

Data Protection Policy

2210 Patisserie Limited

Policy Summary

This policy sets out the obligations of 2210 Patisserie Limited regarding data protection and the right of employees, customers, suppliers and business contacts. This includes obligations in dealing with personal data, in order to ensure that the

Companies comply with the requirements of the relevant Irish Legislation, namely the General Data Protection Regulation (GDPR) which replaced the Irish Data Protection Act (1988) and the Irish Data Protection (Amendment) Act (2003) as and from 25th May 2018.

The GDPR defines personal data as 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 a name, 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.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

Purpose

This policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company's employees, agents, contractors or other parties working on behalf of the Company.

This policy covers both personal and sensitive personal data held in relation to data subjects by the Company and applies equally to personal data held in manual and automated form.

All personal and sensitive personal data will be equally referred to as personal data in this policy, unless specifically stated otherwise.

The Data Protection Principles

This policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. Article 5 in the GDPR states that all personal data must be:

- a) *Processed lawfully, fairly and in a transparent manner* in relation to the data subject;
- b) *Collected for specified, explicit and legitimate purposes* and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes subject to appropriate safeguards, and provided there is no risk of breaching the privacy of the data subject.
- c) *Adequate, relevant and limited* to what is necessary in relation to the processes for which it is processed;

- d) *Accurate and where necessary, kept up to date*; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed is erased or rectified without delay;
- e) *Kept in form which permits identification of data subjects for no longer than is necessary* for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
- f) *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;
- g) Article 5(2) states that *the Controller is responsible for and must be able to demonstrate compliance with the Data Protection Principles*.

Lawful, Fair and Transparent Data Processing

- 4.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject. The Regulation states that the processing of personal data shall be lawful if at least one of the following apply:
- The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - Processing is necessary for the performance of a contract to which the data subject is a 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 Controller is subject;
 - 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;
 - Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject is a child.

The Company will ensure that at least one of the conditions outlined above will be satisfied whenever any processing activities take place.

In order to obtain personal data fairly and in a transparent manner, The Company will make the data subject aware of the following at the time that data is collected directly;

- Identity of the controller and the Data Protection Officer (or equivalent)
- Purpose and legal basis for processing.
- Data subject's rights to withdraw consent, request access, rectification or restriction of processing
- Data subject's rights to complain to the Data Protection Commissioner's Office
- Recipients of the personal data.

Storage periods or criteria used to determine the length of storage.

Legal basis for intended international transfer of data to a third country or organisation, includes the fact that either the receiving country has an adequacy decision from the Commissioner or other appropriate safeguards are in place and how to obtain a copy.

In situations where the data is not being collected directly from the data subject, the Company will provide the source along with the other information listed above to the data subject within a reasonable period after obtaining the data but not more than one month. Information will not be provided to the data subject if it will require disproportionate effort or would render it impossible or seriously impair the purpose of the data processing.

The Company will place a Fair Processing Notice in a highly visible position if it intends to record activity on CCTV or video.

The Data Subject's data will not be disclosed to a third party other than to a party contracted to the Company and operating on its behalf.

Processed for Specified, Explicit and Legitimate Purposes

The Company follows this purpose limitation principle and only collects and processes personal data for specific purposes. The purpose for which we process personal data will be informed to data subjects at the time their personal data is collected or after not more than one month if obtained from a third party.

The Company will not further process personal data in a manner that is incompatible with those purposes unless:

The consent of the data subject has been obtained, or

If the further processing is for archiving purposes in the public interest or scientific and historical research or statistical purposes and the appropriate safeguards are in place and there is no risk of breaching the privacy of the data subject.

Adequate, Relevant and Limited Data Processing

The Company follows this data minimisation principle and only collects and processes personal data for and to the extent necessary for the specific purpose(s) informed to the data subjects.

Timely Processing

The Company does not keep personal data for any longer than is necessary in light of the purposes for which the data was originally collected and processed.

The Company will verify whether statutory data retention periods exist in relation to the type of processing e.g. personal data may need to be kept in order to comply with tax, health and safety, or employment legislation etc. If the law is silent, internal data retention periods will be set to meet the storage limitation principle.

Retention periods will be set considering the purpose or purpose(s) for which the data is collected and used, and once storage periods expire, data will be securely deleted/destroyed in the absence of a sound

new lawful basis to retain it. However, where necessary, personal data may be stored for longer periods by the Company insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, historical research or statistical purposes ensuring appropriate safeguards are in place i.e. irreversibly anonymised.

Secure Processing

The Company will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The state of technological development, the cost of implementing the measures, the nature of the data concerned and the degree of harm that might result from unauthorised or unlawful processing are all taken into account when the Company are determining the security measures that are put in place.

Accountability

Under the GDPR, Organisations are obliged to demonstrate that their processing activities are compliant with the Data Protection Principles. The principle of accountability seeks to guarantee the enforcement of the Principles.

The Company will demonstrate compliance in the following ways:

By keeping an internal record of all personal data collected, held or processed as per Article 30- "Records of Processing Activities". Upon request, these records will be disclosed to the Data Protection Commissioner's Office.

When the Company is acting as a Data Controller this record will contain the following:

- Contact details of the Controller/Representative/Data Protection Officer
- List of personal data being processed
- Categories of data subjects
- Processing activities
- Categories of recipients with whom the data will be shared
- Retention periods
- Deletion methods
- International transfers and measures in place to ensure they are lawful
- Detailed descriptions of the security measures implemented in respect of the processed data

Organisational Measures

The Company will ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

All employees, contractors, or other parties working on behalf of the Company handling personal data:

- Will be appropriately trained to do so;
- Process the data in accordance with the principles of the Regulation and this Policy

All employees, contractors, or other parties working on behalf of the Company handling personal data:

- Will be made aware of their obligations under this policy and will be given an opportunity to read this policy. A document stating that this policy has been read and understood should be signed.

Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed;

Review

This policy will be reviewed from time to time to take into account changes in the law and the experience of the policy.