DATA PROTECTION POLICY AND EMPLOYEE PRIVACY NOTICE

1. Purpose

This notice provides information about the data we collect and hold about you, the reasons why it is collected and your rights under the Data Protection Act 2018 (DPA) and the General Data Protection Regulations 2018 (GDPR)

2. How your information will be used

As your employer, Locker needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left.

This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of Locker and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

3. Processing your information

As your personal data is for in the legitimates interests of managing your employment with Locker, we will **not** ask for your explicit consent to process your data. We will only ask for your consent when we need to collect or process 'special categories' of data (see point 5).

The nature of our legitimate interests are to:

- Manage your employment life-cycle and contract of employment
- Process the payroll and pay you according to legislation

A Locker Group Company
Locker Group Ltd, Farrell Street, Warrington, WA1 2WW
Sales: + 44 (0)1925 406600
https://www.lockergroup.com/
sales@lockergroup.com
Registered No. 5608946 England VAT Reg. No.: GB 896117588

- Process your pension and other benefits
- Ensure appropriate security control
- Provide information technology support and equipment

We will never process your data where these interests are overridden by your own interests, without discussing this with your first.

4. Collecting your personal data.

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees.

The sort of information we collect and hold includes:

- your CV and references
- your contract of employment and any amendments to it
- correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary
- information needed for payroll, benefits, pension and expenses purposes
- right to work information, eg. passport details
- driving licence and insurance details if you drive for the business.
- contact and emergency contact details
- records of holiday, sickness and other absence
- records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records

You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.

5. Special Categories of Data

Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to

consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay, and where appropriate and life or health assurance policies.

Where we process special categories of information relating to medical / health, race or ethnic origin, political opinions, religion and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency.

Where we are processing data based on your consent, you have the right to withdraw that consent at any time. However, where consent to information is not given the business will still need to make decisions about your employment in the absence of any relevant information.

6. Computer and Electronic Communications

We monitor computer (and telephone/mobile telephone) use, as detailed in our *Email, Internet and Social Medial Acceptable Use Procedure,* which can be seen in the Staff Handbook. Your personal data such as work email addresses, or email signatures will be available for others to see as part of your employment and the undertaking of your role.

7. Sharing your data

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for example we may need to pass on certain information to HMRC or the pension administrators.

When we have been asked to disclose information which we are not legally obliged to disclose, or does not fulfil a legitimate interest of Locker, we will seek your explicit consent before any disclosure.

8. Transfer of data

We may transfer information about you to other group companies for purposes connected with your employment or the management of Locker's business.

In limited and necessary circumstances, your information may be transferred outside of the EEA or to an international organisation to comply with our legal or contractual requirements. We will ensure your data is properly safeguarded in these circumstances.

9. Storage and Retention of Records

Your personal data will be stored securing in computerised or manual systems for the term of your employment. Essential information relating to your pay, tax or pension will be retained for up 7 years following the end of your employment.

You have a responsibility to ensure that, within your capability, your own personal information and that of your colleagues and third parties is kept secure.

We will not use the personal data retained for any other purpose that which has been detailed to you. However, if in the future, we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.

10. Your rights

Under the General Data Protection Regulations (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data.

You have the right to:

- request from us access to and rectification or erasure of your personal data
- request the restriction of processing, object to processing as well as in certain circumstances the right to data portability
- if you have provided consent for the processing of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn
- to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

11. Accountability

Locker will demonstrate that it complies with the principles of the new regulations. Locker complies in the following ways:

- A data protection policy is available to employees and other stakeholders. The policy is regularly reviewed and audited.
- Privacy notices are available to customers on the websites
- The data protection policy and principles are reviewed annually as part of the Quality Meeting

12. Identity and contact details of controller

Locker is the controller of data for the purposes of the DPA and GDPR. The Operations Manager should be contacted in the first instance if you have a query regarding data protection.

13. Customers, Third Parties and Marketing

The data of customers and other non-employees is protected in the same way as that of an employee and they have the same rights. Our websites have updated privacy notices advising customers of our policies.

Marketing information will comply with the requirements of GDPR and DPA

- Locker will demonstrate how the data subject (eg. customer / potential customer) has consented to the processing which means Locker will record how and who gave consent.
- The data subject will be able to withdraw consent at any time (the right to object) and it shall be as easy to withdraw consent as to give it.
- Consent will cover all processing activities carried out for the same purposes. If data is required for a different purpose, separate consent will be required.
- Where processing is for multiple purposes, consent should be given for all of those purposes.
- Consent will not be considered freely given if the data subject has no genuine or free choice.
- Silent consent, pre-ticked boxes or inactivity will not constitute consent.

All employees should understand the legislation and the need for confidentiality if they have access to customer data.

14. Personal Data Breaches

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

A personal data breach may mean that someone other than Locker gets unauthorised access to personal data. A personal data breach can also occur if there is unauthorised access within Locker, or if an employee accidentally alters or deletes personal data. Breaches need to be assessed on a case by case basis. For example, Locker will need to notify the Information Commissioners Office (ICO) about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally need to be reported.

Locker must notify the ICO within 72 hours of becoming aware of the essential facts of the breach. Failing to notify a breach when required to do so can result in a significant fine.

15. Reporting a concern, or seeking further advice

If you have any concerns as to how your data is processed you should, in the first instance contact you manager. If your issue is not resolved or you need to speak to someone else please see the Operations Manager, who acts as our Data Protection Officer.

Appendix 1

Employee Data - Record Keeping Schedule

Introduction

It is intended that Locker store and retain personal data only as long as is necessary for the legitimate purpose of managing the employment contract and for meeting legislative requirements. Information may be store manually and electronically.

Statutory Retention Periods

The table below summarises the main legislation regulating statutory retention periods.

Record	Statutory retention period	Statutory authority
Accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Income tax and NI returns, income tax records and correspondence with HMRC	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended

Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894) as amended
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

Recommended (non-statutory) retention periods

(As advised by the Chartered Institute of Personnel and Development)

Record	Recommended retention period
Actuarial Valuation reports	Permanently
Application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the personnel file in any event.
Inland Revenue/HMRC approvals	permanently
Money purchase details	6 years after transfer or value taken
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after benefit ceases
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases

Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy

Locker may retain information beyond the statutory or recommended retention period if there is a clear business need or it is not practical to separate documents with different retention periods.

Andrew Campbell
Chief Executive Officer
Locker Group Ltd

6th January 2025