Dornan Engineering Limited its Subsidiaries and Branches
Hereafter for the purpose of this Policy known as **Dornan**

DORNAN
A Turner Company

DATA PROTECTION POLICY

DORNAN
A Turner Company

SEPTEMBER 2025

CONTENTS

DATA PROTECTION POLICY

Dornan Engineering Limited (hereafter known as Dornan) sets high standards for protecting its data and the information our clients and business partners who have entrusted data to us. Dornan Engineering Limited refers to all entities under the Dornan umbrella, including all wholly owned subsidiaries. The confidentiality, integrity, and availability of data, in all its forms, are critical to the ongoing functioning and good governance of Dornan. Failure to adequately secure data increases the risk of financial and reputational losses from which it may be difficult for Dornan to recover.

This Data Protection Policy outlines Dornan's approach to establishing guidelines around Data Protection. It provides the guiding principles and responsibilities necessary to safeguard the Dornan's personal and confidential information assets.

Dornan is committed to a robust implementation of our Information Security Management System (ISMS). It aims to ensure the appropriate confidentiality, integrity, and availability of its data. The principles defined in this policy shall be applied to all the physical and electronic information and data assets for which Dornan is responsible.

Dornan is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by, and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of data security standard ISO 27001:2022.

1. PURPOSE

The processing of both business and personal data is essential within our business. As part of our social and legal responsibilities, Dornan is committed to protecting all data entrusted to us. Dornan trust in and adhere to the principles of data protection as foundations on which we build trustworthy relationships with our clients, employees, suppliers and vendors, subcontractors, and business stakeholders. It is imperative that Dornan maintains our reputation as a responsible organisation.

This Policy is designed to promote consistent standards and practices in handling all data across Dornan. This requires those who collect and use business and personal data to be transparent about how it is used, to follow the principles on Data Protection and to respect individuals' and company rights.

2. SCOPE

This Policy applies to all of Dornan's employees, sub-contractors, third-party suppliers, and their sub-contractors who work with or on behalf of Dornan and Dornan's third-party suppliers, hereinafter to be referred to as "Suppliers" who store, control and process data (both electronic and physical/paper based) relating to identifiable individuals i.e., Data Subjects.

This policy also applies to Clients, to whom Dornan may supply information to for the purpose of marketing and project tendering and project implementation. This Policy works within the principles of the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)) and the General Data Protection Regulation (GDPR) (Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016) and any information pertaining to data subjects which can take the form of Personal/Business Data.

Where mentioned in this policy, the following meanings are understood for employees, clients, and suppliers:

Employees: Dornan employees, including contractors, temporary employees, and independent service providers.

Clients: Existing, previous, or potential clients.

Suppliers: Sub-contractors, contractors, Internet Service Providers (ISPs), vendors, suppliers, and all relevant third-party suppliers.

2.1. PERSONAL DATA CAN INCLUDE BUT IS NOT LIMITED TO:

- Names of individuals.
- Postal addresses.
- Email addresses.
- Telephone numbers.
- Online Identifiers (IP address, cookies, RFID tags).
- The aggregation of subsets of data relating to the identification of an individual.
- Personal profiles/CVs.
- Any information relating to an individual.

2.2. BUSINESS DATA CAN INCLUDE BUT IS NOT LIMITED TO:

- Communications: E.g., emails/letters/texts/fax/social media messaging.

- Calls: Telephone/messaging applications.
- Bill information.
- Financial information.
- Marketing information.
- Personal profiles/CVs.
- Tender details and pricing.

3. POLICY

3.1. DEFINITIONS:

Personal and business data and information hereafter referred to as personal data.

- **GDPR**

Personal data processed wholly or partly by automated means (that is, information in electronic form); and

personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

- **ePrivacy**

Bill: Includes an invoice, account, statement or other document of similar character and "billing" shall be construed accordingly.

Call: means a connection established by means of a telephone service available to the public allowing two-way communication in real time.

Communication: Means any information exchanged or conveyed between a finite number of parties by means of a public electronic communications service but does not include information conveyed as part of a programme service, except to the extent that such information can be related to the identifiable subscriber or user receiving the information.

