COMPUTAMATRIX LIMITED T/A MATRICA
Data Protection Policy
September 2018

Table of Contents

1. Scope, Purpose and Application to Employees

Computamatrix Limited t/a Matrica ("the company") need to collect certain personal information about people with whom we work in order to carry out our business and provide our services. Personal data may be collected and stored about individuals and current, past and prospective employees and contractors.

Company Policy is to respect the rights of the natural person (data subject) with regard to data held, to hold the data securely, to only use the data for permitted purposes, and to comply with relevant data protection regulations.

This Data Protection Policy sets out the legal and regulatory data protection framework relevant to all persons handling data on behalf of the company, together with actions required to be taken to ensure compliance with the Company Policy.

Compliance with the full policy is mandatory, for convenience particular actions required to be followed by staff and others handling data on behalf of the company are set out in bold italic.

The company takes data privacy seriously and is committed to complying with applicable laws and regulations related ton Personal Data protection in countries where the company operates including the General Data Protection Regulation ("GDPR") which forms the basis of data protection law in the European Union and the provisions of which are incorporated in the Data Protection Act 2018.

This Policy sets forth basic principles that must be applied to the collection, handling, storage and disposal of personal data and are applicable to the company:-

This Policy applies to all full and part-time employees and contractor staff. This policy also applies to all external suppliers and contractors who are collecting, handling, storing or disposing of personal data on behalf of the company.

Employees should be aware that serious consequences can result following a breach of data protection laws including under the GDPR, very substantial fines of up to **20 million Euros or 4% of global annual turnover** – whichever is higher. The company could also face enforcement notices and potential lawsuits by data subjects whose rights may have been breached. The company is highly likely to suffer reputational damage that results from such breaches.

2. Reference Documents

- GDPR
- Data Protection Act 2018
- Data Breach Notification and Procedures
- Data Subject Rights Policy and Procedures
- Data Retention Policy
- IT Security Policy
- Communications, Email and Internet Policy
- Recruitment Policy

3. Definitions

The following definitions of terms used in this document are drawn from Article 4 of the GDPR:

Personal Data – Any information relating to an identified or identifiable natural person ("Data Subject") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Data – Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller – the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor – A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

Processing – An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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 of the data.

Anonymisation – Irreversibly de-identifying personal data such that the person cannot be identified by using reasonable time, cost, and technology either by the controller or by other person. The personal data processing principles do not apply to anonymised data as it is no longer personal data.

4. Data Protection Principles and Standards

The company is both a data controller and processor for the purposes of the GDPR.

The company endorses the six principles of data protection as set out in the GDPR. These principles must be followed at all times when processing or using personal information.

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with these purposes.
3. Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.
4. Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data processed which is inaccurate, is erased or rectified without delay.

5. Data must be kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data is processed.
6. Data must be 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.

In consideration of these principles and through appropriate management and strict application of criteria and controls, the company will meet the following data protection standards:

- Observe fully the conditions regarding the fair collection and use of information including the giving of consent.
- Meet its legal obligations to specify the purposes for which information is used – a privacy notice giving information on how a data subjects data is collected, retention periods and the legal basis for processing the data must be made available either directly or via another party.
- Keep current a written record of the processing of all personal data, which includes business area, categories of data, our legal basis for processing the data, technical and other security measures in place.
- Collect and process appropriate information only to the extent that it is needed to fulfil the company's operational needs or to comply with any legal requirements – **employees must not use data collected for one purpose for any other purpose.**
- Ensure the quality of information used – information retained must be kept accurate and up to date before taking decisions which may affect an individual.
- Ensure that the information is held for no longer than is necessary – the company **Data Retention Policy** will specify applicable retention periods.
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR – the company will ensure that there are mechanisms in place to enable data subjects to exercise their legal rights under GDPR including the right of access, rectification and data portability and adhere to the standards set out in the **Data Subject Rights and Procedures** document.
- Take appropriate technical and organisational security measures to safeguard personal information – data privacy considerations must be identified, managed and documented when designing processes and/or systems where personal data may be processed and an assessment is required to be made of any impact on data subjects.
- Ensure that third party suppliers have controls in place to ensure that personal data is managed in accordance with company standards and regulatory requirements. Contracts entered into with third party suppliers must contain clauses regarding GDPR regulations.
- Ensure that personal information is not transferred out of the EU without suitable safeguards in place for technical and other security measures. Data anonymisation is encouraged wherever possible; otherwise the transfer must be legally permissible under GDPR using an approved mechanism such as the EU model clauses for data transfer. **Employees must consult the Data Protection Lead if intending to transfer any personal data out of the EU.**
- **Ensure that any form of dissatisfaction from an individual relating to data privacy is reported promptly to the Data Protection Lead.**
- Identify, investigate and remedy all data breaches promptly and notify regulators and individuals of any data breaches where required, in accordance with the **Breach Notification Policy and Procedures** document.

