Data Protection Policy of

Cassarcamilleri Ltd.

(the "**Company**")

25th May 2018

Contents

Purpose

The Company 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 document sets forth the policies and procedures in relation to the collection, use, retention, transfer, disclosure, destruction and other Processing of Personal Data by the Company, its employees and related Third Parties.

The Company is fully committed to ensuring continued and effective implementation of these policies and expects all employees and Third Parties to share in this commitment. Any breach of this policies will be taken seriously and may result in disciplinary action or business sanction.

Scope

These policies apply to all cases where a Data Subject's Personal Data is processed:

- In the context of the business activities of the Company;
- For the provision or offer of goods or services to individuals; and
- To actively monitor the behaviour of individuals.

These policies apply to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it's held in manual files that are structured in a way that allows ready access to Personal Data.

These policies have been designed to establish a baseline standard for the Processing and protection of Personal Data by the Company. Where national law imposes a requirement, which is stricter than that imposed by these policies, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this procedure, the relevant national law must be adhered to.

Abbreviations & Definitions

Column	Description
the GDPR	the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (the "EU"). It also addresses the export of Personal Data outside the EU.
Anonymization	Data amended in such a way that no individuals can be identified from the data by any means or by any person
Consent	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 relating to him or her.
Data Backup	Data copied to a second location, solely for the purpose of safe keeping of that data
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Data Controller	A natural or legal person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Encryption	The process of encrypting data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored
Data Encryption Key	An alphanumeric series of characters that enables data to be encrypted and decrypted
Data Processors	A natural or legal person which processes Personal Data on behalf of a Data Controller
Data Protection	The process of safeguarding Personal Data from unauthorized or unlawful disclosure, access, alteration, processing, transfer, or destruction.
Data Protection Authority or Regulator or DPC	The Data Protection Commissioner or any other relevant National Authority tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the EU.
Data Protection Officer (or "DPO")	An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR
Data Subject	The identified or Identifiable Natural Person to which the data refers
DPR	Data Processor Register holding agreements made with a Third Party
DSAR	Data Subject Access Request
Employee	An individual who works part time or full time for a the Company under a contract of employment and has recognized rights and duties. Includes temporary employees and independent contractors

Encryption	The process of converting information or data into code, to prevent unauthorized access
General Data Protection Regulation (the "GDPR")	the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of Personal Data outside the EU.
IAR	Information Asset Register
Identifiable Natural Person	Anyone who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data or one or more factors specific to the physical physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Personal Data	Any information (including opinions and intentions) which relates to a Data Subject
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed
Privacy Impact Assessment	A tool used to identify and reduce the privacy risks of entities by analysing the Personal Data that are processed and the policies in place to protect the data
Processing (or Data Processing)	Any operation performed on Personal Data, whether or not by automated means, including collection, use, recording, etc.
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. To analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location, or movement
Regulation	a binding legislative act that must be applied in its entirety across the EU
Special Categories of Data (or Sensitive 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
Subject Access Right	Also known as the Right to Access, it entitles the Data Subject to have access to and information about the Personal Data that a controller has concerning them
Third Countries	Any country not recognized as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data
Third Party	An external organization with which the Company conducts business and is also authorized to, under the direct authority of the Company, to process the Personal Data of Data Subjects.

Responsibilities

Data Protection Officer

- Keeping management updated about Data Protection responsibilities, risks, and issues
- Reviewing Data Protection procedures
- Arranging Data Protection training and advice for the people covered by this procedure
- Handling Data Protection questions from staff and anyone else covered by this procedure
- Dealing with requests from individuals to see the data the company holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with Third Parties that may handle the Company's Personal Data.

IT Personnel

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any Third Party services, the Company is considering using to store or process data. For instance, cloud computing services.

Marketing/Public Relations Personnel

- Approving any Data Protection statements attached to communications such as emails and letters
- Addressing any Data Protection queries

Human Resources Personnel

- Ensure that all data related to employees is stored and processed in line with this procedure and related legislation.

Data Protection Principles

The Company has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of Personal Data.

- **Lawfulness, Fairness and Transparency**
  Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that the Company must inform the Data Subject of what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection Regulation (lawfulness).

- **Purpose Limitation**
  Personal Data shall be collected for specified, explicit and legitimate purposes and not be subjected to further Processing in a manner that is incompatible with those purposes. This means one must specify 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.

- **Data Minimization**
  Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means that the Company must not store any Personal Data beyond what is strictly required.

- **Accuracy**
  Personal Data shall be accurate and, kept up to date.

- **Storage Limitation**
  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 is undergoing Processing.

- **Integrity and Confidentiality**
  Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing, and against accidental loss, destruction, or damage. Appropriate technical and organizational measures should be in place to ensure the integrity and confidentiality of Personal Data is maintained always.

- **Accountability**
  The DPO shall be responsible for, and able to demonstrate compliance.

Procedures

Data Collection

Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies
- The collection must be carried out under emergency circumstances to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

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 has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the Processing of the Personal Data

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

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

Data Subject Consent

The Company will obtain Personal Data only 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. When Consent is requested it should:

- Ensure the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensure the Consent is freely given (i.e. the Consent is not a pre-condition which is unnecessary for the performance of that contract)
- Document the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consent given.
- Provide a simple method for the Data Subject to withdraw their Consent at any time.

