MIROSLAV TADEJ CONSULTING

Data Protection Policy

Protecting personal data in line with the GDPR and the Data Protection Act 2018

General Data Protection Regulation (EU 2016/679) · Data Protection Act 2018 · Regulated by the Data Protection Commission (Ireland)

Document control

Document title	Data Protection Policy
Document owner	Miroslav Tadej, Principal Consultant (Data Protection Lead)
Organisation	Miroslav Tadej Consulting
Version	1.0
Status	Approved
Classification	Public — issued for tender and client assurance
Effective date	13/06/2026
Next review date	12/06/2027
Approved by	Miroslav Tadej, Principal Consultant

Revision history

Version	Date	Summary of change	Author
1.0	[Insert]	Initial issue of the Data Protection Policy.	M. Tadej

Contents

1. Purpose

This Data Protection Policy sets out how Miroslav Tadej Consulting ("the Consultancy") protects personal data and meets its obligations under the General Data Protection Regulation (EU 2016/679) ("GDPR") and the Data Protection Act 2018. It explains the principles the Consultancy applies, the roles it occupies, the rights it upholds, and the procedures it follows so that personal data is handled lawfully, fairly, and securely.

The Consultancy is committed to protecting the privacy of every individual whose personal data it handles — whether that data belongs to its own contacts and clients, or to the customers and users of the systems it builds and maintains on behalf of clients.

2. Scope

This policy applies to all personal data processed by the Consultancy, in any format, and to the Principal Consultant and any contractor or third party acting under the Consultancy's direction. It covers personal data the Consultancy processes:

- as a data controller — for example, contact details of prospects and clients, enquiry-form submissions, and supplier contacts; and
- as a data processor — personal data belonging to a client's customers or users, which the Consultancy processes only on the documented instructions of that client when building, hosting, or maintaining their systems.

The distinction between these two roles is central to this policy and determines the Consultancy's specific obligations in each engagement.

3. Key definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual (a "data subject").
Special category data	Sensitive personal data — e.g. health, biometric, or data revealing racial or ethnic origin — requiring additional protection.
Processing	Any operation performed on personal data — collection, storage, use, disclosure, or deletion.
Data controller	The party that determines the purposes and means of processing personal data.
Data processor	The party that processes personal data on behalf of, and on the instructions of, a controller.
Data subject	The individual to whom the personal data relates.
DPC	The Data Protection Commission, Ireland's supervisory authority for data protection.

4. Data protection principles

The Consultancy applies the seven principles of the GDPR to all processing of personal data. Personal data shall be:

1. processed lawfully, fairly, and in a transparent manner in relation to the data subject (lawfulness, fairness, and transparency);
2. collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation);
3. adequate, relevant, and limited to what is necessary for the purposes for which it is processed (data minimisation);
4. accurate and, where necessary, kept up to date (accuracy);

5. kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation);
6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage (integrity and confidentiality); and
7. processed by a controller who is responsible for, and able to demonstrate, compliance with these principles (accountability).

5. Lawful basis for processing

Where the Consultancy acts as a controller, it identifies and records a lawful basis for each processing activity before processing begins. The bases relied upon are typically:

- **Contract:** the performance of a contract with the data subject, or steps taken at their request before entering a contract — for example, responding to a consultation enquiry;
- **Legal obligation:** compliance with a legal obligation — for example, retaining records required by law;
- **Legitimate interests:** the legitimate interests of the Consultancy, where these are not overridden by the rights of the data subject — for example, routine business administration; and
- **Consent:** consent, where required — for example, optional marketing communications, which are sent only with clear, freely given consent that can be withdrawn at any time.

Where the Consultancy acts as a processor, the lawful basis for processing is determined by the client (the controller), and the Consultancy processes data only on that client's documented instructions.

6. The Consultancy as controller and as processor

6.1 When the Consultancy is a controller

For its own business data — client and prospect contacts, enquiry submissions, supplier details, and similar — the Consultancy is the controller. It determines why and how that data is processed and is directly responsible for compliance with this policy and the GDPR.

6.2 When the Consultancy is a processor

When building, hosting, or maintaining systems for a client, the Consultancy generally processes the personal data of that client's customers or users as a processor. In this role the Consultancy:

- processes personal data only on the documented instructions of the client;
- ensures that persons authorised to process the data are bound by confidentiality;
- implements appropriate technical and organisational security measures (see section 8);
- engages sub-processors only with the client's authorisation and under equivalent contractual obligations;
- assists the client, taking account of the nature of processing, in responding to data-subject requests and in meeting the client's own security, breach-notification, and impact-assessment obligations;
- deletes or returns personal data at the end of the engagement, as the client directs; and
- makes available the information necessary to demonstrate compliance.

These commitments are formalised in a written data-processing agreement with each client, consistent with Article 28 of the GDPR, before processing begins.

