

1

DEFINITIONS



Terminology	Description
Business partner	Refers to any service provider, temp agency, processor, supplier or commercial partner of 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.
DPO	Means the 'Data Protection Officer' (or DPD, Data Protection Delegate), the person responsible for ensuring compliance with the Regulations.
Keyrus	Refers to Keyrus SA and any company of the Keyrus group that has not implemented its own procedure.
Personal Data / 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.
Processing	Means any operation or set of operations which is performed on Personal data or on sets of 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.
Recipients	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.
Regulations	Means the regulations in force applicable to the Processing of Personal data, in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'GDPR') as well as the local regulations applicable for each country of the European Union (In France: Law n ° 78-17 of January 6, 1978 relating to information technology, files and freedoms and its implementing decree n ° 2019- 536 of May 29, 2019).



2

PREAMBLE

This Charter (hereinafter the “Charter”) provides a framework for the Processing of Personal Data in the context of Keyrus’s relations with its Business partners.

Keyrus, concerned about the protection of Personal Data, undertakes to comply with the Regulations in force applicable to the Processing of Personal Data and in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the “GDPR”) as well as any applicable national Regulation (hereinafter the “Regulations”).

Any **Keyrus** Business partner undertakes to read and fully understand all of the commitments listed in this Charter, as well as to respect all of its principles and accept that their non-compliance may be considered as a serious breach of its contractual obligations.

Any Business partner undertakes to inform all its direct partners and strongly encourage them to follow these same principles and rules of conduct.

3

PRINCIPLES RELATING TO DATA PROCESSING



In the context of its business relations with its Business partners, **Keyrus** makes every effort to be in permanent compliance with the essential principles of the GDPR and assures all of its Business partners that the Personal Data communicated to it is processed in a lawful, fair and transparent manner.

Personal Data is collected for specific, explicit and legitimate purposes and **Keyrus** undertakes not to process it for purposes incompatible with these purposes.

Keyrus respects the principle of data minimization, in accordance with article 5-c of the GDPR, which stipulates that only Personal Data that is adequate, relevant and limited to what is necessary for the purposes defined below is processed.

4



PURPOSES AND LEGAL BASIS OF DATA PROCESSING BY KEYRUS

Purpose	Legal basis
Perform administrative operations related to contracts, orders, receipts, invoices, payments, accounting, follow-up of Business partners, communication (email, mail, phone call, sms, mms and other electronic messages)	The need to perform a contract
Establish payment titles and make payments.	The need to perform a contract
Establish financial and turnover statistics of Business partners	Legitimate interest in ensuring the development of the Keyrus Group
Provide selections of Business partners for the needs of Keyrus or the Keyrus Group	Legitimate interest in ensuring the development of the Keyrus Group
Maintain documentation on Business partners	Legitimate interest in ensuring the development of the Keyrus Group
Maintain documentation on Business partners in accordance with the Regulations	The need to comply with a legal obligation
Carry out commercial prospecting between professionals	Legitimate interest of Keyrus
Recruitment of service providers, processors and temporary workers: Processing of applications (CVs and cover letters) and interview management	The need to carry out pre-contractual measures with the intention of performing an employment contract
Recruitment of service providers, processors and temporary workers: Constitution of a CV-library	Legitimate interest in ensuring the development of the Keyrus Group
Monitor the performance of services	The need to perform a contract
Pre-litigation and litigation management	Keyrus's legitimate interest in ensuring that its rights are respected

FOR ANY SPECIFIC PROCESSING, ESPECIALLY RELATED TO SECURITY (VIDEOSURVEILLANCE, BADGE, ...) OR TO THE USE OF A COMPUTER MEDIA PROVIDED TO A BUSINESS PARTNER BY **KEYRUS** (SOFTWARE, HARDWARE, ...), THE DATA SUBJECTS WILL RECEIVE A SPECIFIC NOTICE OF INFORMATION INFORMING THEM OF THE WAY THEIR PERSONAL DATA IS PROCESSED.