Data Subject Notification

The Company will, when required by applicable law, 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.

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, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent

The disclosures may be given orally, electronically or in writing. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

Data Use

Data Processing

The Company uses the Personal Data of its contacts for the following broad purposes:

- The general running and business administration
- To provide services to customers
- The ongoing administration and management of customer services
- The ongoing administration and management of processes related to employees

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

The Company will process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Personal Data will not be processed unless 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 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 Company is subject
- Processing is necessary 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 Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a Third Party (except where the interests or fundamental rights and freedoms of the Data Subject override such interests, particularly where the Data Subject is a child)

There are some circumstances in which Personal Data may be further processed or purposes that go beyond the original purpose for which the Personal Data was collected. When deciding as to the

compatibility of the new reason for Processing, guidance and approval must be obtained from the DPO before any such Processing may commence.

Special Categories of Data

The Company 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 related 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 specifically authorized 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 or data concerning health.

In any situation where, Special Categories of Data are to be processed, prior approval must be obtained from the DPO and the basis for the Processing clearly recorded with the Personal Data in question.

Children's Data

Children under the age of 16 are unable to Consent to the Processing of Personal Data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Data Quality

The Company will adopt all necessary measures to ensure that the Personal Data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject. The following guidance will be followed:

- Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated will be corrected even if the Data Subject does not request rectification.
- Personal Data will be kept only for the period necessary to satisfy the permitted uses or applicable statutory retention periods.
- Personal Data which is in violation of any of the Data Protection principles or Personal Data that is no longer required will be removed.
- Rather than deletion, restriction of Personal Data will be applied, as far as:
    - A law prohibits erasure
    - Erasure would impair legitimate interests of the Data Subject

- The Data Subject disputes that their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

Data Retention

To ensure fair Processing, Personal Data will not be retained by the Company for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

Retention periods should be defined based on legal and contractual requirements. All Personal Data should be deleted or destroyed as soon as possible where is has been confirmed that there is no longer a need to retain it.

The Company will adopt physical, technical and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing and other risks to which it may be exposed by virtue of human action or the physical or natural environment. The minimum set of security measures to be adopted include to:

- Prevent unauthorised persons from gaining access to data Processing systems in which Personal Data is processed
- Prevent persons entitled to use a data Processing system from accessing Personal Data beyond their needs and authorisations
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data Processing system
- Ensure that in case where Processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Company.
- Ensure that Personal Data is protected against undesired destruction or loss
- Ensure that Personal Data collected for different purposes can and is processed separately
- Ensure that Personal Data is not kept longer than necessary.

Data Subject Requests

The DPO will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access
- Objection to Processing
- Restriction of Processing
- Data Portability
- Data Rectification
- Data Erasure

Data Subjects are entitled to obtain, based upon a request made in writing to the DPO and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the Processing of their Personal Data
- The source(s) of the Personal Data, if it was not obtained from the Data Subject

- The categories of Personal Data stored for the Data Subject
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period
- The right of the Data Subject to:
    - object to Processing of their Personal Data
    - request rectification or erasure of their Personal Data
    - request restriction of Processing of their Personal Data

All requests received for access to or rectification of Personal Data by an employee of the Company must be re-directed to the DPO, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the Company to correct or supplement erroneous, misleading, outdated or incomplete Personal Data.

If the Company cannot respond fully to the request within 30 days, the DPO shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject
- The name and contact information of the individual who the Data Subject should contact for follow up.

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

Data Protection Training

All of the Company's 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, regular data protection training and procedural guidance for staff will be provided.

The training and procedural guidance will consist of:

- The Data Protection principles
- 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
- The correct use of passwords 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
- Any special risks associated with particular departmental activities or duties.

Data Transfers

To Third Parties

The Company 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 Third Countries, they must be made in compliance with an approved transfer mechanism

One of the below transfer scenarios need to occur for transfer of Personal Data to take place:

- The Data Subject has given Consent to the proposed transfer
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer is legally required on the grounds 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

Internal Transfer

In order for the Company to carry out its operations effectively, there may be occasions when it is necessary to transfer Personal Data to a related Company. Should this occur the Company remains responsible for ensuring protection for that Personal Data. In such situations it will be ensured that:

- Only the minimum amount of Personal Data necessary for the particular purpose of the transfer will be transferred.
- Adequate security measures are in place to protect the Personal Data during the transfer.

Data Breach

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data might have occurred, must immediately notify the DPO and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Data Breach has occurred. If a Data Breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination or other significant social or economic damage), the DPO must ensure that the Data Protection Authority is informed of the Data Breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the DPO must ensure that all affected Data Subjects are informed of the Data Breach directly and without undue delay.

Data Breach notifications shall include the following information:

- The categories and approximate number of Data Subjects concerned;
- The categories and approximate number of Personal Data records concerned;
- The name and contact details of the Company's DPO;
- The likely consequences of that Data Breach;
- Details of the measures taken or proposed to be taken by the Company to address the Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

Complaints Handling

Data Subjects with a complaint regarding their Personal Data, should put forward the matter in writing to the Company. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the case. The Data Subject will be informed with the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation, the Data Subject may seek redress through mediation, litigation or via complaint to the Data Protection Authority within the applicable jurisdiction.

Record-keeping

The Company shall retain records of all policies, procedures and decisions in relation to the Processing of Personal Data.