Personnel Records, Data Protection & Data Transfer Policy

Overview

Octavian controls and processes personal information about its clients, staff, and potential staff.

Octavian is committed to ensuring that all personal information handled by us will be processed according to legally compliant standards of data protection and data security. Safeguarding this information is critical to our successful operation. We will treat all personal information we control and process with the same degree of security and confidentiality.

The purpose of this policy is to help us achieve our data protection and data security aims by:

- notifying our staff, consultants, contractors, clients and service enquirers of the types of personal information that we may hold about them, why we request the data and what we do with that information, including who we may need to share the data with;
- ensuring staff, contractors and clients understand our rules and the legal standards for handling personal information relating to staff and others: and
- clarifying the responsibilities and duties of staff and contractors in respect of data protection and data security;
- stating how long we will hold the data for;
- stating the name of our Data Protection Officer;
- ensuring that all contracts and service level agreements (SLA's) between us and external third parties, where personal data is processed, refer to the Act where appropriate.

This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

Who is Responsible for Data Protection and Data Security

Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants, and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Staff**).

The Operations Director has overall responsibility for ensuring that all personal information is handled in compliance with the law and works in conjunction with the appointed Data Protection Officer.

All Staff have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that

measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.

Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy applies to the processing of personal data in manual and electronic records kept by Octavian in connection with its human resources function as described below. It also covers Octavian's response to any data breach and other rights under the General Data Protection Regulation (GDPR).

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Octavian makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf Octavian, Octavian will ensure that the third party takes such measures to maintain the commitment to protecting data. In line with GDPR, Octavian understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of Data held

Personal data is kept in personnel files or within Octavian's HR systems. The following types of data may be held by Octavian, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades

- conduct and performance records such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to Octavian's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

All personal data obtained and held by Octavian will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant, and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

Data Protection Principles

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

Octavian has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for:
  a. the processing and controlling of data

b. the comprehensive reviewing and auditing of its data protection systems and procedures
c. overviewing the effectiveness and integrity of all the data that must be protected.

There are clear lines of responsibility and accountability for these different roles.

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by Octavian
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing, and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. Octavian understands that consent must be freely given, specific, informed, and unambiguous. Octavian will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting, and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally.

Access to Data

Relevant individuals have a right to be informed whether Octavian processes personal data relating to them and to access the data that Octavian holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from HR-UK@octaviangr.com.
- Octavian will not charge for the supply of data unless the request is manifestly unfounded, excessive, or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- Octavian will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform Octavian immediately if they believe that the data is inaccurate, either because of a subject access request or otherwise. Octavian will take immediate steps to rectify the information.

Data Disclosures

Octavian may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data Security

Octavian adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data transfer security policy in this handbook.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a director. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where necessary
- using an encrypted system — a folder should be created to store the files that need extra protection, and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow Octavian's rules on data security may be dealt with via the disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International Data Transfers

While carrying out our business, we may need to transfer your personal information to a country outside the European Economic Area including to any group company or to another person with whom we have a business relationship.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of Octavian becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, Octavian will do so without undue delay.

New employees must read and understand the policies on data protection as part of their induction.

Training

All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

Data transfer security policy

The law

The Company stores a large volume of information electronically. This policy governs the procedures to protect this information and sets out how data should be transferred around the Company, and outside the Company, in a secure and protected way.

The Company's Data Protection Officer is Kiran Ghuman Managing Director.

Data storage is regulated by the General Data Protection Regulations. Standards are set out in the Regulation and the current Data Protection Act and one of the key points for consideration in a data transfer situation is that personal data must not be transferred to a country/territory outside the European Economic Area (EEA) unless that country/territory ensures appropriate safeguards.

Sensitive data

Sensitive data, for the purpose of this policy, includes data which contains:

- personal details about an individual (including those which are classed as special categories of data including data relating to health and race etc)
- confidential data about the Company
- confidential data about goods, products, or services
- confidential data about Company customers and suppliers.

If employees have any doubt as to whether data is or is not 'sensitive data', the employees must refer the matter to their manager who shall liaise with a Director.

Data transfers

Employees must seek consent from a director to authorise the transfer of sensitive data.

Data (sensitive or not) should only be transferred where it is strictly necessary for the effective running of the Company. Accordingly, before any data transfers are requested, the necessity of the transfer should be considered in advance.

After authorisation has been granted, the data must be referred to the Octavian IT Support so that it can be encrypted, compressed and password protected before it is sent.

Data transfers which occur via physical media such as memory cards or CDs must only be dispatched via secure post. The use of first- or second-class Royal Mail is not permitted; only Special Delivery or Recorded Delivery should be used. For non-Royal Mail services, a secure courier service must be used with a signature obtained upon delivery.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the data is being sent so that they are aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The employee responsible for sending the data is responsible for confirming the data has arrived safely.

Access to data

Octavian operates role-based access control (RBAC).

Employees only have access to the information they require to enable them to carry out their duties.

At the end of employment HR request our IT host immediately remove the parties access right to any platform they had authorisation for.

Lost or missing data

If an employee discovers that data has been lost or is missing, the employee is required to inform a director immediately who will refer the matter to the Company's Data Protection Officer.

The Company's Breach Notification Policy will be followed. An investigation will be initiated immediately to establish the events leading to the data loss/theft and to determine whether a breach of personal data has occurred. If it has, a determination will be made as to whether the breach is notifiable under that policy.

The Director must consider referring a matter to the police if it is found that unauthorised individuals have accessed sensitive data. Data which is held in the correct encrypted, compressed and/or password protected formats, which has been accessed by an unauthorised individual, has been accessed unlawfully.

Employees who fail to comply with the requirements of this policy are likely to have their actions considered as gross misconduct, which may result in summary dismissal. Personal data breaches may result in exceptionally large fines for the Company.

Negligent data transfers

Employees must not be negligent when transferring sensitive data. Examples of negligence include failing to obtain authorisation from a director, failing to ensure the Company IT Department encrypted, compressed and password-protected data, or using non-secure post services which are not tracked or insured.

Data Retention & Destruction

- Data will not be kept longer than required – see IMS for defined periods
- Destruction must be approved by the Operations Director
- A review shall take place monthly
- Once data is deleted it will archive for 30 days before completely destroyed.