Information on the protection of the personal data of Elior Group employees

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

The Elior Group protects the personal data of its employees and ensures that such data is used in a responsible, relevant and transparent manner.

The purpose of this newsletter is to inform you in general about the various processes implemented relating to your personal data. **A more detailed information notice is available from the dedicated website** https://privacy.eliorgroup.net.

1. What types of personal data are involved?

The personal data processed vary 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 civil status, 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 identification 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 your 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 encountered at work: any data relating to the establishment of a sanction or any request in the event of a dispute, 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.

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.

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

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

Managing your career and training: the Single Hiring Declaration (DUE), 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 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.

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.

3. To whom do we transfer your personal data?

Transfers to internal recipients within the Elior Group, your personal data is accessible or may be communicated internally only to persons who need access to it in connection with the performance of their duties, namely: the Human Resources Department, your line manager and any duly authorised employee: IT services, legal services, Management and monitoring tool for the vehicle fleet (One Fleet), etc.

Transfers to external recipients, your data may be transmitted outside the Elior Group, but are not communicated to a third party for commercial purposes.

Transfers outside the European Economic Area (EEA) are also possible. In this case, these transfers are supervised by any mechanism guaranteeing an adequate level of protection, and through appropriate legal clauses.

4. How long do we keep your personal data?

The data we collect are retained for a fixed period of time and **at least to meet our legal and contractual obligations, a full information notice concerning the protection of personal data for group employees provides details on retention periods. This notice is available on the dedicated website** https://privacy.eliorgroup.net.

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

Data security is a key issue for Elior Group. There are many ways to protect personal data, whether they are stored in electronic or paper form. To support its employees, the Elior Group provides them with a regularly updated body of documentation, which must be applied.

If you have any questions, you can contact the Elior Group Information Systems Security Manager: it.security@eliorgroup.com.

6. What are your rights to your personal data?

You have a number of rights concerning your personal data. Details of these rights can be found in the full notice **available on the dedicated website** https://privacy.eliorgroup.net.

Elior Group has appointed a personal data protection officer to inform, advise and ensure compliance with personal data regulations. This officer relies on the expertise of a group team and ambassadors.

For any questions relating to the processing of your personal data, you can consult the Personal Data Protection Officer at the following address: gdpr-contact@eliorgroup.com.