective client by Keyrus (software, hardware, etc.), Data subjects shall receive a specific statement telling them how their Personal data is processed.

2

PERSONAL DATA PROCESSED

Data types	Data categories
Identity data	Title, surname, first name, business address, business telephone number (landline and/or mobile), business fax number, business and/or personal mail address, internal Processing code allowing the Client to be identified. A copy of an identity document may be kept as evidence for the exercise of data protection rights (right to access, correct or delete data, or limit or object to Processing, and right to portability of Personal data, where appropriate) or to comply with a legal obligation
Working life	Job, position, company
Data relating to mailing campaign	Location of the recipient, actions of the recipient, IP data of the recipient's device, data on the web browser
Data relating to monitoring of the business relationship	correspondence, discussions and comments from Clients and Prospective clients
Data relating to the organisation and Processing of contests and promotional campaigns	Participation date, responses to contests and nature of prizes offered

If your Personal data has not been collected directly by Keyrus, it may have been received by our database leasing partners or business partners who are the Data controllers of their databases. The databases to which we have access may contain Personal data other than that described above, which we may consult, such as your photo or career history.

2.1 RECIPIENTS

Keyrus undertakes to keep your Personal data secure and confidential pursuant to the regulations in force and to ensure that all Recipients follow appropriate security and confidentiality safeguards.

Recipients who may receive your Personal data include:

- Authorised personnel of Keyus; from the marketing department, the commercial service, the legal department, the service in charge of client relationships and prospective clients, the administrative service, the logistics and IT services, as well as their hierarchical superiors
- Partners and processors of Keyrus;
- Organisations, court officers and legal professionals as part of their debt collection duties;
- The Data Protection Officer.

In the case of a dispute, your Personal data may be sent to:

- People working to resolve the conflict;
- The legal authorities in the case of an offence;
- Judicial or administrative courts, joint or commercial, or an arbitration panel, in order to establish, exercise or defend Keyrus's rights;
- Judicial or administrative courts, in order to execute an enforceable court decision which is binding on Keyrus;
- Any natural or legal person in order to execute an enforceable court decision which is binding on Keyrus.

Authorised suppliers may also have access to your Personal data as part of the services they may provide, including in connection with software solutions or IT resources used to process your Personal data (maintenance, support, hosting, security and monitoring of IT resources, etc.).

2.2 STORAGE PERIOD:

The storage period applicable to your Personal data is determined according to the storage times provided for by law and regulations and the type of data concerned.

The main storage periods for documents relating to Client and Prospective client management include, but are not limited to, the following:

Document type	Storage period	Reference text
Client and Prospective client file management	Personal data relating to Clients may only be stored for as long as is strictly necessary for managing the business relationship, except for data that is required to prove a right or contract, which may be archived pursuant to the provisions of the French Commercial Code relating to the storage period for books and documents created in the course of business activities.	
Exercising the right to access, correct or delete data	1 year	Article 9 of the Penal Procedure Code
Exercising the right to object to data Processing	6 years	Article 8 of the Penal Procedure Code
Contracts signed between traders	5 years	Article L110-4 of the Commercial Code
Order management	10 years	Article L123-22 paragraph 2 of the Commercial Code
Invoice management	10 years	Article L123-22 paragraph 2 of the Commercial Code
Account, in particular Client account management	10 years	Article L123-22 paragraph 2 of the Commercial Code
Client file management	Client data is stored for the duration of the business relationship. It may be stored for marketing purposes for a maximum of 3 years from the end of this business relationship of 3 years from the end of this business relationship	
Creation and management of Prospective clients files	3 years from the date they are put together by the Data controller or the date of last contact from the Prospective client	
Cookies	Information stored on the user's device (e.g. cookies) and any other information used to identify users and allow users to be traced must not be retained for more than 13 months	
Newsletter management	Until the Data subject unsubscribes	Article 5 e) of the GDPR, Article 4 5° of the amended law n°78-17
Sending of marketing materials (emails, telephone calls, faxes, SMS, etc.)	3 years from the date they are put together by the Data controller or the date of last contact from the Prospective client	
Opt-out list management	3 years from the date of entry in the list	

Keyrus shall not store Personal data in a form allowing identification of Data subjects for a period longer than necessary, taking into account the purpose for which the data was originally collected.

