keyrus
make data matter

HR KEYRUS DATA PROCESSING CHARTER

1 PREAMBLE

As a player in digital transformation, the KEYRUS Group is helping to build an innovative, virtuous, responsible and transparent working environment.
We position ourselves to implement good practices in the handling of your personal data within the KEYRUS Group, both for our Employees and for our Candidates.

We wish to adopt ethical practices by taking into account the regulations in force applicable to the processing of your Personal Data, in particular the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) as well as law n°78-17 of 6 January 1978 (I&L law) relating to data processing, files and freedoms (hereinafter the «regulations»). The purpose of this Charter is to inform each Employee and Candidate about the processing of their Personal Data when managing Human Resources within the Keyrus Group.

2 DEFINITIONS

A FEW DEFINITIONS TO HELP YOU BETTER UNDERSTAND THIS CHARTER!

« Candidate » means the person who has applied for and/or been contacted by a Keyrus Group entity or through a recruitment agency in connection with a job or internship offer.

« Associate » refers to the person who has been recruited by an entity of the Keyrus Group, regardless of their status.

« Recipients » means the natural or legal person, public authority, department or other body that receives your personal data, whether or not it is a third party.

« Personal data » means any information relating to an identified or identifiable natural person («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 his physical, physiological, genetic, mental, economic, cultural or social identity.

« KEYRUS Group » refers to the companies Keyrus SA, Kadris consultants, keyrus management, keyrus life science innovation, YOUNICORNS and OPSKY, which are jointly data controllers for the processing operations detailed below.

« IT resources » refers to hardware, files, programmes, software and software packages, all networks (local and external), servers, information systems, electronic mail, instant messaging, storage spaces and collaborative tools belonging to KEYRUS Group entities.

« corporate social network » refers to any internal communication platform of the KEYRUS Group. The corporate social network aims to facilitate collaborative work and to facilitate exchanges between Employees of the same company or group.

« HR or Human Resources » means any department or member of a department involved in personnel management, recruitment, payroll or relations with staff representative bodies within KEYRUS Group entities.

« Data Controller » means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing operation: where the purposes and means of such processing are determined by Union law or by the law of a Member State, the controller may be designated or the specific criteria applicable to his designation may be laid down by Union law or by the law of a Member State.

« Processing » means any operation applied to Personal Data, whether or not by automatic 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.

3
DATA PROCESSING PRINCIPLES

As stated in the preamble to this Charter, the KEYRUS Group makes every effort to comply at all times with the essential principles of the RGPD and assures all its Employees and Candidates that the Personal Data collected is processed lawfully, fairly and transparently.

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

The KEYRUS Group entities comply with the principle of data minimisation, in accordance with Article 5 c of the RGPD, i.e. 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

