Information notice concerning the protection of personal data for group employees

Introduction

This notice specifies the nature of the personal data we collect and the purposes for which they are processed. It also specifies all other information relating to the processing we perform on your personal data.

This notice applies to the personal data of current employees, former employees, interns, temporary workers, service providers and any third party about whom we collect data in the course of the employment relationship.

This notice is made in order to comply with applicable regulations and, in particular, the provisions of European Regulation 2016/679 of 27 April 2016, those of applicable national legislations and the texts enabling their implementation.

This information sheet is part of Elior Group's broader approach aimed at transparency with regard to the use of the personal data it collects in accordance with the principles set out in the Personal Data Protection Policy.

1. Background

Elior Group is committed to protecting its employees' personal data. It guarantees the use of personal data that is responsible, relevant and limited to its strict needs.

Elior Group processes its employees' personal data transparently and respects their rights. We therefore wish to provide you with concise and understandable information on:

- The purposes of processing;
- The legal basis for processing;
- The categories of data collected;
- The data source;
- The recipients of your data;
- The retention periods;
- Your rights;
- The contact details of your data protection officer.

The purpose of this information notice is to inform you in general about the various processes implemented relating to your personal data. This notice may be supplemented, in some cases, by more detailed information when necessary.

2. What categories of personal data do we collect and process?

The personal data processed varies depending on the activity of your entity of attachment, your function and your type of employment contract. This includes in particular the following data:

Your identification data: surname, first name, date and place of birth, social security number, personal contact details, contact details of the person to be contacted in the event of an emergency, your marital status, data relating to your family members, if applicable, data relating to your status as a foreign worker, etc.

Your photograph: which may appear on your workplace access badge, on the Intranet or on various communications media etc.

Your job information: your professional details, your number, your job title, your position in the organisation chart, etc.

Data relating to the entry/exit of the company's workforce: application file, results of recruitment tests, interview files, end of contract documents etc.

Data relating to your training course, managing your performance and your career: your training requests, reviews relating to talent and performance management programmes, professional interviews, your mobility wishes, copy of correspondence in the context of the employer/employee relationship etc.

Compensation and benefits data: your salary and all accessories, changes to your salary, your bank details, documents relating to your professional expenses, transport used, fines received, your tax information required for deduction at source, your proof of income required to obtain certain benefits or services, etc.

Data concerning your absences and attendance: any document providing evidence of an absence (illness, exceptional leave, maternity leave, etc.), data relating to your business travel, if applicable, monitoring working hours and teleworking, etc.

Data concerning any incapacity or disability: medical certificates, workplace accident declarations, disability pension information, file relating to any adjustment or adaptation of the workstation, etc..

Data regarding disciplinary measures taken against you and your requests relating to difficulties at work: any data relating to the establishment of a sanction or any request in the event of a dispute, etc.

Your catering data: balance, coverage rate, cash register receipts history, etc.

Your data on health and safety at work: data shown in audit reports, professional risk assessment documents and incident reports etc.

Your data relating to information systems and security: CCTV, data on connection to and use of information systems, data relating to your badge and access to your workplace, where applicable, data collected during authorization procedures, etc.

3. What is the legal basis for the processing of your personal data?

When collecting your personal data, we take care to inform you about the purpose.

Generally speaking, data are collected in order to comply with the legislation and commitments defined in your contract, the collective agreements or to pursue the legitimate interest of the group. In all other cases, we request your prior agreement.

Performance of the employment contract

Elior Group uses specific tools designed to facilitate your career management and to provide you with access to specific services and benefits. For example, your badge allows you to access the company restaurant.

Compliance with a legal obligation

This is particularly the case for legal formalities relating to the hiring of employees, the sharing of data on salaries with tax authorities, registration for welfare schemes and health organisations, and relations with any other public body.

The pursuit of the group's legitimate interest

Elior Group processes your data in order to offer you new employment opportunities, to assess performance or, more generally, to manage its relationship with you in the course of your work.