5



PERSONAL DATA PROCESSED

Type of Data	Categories of Data
Identity data	Marital status, surname, first names, personal address (postal and e-mail), professional and / or personal address, professional telephone number (landline and / or mobile), personal telephone number (landline and / or mobile), professional fax number, professional and / or personal email address, date of birth, photo (optional), LinkedIn profile address, internal Processing code allowing the identification of the Business partner, a copy of an identity document may be kept at purposes of proof of the exercise of IT rights and freedoms (right of access, opposition, rectification, erasure and limitation of Processing and right to Personal Data portability, if applicable) or to comply with a legal obligation
Professional life	CV, function, position, company, training, diploma and copy of diplomas, experience, cover letter, information provided by the Business partner, interview report, date of interviews, work authorization (yes / no)
Personal life	Leisure indicated on the CV
Economic and financial information	Current remuneration and desired remuneration
Data relating to the monitoring of Business partners	Correspondence, exchanges and comments
Bank and payment details	Terms and conditions of payment (means of payment, bank or postal references, discounts, deposits, rebates)

As part of our commercial relations with our Business partners, the latter may communicate to **Keyrus** the Data of the Data subjects, including the Data of their employees, mentioned in the table above. For more information on the Processing of your Personal Data, we leave it to you to consult the Data protection policy of the Business partner concerned.



6



RECIPIENTS

Keyrus undertakes to preserve the confidentiality and security of your Personal Data in accordance with the Regulations in force and to verify that each of the Recipients respects appropriate security and confidentiality guarantees.

The Recipients who may receive your Personal Data in the companies of the **Keyrus** Group are:

- The personnel authorized within the **Keyrus** Group to process the Data;
- People responsible for audits and inspections (statutory auditors, accountants);
- External companies contractually bound for the execution of a contract;
- Public and financial organizations, exclusively to meet legal obligations;
- In the event of a dispute, Personal Data may be transmitted if applicable, to people working to resolve the conflict; to court officials and ministerial officers as part of their debt collection mission or for all other legal actions; to the courts of the judicial or administrative order to establish, exercise or defend the rights of **Keyrus**; to the courts of the judicial or administrative order in execution of an enforceable court decision opposing **Keyrus**; to any natural or legal person in execution of an enforceable court decision opposing **Keyrus**.

Authorized service providers may also have access to your Personal Data as part of the services they can provide, among others, in connection with the software solutions or IT resources used to process your Personal Data (maintenance, support, hosting, security and control of IT resources, etc.).



7

RETENTION PERIOD

The retention period of your Personal Data is determined according to the legal and regulatory retention periods and according to the type of Data concerned.

The retention periods for the main documents relating to Business partners are as follows (it is an indicative and not exhaustive list):

Type of document	Retention period	Reference text
Order management	10 years	Article L123-22 paragraph 2 of the Commercial Code
Exercise of the right of access, to rectification, erasure, restriction of Processing and portability	1 year	Article 9 of the Code of Criminal Procedure
Exercise of the right to object	6 years	Article 8 of the Code of Criminal Procedure
Contracts concluded between traders	5 years	Article L110-4 of the Commercial Code
Recruitment files	2 years after the last contact with the Data subject, unless opposed by the Data subject Only the formal agreement of the Data subject allows longer storage	
Accounting documents and supporting documents (accounting books and all accounting documents for recording transactions, accounting monitoring items, inventory management, annual accounts (income statement, balance sheet, appendices,), etc...)	10 years from the end of the financial year	Article L123-22 of the Commercial Code

KEYRUS WILL NOT KEEP PERSONAL DATA IN A FORM WHICH ALLOWS THE IDENTIFICATION OF THE DATA SUBJECT FOR A LONGER PERIOD THAN NECESSARY, WITH REGARD TO THE PURPOSE FOR WHICH THE DATA WAS ORIGINALLY COLLECTED.

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

8



SECURITY AND CONFIDENTIALITY

Keyrus implements all the technical and organizational measures it deems appropriate, in accordance with Article 32 of the GDPR in order to guarantee the security and confidentiality of your Personal Data.

We verify that each of the Recipients respects appropriate security and confidentiality guarantees.

Keyrus makes its staff members aware of the security of Personal Data.

For more information regarding the security of your Personal Data, we invite you to contact our Data Protection Officer (DPO).

9



TRANSFER OF DATA TO A THIRD COUNTRY

In the event that your Personal Data is transferred to a recipient located in a non-member state of the European Union, appropriate safeguards will be put in place, in accordance with the provisions of the GDPR and **Keyrus** will inform you by any means.

Transfers of Personal Data within **Keyrus** Group companies not covered by an adequacy decision from the European Commission are generally covered by the signing of Standard Contractual Clauses.

Keyrus has implemented a Data transfer policy. Our DPO is at your disposal for more information.

10



RIGHTS OF DATA SUBJECTS

According to the Regulations, you can access the Personal Data concerning you, request their rectification or their erasure. You also have a right of opposition, a right to restrict the Processing of your Personal Data and a right to Personal Data portability, if applicable.

