HTEC Solutions Ltd

(Fast Dox)

Data Protection Policy

01 November 2019

CONTENTS

1. Purpose

HTEC Solutions Limited (the **Company**) is committed to complying with applicable law and regulations in all its activities, including Data Protection Laws, with the intention of protecting the rights and freedoms and individuals with respect to the processing of their personal data.

This Policy sets out the Company's policy on data protection. It provides an overview of data protection requirements including the expected behaviours of the Company's employees and contractors in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data held within the business.

If you have any questions relating to this policy, please contact the Company's Data Protection Officer (DPO).

The EU General Data Protection Regulation (GDPR), which is incorporated into UK law via the Data Protection Act 2018 (DPA), establishes a framework of rights and duties designed to safeguard personal data. Personal data is any information (including opinions and intentions) which relates to an identified or identifiable living information (as defined in the GDPR and set out in this policy). Personal data is subject to certain legal safeguards and other regulations which impose restrictions on how organisations may process personal data. The Company is responsible for ensuring compliance with the data protection requirements outlined in this policy and associated documents.

The Information Commissioner's Office (ICO) is responsible for upholding information rights in the public interest and enforcing the requirements of UK Data Protection Laws.

The Company is a Data Controller in respect of its clients' and employees' data, as well as other miscellaneous personal data it may hold. The specific objective of this and associated policies is to ensure that all relevant persons understand the obligations of the Company to comply with Data Protection Laws in relation to data held by it and relating to clients, employees, and other third parties.

2. Scope and Applicability

This policy applies to all processing of personal data in whatever format it is held by the Company, regardless of where it is held, including in electronic form (e.g. including electronic mail and documents created with word processing software) and in manual files that are structured in a way that allows ready access to information about individuals.

This policy does not contain an exhaustive set of requirements but aims to provide an overview. All staff should remember that they should comply with the spirit of this policy and not just its actual content.

If any person does not understand how this policy applies to them, or what action they should take they should speak to the DPO.

This policy will apply where a Data Subject's personal data is processed:

- in the context of our business activities; and
- for the provision or offer of services to individuals (including those provided or offered free of charge) by our business.

This policy applies to all employees, contractors or third parties who may handle data on behalf of the Company.

3. Definitions

Data Protection Definitions	
Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable living person.
Identifiable living person	Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Data Controller	A controller determines the purposes and means of the processing of personal data.
Data Subject	The identified or identifiable living person to which the data refers.
Process, Processed, Processing	Any operation or set of operations performed on personal data or on sets of personal data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Protection	The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Protection Definitions	
Data Protection Authority	An independent Public Authority responsible for monitoring the application of the relevant data protection regulations – in the UK this is the ICO.
Data Processors	A person who processes personal data on behalf of a Data Controller.
Consent	Any freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Special Categories of Data	Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
Third Country	Any country or territory other than a Member state.
Profiling	Any form of automated processing of personal data where personal data is used to evaluate certain personal aspects relating to an individual. In particular to analyse or predict certain aspects concerning that individual's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.
Personal Data Breach	A breach of security leading to the accidental or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Encryption	The process of converting information or data into code so only authorised users may access it.
Pseudonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a key that allows the data to be re-identified.
Anonymisation	Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.
GDPR	The EU General Data Protection Regulation.

4. Data Protection Principles

4.1 The Principles

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means the Company must tell the Data Subject what processing will occur and by whom (transparency) (we usually do this by giving individuals appropriate privacy notices either before or at the point when we collect their personal data), handle people's personal data only in ways they would reasonably expect, i.e. the processing must match the description given to the Data Subject (fairness), and it must be for one of six lawful bases specified in the applicable data protection regulation (lawfulness) and not do anything unlawful with the data.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the Company must be clear from the outset exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means the Company must not collect or store any personal data beyond what is needed.

Principle 4: Accuracy

Personal data shall be accurate and kept up to date. This means the Company must have in place processes for identifying out-of-date, incorrect and redundant personal data (having regard to the purposes for which it is processed) and take reasonable steps to erase or rectify such data without delay.

Principle 5: Storage Limitation

Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. This means that the Company must have a clear data retention policy so that

the length of time it may lawfully keep personal data is reviewed and information that is not held lawfully or legitimately is securely deleted.

Principle 6: Integrity and Confidentiality (i.e. security)

Personal data shall be processed in a manner that ensures appropriate security of the personal data. The Company must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.2 Accountability

The Data Controller is responsible for and be able to demonstrate compliance with data protection legislation. This means the Company must be able to demonstrate that the six Data Protection Principles outlined above are met for all personal data for which it is responsible. This is an ongoing obligation.

5. Data Collection and Processing

5.1 Data Sources

Personal data will generally only be collected directly from the Data Subject. If personal data is collected from someone other than the Data Subject, the Data Subject MUST be informed of the collection unless one of the following apply:

- The Data Subject already has the information.
- The information must remain confidential due to a professional or statutory secrecy obligation.
- Proving the information proves impossible or would involve a disproportionate effort.
- A national law expressly provides for the obtaining or disclosing of the personal data.

