

# DATA PROTECTION POLICY

# 1 DATA PROTECTION POLICY

---

## Introduction

### *Purpose*

The Company is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data.

This policy does not apply to the personal data of clients or other personal data processed for business purposes.

The Company has appointed Mick Austen Group Compliance & Training Director, as the person with responsibility for data protection compliance within the Company. He can be contacted at [dataprotection@mayfaircleaning.co.uk](mailto:dataprotection@mayfaircleaning.co.uk). Questions about this policy, or requests for further information, should be directed to him.

### *Definitions*

**"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**Data protection principles** The Company processes HR-related personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing.

- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

The Company will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor, apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds HR-related personal data are contained in its privacy notices to individuals.

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

### **Individual rights**

As a data subject, individuals have a number of rights in relation to their personal data.

#### *Subject access requests*

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the Company has failed to comply with his/her data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

To make a subject access request, the individual should send the request to [dataprotection@mayfaircleaning.co.uk](mailto:dataprotection@mayfaircleaning.co.uk). In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify him/her that this is the case and whether or not it will respond to it.

#### *Other rights*

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to [dataprotection@mayfaircleaning.co.uk](mailto:dataprotection@mayfaircleaning.co.uk).

The Company takes the security of HR-related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

The internal policies and controls are contained in the Company Standard Operating Procedures.

Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

### **Impact assessments**

Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing.

This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

### **Data breaches**

If the Company discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

### **International data transfers**

HR-related personal data may be accessed by countries outside the EEA to process accounts and payroll. Data is accessed outside the EEA on the basis of a declaration of adequacy, binding corporate rules or other safeguards.

### **Individual responsibilities**

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, internship or apprenticeship. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;

- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

The Company's security procedures are contained in the Company Standard Operating Procedures.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

#### **Training**

The Company will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.



**Andrew Prendergast, Chief Executive Officer**

**April 2022**

## 2 EMPLOYEE PRIVACY NOTICE

---

### **Data Controller: The Mayfair Cleaning Company Ltd**

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 information about you. This includes:

- your address, telephone number and email address, etc and contact details of others that you provide, such as who to contact in the event of an emergency, details of your dependents, life assurance beneficiaries, information from welfare forms etc.
- your date of birth and gender;
- the terms and conditions of your employment;
- employment and career history, photograph, termination details, absence and attendance records, health and safety records, sickness records, accident reports, skills and experience records, training records, records of projects you have worked on, etc.
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- your CV, notes of interviews, application forms, decisions to offer employment, background information and third-party references (if recorded), criminal records check file (if applicable), and psychometric test results (if applicable) etc.
- your compensation, benefits and pension arrangements, such as details of your salary and any deductions, bank account, tax codes, national insurance number, corporate credit card usage, employment benefits, travel expenses, company car arrangements, etc.
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- details of your schedule (days of work and working hours) and attendance at work;
- your location (where such information is legally permitted to be collected), such as where recorded by electronic card access systems or non-electronic systems, vehicle trackers;

- information about your use of our computers and phones, etc.(where such information is legally permitted to be collected).
- information about your work activities from operational management services;
- information about your call reporting through the call centre voice recording system;
- 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, 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;
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation and religion or belief; and
- other information which you voluntarily provide in the course of employment that it is necessary to hold or use for our business purposes.

The Company may collect this information in a variety of ways. For example, data might be collected through application forms, CVs; 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 benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

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

Data will be 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).

### **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.



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 carry out the following:

- Workforce Planning and Recruitment, for example business forecasting, employee assignment planning and budgeting, run recruitment and promotion processes, job advertising, interviewing, selecting and hiring staff.
- General Human Resources Management and Administration, for example employee career development, performance management, compensation and benefits management and benchmarking, administering payroll and benefit arrangements, obtaining management and employee satisfaction feedback, 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, managing absences (e.g. sickness, parental leave and other family related and flexible working policies), to operate and keep a record of disciplinary and grievance processes, general headcount reporting, disaster recovery and emergency response planning, equal opportunities monitoring, to obtain occupational health advice, to meet its obligations under health and safety law; to provide references on request for current or former employees and respond to and defend against legal claims.
- Performance of our Business Operations, for example carrying out day to day business activities, allowing us to work together and collaborate, providing services to our customers and ensuring business continuity.
- Security Management, for example to ensure the security of our premises, assets, information, employees and other personnel.
- Marketing, Advertising and Public Relations, for example displaying employees' and personnel's contact details and photographs on our website, or other professional social media websites and on other means of communication such as press releases.
- Legal and Regulatory Compliance, for example to ensure compliance with health & safety requirements and other legal or fiscal obligations, or in connection with litigation or an internal investigation or audit and to ensure compliance with our policies regarding anti-money laundering, bribery and corruption.
- Ensuring compliance with our Code of Conduct, for example to ensure that we are living up to our values

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

Where the Company processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out its obligations and exercise specific rights in relation to employment.