3.2. PRINCIPLES OF PROCESSING DATA

When processing data, the individual rights of the data subjects must be protected through adherence to the principles of Data Protection, as set out below:

3.3. LAWFULNESS, FAIRNESS AND TRANSPARENCY

The personal data shall be processed lawfully, fairly and in a transparent manner. Data Protection laws require that Dornan provides the data subject with information about how their personal data is processed in a concise, transparent, and intelligible manner. This must be easily accessible using clear and plain language. Transparency is achieved by keeping the

individual informed of the processing activities and data we hold about them. Data Subjects must be informed before data is collected and where any subsequent changes are made.

3.4. PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. Processing "for another purpose" requires further legal permission or consent purposes and lawful bases for Dornan's processing activities are outlined in the online Data Privacy Notice. To understand how your personal data is being processed by Dornan, please read this online Data Privacy Notice.

3.5. DATA MINIMISATION

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

We must all ensure that we only collect personal data which is necessary for each specific purpose (but no more than needed) is collected and processed, in terms of the:

- Amount of personal data collected.
- The extent of the processing.
- The period of storage and accessibility.

3.6. DATA ACCURACY

Personal data shall be accurate and, where necessary, kept up to date. Inaccurate or outdated data must be deleted or amended. Dornan and its Suppliers are required to take "every reasonable step" to comply with this principle.

3.7. 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 processed. Personal data no longer needed for the purpose for which it was collected, must be deleted unless there are other grounds for retaining it. A regular review process must be in place with methodical cleansing of data. Further specific records retention information can be found in Dornan's Information Classification Scheme policy and Dornan's Records Retention Policy/Records Retention Schedule.

3.8. INTEGRITY AND CONFIDENTIALITY (SECURITY)

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 or organisational measures. At Dornan, we assess risk, implement protective security controls and, review on a regular basis that our security controls are effective.

3.9. ACCOUNTABILITY

Dornan, Dornan Clients, and its Suppliers shall be responsible for and be able to demonstrate compliance with data protection laws. This includes but is not limited to:

- Documenting, maintaining, and updating the Dornan personal data inventory.
- Documenting, maintaining, and updating the Dornan privacy notices.
- Documenting the obtainment of appropriate consents.
- Using appropriate organisational and technical measures to ensure compliance with the data protection principles.
- Where appropriate, using Data Protection Impact Assessments (DPIAs).

4. ENFORCEMENT

In Ireland, UK and Europe, all EU Directives, UK, and local data protection legislation is enforced by law. All complaints from a Supervisory Authority must be sent to Dornan's Data Protection Officer immediately at dpo@dornangroup.com.

The Data Protection legislation local to each country where Dornan has a location and the GDPR control how personal information is used by organisations, businesses, or the government i.e., Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. The UK General Data Protection Regulation, alongside the UK Data Protection Act and the Data (Use and Access) Act 2025, is the law on data protection and privacy in the UK.

Both the GDPR and the UK GDPR address the transfer of personal data outside the EU, UK, and EEA areas.

Dornan adheres to all legislation and directives governing personal data.

5. PROCESSING PERSONAL DATA

5.1. LAWFUL BASIS FOR PROCESSING

Collecting, processing, and using personal data, regardless of whether the data is from a client, supplier, or a colleague, is permitted only under the following legal basis:

5.1.1. CONTRACTUAL NECESSITY

Personal data may be processed on the basis that such processing is necessary to enter into and/or perform a contract with a data subject. The lawful basis of the processing between Dornan (data controller) and an employee (data subject) is contractual necessity.

5.1.2. COMPLIANCE WITH LEGAL OBLIGATIONS

Personal data may be processed on the basis that Dornan and its Clients and Suppliers have a legal obligation to perform such processing.

5.1.3. VITAL INTERESTS

Personal data may be processed on the basis that it is necessary to protect the "vital interests" of the data subject (this essentially applies in "life-or-death" scenarios).

5.1.4. PUBLIC INTEREST

Personal data may be processed on the basis that such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest, such as the relevant State authorities or government departments.

5.1.5. LEGITIMATE INTERESTS

Personal data may be processed on the basis that the controller has a legitimate interest in processing those data, provided that such legitimate interest is not overridden by the rights or freedoms of the affected data subjects.

