

1. Introduction

This Policy sets out the obligations of Don O'Malley & Partners Ltd, a company registered in the Republic of Ireland under number 379649, whose registered office is at 92 O'Connell Street, Limerick, Ireland, V94RKT1 ("the Company"), regarding data protection and the rights of all our business contacts in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR"). The GDPR defines "personal data" as any information relating to an identified or identifiable natural person.

2. Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- 2.1 The data subject has given consent;
- 2.2 The processing is necessary for the performance of a contract;
- 2.3 The processing is necessary for compliance with a legal obligation;
- 2.4 The processing is necessary to protect the vital interests of the data subject;
- 2.5 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 data controller; or
- 2.6 The processing is necessary for the purposes of the legitimate interests.

3. Specified, Explicit, and Legitimate Purposes

- 3.1 The Company collects and processes the personal data. This includes:
 - Personal data collected directly from data subjects; and
 - Personal data obtained from third parties.
- 3.2 The Company only collects, processes, and holds personal data for specific purposes set out in Part 14 of this Policy (or for other purposes expressly permitted by the GDPR).

4. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

5. Accuracy of Data and Keeping Data Up-to-Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date.

6. Data Retention

- 6.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- 6.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

7. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

8. Data Subject Access

Data subjects may make subject access requests ("SARs") in writing at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

9. Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

10. Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- 10.1 It is no longer necessary for the Company to hold that personal data
- 10.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- 10.3 The data subject objects to the Company holding and processing their personal data
- 10.4 The personal data has been processed unlawfully;
- 10.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

11. Restriction of Personal Data Processing

- 11.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- 11.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

12. Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests.

13. Personal Data Collected, Held, and Processed

The following personal data maybe collected, held, and processed by the Company:

Type of Data	Purpose of Data	Legal Basis	Retention Period
Business contact information (i.e. name, company, telephone number, email address, banking details (where relevant etc.))	For communication on business relationship matters (i.e. accounts administration, buying & selling of goods & services, service of contract, tendering).	Service contract or the legitimate interest of maintaining a working business relationship.	While there is an existing business relationship (i.e. contract, on-going trading or working relationship) and up to 6 years after a business relationship ends (to cover legislative reporting if required, e.g. revenue and for tendering purposes).
Data related to employees' information e.g. PPS Numbers; Date of Birth, Bank Details, Marital Status, Address, and any other information required in the employer/employee relationship	For the processing of salaries.	Employment Contract	Whilst in the employ of the company and 6 years thereafter as is required by law.

14. Data Security - Transferring Personal Data and Communications

The Company shall ensure safe and confidential measures are taken with respect to all communications and other transfers involving personal data.

15. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- 15.1** All electronic copies of personal data should be stored securely on the Company systems and will be protected by appropriate security measures (i.e. firewall and passwords). Backups will be taken regularly to protect against loss due to system failure and data corruption;
- 15.2** All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet, or similar.

16. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason it should be securely deleted and disposed of.

17. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- 17.1** All authorised parties of the Company should be instructed on how to handle any personal data with care
- 17.2** No personal data should be shared with parties not authorised by the Company;
- 17.3** No personal data should be left on view or unattended for any period of time.

18. Data Breach Notification

- 18.1** All personal data breaches must be reported immediately to the Company's Operations Director or any other director available at the time.
- 18.2** If a personal 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, reputational damage, or other significant social or economic damage), the Company's board of directors must inform the Data Protection Commissioners Office in Ireland of the breach within 72 hours after having become aware of it.

19. Implementation of Policy

This Policy shall be deemed effective as of 25/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

20. Contact Details of the Data Protection Officer

You can contact us with any queries relating to this policy or to exercise any of your rights using the following contact details:

- Online:** www.domalley.com
- Email:** accounts@domalley.com
- Phone:** +353 61 318677
- Address:** 92 O'Connell Street, Limerick