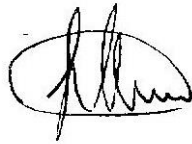


Time2Train Ltd

GDPR Policy

Signed:



Director: John Young

Date: 18/07/2023

Next review Date: 18/07/2024

CONTENTS

Introduction.....	2
Definitions	2
Scope	4
Who is responsible for this policy?	4
Our procedures	4
Privacy Notice.....	5
Sensitive personal data	5
Data security.....	5
Training.....	7
GDPR provisions	7
Privacy Notice - transparency of data protection	7
Justification for personal data.....	8
Consent.....	8
Criminal record checks	8
Data portability.....	8
Right to be forgotten.....	9
Privacy by design and default.....	9
International data transfers	9
Data audit and register.....	9
Reporting breaches	9
Monitoring.....	9
Consequences of failing to comply	9

INTRODUCTION

Time2Train (T2T) hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

DEFINITIONS

INSPIRE, PROVIDE AND SUPPORT ACHIEVEMENT

Business purposes: The purposes for which personal data may be used by us eg: Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

Personal data Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

- Personal data we gather may include:
- individuals' contact details
- educational background
- financial and pay details
- details of certificates and diplomas, education and skills
- marital status
- nationality
- job title
- CV.

Sensitive personal data: Any use of sensitive personal data should be strictly controlled in accordance with this policy. Personal data may include information about an individual's:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership (or non-membership)
- physical or mental health or condition
- criminal offences, or related proceedings.

SCOPE

This policy applies to all staff who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

WHO IS RESPONSIBLE FOR THIS POLICY?

Our Data Protection Officer, John Young, has overall responsibility for the day-to-day implementation of this policy.

OUR PROCEDURES

Fair and lawful processing

T2T will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we will not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by [company name]
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Operations Manager:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data will be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

PRIVACY NOTICE

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as our funders and the ESFA
- Provides that customers have a right of access to the personal data that we hold about them

SENSITIVE PERSONAL DATA

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO, John Young.

Your personal data

We will take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

DATA SECURITY

We must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks will be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Data will be regularly backed up in line with the company's backup procedures
- Data will never be saved directly to mobile devices such as laptops, tablets or smartphones
- All hardware containing sensitive data will be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

Time2Train does not trade internationally however, there are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. If we receive a subject access request, we will refer that request immediately to the DPO. We may ask you to help us comply with those requests. Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

We will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

We will not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Staff must contact the DPO for advice on direct marketing before starting any new direct marketing activity.

be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

JUSTIFICATION FOR PERSONAL DATA

We will process personal data in compliance with all six data protection principles.

1. Lawfulness, fairness and transparency
T2T will make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects.
2. Purpose limitation
T2T will only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.
3. Data minimisation
T2T will only process the personal data that they need to achieve its processing purposes. Doing so has two major benefits. First, in the event of a data breach, the unauthorised individual will only have access to a limited amount of data. Second, data minimisation makes it easier to keep data accurate and up to date.
4. Accuracy
The accuracy of personal data is integral to data protection. T2T will take every reasonable step to erase or rectify data that is inaccurate or incomplete. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.
5. Storage limitation
T2T will delete personal data when it's no longer necessary. This may vary between organisations and the reasons that data is collected.
6. Integrity and confidentiality
T2T will ensure that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

T2T will also document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

CONSENT

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

CRIMINAL RECORD CHECKS

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

DATA PORTABILITY

Upon request, a data subject has the right to receive a copy of their data in a structured format. These requests will be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This will be done for free.

RIGHT TO BE FORGOTTEN

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

PRIVACY BY DESIGN AND DEFAULT

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

INTERNATIONAL DATA TRANSFERS

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA. At present the company has no plans to transferr data outside of the EEA.

DATA AUDIT AND REGISTER

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

REPORTING BREACHES

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

MONITORING

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

CONSEQUENCES OF FAILING TO COMPLY

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

INSPIRE, PROVIDE AND SUPPORT ACHIEVEMENT

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO – John Young tel 0191 5438995 or email john.young@time2train.org.uk.