Curmi & Partners Ltd

DATA PROTECTION POLICY (DPP)

Last Updated: November 2021

Document history

Version	Date	Author/Editor	Details of Amendment	Date of approval by BoD	Date Distributed to Staff
1.0	10/11/2021	F&F / Kasia Bronzewska	New	-	-
1.0			Approval	04/02/2022	04/02/2022

I. Introduction and Purpose

Curmi & Partners Limited ('C&P) is committed to complying with all aspects of the data protection legislation including its handling of personal information relating clients and employees, amongst others.

This Data Protection Policy (hereinafter referred to as the 'Policy') aims to ensure that any personal data relating to data subjects which processed by C&P is protected in accordance with applicable data protection legislation, including but not limited to, Regulation [EU] 2016/679, or as it is otherwise known, the General Data Protection Regulation ('GDPR').

This Policy applies to all employees, staff, engaged interested third parties (hereinafter referred to as 'Authorised Persons' as defined below) of C&P. Consultants and any other third parties working with or for C&P, and who have or may have access to personal data will be expected to have read, understood and to comply with the provisions of this Policy, or any versions thereof as contained within separate contracts and agreements regulating the relationship between them and C&P. All employees will be provided with a declaration form (Appendix A) confirming they have read and understood this Policy and obligations stemming from it

If you are unsure of whether this Policy applies to you or have any questions on the contents therein, please contact C&P's Data Protection Officer ('DPO') on dpo@curmiandpartners.com

II. Definitions

i. **Authorised Person/s** shall mean any persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process Personal Data;

ii. **Consent** shall mean any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data in question;

iii. **Data Controller** shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data and therefore exercises control on the same Personal Data;

iv. **Data Processor** shall mean the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

v. **Data Subject** shall mean any living individual in relation to whom Personal Data is the subject of the processing activity;

vi. **Personal Data** shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;

vii. **Personal Data Breach** shall mean 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;

viii. **'Processing', 'Process', 'Processed' and any variation thereof** shall mean any 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;

ix. **Profiling** shall mean any form of automated processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or

predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour;

x. **Recipient** shall mean a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a Third Party or not;

xi. **Special Categories of Personal Data** shall mean Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of 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;

xii. **Supervisory Authority** shall mean an independent public authority which is established by a European Union Member State, which for the state of Malta shall mean the Information and Data Protection Commissioner ('IDPC');

xiii. **Third Country** shall mean a country other than the Member States of the European Union and any other countries (such as EEA countries) that have adopted a national law implementing Regulation [EU] 2016/679;

xiv. **Third Party** shall mean a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and Authorised persons;

III. Relevant data protection legislation

The GDPR is a European-wide law which came into effect on 25th May 2018 and which applies to any processing carried out by an organisation within the EU and outside the EU, where these offer goods and services to individuals within the EU. The Data Protection Act, Chapter 586 of the Laws of Malta, (hereinafter referred to as the 'Act') is the legislation that implements and further specifies provisions set out by the GDPR.

IV. Relationship between the Data Controller and Data Processor

Data Controllers have a higher degree of responsibility and more obligations than Data Processors, however it must be noted that the Data Processors must provide sufficient guarantees to ensure that the processing meets the requirements set out by the GDPR and

ensures the protection of the rights of the Data Subject. They remain fully responsible for their actions and the security of the Personal Data where a Data Controller engages a Data Processor, it shall ensure that the relationship between the parties is regulated by a contract, that is a Data Processing Agreement (hereinafter referred to as a 'DPA'), or by virtue of any other legal act under EU law or local law, that is binding on the Data Processor with regard to the Data Controller, and the Personal Data the Data Processor processes on the Data Controller's behalf.

C&P shall ensure that, regardless of whether it constitutes the Data Controller or the Data Processor of a specific processing operation, the relationship with any other Data Controllers/Data Processors is regulated by a relevant DPA or similar document.

V. The Data Protection Principles

In order to stay compliant at all times, C&P shall ensure that the following principles are adhered to;

1. Personal data shall be **processed lawfully, fairly and in a transparent manner** in relation to individuals**.**
2. Personal data shall be **collected for specified, explicit and legitimate purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purpose or purposes for which they are processed.
4. Personal data shall be **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Personal data shall **be kept in a form which permits identification of Data Subjects for no longer than is necessary** for the purposes for which the Personal Data are processed.
6. Personal data shall 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 and organisational measures.

In addition to the above, it must be noted that the Data Controller shall be responsible for, and be able to demonstrate compliance with, the aforementioned principles. Specifically, C&P shall

maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs (Data Processing Impact Assessments), comply with requirements for prior notifications, or approval from supervisory authorities. In order to fulfil its obligations arising under the 'Storage Limitation' Principle (Principle No. 5), C&P has set out a Records Retention Policy, including a Records Retention Schedule, which dictates the relevant periods of retention for the different categories of data it processes and also the modus operandi to be followed at the end of the lifecycle of the data.

