GDPR Data Protection Policy

Document Reference: CPR Computers Limited
Revision Date: 10th April 2018
Revision Number: 001
Classification: Restricted

Table of Contents

1. Introduction

CPR Computers Limited ("CPR") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of CPR Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a CPR Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. CPR, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy.

Non-compliance may expose CPR to complaints, regulatory action, fines and/or reputational damage.

CPR's leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all CPR Employees and Third Parties to share in this commitment.

Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy has been approved by CPR's Chief Executive Officer, Tim A B White.

2. Scope

This policy applies to all CPR Entities where a Data Subject's Personal Data is processed:

• In the context of the business activities of the CPR Entity.

• For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by a CPR Entity.

• To actively monitor the behaviour of individuals.

• Monitoring the behavior of individuals includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking to profile an individual with a view to:

• Taking a decision about them.

• Analysing or predicting their personal preferences , behaviours and attitudes.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a worldwide baseline standard for the Processing and protection of Personal Data by all CPR Entities. Where national law imposes a requirement which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

If there are conflicting requirements in this policy and national law, please consult with the Officer for Data Protection for guidance.

The protection of Personal Data belonging to CPR Employees is not within the scope of this policy.

3. Definitions

Third Country
Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Profiling
Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location or movement.

Binding Corporate Rules
The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

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, to prevent unauthorised access.

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.

4. Policy

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, CPR has established an Officer for Data Protection. The Officer operates with independence and has been granted all necessary authority. The Officer for Data Protection reports to the CPR Board of Directors. The Officer for Data Protections role includes:

• Informing and advising CPR and its Employees who carry out Processing pursuant to Data Protection regulations, national law or Union based Data Protection provisions;

• Ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions;

• Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);

• Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);

• Determining the need for notifications to one or more DPAs as a result of CPR's current or intended Personal Data processing activities;

• Making and keeping current notifications to one or more DPAs as a result of CPR's current or intended Personal Data processing activities;

• The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;

• The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

For example, it would clearly be within a Contact's expectations that their details will be used by CPR to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that CPR would then provide their details to Third Parties for marketing purposes.

Each CPR Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, CPR will not Process Personal Data unless at least one of the following requirements are 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 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 performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

• Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Officer for Data Protection before any such Processing may commence.

In any circumstance where consent has not been gained for the specific Processing in question, CPR will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

• Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.

• The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Data Controller.

• The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.

• The possible consequences of the intended further Processing for the Data Subject.

• The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

4.4.2
Special Categories of Data
CPR will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

• The Processing relates to Personal Data which has already been made available by the Data Subject.

• The Processing is necessary for the establishment, exercise or defense of legal claims.

• The Processing is specifically authorised or required by law.

• 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.

• Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

4. Policy

4.7
Data Subject Requests

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual.

In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Detailed guidance for dealing with requests from Data Subjects can be found in the CPR 'Data Subject Request Handling Procedures' document.

4.8
Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared 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.

If a CPR Entity Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If any CPR Entity receives a request from a court or any regulatory or law enforcement authority for information relating to a CPR Contact, you

must immediately notify the Officer for Data Protection who will provide comprehensive guidance and assistance.

4.9
Data Protection Training

All CPR Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each CPR Entity will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance set forth will consist of, at a minimum, the following elements:

• The Data Protection Principles set forth in Section 4.2 above.

• Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.

• The need for, and proper use of, the forms and procedures adopted to implement this policy.

• The correct use of passwords, security tokens and other access mechanisms.

• The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.

• Securely storing manual files, print outs and electronic storage media.

• The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.

• Proper disposal of Personal Data by using secure shredding facilities or authorised data wiping software.

• Any special risks associated with particular departmental activities or duties.

4.10
Data Transfers

CPR Entities may transfer Personal Data to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects.

Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism

CPR Entities may only transfer Personal Data where one of the transfer scenarios list below applies:

• The Data Subject has given Consent to the proposed transfer.
• The transfer is necessary for the performance of a contract with the Data Subject.

[7] For a list of countries recognised as having an adequate level of legal protection see Appendix B.

[8] For a list of Third Country transfer mechanisms recognised as providing adequate protection see Appendix B.

The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.

• The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.