5.1.6. CONSENT

Personal data may be processed on the basis that the data subject has consented to such processing.

A legal basis is also required if the purpose of collecting, processing, and using personal data if it is to be changed from the original purpose.

For any other purposes not in Dornan's Privacy Notice, guidance must be sought from the Data Protection Officer before collecting any personal data. This shall enable Dornan to ensure we collect the data in a legal manner, whilst upholding these principles of Data Protection.

5.2. PROCESSING SENSITIVE PERSONAL DATA

Below are the classes of personal data which are "sensitive" or "Special Categories of Personal Data":

- Information relating to race.
- Information relating to ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Health data.
- Data concerning sex life or sexual orientation.

5.3. GENERAL EMPLOYEES AND THIRD-PARTY GUIDELINES

- Access to personal data shall be on a need-to-know basis only.
- Dornan shall provide training to all employees to help them understand their responsibilities when handling personal data.
- Employees shall keep all data secure, by taking sensible precautions and following the Data Protection Principles in this Policy.
- Personal data gathered online via websites, social media sites etc must be treated in the same manner as personal data provided to Dornan via other sources. This data must only be used for marketing purposes (if the data subject has provided their consent) or for business purposes, as outlined in our privacy notice.
- Personal Data must be regularly reviewed and updated if it is found to be out of date or incorrect.
- Where Personal Data is no longer required, it must be deleted and disposed of in accordance with the organisation's Records Retention Policy and Records Retention Schedule.
- Employees must request guidance from the Data Protection Officer if they are unsure about any aspect of data protection.
- Personal data in relation to employees (names, bio) may be submitted to clients or potential clients as part of the tender process. Employees shall keep all data secure, by taking sensible precautions and following the Data Protection Principles in this Policy in order to protect the personal data of other employees.
- Personal data in relation to third parties' employees (names, identification number) may be processed as part of the client billing process. Employees shall keep all data secure, by taking sensible precautions and following the Data Protection Principles in this Policy in order to protect the personal data of third parties' employees.

5.4. PRIVACY NOTICE

Dornan's Privacy Notice describes Dornan's privacy practices in relation to all information that Dornan processes. The Privacy Notice outlines:

1. Who we are.
2. Explanation of terms.
3. What information we collect.
4. How we collect the information, the purpose and the lawful basis.
5. How we share information that we collect.
6. How we store and secure information that we collect.
7. Your rights as a data subject.
8. How you can access and control your information.
9. Other important details.

Please read this important document to understand how we process personal data, including your personal data. If you have any questions, please contact the DPO (dpo@dornangroup.com).

5.5. PERSONAL DATA STORAGE (PAPER)

These rules describe how and where data must be safely stored:

- When not required and/or not being used, the paper files must be kept in a locked drawer or filing cabinet.
- Employees must make sure paper is not left where unauthorised people could see or access, like on a printer, fax, or photocopier.
- When no longer required, paper records bearing STRICTLY CONFIDENTIAL/CONFIDENTIAL protective marking must be shredded or placed into confidential waste bins.

Please notify the Data Protection Officer immediately if your business area does not have lockable paper file systems or a confidential waste bin. Email: dpo@dornangroup.com

5.6. ELECTRONICALLY STORED PERSONAL DATA

When data is stored electronically, it must be protected from cyber-attack:

- Data must be protected by strong passphrases. The Acceptable User Agreement provides guidance on suitable passphrases.
- Personal Data must only be stored on designated drives and servers and must only be uploaded to approved cloud services.
- Data supplied for the purposes of Marketing, Pre-qualification and Tendering must be password protected and issued as read-only.

5.7. DATA USE

When Personal Data is accessed and used it is at the greatest risk of loss, corruption, or theft. Therefore, the following precautions shall be adhered to when using personal data:

- When working with personal data, employees must ensure the screens of their computer are always locked when left unattended.
- Personal data must always be shared on a "Need-to-Know" basis and encrypted before being shared electronically. The Data Protection Officer can provide guidance on how to do this for authorised external contacts.
- Personal Data must never be transferred outside the European Economic Area (EEA) or the UK without the express approval of the Data Protection Officer.
- Employees shall not save copies of Dornan personal data to their own computers and devices.

