

Data controller: Liftec Lifts Ltd.
Unit 7, Orbital One,
Green Street Green Road
Dartford
DA1 1QG

Data protection officer: Andy Ward – Compliance Manager

Introduction

Liftec Lifts Ltd (the Company) is committed to protecting the privacy and security of your personal information.

This Privacy Notice describes how the Company collects and uses personal information about you during and after your working relationship with the Company, in accordance with the General Data Protection Regulation (**GDPR**).

It applies to all employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services and the Company may update this notice at any time.

Liftec Lifts Ltd. is a “Data Controller”. This means that the Company is responsible for deciding how it holds and uses personal information contained in this privacy notice.

It is important that you read this notice together with any other privacy notice the Company may provide on specific occasions when it is collection or processing personal information about you, so that you are aware of how and why the Company is using such information.

Data protection principles

Liftec Lifts Ltd will comply with data protection law. This says that the personal information the Company holds about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that the Company has clearly explained to you, and not used in any way that is incompatible with those purposes;
- relevant to the purposes the Company has told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes the Company has told you about and
- kept securely.

The Company collects and processes personal data relating to its employees to manage the employment relationship.

The Company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the Company collect?

The Company collects and processes a range of personal data, or personal information about an individual from which that person can be identified. It does not include data where the identify has been removed (anonymous data). The personal information that the Company collects about you includes:

- your name, address and contact details, including personal email address and telephone number, date of birth and gender;
- marital status and dependants;
- next of kin and emergency contact information;
- continuous service start date;
- location of employment or workplace;
- salary remuneration and benefits history;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- Photographs in digital or hardcopy formats.
- information obtained through electronic means such as swipe card records; tracker devices on company owned / leased vehicles; and finger print attendance recording devices (The Company's monitoring policy is available on request).
- information about your nationality and entitlement to work in the UK;
- information about your criminal record (*Role dependent*);
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments;
- details of trade union membership; and

- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

How is your personal information collected?

The Company collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as clients security application forms); from correspondence with you; or through interviews, meetings or other assessments.

The Company has operational CCTV on its premises and a moving image of you may be captured on a recording device linked to the system. The recordings are cleared automatically after a seven day period.

In some cases, the Company collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, and information from criminal records checks permitted by law.

Where is your personal data held?

Your personal data is stored in a range of different places, including in your personnel file, in the Company's HR management systems and in other IT systems (including the Company's email system). Company compliance and Health and Safety Records.

Why does the Company process personal data?

The Company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer [benefit, pension and insurance entitlements].

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. [For certain positions, it is necessary to carry out criminal records checks and submit security clearance applications to ensure that individuals are permitted to undertake the role in question at specific high secure customer premises.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Company to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- Checking that you are legally entitled to work in the UK or EU
- paying you and, if you are an employee, deducting tax and National Insurance contributions.
- administering any court mandated deductions from your salary.
- business management and planning, including accounting and auditing
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- gathering evidence for possible grievance or disciplinary hearings.
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- dealing with legal disputes, involving you, or other employees, worker and contractors, including accidents at work.
- complying with health and safety obligations.
- to prevent fraud.
- to monitor your use of our information and communication systems to ensure compliance with our Computer and Phone policies.
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.
- some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Use of Particularly personal information

“Special Categories” of particular sensitive personal information require higher levels protection. The Company will need to have further justification for collection, storing and using this type of personal information. The Company may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where it needs to carry out its legal obligations of exercise rights in relation to your employment with the Company. The Company has in place an appropriate policy document; contract and safeguards which it is required by law to maintain when processing such data;
- where it is needed in the public interest.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the Company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the Company uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Applicants are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Change of purpose

The Company will only use your personal information for the purposes for which it has collected it, unless it reasonably considers that it needs to use the information for another reason and that reason is compatible with the original purpose, the Company will notify you and will explain the legal basis which allows the Company to do so.

Please note that the Company may process your personal information without knowledge of consent, in compliance with the above rules, where this required or permitted by law.

Who has access to data?

Your information will be shared internally, including with [members of the HR, and payroll and finance team, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The Company shares your data with third parties in order to [obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The Company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Company also shares your data with third parties that process data on its behalf [, in connection with payroll, the provision of benefits, nominated vehicle leasing company that manages the Company fleet and the provision of occupational health services.

The Company will not transfer your data to countries outside the European Economic Area.

How does the Company protect data?

The Company takes the security of your data seriously. The Company has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees and third party archiving providers in the performance of their duties.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data. Furthermore the Company has implemented the following measures to mitigate data breaches.