• The transfer is legally required on important public interest grounds.

• The transfer is necessary for the establishment, exercise or defence of legal claims.

• The transfer is necessary in order to protect the vital interests of the Data Subject.

4.10.1

Transfers between CPR Entities

In order for CPR to carry out its operations effectively across it's various CPR Entities, there may be occasions when it is necessary to transfer Personal Data from one CPR Entity to another, or to allow access to the Personal Data from an overseas location.

Should this occur, the CPR Entity sending the Personal Data remains responsible for ensuring protection for that Personal Data.

CPR handles the transfer of Personal Data between CPR Entities, where the location of the recipient Entity is a Third Country, using the Binding Corporate Rules transfer mechanism. Binding Corporate Rules provide legally binding, enforceable rights on Data Subjects with regard to the Processing of their Personal Data and must be enforced by each approved CPR Entity, including their Employees.

When transferring Personal Data to another CPR Entity located in a Third Country, you must:

• Ensure that the recipient CPR Entity is included on the approved list of CPR Entities subject to the CPR 'Binding Corporate Rules Agreement'. The approved list is held and maintained by the Officer for Data Protection.

• Only transfer the minimum amount of Personal Data necessary for the particular purpose of the transfer (for example, to fulfil a transaction or carry out a particular service).

• Ensure adequate security measures are used to protect the Personal Data during the transfer (including password-protection and Encryption, where necessary).

4.10.2

Transfers to Third Parties

Each CPR Entity will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, each CPR Entity will first identify 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, the CPR Entity will enter into, in cooperation with the Officer for Data Protection, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, the CPR Entity will enter into, in cooperation with the Officer for Data Protection, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with CPR 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.

CPR has a 'Standard Data Processing Agreement' document that should be used as a baseline template.

When a CPR Entity is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include, in cooperation with the Officer for Data Protection, adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

CPR has a 'Standard Provisions for Outsourcing Agreement' document that should be used for guidance.

The Officer for Data Protection shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place.

Any major deficiencies identified will be reported to and monitored by the CPR Executive Management team.

4.11
Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Officer for Data Protection. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Officer for Data Protection will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Officer for Data Protection, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

4.12
Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Officer for Data Protection providing a description of what occurred.

Notification of the incident can me made via e-mail odp@cprcomputerrecycling.co.uk or by calling 01293 731222

The Officer for Data Protection will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Officer for Data Protection will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the CPR Group General Counsel will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

.

5. Policy Maintenance

All inquiries about this policy, including requests for exceptions or changes should be directed to the Officer for Data Protection via e-mail odp@cprcomputerrecycling.co.uk

5.1 Publication

This policy shall be available to all CPR Employees through the CPR Handbook or via alternative means as deemed appropriate by the Officer for Data Protection.

5.2 Effective Date

This policy is effective as of 10 April 2018.

5.3 Revisions

The Officer for Data Protection is responsible for the maintenance and accuracy of this policy. Notice of significant revisions shall be provided to CPR Employees. Changes to this policy will come into force when published on CPR website https://www.cprcomputerrecycling.co.uk

Listed below are documents that relate to and are referenced by this policy.

- Internet Privacy Notice template
- Internet Cookie Notice template
- Client Data wiping Policy

6. Related Documents Appendix A - Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification With Consent /Without Consent

• The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.

• The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.

• The contact details of the Data Protection Officer, where applicable.

• The purpose(s) and legal basis for Processing the Personal Data.

• The categories of Personal Data concerned.

• The recipients or categories of recipients of the Personal Data.

• Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.

• Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.

• The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.

• Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.

• The existence of Data Subject rights allowing them to request from the Data Controller- information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.

• Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.

• The right to lodge a complaint with a Data Protection Authority.

• The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.

• Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.

Appendix B - Adequacy for Personal Data Transfers

The following are a list of countries recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.

• EU Countries
(Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK)
• Iceland
• Liechtenstein
• Norway
• Andorra
• Argentina
• Canada (commercial organisations)
• Faeroe Islands
• Guernsey
• Israel
• Isle of Man
• Jersey
• New Zealand
• Switzerland
• Uruguay
• United States (Privacy Shield certified organisations)

All other Countries are deemed not to have an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of their Personal Data.