Where a Data Subject is notified of data collection from a third party, this should be done within a reasonable period of collection and in any case no later than:

- One calendar month from the first collection or recording of the personal data.
- At the time of first communication if it is to be used for communication with the Data Subject.
- At the time of disclosure if the data is to be disclosed to another recipient.

The notification must contain the information required by data protection legislation (which is broadly equivalent to the information the Company provides via its Privacy Notice).

5.2 Data Subject Consent

The Company will only obtain personal data by lawful and fair means and, where appropriate, with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, the Company is committed to seeking such consent. Consent must be freely given and a data subject must be able to withdraw their consent as easily as it has been given.

5.3 Data Subject Notification/External Privacy Notices

The Company will, when required by applicable law, by contractual obligation, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their personal data. We will do this through our Privacy Notice. The most up to date version of our Privacy Notice can be found on our website.

When a Data Subject is asked to give consent to the processing of personal data and when any personal data is collected from the Data Subject, all appropriate disclosures will be made to the Data Subject in a manner that draws attention to these disclosures. However, it is not necessary to provide information where one of the following applies:

- The Data Subject already has the information.
- A legal exemption applies to the requirements for disclosure and/or consent (e.g. where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort).

5.4 Data Use and Processing

The Company processes personal data for the following broad purposes:

- Via the Fast Dox product offered by the Company, which provides a structured and secure document collection for clients. A primary function of Fast Dox is document collection which may include personal data collected by the Company's clients, which the Company will then hold on behalf of the Client in accordance with the agreed service;
- for human resource purposes (i.e. staff records, recruitment records) and to keep records of service providers; and
- to comply with employment law and other legal obligations.

The use of the Data Subject's information should always be considered from their perspective and whether the use will be within their reasonable expectations and whether they are likely to object.

The Company will process personal data in accordance with all applicable laws and any contractual obligations to which it is subject. The Company will only process personal data where one of the following conditions is met:

- The Data Subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party (e.g. the terms of business with the Company) or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or those of a third party.

5.5 Special Categories of Data

The Company will only process special categories of data (also known as sensitive data) (e.g. racial/ethnic origin, political opinion, trade union membership) where the Data Subject expressly consents to such processing or where one of the following conditions apply (this list is not-exhaustive):

- the processing relates to personal data which has already been made public by the Data Subject;
- the processing is necessary for the establishment, exercise or defence of legal claims;
- the processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- where processing is necessary for reasons of substantial public interest based upon national law and where processing is necessary for reasons of public interest in the area of public health.

Staff who are unsure what lawful bases apply to personal data they intend to process should seek advice from the DPO.

5.6 Data Quality

The Company's employees will ensure so far as reasonably possible that the personal data they collect and process is complete and accurate in the first instance, and is updated when necessary to reflect the current situation of the Data Subject by:

- having appropriate processes in place to check the accuracy of data collected and to record the source of that data;
- having a process in place to identify when we need to keep the data updated properly to fulfil our purpose and to correct personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification;
- having a process in place to comply with the Data Subject's right to rectification and to carefully consider any challenges to the accuracy of the personal data is clear.

6. Digital Marketing

The Company does not undertake marketing as at the date of this Policy. In the future, it may consider sending promotional or direct marketing material to clients through digital channels such as mobile phones or email where their details have been obtained through the provision of our services to them and where the materials relate to a similar service which the Company believes may be of benefit to them.

We will only use personal information to send marketing material if we have the data subject's permission or a legitimate interest as described in our Privacy Policy. If a data subject does not want to receive emails from us, they will be able to click on the 'unsubscribe' link in the marketing emails we send. If they don't want to receive texts from us they will be able to contacting us at any time. We will retain a list of data subjects who have informed us that they do not wish to receive marketing from us.

7. Data Retention

Personal data will not be retained by the Company for longer than necessary to perform the processing for which it was originally collected. This is subject to any legal or regulatory obligations which may require the Company to retain personal data for specified periods of time. Further details are set out in the Company's Data Retention Policy which outlines how long the various classes of records and other data should be kept.

8. Data Security

The Company will adopt physical, technical and organisational measures to ensure the security of personal data, including the prevention of loss or damage, unauthorised alteration, access of processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The Company's data security and protection measures are set out in our Information Security Management Policy.

9. Data Subject Rights and Data Subject Access Requests

9.1 Data Subject Rights

The DPA grants rights to Data Subjects in respect of their personal data. These rights include:

- the right to be informed;
- the right of access to information (commonly known as a Subject Access Request Procedure);
- the right to object to processing;
- the right to objection to automated decision-making and profiling;
- the right to restriction of processing;
- the right to data portability;
- the right to data rectification;
- the right to data erasure.

If a Data Subject makes a request relating to any of the rights listed above, we will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee may be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

9.2 Data Subject Access Requests

Data Subjects are entitled to obtain, based upon a request made in writing, and upon successful verification of their identity, certain information about their own personal data as set out in the DPA. All such requests will be dealt with in accordance with the Company's Subject Access Request Policy.