Purposes	Legal basis
Recruitment: Searching for relevant profiles: creating a platform for posting applications on a company's job site (spontaneous or in response to a job offer), using websites offering job offers on the Internet to applicants (e.g. Pôle emploi, Indeed, APEC), etc.	Legitimate interest in ensuring the development of the KEYRUS Group.
Recruitment: Pre-selecting candidates: sorting, recording and filing CVs and covering letters on paper or in a database, etc.	The need to take pre-contractual steps with a view to concluding a contract of employment
Recruitment: Contacting the candidate to assess their suitability for a job and measure their professional aptitude: processing information gathered during telephone interviews, face-to-face interviews, etc.	Legitimate interest in ensuring the development of the KEYRUS Group
Recruitment: Use of innovative tools and technologies to assess a candidate's suitability for a job and measure their professional aptitudes: personality tests, video interviews, profiling tools, etc.	Legitimate interest in ensuring the development of the KEYRUS Group
Recruitment: Creating a CV library	Legitimate interest in ensuring the development of the KEYRUS Group
Recruitment: Production of statistical reports or lists of candidates to meet recruitment management needs.	Legitimate interest in ensuring the development of the KEYRUS Group and the replacement of staff
Identifying candidates' expectations	Legitimate interest in mobilizing and developing human resources in support of KEYRUS Group strategy
Sending out a satisfaction survey	Legitimate interest of the KEYRUS Group to measure the satisfaction of applicants and employees
Production of statistical reports or employee lists	Legitimate interest in ensuring the development of the KEYRUS Group and the replacement of staff
Management of employees' professional files, kept in accordance with the legislative and regulatory provisions, as well as the provisions of the articles of association, collective bargaining agreements or contracts governing the persons concerned.	The need to perform the employment contract
Management of employment contracts	The need to perform the employment contract
Management of internal directories and organisation charts	Legitimate interest in managing human resources
Management of occupational medicine follow-up	The need to comply with a legal obligation
Management of HR development action planning	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Identifying employee expectations	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Organisation of training sessions and assessment of knowledge and training	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Management of training requests and training periods completed	The need to perform the employment contract
Management of employee benefits (savings, supplementary health, provident fund, etc.)	The need to perform the employment contract
Management and validation of business expenses (expense reports, business bank cards, mileage allowances, etc.)	Legitimate interest
Drawing up pay slips and providing pay slips	The need to perform the employment contract
Management of partial activity	Legitimate interest
Managing withholding tax	The need to comply with a legal obligation
Nominative Social Declaration	Legal obligation
Management of individual allocations of supplies, equipment, vehicles, and payment cards.	Legitimate interest
Management of professional elections	The need to comply with a legal obligation
Organisation of meetings of employee representative bodies	The need to comply with a legal obligation
Expatriate management	The need to perform the employment contract

Purposes	Legal basis
For employee shareholders: managing employee shareholdings (choice of shares or funds), holding shares in savings plans, organising and managing employee votes for the election of directors, etc.	The need to comply with a legal obligation
Monitoring and maintenance of IT equipment	The legitimate interest in securing the KEYRUS Group's information system and means of communication
Management and administration of access rights to applications and IT systems	The legitimate interest in securing the KEYRUS Group's information system and means of communication
Management of IT directories to define access authorisations for applications and networks	The legitimate interest in securing the KEYRUS Group's information system and means of communication
Helpdesk management	Legitimate interest in following up requests from users of the information system
Management of mobile and landline telephones Provision of staff Management and maintenance of the telephony infrastructure Management, administration and control of telephone communications	Legitimate interest in providing means of communication
Management of fixed and mobile telephony services Provision of staff Management and maintenance of the telephony infrastructure Management, administration and control of telephone communications	Legitimate interest in providing means of communication
Implementation of systems to ensure the security and smooth operation of IT applications and networks	Legitimate interest in securing the information system and means of communication of the KEYRUS Group
Professional e-mail management	Legitimate interest in providing means of communication
Diary management and professional projects	Legitimate interest in being able to monitor the planning of employee activity
Implementation of an internal collaborative network for KEYRUS employees to enable employees to get in touch and share information.	Legitimate interest in connecting employees and sharing information
Virtual private networks within the organisation for the dissemination and collection of data relating to the administrative management of personnel	Legitimate interest
Management and monitoring of defence secret and basic control clearances in accordance with the obligations set out in the order of 30 November 2011 approving interministerial general instruction no. 1300 on the protection of defence secrets, including: management of clearance and basic control files (clearance requests, individual notices); keeping a register of staff members holding a clearance and to whom access is authorised; keeping clearance decisions, updating files, etc.	The need to comply with a legal obligation
Catering management (luncheon vouchers and company restaurant)	Legitimate interest
Professional appraisal of staff, in compliance with the relevant laws, regulations and agreements.	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Career and skills management	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Operations management and industrialisation of associated processes to identify the resources best suited to a customer's needs (scoring, matching, profiling) - PSA (Professional Services Automation)	Legitimate interest in mobilising human resources to support KEYRUS Group strategy
Forward-looking employment and skills management (GPEC)	Legitimate interest in mobilising and developing human resources in support of KEYRUS Group strategy
Mobility and travel management	The need to perform the employment contract
Telework management	The need to fulfil the employment contract or comply with a legal obligation (depending on the reason for teleworking)
verification of the integrity of bank details for internal control purposes	Legitimate interest
Case management - COVID 19	Safeguarding the vital interests of the data subject
Building staff loyalty (birthdays, gifts, etc.)	Legitimate interest in delivering human resources to support the strategy of the KEYRUS group
Working time management (time sheets or activity reports (CRA))	The need to perform the employment contract
Electronic signature of contractual documents on the Kosmos Platform	The need to perform the employment contract or pre-contractual measures taken at the employee's request.
Keyrus CSR	Keyrus' legitimate interest in implementing a CSR policy within the KEYRUS group Legal obligation for the declaration of extra-financial performance (DEFP) and the carbon footprint.
Health and Disability Helpline	Legitimate interest

