Data Ethics Policy – The Typing Works Limited

Introduction

The Typing Works Limited Data Ethics Policy has been prepared as an overall framework and it applies to the services provided by The Typing Works Limited ("the Company").

The Data Ethics Policy is about responsible and sustainable use of data and new technologies and complements e.g., the principles of transparency and data minimisation in the Company Data Protection Policy, the Company Data Retention Policy, the Company Information Security Policy as well as rules on integrity and confidentiality.

The policy also supplements related policies on handling of personal data, use of cookies etc.

The Typing Works Limited is a responsible employer and a trusted partner to our customers and business partners. We do our utmost to ensure that data is used in a safe and responsible manner.

We have taken a strategic approach to data ethics and have established an initial global policy regarding use of data and new technologies. The Company will continue its proactive work with data ethics based on the four principles set out below.

Data Ethics Principles

We operate by the following four principles with respect to data protection and data ethics in general:

Principle 1 – Lawfulness, fairness and transparency

Data and technology shall be used in a lawful, fair and transparent manner ensuring fair and non-discriminatory efforts to eliminate harmful biases.

Principle 2 – Data accuracy and quality

Data shall be accurate and kept up to date. Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Principle 3 – Integrity and confidentiality

Data and new technologies shall be processed and used in a manner that ensures appropriate security, privacy and ethics by design, including securing a high level of integrity and protection against unauthorised or unlawful use.

Principle 4 – Responsible use

Collection of data and use of new technologies shall take place in a responsible manner, ensuring that the data and technology in question does not deliver results that may be biased or discriminatory.

File Upload and Related Data Storage Information

Security Protocol

We fully recognise the importance of the security of information within our company amongst all our stakeholders, but especially in relation to our clients and customers. As such, we are fully engaged with operating, maintaining and continually improving a relevant Information Security Management System. We sign confidentiality undertakings as required.

Data

In transit: TLS 1.2 with strict transport security. HTTPS and SFTP.

At rest: data is protected with AES-256 bit encryption.

Firewall and Intrusion Detection

Our networks are protected by stateful packet inspection firewalls. All ports, other than those required for the provision of service are closed. We operate intrusion detection.

Monitoring

The service is monitored by over 100 monitoring daemons continuously probing for fault conditions at levels ranging from basic hardware health to emulated file transactions. Ports are monitored for suspicious activity such as password scams or Dos attack.

Security Patching

Governed by ISMS OP 29 Security and Patching Policy, critical security patches are installed when they become available.

Virus Scanning

All files uploaded are scanned using ClamAV to inspect uploaded files.

Penetration Testing

Annual penetration tests conducted by a CREST member company and a CESG CHECK scheme “Green Light” subscriber authorised to conduct testing on government systems under the terms of the CHECK scheme.

Vulnerability Scanning

Daily vulnerability scanning and PCI-DSS conformance scanning using McAfee Secure.

Transcription File Returns

All transcriptions are encrypted with a Word document password. Returns are via Egress encrypted email, which adds an extra layer of protection to the file. Further information on email returns is available here: https://www.tptranscription.co.uk/data-security-and-emails/

Use of Data and New Technologies

Data is an integrated part of our work and our service offering. When we use data, we only use data when relevant, with a proper legal basis to do so. Our Data Privacy Policy describes in details how, when and why we use certain datatypes, including the use of consent for marketing purposes, where relevant.

In our use of new technologies, we strive to ensure that such technologies do not deliver results that may be biased or expose humans to discrimination or stigmatisation.

Data Ethics Awareness

We strive to ensure that our employees are well-informed about data ethics and that they handle data and new technologies in accordance with our Data Ethics Principles. This includes mandatory training in both GDPR, Business ethics and Information Security for employees. We continuously support the understanding of the importance of data ethics across the organisation. We have an open and honest culture about errors and problems, so that we continuously improve our use of data and technology.

Data Governance

Data governance is the responsibility of the board of directors. The board of directors is responsible for escalation of data ethical dilemmas as well as evaluating the need for updating the policy.

Approved September 2024 by the Board of Directors. Renewal date – September 2025.