Your consent to the processing of your data

In some cases, where the processing cannot be justified by one of the grounds mentioned above, the processing of your data is based on your prior, explicit consent. This consent will be requested in order to respect your choice and to inform you precisely about the processing applied.

4. How and on what occasions do we collect your personal data?

We collect your personal data mainly from you, during your recruitment and throughout the performance of your employment contract.

You are invited to enter your data directly into the information systems (e.g. HR Intranet, e-mails, etc.). You can keep them up to date directly or inform us if data prove to be incorrect.

We also collect data through the Human Resources Department and your management (for example, annual performance reviews). We may also receive personal data about you from third parties (administration, mutual insurance, welfare insurance, occupational health service, skills assessment firm, etc.).

Finally, your personal data may be collected indirectly from information and communication tools and technologies (e.g. workplace access control, recording and history of telephone calls, logging of Internet connections and geolocation), in strict compliance with the applicable regulations and the Group's internal rules.

5. What are the reasons why we use your personal data?

Your personal data are processed in order to meet specific purposes.

Payroll management and its accessories, the management of wage increases, compensation and stock options plans, the deduction of tax at source, the provision of the pay slip in electronic form etc.

Managing your career and training: legal formalities linked to your recruitment, contact forms, professional assessment, skills management, confirmation of prior experience, career simulation, management of professional mobility and follow-up of training initiatives, etc.

Work organisation: managing work agendas and schedules, managing travel, managing on-call time, managing applications to facilitate professional communication, managing tasks, managing work time as well as monitoring your days of absence, teleworking, time spent, assignments and the business continuity system, workstation adaptation measures, etc.

Catering and concierge service management

Provision of IT resources: the management of business tools, the proper functioning of IT services, monitoring, maintenance and support of computer equipment, the management of computer directories and access authorisations, the implementation of security systems etc.

Security of property and people: access control, video surveillance, systems for accessing IT tools, where applicable, accreditation or any other specific authorisation, insurance management, any approach related to occupational health, etc.

Formalities and declarations to the authorities (court clerks, tax authorities, etc.) in connection with the administrative formalities relating to company rights, etc.

Litigation management: exercising and defending the interests of the Elior Group in the context of an internal investigation, disciplinary action, litigation, request, injunction or any other purpose involving the Elior Group, etc.

6. To whom do we transfer your personal data ?

Transfers to internal recipients

Your personal data are accessible or may be communicated internally only to persons who need access to them in the performance of their duties, namely:

- The human resources department;
- Your manager;
- Any duly authorised Group employee in particular IT system administrators.

However, certain personal data (such as surname, first name, position, and business telephone, postal and electronic contact details) are accessible to all employees via the directory.

Transfers to external recipients

Your data are transmitted, in particular:

- To public and private bodies as part of our legal obligations;
- To welfare, supplementary health insurance and collective savings schemes for the purposes of affiliation;
- To third party organisations involved in organising work, in particular concerning business travel;
- To Works Councils, unless you object;
- To our subcontractors in the areas of payroll and benefits management, training or career management;
- To our technical and IT subcontractors.

They are not sold to a third party for commercial purposes.

Transfers outside the European Economic Area (EEA)

Transfers to third parties located outside the EEA may also be made.

In this case, these transfers are governed either by the standard contractual clauses of the European Commission or Binding Corporate Rules (BCR), or by membership of the Privacy Shield, or by any other mechanism guaranteeing an adequate level of protection.

7. How long do we keep your personal data?

The data we collect are retained for a fixed period of time. They are retained by us at least to meet our legal and contractual obligations.

The table below shows the retention periods for your data by purpose.

In some cases, particularly in the context of litigation, we may have to keep these data for a longer period of time.