7. Data subject rights

The Consultancy upholds the rights of data subjects under the GDPR. Where the Consultancy is the controller, it responds to requests directly and without undue delay, and in any event within one month. Where it is a processor, it promptly forwards any request to the relevant client and assists that client in responding. The rights are:

Right	Summary
Right to be informed	To be told how their personal data is used, through clear privacy information.
Right of access	To obtain a copy of their personal data and related information.
Right to rectification	To have inaccurate or incomplete personal data corrected.
Right to erasure	To have personal data deleted in certain circumstances (“right to be forgotten”).
Right to restrict processing	To limit how their personal data is used in certain circumstances.
Right to data portability	To receive their data in a structured, commonly used, machine-readable format.
Right to object	To object to processing based on legitimate interests or to direct marketing.
Rights re. automated decisions	Not to be subject to solely automated decisions producing legal or similarly significant effects.

Requests can be made to the Consultancy using the contact details in section 13. Identity is verified before any request is actioned, and requests are handled free of charge save where permitted otherwise.

8. Security of personal data

The Consultancy implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in line with its Information Security Policy. These measures include:

- encryption of personal data in transit (TLS) and at rest;
- strong authentication, multi-factor authentication, and role-based access control restricting data to those who need it;
- secure software development following the OWASP Top 10, including parameterised database queries and validated input;
- logging, monitoring, and timely patching of systems and dependencies;
- encrypted, tested backups and documented recovery arrangements; and
- data-protection by design and by default — building privacy and minimisation into systems from the outset.

9. Personal data breach management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Consultancy maintains a process to detect, report, and respond to such breaches.

8. Any suspected breach is recorded and assessed without delay to establish the facts, the data and individuals affected, and the level of risk.
9. Where the Consultancy is the controller and the breach is likely to result in a risk to the rights and freedoms of individuals, it notifies the Data Protection Commission without undue delay and, where feasible, within 72 hours of becoming aware of the breach; where notification is later than 72 hours, the reasons for the delay are recorded.
10. Where the breach is likely to result in a high risk to individuals, the Consultancy communicates it to the affected data subjects without undue delay.
11. Where the Consultancy is a processor, it notifies the affected client (controller) without undue delay after becoming aware of the breach, and supports the client in meeting its own notification obligations.
12. All breaches — including those not notified — are documented in a breach register, with the facts, effects, and remedial action recorded, and lessons are fed back into the Consultancy’s controls.

10. Data retention and disposal

Personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, to satisfy legal or contractual obligations, or to handle potential disputes. Retention periods are recorded in the Consultancy's record of processing activities. When personal data is no longer required, it is securely deleted or anonymised; physical media is securely destroyed, and digital data is erased using methods that prevent recovery. Where the Consultancy processes data on behalf of a client, data is returned or deleted at the end of the engagement in accordance with the client's instructions.

11. International data transfers

The Consultancy primarily stores and processes personal data within the European Economic Area (EEA). Where personal data is transferred outside the EEA — for example, through a cloud or sub-processor — the Consultancy ensures an appropriate safeguard is in place, such as an adequacy decision or the European Commission's Standard Contractual Clauses, so that the protection afforded by the GDPR travels with the data. Sub-processors and their locations are disclosed to clients where the Consultancy acts as a processor.

12. Accountability and records

The Consultancy demonstrates compliance through documented accountability measures, including:

- a record of processing activities describing the personal data processed, the purposes, the lawful bases, retention periods, and recipients;
- data-processing agreements with clients and sub-processors;
- data-protection impact assessments where a type of processing is likely to result in a high risk to individuals;
- a breach register; and
- this policy and the related Information Security and Secure Development policies, kept current and reviewed regularly.

The Consultancy has assessed that it is not required to appoint a statutory Data Protection Officer; the Principal Consultant acts as the Data Protection Lead and the point of contact for all data-protection matters. This assessment is reviewed as the practice grows.

13. Contact and complaints

Questions about this policy, or requests to exercise data-subject rights, can be directed to:

Data Protection Lead	Miroslav Tadej, Principal Consultant
Organisation	Miroslav Tadej Consulting, Dublin, Ireland
Email	[Insert contact email]

Individuals have the right to lodge a complaint with the Data Protection Commission if they believe their personal data has not been handled in accordance with the law. The DPC can be contacted at www.dataprotection.ie. The Consultancy asks to be given the opportunity to address any concern first, but this does not affect the right to complain to the DPC.

14. Review

This policy is reviewed at least every twelve months, and additionally in response to changes in the law, regulatory guidance, the Consultancy's services, or following a significant incident. The Consultancy monitors guidance issued by the Data Protection Commission and the European Data Protection Board and updates its practice accordingly.

15. Related documents

- Information Security Policy

- GDPR Compliance Statement
- Secure Development Policy
- Business Continuity & Disaster Recovery Plan
- Quality Management Statement

16. Approval

This Data Protection Policy is approved and issued by the Principal Consultant of Miroslav Tadej Consulting and takes effect from the effective date recorded in the document-control table above.

Name & role	Signature	Date
Miroslav Tadej Principal Consultant	Miroslav Tadej	13/06/2026