VI. Lawful basis for processing

C&P shall ensure that any processing of Personal Data shall have a lawful valid basis, which is most appropriate depending on the purpose of the processing operation and the relationship with the Data Subject. Especially where it is acting as a Data Controller, C&P shall determine the lawful basis before processing is initiated. At least one of the following six lawful grounds must apply whenever C&P processes personal data:

LG1: The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes;
LG2: The 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;
LG3: The processing is necessary for compliance with a legal obligation to which the Data Controller is subject;
LG4: The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
LG5: The 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 controller;
LG6: The 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 which require protection of Personal Data, in particular where the Data Subject is a child.

Due to its sensitive nature, where C&P processes Special Categories of Personal Data, it shall identify a lawful basis for general processing and one additional condition for processing this type of data, as listed below:

SP1: The Data Subject has given explicit consent to the processing of those Personal Data for one or more specified purposes, except where Union or Member State law provide that the prohibition of processing of Special Categories of Personal Data may not be lifted by the Data Subject;

SP2: The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;

SP3: 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;

SP4: The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;

SP5: The processing relates to Personal Data which are manifestly made public by the Data Subject;

SP6: The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

SP7: The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

SP8: The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

SP9: The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical

devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy;

SP10: The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

VII. Data Subject Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

i. The right to be informed
ii. The right of access
iii. The right to rectification
iv. The right to erasure
v. The right to restrict processing
vi. The right to data portability
vii. The right to object
viii. Rights in relation to automated decision making and profiling.

The DPO will be responsible for handling any such requests that are received by C&P, and this in accordance with the Data Subject Rights Policy, and ensuring that information is released in accordance with the Act and the Data Subject Rights Policy.

VIII. Transfers to Third Parties

The sharing of Personal Data with Third Parties shall be construed as the disclosure of Personal Data by transmission, dissemination or otherwise making it available, and shall include instances where C&P gives Personal Data to a Third Party, by whatever means; as well as when a Third Party is given access to Personal Data on or via its IT systems. Sharing of Personal Data with Third Parties shall not include the Sharing of Personal Data with employees, or with processors.

Prior to undertaking sharing with Third Parties, C&P shall consider the same in light of its overall compliance with applicable data protection obligations, and therefore if the situation so requires, that is, where the situation may be of high risk to the Data Subjects, amongst other factors, C&P shall carry out a Data Privacy Impact Assessment (DPIA).

If the situation does not require the undertaking of a DPIA, or the result of the DPIA is that the Sharing will not result in an adverse effect on the rights and freedoms of data subjects, C&P shall enter into a relevant agreement to regulate the sharing of Personal Data with Third Parties.

Where the transfer of Personal Data is being made between Data Controller and Data Processor, C&P shall ensure that the relationship is regulated through a Data Processing Agreement ('DPA'), which shall include the following details vis-à-vis the processing activity:

- Subject-matter and duration of the processing activity;
- Nature and purpose of the processing activity;
- Type of Personal Data Involved;
- Categories of Personal Data Involved;
- Obligations and Rights of the Data Controller;
- Documented instructions from the Data Controller vis-à-vis processing activity;
- Documented instructions vis-à-vis transfers of personal data;
- Documented instructions vis-à-vis engagement of Sub-Processors;
- Warranties that Data Processor shall ensure that its Authorised Persons are committed to confidentiality;
- Warranties that Data Processor shall assist the Data Controller through implementation of technical and organisational measures for purposes of security; handling of personal data breaches and handing of Data Subject rights;
- The obligation of the Data Processor to delete or return all the personal data, at the choice of the Data Controller, to the Data Controller after the end of the provision of services relating to processing;
- The obligation of the Data Processor to make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down within the DPA and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller;
- The obligation of the Data Processor to inform the Data Controller immediately if, in its opinion, an instruction of the Data Controller infringes applicable data protection law.

Where the transfer of Personal Data is being made between a Data Processor and a Sub-Processor, C&P shall ensure that the same data protection obligations as set out in the DPA between the Data Controller and the Data Processor are being applied.

Where the transfer of Personal Data is being made between two or more Data Controllers that are determining the purposes and means of the processing, C&P shall ensure that the relationship is regulated through a Joint Data Processing Agreement ('JDPA'), which shall include the following details vis-à-vis the processing activity:

- Subject-matter and duration of the processing activity;
- Nature, purpose and legal basis of the processing activity;
- Type of Personal Data Involved;
- Categories of Personal Data Involved;
- Obligations and Rights of each respective Data Controller, including which Data Controller shall be responsible for handling any exercise of Data Subject rights and who shall be responsible to provide information to Data Subjects in accordance with Articles 13 and 14 of the GDPR;
- Terms on engagement of Data Processors;
- Respective notification obligations of each Data Controller, particularly vis-à-vis notification of personal data breaches.

Where the transfer of Personal Data is being made between two or more Data Controllers between them for purposes separately determined and pursued, they shall be deemed to be Separate Data Controllers in their own right. Although the regulation of this relationship is not specifically catered for under applicable data protection law, C&P shall strive to ensure that the relationship is regulated through the implementation of a Data Sharing Agreement ('DSA'), which shall set out the following details vis-à-vis the sharing of Personal Data:

- The means through which the Personal Data is being shared;
- The technical measures being applied to safeguard the security of the Personal Data being shared.