Keyrus may store data for longer periods if Personal data is processed for filing purposes in the public interest, scientific or historical research or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of Data subjects.

2.3 SECURITY AND PRIVACY :

Keyrus implements all the technical and organisational measures it deems appropriate, in accordance with Article 32 of the GDPR, in order to ensure the security and privacy of your Personal data.

We ensure that all Recipients comply with the appropriate security and privacy safeguards.

Keyrus cares about Personal data protection, and makes its staff aware of Personal data security.

For further information regarding your data security, please contact our DPO.

2.4 DATA TRANSFER :

In the case of your Personal data being transferred to a recipient located in a non-European Community Member State, appropriate safeguards shall be put in place, in accordance with the GDPR, and Keyrus shall inform you of these by any means possible.

Personal data transfer within entities of the Keyrus Group not covered by a European Commission adequacy decision generally involves the signing of standard contract terms.

Keyrus has implemented a data transfer policy. Please contact our DPO for more information.

2.5 RIGHTS OF DATA SUBJECTS

In accordance with the regulations, you may access Personal data concerning you and request for it to be corrected or deleted. You also have the right to limit or object to the Processing of your Personal data and the right to portability of your data, where appropriate.

To gain a full understanding of these rights and the means of exercising them, you can send your questions and/or requests to our Data Protection Officer (DPO) by:

- Post to KEYRUS SA, 155 rue Anatole, 92300 LEVALLOIS-PERRET, France, with the subject « Personal data »
- Email to Keyrus.DataProtection@keyrus.com

The DPO shall reply to you as quickly as possible.

You also have the right to make a complaint to the French Data Protection Agency (CNIL), which is currently located at the following address: 3 place de Fontenoy, 75007 Paris.

3

KEYRUS DATA PROCESSOR

As part of the provision of its services, Keyrus may process Personal data on behalf of the Client. In this case, the Client is the Data controller and Keyrus is the Data processor.

As a Data processor, Keyrus undertakes to process Personal data in accordance with the Client's written instructions.

Pursuant to article 28 of the GDPR, Keyrus and the Client shall sign a contract defining in particular the subject and duration of the Processing, the nature and purpose of the Processing, the type of Personal data and categories of Data subjects, and the rights and responsibilities of the Data controller. In this context, Keyrus makes its Data Processing Contract ('DPC') template available to the Client under a confidentiality obligation.

Keyrus undertakes to comply with the technical and organisational measures defined by mutual agreement with the Client in accordance with article 32 of the GDPR in order to ensure data security and privacy. Keyrus makes its Information Security Systems Policy (ISSP) available to the Client under a confidentiality obligation. Where necessary, the Parties may agree on a Security Assurance Plan (SAP).

If Keyrus calls upon a subsequent Data processor to perform part of the services conferred upon it, the latter may have access to Personal data. In this case, Keyrus shall ensure that the Data processor is also bound by the obligations in force regarding data protection.

In the case of your Personal data being transferred to a Recipient located in a non-European Community Member State, appropriate safeguards shall be put in place, in accordance with the GDPR.

The support and assistance provided by Keyrus to the Client is defined in the contract, as well as the audit conditions. Keyrus shall comply with the provisions of the GDPR relating to notifications it must make to the Client.

Keyrus ensures that persons authorised to process Personal data undertake to respect privacy or are subject to an appropriate legal confidentiality obligation.

4

AMENDMENTS TO THE POLICY

This Policy may be amended by Keyrus management in order to take into account recommendations from the CNIL, changes in the law, case-law or information technology and, more generally, on the basis of any developments in IT and communications technology.