5.8. ENSURING DATA ACCURACY

It is the responsibility of all employees who work with Personal Data to take steps to ensure it is kept as accurate and up to date as possible:

- Personal Data must not be duplicated. Any duplicates of data not required must be deleted.
- Retention of personal data shall be in accordance with the Data Retention, Media Destruction and Backup Policy.

6. DATA SUBJECT ACCESS RIGHTS

Individuals, be they current or former Clients or employees, have specific rights under Data Protection Laws. Dornan employees must notify the Data Protection Officer immediately if they get a request from an individual who wishes to exercise one of their below rights:

6.1. RIGHT TO BE INFORMED

All individuals have the right to be informed of how we collect and use their data. This is typically done through Dornan's Privacy and Cookies Notices.

6.2. RIGHT TO RECTIFICATION

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. We have an obligation to correct the inaccuracies and to respond to the request within one month.

6.3. RIGHT TO ERASURE

The right to erasure is also known as 'the right to be forgotten'. This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

However, the right to erasure does not provide an absolute 'right to be forgotten'. Certain records must be kept under Statutory Law and regulations. The following types of documents provide a brief example of records required to be kept.

- Financial Records - 7 Years
- Health Information - up to 40 years

Individuals have a right to have personal data erased and to prevent processing in some specific circumstances:

Where the personal data is no longer necessary in relation to the purpose for which it was originally collected / processed.

- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data must be erased to comply with a legal obligation.

6.4. RIGHT TO RESTRICT PROCESSING

Individuals have a right to 'block' the processing of their personal data. If we receive such a request, we must ensure that we retain just enough information, so the restriction is respected in the future.

6.5. RIGHT TO DATA PORTABILITY

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

6.6. RIGHT TO OBJECT

Individuals have the right to object to Dornan processing their personal data based on legitimate interests and/or direct marketing (including profiling).

6.7. RIGHT OF ACCESS

All individuals who are a subject of personal data held by Dornan are entitled to:

- Obtain a confirmation of the processing.
- Be informed the Personal Data we hold about them.
- Be informed of the categories of Personal Data concerned.
- Obtain a copy (subject to certain limitations and exemptions).

6.8. RIGHTS IN RELATION TO AUTOMATED DECISION MAKING

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal (or similarly significant) effects concerning the individual without any human intervention (e.g., automatic refusal of an online credit application or decisions on recruitment).

Dornan does not make any decisions about an individual solely based on automated decision making.

If an individual contacts Dornan requesting the execution of any of these rights, the individual must be asked to email Dornan's Data Protection Officer on: dpo@dornangroup.com.

- Under Data Protection Laws we must respond to valid requests within no more than one month.
- For more info, please see the Subject Access Request Policy & Guidance, or email Dornan's Data Protection Officer: dpo@dornangroup.com.

7. COLLEAGUE MONITORING

Dornan may undertake the monitoring of employees in the workplace to protect the commercial interests of the business, to ensure a safe working environment for all employees, for the prevention and detection of crimes and to comply with legal obligations (e.g., subject access requests). Monitoring of employees may be carried out by:

- Recording using CCTV Cameras.
- Viewing company emails.
- Manual and automated tracking of emails.
- Recording logs of websites visited.
- GPS/Geolocation tracking of Dornan vehicles.

8. DISCLOSURE TO LAW ENFORCEMENT

In certain circumstances, the Data Protection Laws and directives allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

In such circumstances, Dornan shall disclose requested data. We must ensure the request is legitimate. If you receive such a request, seek assistance from the Data Protection Officer. Email: dpo@dornangroupo.com.

9. DISCLOSURE TO THIRD PARTIES WORKING ON OUR BEHALF

Dornan has a process for appointing suppliers to process Personal Data. To onboard a new supplier, please contact Dornan's Data Protection Officer for guidance. Email: dpo@dornangroupo.com.

10. SENDING PERSONAL DATA OUTSIDE OF THE EEA

Data Protection Laws and Directives place restrictions on transferring personal data outside of the European Economic Area or the UK. Any Dornan employee, Client, or Supplier must seek guidance and permission from Dornan's Data Protection Officer prior to attempting to undertake such action, in order to allow any privacy impacts to be assessed and associated safeguards and mitigation controls can be established.