Your Personal Data may also be collected indirectly from external sources:

Category of data collected indirectly Sources	Sources
Identification data	Cooptation
	Job site (jobboard)
	Badges
	Host company
	Social networks
	Recruitment agencies
	Works Council
	Tax authorities
Information about your professional life	Cooptation
	Social networks
	Recruitment agencies
	Job site (jobboard)
Connection data	Connection recorders
Report drawn up by the tax authorities in response to each nominative social declaration (NSD) or PASRAU «levy at source on other income» declaration submitted by the collector, which includes, in particular, its own identifier, information specific to each recipient of income paid by the RAS debtor, the registration number in the national identification register of natural persons or a waiting identification number allocated by the national old-age insurance fund for salaried workers, or the provisional identification numbers allocated by the employer if the first two numbers are not known, the rate of withholding tax applicable, except where the proportional rate is applied (by operation of law or at the option of the beneficiary), any anomalies detected by the tax authorities in the SND or PASRAU declaration prior to the report being issued.	Tax authorities

In the context of recruitment procedures, certain Personal Data may be obtained from a source other than the Data Subject, in particular job sites such as Monster, APEC or HelloWork, but also from social networks such as LinkedIn.
Recruitment agencies or other service providers may provide us with personality tests, for example: Test SOSIE.
If any of your Personal Data is processed by such companies, we invite you to refer to their data management policy. The KEYRUS Group cannot be held responsible for any violation of the Regulations in force by one of these companies.
Connection data such as «Logs» are collected indirectly by a connection recorder.

5
TYPOLOGY OF PERSONAL DATA

To help you better understand this Charter, please find below a table listing the main categories of Personal Data

Types of data	Categories of data
Current personal data	Personal life (lifestyle, family situation, excluding sensitive or dangerous data, etc.)
	Professional life (resume, education, professional training, awards, etc.)
	Economic and financial information (income, financial situation, tax situation, etc.).
	Connection data (IP addresses, event logs, etc.)
	Location data (movements, GPS, GSM data, etc.)

Types de données	Catégories de données
Personal data perceived as sensitive	Social security number (SSN)
	Bank details
Personal data perceived as sensitive	Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning the sex life or sexual orientation of an individual.
	Offences, convictions, security measures

6

PERSONAL DATA COLLECTED

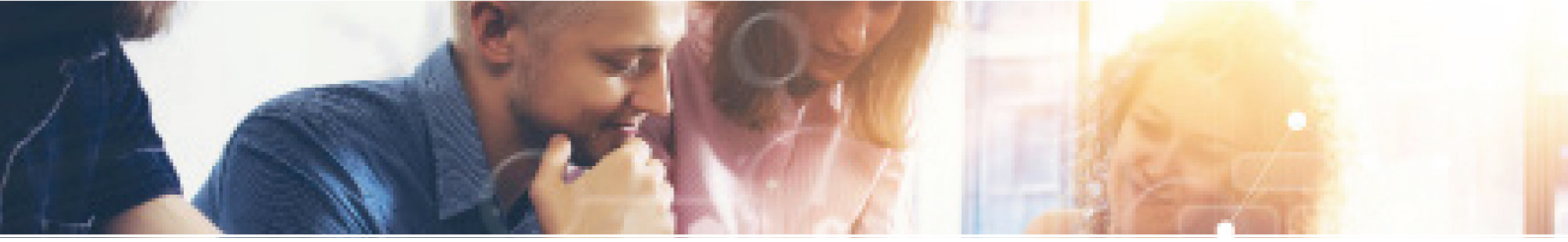
With regard to the purposes and legal bases defined above, the KEYRUS group holds and processes the following personal data:

