Threads Direct Ltd

DATA PROTECTION POLICY

Introduction

The Company is committed to complying with Data Protection legislation and the associated Data Protection principles. As a consequence, the Company seeks to operate in a transparent manner in relation to what data it collects, how it uses and processes the personal data and the reasons for such processing.

This policy then sets out the Company's commitment to data protection, as well as individual rights and obligations in respect to personal data.

This policy applies to the personal data of candidates for jobs, employees, any other individuals engaged in any other form of work by the Company, and ex-employees' personal data. In addition, this policy applies as far as it can to any personal data relating to clients, customers or suppliers. However, there are some sections of this policy which will only apply specifically to employment related personal data of the Company's staff and candidates for jobs. Where the exact provisions set out below cannot be applied to the personal data of others, such as clients, customers or suppliers due to any difference in the nature of the personal data or due to different legal requirements, then an alternative relevant and lawful standard of practice will be adopted as appropriate. At all times the Company will only process personal data where it has lawful grounds for doing so.

The person with responsibility for compliance with data protection legislation within the Company is Joseph Charles who is the Data Controller. He can be contacted at:

Email address: Joseph@threadsdirect.co.uk Tel No. 0116 2870741

Address: Threads Direct Ltd, Unit 1C, Mill Lane Industrial Estate, Glenfield, Leicestershire, LE3 8DX

If you have any queries about this policy, or require further information, or wish to make a subject access request or exercise your rights then such enquiries or contact should be sent to the above individual who is the identified Company contact for such matters.

Definitions

Criminal records data: means information about an individual's criminal convictions and offences.

Personal data: means any information relating to an individual who can be identified from the information in question.

Processing: means any use that is made of information such as collection, recording, organisation, storage, amendment, disclosure, retrieval, erasure or destruction of 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, biometric data, health, sex life or sexual orientation.

Data Protection Principles

The Company processes personal data in accordance with the following data protection principles. Personal data shall be:

- processed lawfully, fairly and in a transparent manner.
- collected only for specified, explicit and legitimate purposes.
- adequate, relevant and limited to what is necessary.
- accurate and, where necessary, up to date.
- kept only for the period necessary for which it is processed.
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

Lawful Grounds for Processing

The Company in considering the data it processes or might process will only process data which can be lawfully processed. In terms of HR related personal data the Company relies upon the following lawful grounds for processing work related personal data: processing is necessary for the performance of the employment contract or work contract or in order to enter into such a contract, or the processing is necessary for compliance with a legal obligation (such as complying with Equal Opportunities legislation), or it is necessary for the purposes of a legitimate business interest. These matters are set out in the privacy notice issued or available to all job applicants and or workers of the Company.

In terms of non HR data including any personal data relating to clients, customers and or suppliers the Company relies upon the lawful grounds set out in article 6 of the GDPR.

Data Management Procedure

The Company maintains a record of its HR processing activities in a register of the (employment related) data it processes.

The Company, by the use of privacy notices, advises job applicants and its workers of the personal HR data it processes, the purposes for the processing, to whom personal data is disclosed, the legal basis of the processing, the time period for storage, the individual's rights in respect to the data, and the source of the data.

The Company will update personal data promptly where an individual advises that information relating to them has changed or is inaccurate.

Personal data on job applicants and or workers of the Company collected or received by the Company will be held in the individual's personnel file and or on any computer system, electronic system, email system, cloud system, filing system and or HR/payroll system we operate. The duration for which such personal data is held is as set out in the privacy notices issued or available to job applicants and or workers of the Company.

The Company will only process data where it has lawful grounds.

All data including special category data will only be used or processed for legitimate purposes, and will be handled confidentially. Access to such data is strictly controlled and

only authorised individuals who have been trained in this policy, the data protection principles and the need for treating data with confidentiality have access to such data.

In addition, Data Security procedures are followed as set out below in the Data Security section.

The Company will conduct audits to ensure this Policy is being followed and the Data Protection Principles are being observed.