Management are responsible for ensuring that processes are in compliance with the principles set out above and in particular should ensure the record of the processing

of personal data in their business area: Categories of data, our legal basis for processing the data, technical and other security measures in place is accurate.

All employees are required to follow procedures on personal data including any anonymisation requirements and complying with all implemented technical and security information to safeguard personal data (e.g. password protection or encryption requirements). All employees are responsible for raising with their direct managers or the Data Protection Lead any concerns with regard to compliance with Corporate Policy.

5. Data Subject Rights

The company will comply with data subject rights set out in the GDPR relating to:-

- Data Subject Access Requests
- Challenge to automated decision making
- Right to be informed
- Data Portability
- Rectification of data
- Right to erasure (Right to be forgotten)

Requests for access to personal data must be given a response within 30 days therefore any employee who receives a contact from a third party requesting access to personal data or otherwise seeking to exercise their rights under Data Protection law must contact the DPL who will coordinate the company response to the request in accordance with the "Data Subject Rights Policy and Procedures".

Employees must also contact the DPL immediately if they receive any expression of dissatisfaction from a third party with respect to the treatment of their personal data.

6. Disposal of Personal Data

Under Data Protection law the company may keep personal data only as long as is necessary for the purposes for which it was collected.

- ***Employees must refer to the Document Retention Policy before the destruction of any personal data to ensure that there is no conflict with the Policy.***
- ***Employees should seek advice from the Data Protection Lead should any doubt arise as to whether documents containing personal data should be destroyed.***
- ***It is determined that the destruction of documents containing the personal data is not in conflict with legitimate business needs and the Document Retention guidelines then the following should apply:***
  - ***Disposal of Paper material – including manual records, handwritten notes and printed material. This material must be shredded.***
  - ***If any employee is working with paper documents containing personal data outside of our business premises, documents must be returned to the office to be destroyed. Such document must not be placed in domestic waste.***
  - ***Disposal of Electronic Data held on CD's and Disks or other electronic media employees should refer to Admin for assistance with disposal.***

7. Data Protection Contacts

The Data Protection contacts for the company are:

Admin: Sandra Allbury
The Data Protection Lead (DPL) for the company is Lorraine Hale
Directors: Prudence Mauthoor, Natasha Knight

The DPL may be contacted for any guidance required in this policy or Data Protection in general. The DPL must be contacted in the following circumstances:-

- ***Any suspected or known data breaches which involve or may involve personal data must be reported immediately to the Data Protection Lead or Directors. This will include inadvertent destruction, loss or theft of personal data.***
- ***The loss or theft of any company owned devices or your own personal device where you have been permitted to use the device for business purposes must be reported to the DPL and the Directors.***
- ***Any expression of dissatisfaction from an individual relating to data privacy.***
- ***Any request for access to personal data or the exercise of other data subject rights made by a third party who is not an employee.***
- ***Any proposed transfer of personal data to a person or company outside of the EU.***

Appendix A

GDPR controls

Requirements	GDPR Article	Description	Control
Principles	5	Processing of personal data (lawfully, fairly, transparently, legitimate purpose, accurate and kept up to date and appropriate security)	○ Fair processing notices ○ Record of Processing documents (description of processing, data subjects, legal bases for processing, categories of documents, recipients)
	6	Lawfulness of processing (inc. consent and necessity)	
	7-8	Conditions of consent (inc. children)	
	9-10	Processing of special category data (i.e. sensitive data) and criminal convictions	
Data Subject Rights	12	Transparent information, communication and modalities for the exercise of the rights of the data subject	○ Fair processing notices ○ Data Subject Rights Policy and Procedure document
	13	Information to be provided where personal data are collected from the data subject	
	14	Information to be provided where personal data have not been obtained from the data subject.	
	15	Right of access by the data subject	
	16	Right to rectification	
	17	Right to erasure	
	18	Right to restriction of processing	
	19	Notification obligation regarding rectification of personal data or restriction of processing	
	20	Right to data portability	
	21	Right to object	
	22	Automated decision making and profiling	
	23	Restrictions	
Responsibilities of the Data Controller and Processor	24	Responsibilities of the controller (inc. storage limitations i.e. retention and deletion)	○ Data Protection Policy ○ Document Retention Policy ○ Data Protection Impact
	25	Data protection by design and by default	
	26	Joint controller responsibilities	

	28	Responsibilities of the processor	Assessments ○ Data Breach Notification and Response Procedures ○ IT Security Policy
	30	Records of processing	
	32	Security measures for processing	
	33-34	Data breach notification	
	35-36	Data Protection impact assessment	
Transfer of personal data	45-46	Data transfers out of the EU	○ Fair Processing notices ○ Record of Processing ○ Data Transfer Agreements containing EU model clauses