For recruitment management purposes:

- Identity data (title, surname, first names, address (postal and email), telephone number, date of birth, photo (optional), LinkedIn profil address, information on nationality limited to «French / foreign / «European Union» or «non-EU» national»);
- Professional life (resume, training, diplomas and copies of diplomas, experience, covering letter, information provided by the Candidate, interview reports, date of interviews, work authorisation (yes/ no), message that may be sent by the Candidate on the KEYRUS Group website, etc.);
- Personal life (hobby indicated on the Candidate's resume);
- Economic and financial information (current and desired remuneration)
- Type, serial number and copy of work permit for foreign employees pursuant to Article R. 620-3 of the French Labour Code
- Health data provided by the applicant, including recognition of their status as a disabled worker (RSDW)
- Data relating to tests carried out by candidates during recruitment;

In the performance of an employment contract:

- Identification data civility (name, married name, first names, sex, date and place of birth, age, address, numbers allocated by social insurance, retirement and welfare organizations, photo (optional), email address, nationality, passport reference (only for people traveling abroad)), internal identifiers, signature;
- Copy of identity card;
- Photos taken during events organized by the Company Social Committee (CSC);
- Type, serial number and copy of the title serving as work authorization for foreign employees in application of article R.620-3 of the French Labour Code;
- Type of driving license held by the employee and a copy of the Employee's vehicle registration document for payment by the company of mileage allowances;
- Professional life (CV, place of work, internal identification number, date of entry into the company, seniority, job held and hierarchical coefficient, nature of the employment contract, dates of evaluation interviews, identity of the evaluator , professional skills of the employee, objectives assigned, results obtained, assessment of professional skills on the basis of objective criteria and presenting a direct and necessary link with the job held, observations and wishes formulated by the employee, career development forecasts, career simulation, disciplinary sanctions, professional achievements, professional agendas (date, places and times of professional meetings, subject, people present, attached documents), assigned tasks (identification of personnel concerned, distribution of tasks), electronic messaging messages , deliverables of the Collaborator, availability of the Collaborator,



