300 SPARTANS LIMITED

DATA PROTECTION POLICY

Issue: November 2022

Address: Unit 33, Broadfield Lane

Boston, PE21 8DR

Tel: 07724025516

Email: info@300spartans.uk

300 SPARTANS LIMITED

Data Protection Policy

Introduction

The organisation is committed to being transparent about how it collects and uses personal data of its workforce and to meeting its data protection obligations. This policy sets out the organisation's commitments to data protection, and individuals right and obligations in relation to personal data.

This policy applies to the personal data of; job applicants, employees and contractors, 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.

Definitions

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

"Sensitive 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 genetic 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 Subject" means person whose data it is.

Data Controller" means organisation who determines the legitimate purpose for data use.

"Data Processor" means people who process data on behalf of the controller.

Data protection principles

The organisation processes HR related personal data in accordance with the following data protection principles.

- be fairly and lawfully processed.
- be processed for limited purposes and not in any manner incompatible with those purposes.
- be adequate, relevant, and not excessive.
- be accurate.
- not be kept longer than is necessary.
- be processed in accordance with individual's rights.
- be secure.
- not be transferred to countries without adequate protection.

The organisation 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 organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation 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 organisation 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 contract is held in the individual's personnel file (in hard copy, electronic format, or both). The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

The organisation 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 request

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

- whether or not his/her data is processed and 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.

- 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 organisation has failed to comply with his/her data protection rights.
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation 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 organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data).
- stop processing or erase data if processing is unlawful.
- 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 organisation's legitimate grounds for processing data.

To ask the organisation to take any of these steps, the individual should send the request in writing to the Manager.

Data security

The organisation takes the security of HR-related personal data seriously. The organisation 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.

Where the organisation 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 confidential and are obligated to implement appropriate technical and organisational measures to ensure the security of data.

Impact assessments

Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation 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 organisation 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 organisation 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 has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual move to a new house, changes telephone number or changes his/her bank details.

Individuals may have access to the personal data of other individuals in the course of their employment contract. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff.

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 organisation) 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 organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- not to store personal data on local drives or on personal devices that are used for work purposes.
- to report data breaches of which they become aware to Manager immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation'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.

Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles (see above) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

Taking employment records off site

An employee must not take employment records or any personal information off site (whether in electronic or paper format) without prior authorisation from Director.

Any employee taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

Breaches of this policy may constitute gross misconduct and a dismissal outcome.

Employee Privacy Notice

Data controller: 300 Spartans Limited

Unit 33, Broadfield Lane

Industrial Estate

Boston

PE21 8DR

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender.
- 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 organisation.
- references received from previous employers.
- 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.
- information about your nationality and entitlement to work in the UK.
- information about your criminal record.
- details of your schedule (days of work and working hours) and attendance to 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.
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments.
- details of trade union membership.
- equal opportunities monitoring information, including information about your ethnic origin.
- next of kin details.
- driving license checks to enable you to drive company vehicles.

The organisation collects this information in a variety way. For example, data is collected through; application forms, CV, s obtained from your passport or other identity documents; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers at the start of your employment.

Data is stored in a range of different places, including in your personnel file, in the organisation's management systems and in other accounts systems.

Why does the organisation process personal data?

The organisation 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 assurance entitlements.

In some cases, the organisation 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, to enable employees to take periods of leave to which they are entitled.

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

- run recruitment and promotion processes.
- maintain accurate and up-to-date employments records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights.
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace.
- 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.
- 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 organisation 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.
- respond to and defend against legal claims.
- maintain and promote equality in the workplace.
- prove compliance and ethical trading in customer audits.

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 organisation to change incorrect or incomplete data.
- require the organisation 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 organisation is relying on its legitimate interests as the legal ground for processing.
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.
-

What if you not provide personal data?

You have some obligations under your employment contract to provide the organisation 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 organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlement. 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 organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently. This may result in employment being forced to end.