11. CONFIDENTIALITY OF PROCESSING

Employees, Clients, and Suppliers may have access to personal data only as is appropriate for the type and scope of the task required.

Employees, Dornan Clients, and Suppliers are forbidden to:

- Use personal data for private or commercial purposes,
- Disclose it to unauthorised persons, or
- Make it available in any other way.

Line Managers must inform their employees at the start of the employment relationship about their obligations under Data Protection. These obligations shall remain in force even after employment has ended.

At all times, the "Need-to-Know" Principle must be followed.

12. SECURITY OF PERSONAL DATA

We must ensure that the appropriate technical and organisational security measures are in place to safeguard personal data against unauthorised or unlawful processing, including preventing unauthorised access, accidental loss, destruction, or damage to personal data.

We must always exercise extreme caution when disclosing Personal Data via any means. In particular, the requesting person's identity must be checked to ensure the information is only given to those who are legally entitled to it, whether they are inside or outside of Dornan.

Dornan employees are not to provide any personal information if they are in any way unsure of the requestor's identity.

Further specific information can be found in Dornan's Data Subject Access Request and Right to be forgotten procedure.

13. REMOTE WORKING

All remote workers must use a Dornan IT Department installed secure VPN connection to the organisation's network.

Remote access is enabled via company deployed VPN for all users. Information accessed via remote working is the exact same as if the user were internally in a Dornan Office/Site.

The physical security of the building and local environment being worked in must be considered to ensure that there is no loss to company property/data or to any third-party utilising Dornan Computer equipment.

Devices used for remote access must always be kept under the allocated employee's protection.

The company requires users to act with care in public places to avoid the risk of confidential information being overlooked by unauthorised persons.

The IT Department shall ensure that any remote access to network components is strictly controlled on a least privilege access method and may be monitored when used.

Initial access/Login is enforced via strong password authentication and/or via multifactor authentication.

Where access to limited company resources such as Company Webmail, LMS and other similar Web based applications is being carried out over personal devices, the same policy items (as defined above) apply.

Non-compliance with these remote working obligations may result in revocation of access rights, return of equipment, disciplinary action, termination of the remote working arrangement or any combination.

14. DATA PROTECTION CONTROL

Compliance with the Dornan Data Protection Policy and all applicable Data Protection Laws is checked regularly within data protection audits and via other controls. The performance of these controls is the responsibility of each department, the Data Protection Officer and other company compliance teams.

The results of the data protection audits must be reported to Dornan's Board of Directors, or individual representatives of the Board. Functional Directors shall be responsible for ensuring that the recommendations and conclusions are actioned/mitigated.

15. COMPLIANCE

Dornan has an obligation to comply, and demonstrate its commitment, to all relevant laws and contractual requirements. This Data Protection Policy forms part of the Information Security/Data Privacy suite of policies and is designed to help ensure Dornan's information is handled in the most secure manner throughout its lifecycle – from creation to retention and/or destruction.

16. BREACHES OF POLICY

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Dornan's assets, or an event which is in breach of Dornan's security procedures and policies.

All employees, third-party suppliers, subcontractors, and customers/clients of Dornan have a responsibility to report security incidents and breaches of this policy as quickly as possible through Dornan's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of Dornan.

Dornan shall take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

17. REFERENCES

17.1. LEGISLATIVE

- Data Protection legislation local to each country where Dornan has a location.
- Regulation on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (Data Protection Directive) (GDPR).

17.2. DORNAN RELATED POLICIES AND PROCEDURES

- Dornan Privacy Notice.
- IT Operations Security Policy.
- Organisation Information Security Policy.
- Electronic Communications Policy.
- Dornan Backup and Recovery Strategy.
- Dornan GDPR Procedure.

- Data Protection Impact Assessment.
- Dornan's Data Subject Access Request procedure.
- Right to be forgotten procedure.
- Data Records Retention Policy and Records Retention Schedule.

18. DOCUMENT OWNER AND APPROVAL

The Data Protection Officer is the owner of this table and is responsible for ensuring that this document is reviewed on an annual basis.