All data will be retained during the course of employment. Following employment, the data will be retained for a period of up to 6 years from the end of the tax year following any such employment/engagement, in part due to the need to retain records for certain legal reasons. However, basic information such as personal details, job title, reason for leaving may be retained beyond this period for the purposes of giving references if consent is given. In respect to applicants for jobs who are unsuccessful their details will be retained for up to 6 months.

In erasing personal data, a schedule is followed at least annually to check if given time periods erasure should take place. Where erasure is necessary the relevant electronic sources of data are identified and erased. In addition hard copy personal data is shredded and or disposed of securely. A record is retained of the erasure.

Other procedural steps relating to data management are set out in this policy.

Special Category Data

In the event the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights under employment legislation, this is performed in accordance with this policy, including the procedures it sets out, and in accordance with this section.

The Company only collects HR data for relevant work related matters and does not seek to specifically gather or receive special category information unless it is relevant. Such special category data will only be collected for specific legitimate workplace matters and will not be processed in any way incompatible with that purpose.

This essentially means that such information will only be collected, used, processed and or retained where it is necessary to do so for the purposes of carrying out the obligations and exercising specific rights of the Company or of the individual in question in connection with the field of employment. So, for example such processing may be required to comply with the Equality Act 2010, or other pieces of employment legislation or in respect of the law relating to statutory sick pay.

Individual Rights

Individuals have certain rights in respect to their personal data. These are set out below.

Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will inform them:

- whether or not their data is processed

- the purpose of the processing
- the categories of personal data concerned
- the recipients or categories of recipients to whom the personal data have been or will be disclosed
- the envisaged period the personal data will be stored or the criteria for determining that period
- the individual's right to request rectification, erasure, restriction of processing or to object to processing of personal data;
- the individual's right to complain to the Information Commissioner;
- the source of the data where it is not collected from the individual;
- the existence of any automated decision-making, and meaningful information about the logic involved in any such decision-making
- where personal data are transferred to a third country or an international organisation the appropriate safeguards that apply.

The Company shall also provide the individual with a copy of the personal data undergoing processing. If the individual requires further copies, the Company will charge a reasonable fee, which will be based on the administrative cost of providing the further copies. Unless the individual otherwise requests, the copy of personal data provided will be in a commonly used electronic form if the individual has made the request electronically.

If an individual wishes to make a subject access request, they should send the request to the Company contact identified above in the Introduction. In some circumstances proof of identification may be needed before the request can be processed. The Company will advise the individual if their identity needs to be verified and what verification and or documents are required.

The Company will respond to a request within one month from the date the request is received. That period can be extended by a further two months where necessary, taking into account the complexity and number of requests. In such circumstances the Company will write to the individual within one month of receipt of the request advising of the extension and reasons for it.

Where a request is manifestly unfounded or excessive, the Company may charge a reasonable fee, taking into account the administrative cost of responding to the request or refuse to act on the request. A subject access request can be manifestly unfounded or excessive where it is repetitive. In the event an individual makes a request that is manifestly unfounded or excessive, then the Company will advise the individual accordingly and whether or not it will respond to the request.

Other Rights

Individuals also have the following rights in relation to their personal data and can in certain circumstances may require the company to rectify inaccurate data, erase data or restrict processing; individuals also in certain circumstances have the right to object to processing, or to request the right to data portability.

The below gives examples of such circumstances. Individuals have the right to;

- the rectification of inaccurate data or to the restriction of its processing;
- the erasure of data or to restrict the processing of data that is no longer necessary for the purposes for which it was collected or processed;
- the erasure of data where consent is withdrawn and there is no other legal ground for the processing

- the erasure of data or restriction of processing, where the Company relies on legitimate interests as a reason for processing data, if the individual's interests override the Company's legitimate grounds for processing data;
- the erasure of data or restriction on processing if it has been unlawfully processed
- erase data for compliance with a legal obligation based on legislation; and
- the restriction of processing 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.
- the right to data portability where the processing is based on consent and the processing is carried out by automated means.