Purposes of the processing	Retention period	Legal basis
Personnel management	5 years from the employee's departure	NS46
Payroll management	5 years from payment of the salary	Article L3243-4 of the French Labour Code
Recruitment files	Immediate destruction if the candidate is not selected either for the position to be filled or in connection with a future recruitment 2 years after the last contact with the candidate if there is a wish to retain the application	CNIL recommendation
Training	1 month after operations required to manage personal training accounts	AU 044
Video surveillance	1 month from image capture	Law 95-73 of 21/01/1995 as amended

Directory management	Duration of the employee's employment period	NS46
Monitoring of Internet use by employees	6 months for log-in histories from log creation	CNIL recommendation
Telephony management (data relating to the use of telephone services: numbers called, numbers of incoming calls, etc.)	1 year from receipt of the data	NS47
Geolocation of company vehicles	2 months (travel history) from receipt of the data	NS51
Time check	5 years from receipt of the data	NS42
Catering Management	3 months (electronic payment data) from receipt of the data	NS42
Access control	3 months (passage logs) from receipt of the data	NS42
Disciplinary sanctions	3 years rolling from the announcement of the sanction	Art L1332-5 Labour Code
Recording of telephone conversations for stock market order evidence purposes	5 years maximum after recording the conversation	Articles 321-78 and 321-79 of the AMF Regulation
Integrating disabled people into work	5 years (DOETH) from the sending of the declaration	Art. 5212-13 of the Labour Code
Management of expense claims	10 years from receipt of the expense claim	Commercial Law
Professional alert	Duration of the procedure	AU 004
Vehicle fleet	Duration of use of a professional vehicle + 6 months in the event of a fine	CNIL recommendation
Ticketing tool	2 years from receipt of the ticket	Term defined by Elior
Management of fines	45 days from receipt of the fine 2 years from receipt of the fine	AU 010 Term defined by Elior
Litigation management	The data processed to manage pre-litigation must be deleted as soon as the dispute is settled amicably or, failing that, as soon as the corresponding legal action expires. Data processed to manage litigation must be deleted when appeals against the decision taken to enforce it are no longer possible.	AU 046

8. What security measures are taken regarding your personal data?

Data security is a key issue for the group. Failure to ensure the security of data over their entire life cycle, from collection to destruction, may lead to significant harm. Increased vigilance must be given to the security of external providers when they are stakeholders in the processing of personal data.

There are many ways to protect personal data, whether they are stored in electronic or paper form. In order to support its employees, the Elior Group offers them a state-of-the-art body of documents, which must be applied:

- A security policy for information systems and associated directives detailing the requirements applicable to Elior Group information systems;
- Security requirements that are a prerequisite to any contract with an IT service provider.

The recommendations presented below are adapted on a case-by-case basis and according to the risks incurred by data processing on the freedoms and privacy of the persons concerned:

- Applications must be protected by authentication systems (username and password) in accordance with the information security policy.
- Access to personal data is only authorised for persons accredited to have access to the data in question, this is "the right to know ".

For any questions, please refer to the Elior Group Information Systems Security Manager.

9. What are your rights to your personal data?

The Elior Group undertakes to process your personal data in accordance with the applicable regulations and to keep them up to date.

You have a number of rights to your personal data:

Right to information: be informed of how Elior Group will use and share your personal data.

Right to rectification: have any inaccurate or incomplete personal data rectified.

Right to erasure: request the erasure of certain information about you, also called the "right to be forgotten". This is not an absolute right to the deletion of all personal data, as Elior Group must also comply with its legal obligations and protect its legitimate interest.

The right to restrict the processing of personal data: restrict the processing of your personal data in certain circumstances.

The right to portability of personal data: request a copy of your personal data in a commonly used electronic format.

The right to object: object to the processing of your personal data. If an objection is raised to personal data processed for reasons of legitimate interest, for compliance with contractual requirements or the public interest, then a balancing of interests must be carried out. It will determine whether there are compelling legitimate grounds for continuing to process the data. In each case, the outcome of this decision and the reasons for it will be documented.

Elior Group has appointed a personal data protection officer to inform, advise and ensure compliance of the processing with personal data regulations.

In the event of difficulties encountered in exercising these rights, or for any question relating to the processing of your personal data, you may refer the matter to the personal data protection officer at the following address: gdpr-contact@eliorgroup.com. If you feel, after contacting the DPO, that your rights have not been respected, you can submit a complaint online or by post to the CNIL.