## **Email Monitoring**

We may monitor emails sent to and from our employees and other personnel. The information such emails contain (which may include personal data relating to third parties) may be used when investigating incidents. Although we endeavour not to review the contents of personal emails, there may be occasions in which this is necessary, for example, to investigate a breach of security or to investigate a disciplinary matter.

## **Who has access to data?**

Your information may be shared internally, including with members of the HR, administration and recruitment team (including payroll), 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 HR, accounts, payroll, the provision of benefits, the provision of occupational health services and disaster recovery and back up e-mail archiving.

HR-related personal data may be accessed by countries outside the EEA to process accounts and payroll. Data is accessed outside the EEA on the basis of a declaration of adequacy, binding corporate rules or other safeguards.

Whenever we allow access to your Employment Data outside of the EEA or the UK, we will take legally required steps to ensure that adequate safeguards are in place to protect your Employment Data and to make sure it is treated securely and in accordance with this Notice.

You may contact us for a copy of the safeguards which we have put in place to protect your Employment Data and privacy rights in these circumstances.

## **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 in the performance of their duties.

The internal policies and controls are contained in the Company Standard Operating Procedures, Information is stored securely on the encrypted data sever.

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 organisational measures to ensure the security of data.

### **For how long does the Company keep data?**

The Company will hold your personal data for the period specified in our Data Retention Policy.

### **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; and
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights please contact [dataprotection@mayfaircleaning.co.uk](mailto:dataprotection@mayfaircleaning.co.uk).

Any request to exercise one of these rights will be assessed by us on a case by case basis. There may be circumstances in which we are not legally required to comply with your request or because of relevant legal exemptions provided for in applicable data protection legislation. If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner.

### **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.

### **Automated decision-making**

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

### **Updates to this Notice**

We may change this Notice from time to time in order to reflect changes in the law, regulatory guidance or our data privacy practices in compliance with the law. When this happens and where required by law, we will provide you with a new or an updated notice detailing how the use of your Employment Data is changing and, if necessary, obtain your consent for the further processing.



**Andrew Prendergast, Chief Executive Officer**

**April 2022**

### **3 JOB APPLICANT PRIVACY NOTICE**

---

#### **Data controller: The Mayfair Cleaning Company Ltd**

As part of any recruitment process, the Company collects and processes personal data relating to job applicants. 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 a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the Company needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

The Company may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

The Company may also collect 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. The Company will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR and administration management systems and on other IT systems (including email).

#### **Why does the Company process personal data?**

The Company needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

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 a successful applicant's eligibility to work in the UK before employment starts.

The Company has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Company to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The Company may also need to process data from job applicants to respond to and defend against legal claims.

The Company may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. It may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. The Company processes such information to carry out its obligations and exercise specific rights in relation to employment.

For some roles, the Company is obliged to seek information about criminal convictions and offences. Where the Company seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The Company will not use your data for any purpose other than the recruitment exercise for which you have applied.

#### **Who has access to data?**

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of HR, administration and recruitment, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The Company will not share your data with third parties unless your application for employment is successful and it makes you an offer of employment. The Company will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

#### **How does the Company protect data?**

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

The Company's security procedures are contained in the Company Standard Operating Procedures.

#### **For how long does the Company keep data?**

If your application for employment is unsuccessful, the Company will hold your data on file for six months after the end of the relevant recruitment process.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment.

The periods for which your data will be held will be provided to you in a new privacy notice and our Data Retention Policy.

### **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; and
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights please contact [dataprotection@mayfaircleaning.co.uk](mailto:dataprotection@mayfaircleaning.co.uk)

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

### **What if you do not provide personal data?**

You are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if you do not provide the information, the Company may not be able to process your application properly or at all.

### **Automated decision-making**

Recruitment processes are not based solely on automated decision-making.



**Andrew Prendergast, Chief Executive Officer**

**April 2022**