- Data relating to telephony management (telephone number called and incoming, service used, operator called, nature of the call (in the form: local, departmental, national, international), duration, date and time of start and end of the call, billing elements (number of charges, volume and nature of the data exchanged excluding the content thereof and cost of the service used) SIM card number, IMEI number, PUK code); PIJKI code IP and MAC addresses, technical data linked to our networks
- Log files data
- Connection data (username and password)
- Data used to control internet use by employees;
- Administrative follow-up of employee medical
- Data used to control the use of messaging (tools for measuring the frequency and size of electronic messages, tools for analyzing attachments, etc.);
- Frequency data, email message size;
- Content of the Collaborator's email and address book;
- Validation of acquired experience (date of validation request, diploma, qualification title or certificate concerned, professional experience subject to validation, validation (yes/no), date of decision;
- Personal life (family and marital situation, dependent children, contact details of people to be notified in the event of an emergency, elements giving rights to special leave, leisure activities);
- Health data transmitted by the Employee including recognition of the status of disabled worker (RQTH), proof of MDPH recognition and, where applicable, information concerning the layout of the workstation
- Declaration of work accident and occupational disease (contact details of the occupational doctor, date of the accident or first medical observation of the occupational disease, date of the last day of work, date of return, reason for the stoppage (work accident or occupational illness), work not resumed to date) and other elements necessary for said declarations;
- Check-ups (dates of check-ups, fitness for work (fit or unfit), proposals for adaptation of the workstation or assignment to another workstation formulated by the occupational physician).
- Disability rate, CDAPH category (A,B,C), other categories of beneficiaries of law n°87-517 of July 10, 1987 (invalid pensioner, war disabled person, war disabled person assimilated)
- Elements of remuneration (system and basis for calculating remuneration, nature, compensation for partial activity, rate and base of social security contributions, leave and absences giving rise to deductible or compensable deductions as well as any deduction legally made by the employer, professional fees, method of payment, bank or postal identity): information relating to the interest
- Training (degrees, certificates and attestations, foreign languages used, follow up of vocational training requests and training sessions, evaluation of knowledge and training)
- Professional elections (establishment of the electoral list (identity of voters, age, seniority, college), management of candidacies (identity, nature of the mandate sought, information enabling compliance with eligibility conditions to be verified, trade union or trade union representative mandate (at the initiative of the candidate), where applicable trade union membership declared by candidates in the first round) and publication of results (identity of candidates, mandates obtained, identity of staff elected and, where applicable, trade union membership of those elected and, where applicable, the union affiliation of those elected);
- Meetings of employee representative bodies (invitations, preparatory documents, minutes);
- Particular hardships entitling employees to special leave or a credit for delegation hours (such as holding an elective or representative trade union office, participation in the operational reserve or volunteer firefighter missions);
- Individual allocations of supplies, equipment, vehicles and payment cards (management of requests, type of allocation, allocation, maintenance and withdrawal dates, budget allocations);
- Data for monitoring IT resources and authorizations: Date and time of the User's request, follow-up of the request, description of the request, list of the User's equipment, dates on which the equipment was made available (allocation and withdrawal dates).

- Active Directory account data (creation and modification date and time, Id number)
- Catering management (employee choice of meal voucher or RIE)
- Report drawn up by the tax authorities on the return of each «déclaration sociale nominative» (DSN) or «prélèvement à la source revenus autres» (PASRAU) declaration filed by the collector, including a unique identifier, information specific to each beneficiary of income paid by the RAS debtor, registration number in the national personal identification register, or a waiting identification number assigned by the Caisse Nationale d'Assurance Vieillesse des Travailleurs Salariés, or the provisional identification numbers assigned by the employer if the first two numbers are not known, the rate of withholding tax applicable except where the proportional rate is applied (by right or at the option of the beneficiary), any anomalies detected by the tax authorities during the DSN or PASRAU declaration that gave rise to the issue of the report ;
- Home working management (management of telework requests, eligibility conditions (type of employment contract, validation of trial period, minimum technical requirements (dedicated workspace, high-speed Internet connection, compliant electrical installation)), period (start and end dates), day requested for homeworking, certificate of compliance of electrical installation at home, comprehensive householder's insurance certificate, access conditions (position can be carried out remotely, sufficient autonomy at the workstation, compatibility of homeworking with the smooth running of the department and the team, feasibility in relation to the customer assignment carried out), duration of the agreement (start date and end date)).
- Checking the integrity of bank details for internal control purposes (date, name of bank N, name of bank N-1, account number, first name, last name and personnel number)
- Management of contact cases - COVID 19 (symptoms, test results (positive or negative), identity (surname, of potential contact cases).
- Electronic signature on the KOSMOS Platform (date and time of signature, action effected (signed or refused), operating system used, browser used, geolocation data, signature status, IP and biometric data of the quoted signature (writing angle, speed, acceleration, pressure or pseudo-pressure, letter formation and direction of signature strokes)).
- Permanence Health Handicap (surname, first name, professional email address, information about the appointment with the external disability consultant).
- Declaration of extra-financial performance (DPEF) (surname, first name, gender, date of birth, age, internal ID number, seniority, date of joining the company, seniority, function, date of leaving, legal entity to which the employee belongs, reason for the fin of contract, date of departure and fin of an absence, duration of the absence, equivalent days worked, date of start and fin of training, title of training, duration of training in hours).
- In exceptional cases, justified by the nature of the position to be filled, Keyrus may take note of the «yes/ no» verification of the candidate's or employee's bulletin n°3.

