Introduction

Purpose

TRUMPF Laser UK Limited ("the Company") is committed to being transparent about how it collects and uses personal data, including the personal data of its workforce, suppliers, clients and customers, 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.

Under data protection laws the Company is the "data controller" of personal information held about its staff, suppliers, clients and customers.

This Policy applies to all our staff regardless of whether they are employees, temporary workers, consultants, or contract staff, and whether they are permanent or temporary staff.

In the course of your work you may come into contact with or use confidential information about employees, suppliers, clients and customers, for example, their names and addresses. The General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 ("DPA") contains principles affecting employees’ and other personal records. Information protected includes not only personal data held on computers but also certain manual records containing personal data, for example employee personnel files that form part of a structured filing system. The purpose of these rules is to ensure that you do not breach these regulations.

The Company has appointed a Data Protection Coordinator ("DPC"), Graham Parsons, HR Director. His role is to inform and advise the Company on its data protection obligations. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Graham Parsons.

You should be aware that, under the DPA, you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence for you to knowingly or recklessly obtain, disclose or procure personal information without the consent of the data controller.

Data protection principles

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

- processes personal data lawfully, fairly and in a transparent manner.
- collects personal data only for specified, explicit and legitimate purposes.
- processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- keeps personal data only for the period necessary for processing or for legal purposes
- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Our commitment to processing personal data

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

- Personal data gathered during your employment is held in your 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 notice for staff

Your right to access personal information – Subject Access Requests (SAR)

You have the right, on request, to receive a copy of the personal information that the Company holds about you, and to request that any inaccurate data be corrected or removed. You also have the right on request to:

- Be told by the Company whether and for what purpose personal data about you is bring processed
- Be given a description of the data and the recipients to whom it may be disclosed
- Have communicated in an intelligible form the personal data concerned, and any information available as to the source of the data

Upon request, the Company will provide you with a list of personal data held about you. It will state all the types of personal data the Company holds and processes about you and the reasons for which they are processed. If you wish to access a copy of any personal data being held about you, you must make a written request to our DPC, Graham Parsons, HR Director.

The Company will normally respond to a request within a period of one month from the date it is received. For complex or numerous requests, the Company 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 and the reasons for the delay.

If a subject access request (SAR) is manifestly unfounded or excessive, the Company is not obliged to comply with the request. Alternatively, the Company can agree to respond but will charge a reasonable fee, which will be based on the administrative cost of responding to the request. A SAR 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 request 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 the DPC, Graham Parsons, HR Director.

Data security

The Company takes the security of 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.

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.

Data Breaches

If the Company discovers that there has been a breach of 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 advise 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

The Company will neither transfer, nor permit a transfer, of personal data to countries outside the European Economic Area EEA without providing appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The Company will not transfer HR-related personal data to countries outside the EEA, with the exception of information that is stored on the internet, intranet and any other IT systems that are shared with our parent company TRUMPF e.g. Workday and “Who’s who”.

Individual responsibilities

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

Individuals may have access to the personal data of other individuals, suppliers, customers and/or clients in the course of their day to day role. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff, suppliers, 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;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- to keep personal data up-to-date;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure e.g. 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 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 complete relevant training as required; and
- to report data breaches of which they become aware to Graham Parsons, the DPC, immediately.

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.

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