If an individual wishes to request any of the above actions of the Company they should send the request to the Company contact identified above in the Introduction.

Data Security

The Company takes the matter of security for personal data seriously. The Company has established policies, procedures and measures to protect personal data from loss, accidental destruction, improper disclosure or misuse, and to ensure against data breaches or unauthorised access to data. Only authorised individuals in the proper performance of their job roles can access such data.

The Company uses encryption and or passwords to protect computers, other devices and documents. Appropriate cyber security systems are operated by the Company to protect the Company's electronic systems and these security systems are regularly monitored and checked.

The Company also ensures that a clean desk policy operates in respect to departments dealing with any personal data. In addition, storage space such as cupboards are used for storing any hard copy personal data and such storage space is secured by lock and key and is only accessible to authorised personnel.

In addition, access to personal data is allowed only on a need to know basis. Staff authorised to access personal details are provided with training in Data Protection and are given clear instructions in the importance of confidentiality.

Where the Company makes use of third parties to process personal data on its behalf, then these third parties only do so on the grounds of written instruction and authorisation from the Company and under an agreement with the Company. In addition, they are under a duty of confidentiality and are required to adopt appropriate technical and organisational measures to protect and ensure data security.

Impact Assessments

In the event processing would be likely to result in a high risk to the rights and freedoms of an individual, the Company will conduct an impact assessment. The assessment will: describe the envisaged processing operations; the purpose of the processing; the necessity and proportionality of the processing operations; assess the risks to the rights and freedoms of individuals; and measures and safeguards to address such risks.

Data Breaches

In the case of a data breach that poses a risk to the rights and freedoms of individuals, the Company will report it to the Information Commissioner within 72 hours of having become aware of the breach.

All data breaches will be documented. This will include the facts relating to the data breach, its effects and remedial action.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will communicate to the data subject that there has been a breach. In addition the Company will provide them with appropriate information about the nature of the breach, the appropriate contact in the Company if they require more information, the likely consequences of the breach and the mitigation steps taken to address any adverse effects.

International Data Transfers

It may be that personal data will be transferred outside the European Economic Area (EEA) for example through the use of cloud storage or technology. In such circumstances relevant safeguards, including obligations of confidentiality will apply as required. The safeguards will include where required an adequacy decision by the EU Commission. In the absence of any such adequacy decision relevant safeguards such as standard data protection clauses adopted by the Commission, or by the ICO and approved by the Commission, or contractual clauses as authorised by the ICO and or other safe guards as set down by article 46 of the GDPR will apply. A copy of safeguards or where they can be obtained from can be provided via the Data Controller.

Individual Responsibilities

Individuals should assist the company keep their personal data accurate and up to date.

Individuals should advise the Company as soon as possible if any information they have provided to the Company changes, such as personal details, a change of address or a change in bank details.

Where individuals have access to personal data relating to others, then they must recognise and comply with their responsibilities under Data Protection legislation.

Any individual who has access to personal data must:

- only access personal data they have been given authority to access
- only access personal data for authorised purposes;
- not disclose personal data to others unless they are authorised individuals;
- ensure data is kept secure and retained where it cannot be accessed by unauthorised personnel;
- ensure personal data, or devices containing or that can be used to access personal data, are not removed from the Company's premises without appropriate security measures being used to secure the data and the device (ie encryption or password protection);
- only store personal data on authorised devices;
- comply with the Data Protection principles.

All employees should understand that a breach of this policy may be treated as a disciplinary offence and in cases of a severe breach may be treated as gross misconduct.

Training

The Company will provide training to all individuals so they understand this policy and their responsibilities in respect to data protection.

Additional training will be provided to employees whose roles are such they have access to personal data or have a responsibility for implementing this policy or dealing with subject access requests. They will be given particular instruction on the secure handling and confidentiality to be attached to special category data.