9.3 Law Enforcement Requests & Disclosures

In certain circumstances the Company may be required to share personal data to others without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of a tax or duty;
- by the Order of a court or by any rule of law.

In the above cases, the Controller (i.e. the Company) is exempted from having to comply with the provisions of the DPA, but only to the extent that complying with these provisions would be likely to *prejudice* the purposes of processing. If this is not so, you must comply with the DPA as normal. If any employee receives a request from a Court or any regulatory or law enforcement authority for information relating to a client this must be immediately brought to the attention of the DPO.

9.4 Data Transfers

The Company may occasionally need to transfer data to third parties in order to meet business requirements. If data is sent outside the European Economic Area (EEA) the Company must put in place certain safeguards as required by the DPA.

We will only transfer data to third party recipients outside the EEA where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects, where the appropriate security measures are in place and in line with the requirements of data protection legislation. This will be determined on a case by case basis by the DPO.

9.5 Transfers to Third Parties

As at the date of this Policy, the Company does not transfer data to third parties.

In the event that the Company changes its Policy, it will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and securely by the recipient. Where third party processing takes place, we will first identity if, under applicable law, the third party is considered a Data Controller, or a Data Processor of the personal data being transferred.

Where the third party is deemed to be a Data Controller we will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the personal data transferred in accordance with the DPA.

Where the third party is deemed to be a Data Processor we will enter into an appropriate processing agreement with the Data Processor, again in accordance with the DPA.

In accordance with data protection legislation, the agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with our instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches within required timeframes to enable us to comply with our obligations under the data protection legislation.

10. Complaint Handling

Data Subjects who make a complaint about the processing of their personal data should direct their complaint for the attention of the DPO.

An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.

The DPO will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved satisfactorily through consultation between the Data Subject and the DPO, then the Data Subject may refer the complaint to the ICO.

Any person who receives a complaint should forward it to the DPO immediately.

11. Data Breaches and Data Breach Reporting

Personal data shall not be disclosed to any unauthorised party in any form, either accidentally or otherwise. It is the responsibility of all users of personal data throughout the Company to ensure that personal data is kept securely. Any breach of or failure to comply with this Policy or any guidance issued by us from time to time, particularly any deliberate release of personal data to an unauthorised third party, may result in disciplinary or other appropriate action.

Any individual who suspects that any unauthorised access to or disclosure of personal data or other data security breaches have occurred must immediately notify the DPO. See also our Data Breach Management Procedure.

12. Data Protection by Design and Default

The GDPR requires the Company to put in place appropriate technical and organisational measures to implement the data protection principles and to safeguard individual rights. This is referred to as data protection by design and by default, i.e. the Company has to integrate data protection into its business practices and consider data protection issues at the outset in everything that we do. This is intended to ensure that the Company complies with the fundamental principles and requirements of data protection legislation and forms part of the focus on the Company's accountability under the legislation.

To ensure that the Company identifies all data protection requirements when designing new systems or processes and/or when reviewing or expanding existing systems or processes, a Data Protection Impact Assessment (DPIA) must be conducted as early as possible.

13. Training and Development

All relevant persons will have their responsibilities under this policy outlined to them as part of their induction training. All staff will be required to complete an annual refresher of this training. The Company will provide further training and guidance if there are any updates made to this policy and/or the associated policies and procedures, when considered necessary.

14. Record Keeping

The Company is required to maintain a record of processing activities containing the information required by data protection legislation which shall include the following:

- the name and contact details of the Controller, any joint controller and any DPO appointed;
- the purposes of the processing;
- a description of the categories of data subjects and the categories of personal data;
- the categories of recipients to whom personal data has been or will be disclosed;
- details of any transfers to Third Countries or international organisations of personal data and appropriate safeguards;
- envisaged time limits for erasure of different categories of personal data;
- a general description of the technical and organisational security measures implemented, if possible.

15. Monitoring Compliance

An annual Data Protection Compliance Audit will be carried out by the DPO to assess:

- Compliance with this policy in relation to the protection of personal data, including;
  - the assignment of responsibilities,
  - raising awareness,
  - training of staff.
- The effectiveness of data protection related operational practices, including;
  - a Data Subject's rights;
  - transfers of personal data;
  - personal data breach management;
  - personal data complaints handling.
- The level of understanding of data protection policies and privacy notices.
- Whether data protection policies and privacy notices require updating or amending.
- The accuracy of personal data being stored.
- The conformity of data processor activities.
- The adequacy of procedures for redressing poor compliance and personal data breaches.

Key business stakeholders are responsible for developing a plan for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the DPO.

16. Review

This policy will be reviewed at least annually by the Policy Owner. We will provide information and/or training on any changes we make where this is deemed necessary.

17. Policy Owner

This policy is owned by the DPO.

18. Document Control

Document Information

	INFORMATION
Document Id	V4
Document Owner	Data protection officer
Issue Date	01/11/2019
Last Saved Date	15/07/2018
File Name	Fast Dox Data Protection Policy Nov19 V4