IX. Transfers to Third Countries

Personal Data shall not be transferred to a Third Country unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of Data Subjects in relation to the processing of Personal Data. The transfer of Personal Data to Third Countries is prohibited unless one or more of the specified safeguards or exceptions, as listed below, apply. In this regard, an assessment of the adequacy by C&P, taking into account the following factors must be undertaken:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long; and

- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations.

C&P may, if applicable, adopt approved Binding Corporate Rules for the transfer of data outside the EU to other companies which form part of the same group of undertakings. This requires submission to the relevant Supervisory Authority for approval of the rules that C&P is seeking to rely upon.

C&P may also adopt approved model contract clauses for the transfer of data outside of the EU as approved and issued by the European Commission. If applicable, C&P may also transfer data outside of the EU on the basis of approved codes of conducts or approved certification schemes.

In the absence of an adequacy decision taken by the EU Commission, or any of the aforementioned data transfer mechanisms, a transfer of Personal Data to a Third Country, or an international organisation, shall take place only on one of the following conditions:

- the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the Data Subject and C&P, or the implementation of pre-contractual measures taken at the Data Subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between C&P and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- 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 or of other persons, where the Data Subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Where none of the derogations outlined above are applicable, a transfer to a Third Country may take place only if the transfer is:

i. not repetitive;
ii. concerns only a limited number of Data Subjects
iii. is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interests or rights and freedoms of the Data Subject, and
iv. the Data Controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data;

In this case, the Data Controller is obliged to inform the Supervisory Authority of the transfer, as well as inform the data subject of the transfer and on the compelling legitimate interests pursued. Reliance on the derogations set out in Article 49 of the GDPR can only be undertaken where certain conditions are met and in specific situations – this reliance cannot become the 'rule' in practice.

Once the transfer mechanism has been identified, C&P must also assess whether there exist any issues within the Third Country which impinge on the efficiency of the data transfer mechanism in question, and whether any supplementary measures should be adopted.

X. Data Breach

In the event that that a Personal Data Breach is suffered, Authorised Persons shall ensure that the DPO is immediately informed, and this in order to satisfy C&P's obligation of notifying the Supervisory Authority of the same breach, and this without undue delay and where feasible, not later than seventy-two (72) hours after having become aware of the breach. Where the breach is likely to result in a high risk to the rights and freedoms of the natural persons, the DPO of C&P shall communicate the Personal Data Breach to the Data Subject without undue delay.

A Personal Data Breach Protocol is set up and maintained by the DPO and this to satisfy C&P's obligation of documenting any personal data breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

XI. Data Protection Officer

C&P has appointed a Data Protection Officer/DPO to ensure its continued compliance with the GDPR and its internal policies and notices and has notified the Supervisory Authority of the relevant engagement in accordance with local obligations.

The DPO reports directly to the highest level of management and is given the required independence to perform their tasks. When doing so, the DPO shall have due regard to the risk associated with processing operations, and takes in account the nature, scope and context and purposes of processing.

In order to ensure that the DPO is easily accessible as a point of contact for all Authorised Persons, Data Subjects, Third Parties and Supervisory Authority, C&P has set up a specific email address dpo@curmiandpartners.com and published these relevant contact details to interested parties accordingly.

C&P shall involve the DPO, in a timely manner, in all issues relating to the protection of Personal Data. C&P shall support the DPO in performing their tasks by providing resources necessary to carry out those tasks and access to Personal Data and processing operations. The DPO will act as a contact point for the Supervisory Authority and cooperate with the latter, including in cases where prior consultations are required.

XII. Security of Processing

C&P shall ensure that it has implemented appropriate technical and organizational measures to protect the security of the Personal Data it processes. It shall further ensure that all departments establish appropriate protocols of security for storing Personal Data, which shall only be accessed where strictly necessary and only by those with the authority to do so.

C&P shall ensure that any transfers of Personal Data made to Third Parties, are made subject to appropriate security measures, and this especially in relation to the transfers considered in Section IX of this Policy.

XIII. Procedure

In order to assist in the implementation of these principles, the following measures, amongst others, must be applied:

- Data protection queries should be directed to the DPO;

- Where relevant, Authorised Persons must undergo training in relation to data protection issues;

C&P will conduct regular audits of personal data, which is being stored, and the uses to which such information is being put, with the aim of monitoring compliance with the data protection principles described above and will consider exercising sanctions in the event of breach.

XIV. Roles and responsibilities

The Board is responsible for this policy and approval of any significant changes to it. The DPO, together with the Compliance Officer is responsible for ensuring that this Policy is regularly reviewed and complied with.

Appendix A

DECLARATION OF POLICY ACKNOWLEDGEMENT

I, _____, the undersigned, declare that I have received a copy of the Data Protection Policy.

I have read the Policy, understand its meaning, and agree to conduct myself in accordance with the Policy. I also understand that this acknowledgement will be kept in my personnel file or such other file as may be appropriate.

Date signed _____,

Declarant Signature
_____

Declarant Name _____

Position in the Company
_____

Please complete, date, and sign this form.
Return the original copy to the Compliance Officer as soon as possible.