Blank Data Collection Forms posted pre start of employment, returned in person on starting alongside identification and proof of address.

Forms stored on personnel files, locked away in filing cabinet in HR office; which is also locked when staff not present.

Data transferred by HR personnel for clearance applications and employees asked to attend Head Office for signing where necessary. In the event that this is not possible, blank forms are posted for signing then completed upon return.

Submission of forms are mainly electronic to specified email addresses, excluding Houses of Parliament which is via the postal service in this instance I sent them signed for. BPSSVR forms and verified documents are ONLY sent electronically to safeguard.

Network based mitigation

- Installed IDS/IPS with the ability to track floods (such as SYN, ICMP, etc.)
- Installed a firewall that has the ability to drop packets rather than have them reach the internal server. The nature of a web server is such that we allow HTTP to the server from the Internet. We monitor our server to know where to block traffic
- Daily antivirus (AVG) and anti-malware check
- 128-bit SQL server encryption
- We use WinZip AES-256 to encrypt sensitive data/documents
- Have contact numbers for our ISP's emergency management team (or response team, or the team that is able to respond to such an event). We need to contact them in order to prevent the attack from reaching your network's perimeter in the first place
- Monthly or (for sensitive contracts) weekly password changes. Use of 12 character strong alphanumeric passwords; password lock-out for 5 failed attempts; password history of 20; password expiry 45 days

Host based mitigation

- Ensure that HTTP open-sessions time out at a reasonable time.
- Ensure that TCP also time out at a reasonable time
- Install a host-based firewall to prevent HTTP threads from spawning for attack packet

Penetration testing and vulnerability scanning

- We conduct internal phishing campaigns to test cyber awareness of our own employees
- External assessments of our infrastructure and security policies (Microfix Ltd.)

All employees who in their roles are responsible for processing personal data are bound by confidentiality agreements.

For how long does the Company keep data?

The Company will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the relevant retention periods.

Documentation relating to a Construction contract and/or Minor Works (CP job) – 10 years*

Documentation relating to a Repair Contract/small repair works/service (RC job) – 2 years*

Documentation relating to a service/maintenance contract (SC job) – 2 years*

Accounts/Tax information – 7 years*

Employee / Personnel Records - Statutory requirements to retain for up to 6 years*

(personnel files will contain human resource information, training, particularly asbestos awareness type training and DSE assessments. The last two items can mean that an individual's personnel records, could be required to be held for up to 40 years due to the potential claims that could come in as a result of long term health affects)

*** It should be noted, that in the event of a legal case being held against any contract file, the length of time the documentation is required to be retained for, can be extended.**

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Company to change incorrect or incomplete data;
- require the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing; and
- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data.
- request the transfer of your personal information to another party.

If you would like to exercise any of these rights, you can make a subject access request by completing the Company's form for making a subject access request. You can request this form from the HR Department or the Company's DPO (Data Protection Officer).

If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner.

Your consent

The Company does not need your consent if it uses special categories of your personal information in accordance with its written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, the Company may approach you for your written consent to allow it to process certain particularly sensitive data. If the Company does so, it will provide you with full details of the information that it would like and the reason it is required, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with the Company that you agree to any request for consent.

Information about criminal convictions

The Company may only use information relating to criminal convictions where the law allows it to do so. This will usually be where such processing is necessary to our its contractual obligations in the case of high level security clearances for public sector buildings and in line with the Company's safeguarding policy.

Less commonly, the Company may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interest (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The Company may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

The Company envisages that it will hold information about criminal convictions and will only collect this information it is appropriate given the nature of the role where legally able to do so. The Company will collect information about criminal convictions as part of the

recruitment process or be notified of such information during an employee working for the Company. The company will use information about criminal convictions and offence in the following ways:

- making decisions about your continued employment or engagement.
- gathering evidence for possible grievance or disciplinary hearings
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- assessing suitability for a particular job role or task

The Company can use your personal information in this way to carry out its obligations and have in place the appropriate policy and safeguards that is required by law to maintain when processing such data.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the Company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Company to enter a contract of employment with you. If you do not provide other information, this will hinder the Company's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Data Protection Officer

The Company has appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how the Company handles your personal information, please contact the DPO, andy.ward@liftec.co.uk.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Changes to this privacy notice

The Company reserves that right to update this privacy notice at any time, and will provide you with a new privacy notice when substantial updates are made. The Company may also

inform you in other ways from time to time about the processing of your personal information.