7

DATA RETENTION DURATION

The retention period for your Personal Data is determined according to the legal and regulatory retention periods specific to each type of data. Unless otherwise stipulated by law or in the tables below, Personal Data concerning Employees is kept in an active database for the duration of the Person's employment. When the Employee leaves, the data is archived in an intermediate archive in accordance with legal or regulatory deadlines. At the end of these periods, the Personal Data is destroyed.

For information purposes only, the retention periods for the main documents relating to the management of human resources and the social life of the KEYRUS Group are as follows:

Document types	Storage time	Reference text
Recruitment files	2 years after the last contact with the Candidate, unless the Candidate objects Only with the formal agreement of the Candidate can data be kept for longer. At the end of the recruitment process, the information information relating to unsuccessful candidates may be kept for a period of 5 years (intermediate archiving - data kept in the event of litigation)w	Article L1132-1 of the Labour Code Article L1134-5 of the Labour Code
Pay slip	5 years from the employee's 50th birthday in the paperless version (For more information, please Digipost's Data Protection Charter)	Article L3243-4 of the Labour Code Article D. 3243-8 of the Labour Code
Information required to calculate the tax base	1 month in active base then 6 years in intermediate archive	L. 243-16 of the Social Security Code
Entry of calculated data (DSN)	the time required to complete the declaration in the active database, then 6 years in the intermediate archive	L. 243-16 of the Social Security Code

Transfer order for payment	The time required to issue the pay slip on an active basis, then 10 years from the end of the accounting period for intermediate archiving.	L. 123-22 of the French Commercial Code
Single personnel register	5 years from the date of departure of the Employee	Article R1221-26 of the Labour Code
Documents concerning employment contracts, salaries, bonuses, allowances, pension schemes, etc.	5 years from the date of departure of the Employee	Article 2224 of the Civil Code
Document relating to social security contributions and payroll tax	3 years	Articles L244-3 of the Social Security Code and L169 A of the Book of Tax Procedures
Accounting for days worked by employees under fixed-term contracts	3 years	Article D3171-16 of the Labour Code
Recording of employees' working hours, on-call time and compensation for on-call time	1 year	Article D3171-16 of the Labour Code
Observation or formal notice from the labour inspectorate verification and control by the CHSCT	5 years	Article D4711-3 of the Labour Code
Declaration of accident at work to the primary health insurance fund	5 years	Article D4711-3 of the Labour Code
Data relating to telephony management (data relating to the use of telephony services: numbers called, numbers of incoming calls, etc.).	1 year	
Log file data	6 months	
Data used to monitor employees' use of the Internet	6 months for connection history	
Data used to monitor email usage (tools for measuring the frequency and size of emails, tools for analysing attachments, etc.).	6 months	
Content of the employee's electronic mailbox	5 years intermediate archiving from the date of departure of the employee	
Catering management	payment data kept for 3 months	
Report drawn up by the tax authorities	6 years	Article L. 102 B of the Book of Tax Procedures (BTP)
accounting documents and supporting evidence (ledgers and all accounting documents used to record transactions, accounting monitoring data, stock management data, annual accounts (profit and loss account, balance sheet, notes...), etc.)	10 years from the end of the financial year	Article L123-22 of the French Commercial Code
employment contract	5 years after the end of the employment contract	
Single risk assessment document	Unlimited duration	
Documents drawn up at the time of termination, expiry or breach of the employment contract	Unlimited duration	
Time sheets or activity reports (CRA)	5 years from the employee's departure	Article 2224 of the Civil Code
Individual profit-sharing and incentive allocation form	30 years	Article D.3313-11 of the Labor Code
Medical form drawn up by the occupational physician after each compulsory examination	Unlimited duration	
Observations and formal notices from the labor inspectorate (health and safety, occupational medicine, etc.)	5 years	
Receipt for all accounts and balances of all accounts	Unlimited duration	
Internal regulations	Unlimited duration	
Transaction	5 years	
training, qualifications, CV, position held, department, professional email, diplomas, recruitment data and interviews of people conducting a clinical study	25 years after the end of the clinical trial	Article 58 Regulation (EU) No 536/2014 of 16 April 2014 on clinical trials on medicinal products for human use and repealing Directive 2001/20/EC
Management of employee representative mandates Nature of mandate and trade union affiliation	6 months after the end of the term of office in active storage, then 6 years in intermediate storage	L. 2411-5 of the French Labour Code
Management of employee representatives' mandates Data relating to special hardship entitling employees to special leave or credit for delegation hours	The period of hardship for the employee concerned on an active basis, then 6 years in intermediate storage	L. 2142-1-3 of the French Labour Code
Exercise of the right to rectification, modification, portability or deletion	1 year	Article 9 of the Code of Criminal Procedure
Exercising the right to object and the right of access	6 years	Article 8 of the Code of Criminal Procedure