You can become fully aware of these rights and the means to exercise them by sending your questions and / or requests to our Data Protection Officer (DPO) by:

- Mail to **KEYRUS SA** - 155 rue Anatole France - 92300 LEVALLOIS-PERRET, indicating in the subject line « Personal data »
- Email to KEYRUS.DataProtection@KEYRUS.com

You also have the right to lodge a complaint with the CNIL as a supervisory authority whose current address is: 3 place de Fontenoy, 75007 Paris.

11



COMMITMENTS OF BUSINESS PARTNERS TOWARDS KEYRUS

Any Business partner processing Personal Data as a Data Processor within the meaning of the GDPR on behalf of **Keyrus** or as a Sub-processor on behalf of one of its customers undertakes to:

- sign the Personal Data Processing contract proposed by **Keyrus**, in order to comply with the provisions of Article 28 of the GDPR
- respect the Regulations
- process the Data only for the sole purpose(s) defined by the Data Controller
- process the Data in accordance with the documented instructions of the Data Controller
 - if the Business partner considers that an instruction constitutes a breach of the Regulations, it immediately informs it
 - if the Business partner is required to transfer Data to a third country or to an international organization, under Union law or under the law of the Member State to which it is subject, it must inform the Data Controller of this legal obligation before the Processing, unless the law concerned prohibits such information for important reasons of public interest
- guarantee the confidentiality and security of the Data processed
- ensure that the persons authorized to process the Data undertake to respect the confidentiality of the Data and receive the necessary training in Data protection
- take into account, with regard to its tools, products, applications or services, the principles of Data protection by design and of Data protection by default

- As far as possible, the Business partner must help the Data Controller to fulfill his obligation to respond to requests to exercise the rights of Data subjects: right of access, to rectification, erasure and opposition, right to restrict Processing, right to Data portability, right not to be subject to an individual automated decision.
- If the Data subjects make requests to the Business partner to exercise their rights, the Business partner will notify these requests in writing upon receipt to the Data Controller
- The Business partner immediately notifies the Data Controller in writing of any Data breach after becoming aware of it. This notification is accompanied by all the necessary documentation to allow the Data Controller, if necessary, to notify this breach to the competent supervisory authority
- Where applicable, the Business partner will provide the necessary assistance (i) for the performance by the Data Controller of impact assessments relating to Data protection and (ii) for the performance by the Data Controller of the prior consultation of the supervisory authority
- The Business partner undertakes to implement the appropriate technical and organizational measures in accordance with the GDPR and to communicate them on first request
- At the end of the services, the Business partner undertakes, at the option of the Data Controller, to (i) destroy all the Data; or (ii) to return all Data to the address communicated to it. In the event of return of the Data, the Business partner will destroy all existing copies in its possession and will inform the Data Controller of this destruction.
- The Business partner communicates to the Data Controller the name and contact details of his Data Protection Officer, if he has appointed one in accordance with Article 37 of the GDPR
- The Business partner does not recruit another processor without the prior written consent of the Data Controller and / or the Data Processor, if he is a Sub-processor. If it is accepted that a Sub-Processor carries out specific Processing activities on his behalf, the same Data protection obligations as those laid down in the contract signed with the Data Controller will be imposed on this Sub-processor, in particular with regard to providing sufficient guarantees regarding the implementation of appropriate technical and organizational measures so that the Processing meets the requirements of the GDPR. The Business partner remains fully responsible for the performance by the Sub-processor of his obligations in terms of Data protection
- The Business partner undertakes to only process the Data within the European Union. If the Business partner is authorized by the Data Controller to transfer the Data outside the European Union to a country that is not suitable according to the European Commission, the Business partner undertakes to implement appropriate safeguards for this transfer and to inform the Data Controller of the appropriate guarantees taken
- The Business partner guarantees to assist the Data Controller and the Data Processor, if he is a Sub-processor, in keeping his records of all categories of Processing activities
- The Business partner provides **Keyrus** with the necessary documentation to demonstrate compliance with all its obligations
- The Business partner accepts that the Data Controller and / or the Data Processor, if he is a Sub-processor, may carry out audits, including inspections, by himself or a third party auditor that he would have appointed and guarantees his contribution to these audits or inspections

12



NULLITY OF A CLAUSE

If one or more stipulations of this Charter are held to be invalid or declared as such in application of a law or another legislative text or following a final decision of a competent court, the other stipulations shall remain in force to their full extent.

13



AMENDMENTS TO THE CHARTER

This Charter may be amended by **Keyrus** in order to take into account recommendations from the CNIL, changes in the law, case-law, computer techniques and, more generally, on the basis of any developments in information and communication technology.