8

ROCESSING OF DATA COLLECTED BY COMPUTER

When working within the KEYRUS Group, you are required to use its IT resources on a daily basis (platforms, Corporate Social Networks, applications, software, etc.) which require your individual authentication and are likely to process your Personal Data. Each of these IT resources has its own data protection policy, failing which this Charter will apply to govern the processing of your Personal Data. It is the Employee's responsibility to familiarise themselves with these documents and to implement the obligations incumbent upon them as a result.

For any specific Processing, particularly in relation to security (video surveillance, badges, etc.), the use of IT resources made available to the Employee or individual supplies and equipment (hardware, software, badges, cars, etc.), Employees will receive specific information informing them of the way in which their personal data will be processed.

For more information on the use of IT resources within the KEYRUS Group, we encourage you to read the KEYRUS IT Charter. You also have the right to lodge a complaint with the CNIL as the supervisory authority.

9

DATA RECIPIENTS

The KEYRUS Group is responsible for processing the personal data of its Employees and Candidates. It undertakes to transmit such data only to authorized recipients, i.e.:

Within the framework of personnel management :

- Authorized persons in charge of personnel management, individual staffing and IT resources;
- The hierarchical superiors of the employees concerned, excluding data relating to social action directly implemented by the employer;
- Staff representative bodies: after obtaining the express agreement of the parties concerned, professional contact details of employees and data strictly necessary for their representation;
- The social and economic committee, provided the beneficiary has requested it;
- Trade union delegates: employees' professional details after formal agreement with the employer and express consent of those concerned, and data strictly necessary to defend employees' interests
- Training providers and organisations
- Internal training staff
- Catering service providers
- Edenred for the implementation of the luncheon voucher card;
- The telecom operator for telephony management;
- «COVID 19 referents» for contact case management.

Within the framework of payroll management:

- Personnel administration and payroll departments;
- Company financial control departments
- Authorised persons responsible for personnel management
- Bodies managing the various social insurance, unemployment insurance, retirement and provident schemes, holiday pay funds, public bodies and administrations legally entitled to receive them;
- The statutory auditors
- Financial organisations involved in the management of company and employee accounts
- La Poste and its service providers and the service providers offering the electronic pay slip service

Within the framework of recrutment:

- Recruitment departments
- Authorised persons responsible for personnel management
- Employees concerned by recruitment
- Recruitment agencies

Authorised service providers may also have access to your Personal Data as part of the services they provide 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.).

In the event of a dispute, your Personal Data may be transmitted to:

- The legal department and, where appropriate, those involved in resolving the dispute
- To the judicial authorities in the event of an offence
- Judicial or administrative, joint or consular, arbitration, to establish, exercise or defend the rights of an entity of the KEYRUS group.
- To the judicial or administrative, joint or consular courts, in execution of an enforceable court decision against a KEYRUS Group entity.
- To any natural or legal person in execution of an enforceable court decision against a KEYRUS Group entity.

Keyrus Group employees may have access to your Identification Data (last name, first name, professional email address and telephone number, position) in order to communicate with you.

For service reasons, authorised personnel of the KEYRUS Group, companies and members of their staff who have business relations with the KEYRUS Group may also have access to your identification data and your professional data (surname, first name, e-mail address, professional telephone number, position, CV and professional skills).

Furthermore, in the context of a transfer of employees, VIE or internship abroad, your Personal Data may be transferred to a KEYRUS Group entity outside the European Union located in a third country that does not ensure an adequate level of personal data protection according to the European Commission. Any such transfer will only be made on the basis of appropriate safeguards such as the signing of Standard Contractual Clauses.
In the event of an audit or inspection, your Personal Data may be communicated to the auditor, whether internal or external.

Our Data Protection Officer (DPO), our CISO, and KEYRUS Group Management are also Recipients.

In order to verify the integrity of bank details for internal control purposes, the payroll department and internal control are recipients of personal data.

The CSR department and disability representatives (both internal and external to the company) may have access to your Personal Data in the course of their duties.

10

SECURITY AND CONFIDENTIALITY

We implement all the technical and organisational measures that the KEYRUS Group considers appropriate, in accordance with Article 32 of the RGPD, in order to guarantee the security and confidentiality of your personal data.

We check that each Recipient complies with the appropriate security and confidentiality guarantees.

Employees are responsible for complying with their obligations in terms of security, and in particular for implementing the provisions of the KEYRUS IT Charter.
For more information about data security, please contact our DPO.

11

ENGAGEMENTDESPARTENAIRESECONOMIQUESENVERSKEYRUS

In specific cases such as a transfer of employees, expatriation, VIE or internship abroad, your personal data may be transferred to a KEYRUS group entity located in a third country that does not ensure an adequate level of personal data protection according to the European Commission. In this case, the KEYRUS Group undertakes to take all appropriate safeguards in accordance with the RGPD, such as signing Standard Contractual Clauses.

As part of telephony management, our telecom operator stores (or entrusts storage to a trusted service provider) the Personal Data that we communicate to it in the European Union.

As part of the use of the MYKLX training platform, your Personal Data is transferred to our service provider located in Israel. This transfer is based on an adequacy decision of the European Commission.

As part of the use of the PSA platform, your Personal Data is hosted in France. They are transferred to subcontractors outside the European Union located in the United States, a third country that is not adequate according to the European Commission, as part of the services provided by the PSA platform. This transfer is governed by standard contractual clauses signed by the platform publisher with the service providers concerned.

In the event of the transfer of your Personal Data to a Recipient located in a country that is not a member of the European Community, appropriate guarantees will be put in place, in accordance with the provisions of the RGPD and the KEYRUS Group will inform you by any means.

For further information, please contact our DPO.

12

RIGHTS OF PERSONS CONCERNED

In accordance with the regulations, you may access your personal data and request that it be corrected or deleted. You also have a right to object, a right to limit the Processing of your Personal Data and a right to the portability of your Personal Data, where applicable.

You can find out all about these rights and how 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, with « personal data » in the subject line;
- Email to KEYRUS.DataProtection@KEYRUS.com

He will get back to you as soon as possible.

Our telecom operator is responsible for processing your Personal Data in connection with electronic communication services. However, you should address your questions and/or requests to our DPO.

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

13

INVALIDITY OF CLAUSE

If one or more stipulations of the charter are held to be invalid or declared as such in application of a law or other legislative text or following a definitive decision by a competent court, the other stipulations will retain all their force and scope.

14

EVOLUTION OF THE CHARTER

The charter may be amended by KEYRUS management in order to take account of recommendations from the CNIL, changes in the law, case law, IT techniques and, more generally, any changes in information and communication technologies.

Signed in Levallois-Perret, on October the 23 2023