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

DATA SUBJECT REQUEST AND RIGHT TO BE FORGOTTEN PROCEDURE

SEPTEMBER 2025

CONTENTS

1. SCOPE 2
2. RESPONSIBILITIES 2
2.1. DATA PROTECTION OFFICER FUNCTION 2
2.2. ALL EMPLOYEES 2
3. WHAT INDIVIDUALS ARE ENTITLED TO/WHAT TO EXPECT 2
4. GENERAL CONSIDERATIONS 3
4.1. POINTS TO NOTE 4
5. BALANCING THE RIGHTS OF OTHERS AGAINST THE RIGHTS OF INDIVIDUALS 5
6. PROCEDURE STAGES 5
6.1. STEP 1 – RECOGNISE 5
6.1.1. IS IT A DSAR? 6
6.2. STEP 2 – INFORM 6
6.3. STEP 3 – VERIFY 6
6.3.1. RESPONDING TO A REQUEST MADE ON BEHALF OF ANOTHER PERSON? 7
6.4. STEP 4 – ACKNOWLEDGE/REFUSE 7
6.4.1. ACKNOWLEDGE 7
6.4.2. REFUSE 8
6.5. STEP 5 – ENGAGE WITH REQUESTOR 8
6.6. STEP 6 – PLAN/FIND/RETRIEVE 9
6.7. STEP 7 – PRODUCE DATA/DESTROY DATA 9
6.7.1. REDACTION OF DATA 9
6.7.2. PRODUCTION OF DATA 9
6.7.3. DESTRUCTION OF DATA 10
6.8. STEP 8 – DOCUMENT/LOG ACTIVITIES 10
7. BREACHES OF POLICY 10
8. DOCUMENT OWNER AND APPROVAL 11

DATA SUBJECT REQUEST AND RIGHT TO BE FORGOTTEN PROCEDURE

1. SCOPE

The purpose of this document is to ensure that everybody in Dornan is aware of the rules and their responsibilities around responding to a Data Subject Access Request (DSAR) or a Right to be Forgotten (RTBF) instruction. Dornan refers to all entities under the Dornan umbrella, including all wholly owned subsidiaries.

2. RESPONSIBILITIES

2.1. DATA PROTECTION OFFICER FUNCTION

Dornan's Legal, Compliance and Data Protection (LCD) Department, under the guidance of the Data Protection Officer (DPO), will be responsible for managing and coordinating all activities required to administer DSARs and RTBF requests.

- Oversee compliance with data protection laws and this procedure.
- Approve all DSAR and RTBF responses before release.
- Act as the primary point of contact for data subjects and supervisory authorities.
- Ensure that retrieval, review, redaction, and secure delivery of personal data are completed within statutory timelines.

2.2. ALL EMPLOYEES

It is the responsibility of all employees within Dornan to recognise a DSAR and understand the process in responding to one. This process is managed by Dornan's Legal, Compliance and Data Protection Department under the direction of the DPO. Any requests for personal information **must be raised immediately** with the DPO by emailing dpo@dornangroup.com.

3. WHAT INDIVIDUALS ARE ENTITLED TO/WHAT TO EXPECT

The General Data Protection Regulation (GDPR) provides individuals with certain rights (when specific conditions are met). These rights include:

- The right to be informed;
- The right to rectification;
- The right to restrict processing;
- The right to data portability;

- The right to object to processing of personal data;
- The right to object to automated decision making;
- The right to be forgotten (right to erasure) and;
- The right of access.

These rights apply to all individuals, including internal and external stakeholders. This procedure focuses on the last two rights, namely the RTBF and the right of access. The right of access is more commonly referred to as a DSAR. Information on the other six rights can be found in Dornan's Data Protection Policy. Data subjects can exercise their rights at any time and Dornan must facilitate these requests.

4. GENERAL CONSIDERATIONS

It is always important to understand the type of information and the types of requests that may be received with regards to subject access. The timescale for responding to a DSAR is one calendar month.

Dornan cannot charge a fee for responding to a DSAR. However, where the request is deemed to be excessive or manifestly unfounded, Dornan can charge a "reasonable fee" to cover the administrative costs of complying with the request. There is also the ability to charge a "reasonable fee" if an individual requests further copies of their data. The DPO will decide whether a fee may be charged or not. Article 15 of the GDPR sets out the information that individuals have the right to be provided with. Broadly this includes providing information about:

- What personal data it is being processed.
- The purposes for which the personal data is being used.
- Who the personal data has or will be disclosed to?
- The existence of any automated decision-making, including profiling and, where this produces legal or similarly significant effects, what logic is being used for that purpose.
- How long the data will be retained for (or the criteria used to determine this).

Data subjects are entitled to be told if any personal information is held about them and, if it is, to be given:

- A copy of the information in an easily accessible, machine-readable format.
- An explanation of any technical or complicated terms.
- Any information Dornan has about where they obtained the information.
- A description of the information being held on them, the purposes for processing their personal information and who Dornan is sharing the information with.

A valid DSAR may be made via any of the following channels:

- A hard copy (via post or hand delivered).
- Email.
- Phone.
- A message/post via social media.

Some important elements of an application that often require further consideration as part of the process include:

- The legal basis under which Dornan accesses the data.
- The security of Dornan's data handling and storage facilities.
- Technical feasibility - can Dornan provide what is being requested?
- The purpose for wanting the data, including what benefits will be yielded for the individual.

Consider this:
It is best practice to contact the requester directly back on the medium they have used to request this information from you and ask them to complete Dornan's DSAR form as this is the easiest way to validate and verify a request.

4.1. POINTS TO NOTE

For a DSAR to be valid it must come from the individual themselves or an authorised third party, such as a solicitor/parent/guardian. It is especially important to establish that the individual asking for the information is who they say they are, to avoid the damage of inadvertently disclosing personal information to the wrong person. If the information the individual has provided in their request is insufficient, you must issue a response to the individual requesting the details that you need to fulfil the request. For example, you may need to:

- Request proof of ID (if the requester is an employee or ex-employee this may not be necessary if it is obvious to you who they are).
- Request proof of relationship/authority (for example if information is requested about a child or by a third party).
- Ask if they are interested in specific information. i.e., HR File or Payroll etc.
- Ask what their relationship is with Dornan.
- Ask if they require the information to be provided in hard copy or whether they will accept it in an electronic from.

Dornan must respond formally within one calendar month. The one-month period starts on the day the request is received (or the day identity verification is completed, if required).
If the same date does not exist in the following month, the deadline is the last day of that month. If the request is complex or numerous, the response period may be extended by up to two additional calendar months. If an extension is applied, the requester (or their authorised representative) must be informed within the initial one-month period, including:

- The reason for the delay.
- The new expected deadline.

5. BALANCING THE RIGHTS OF OTHERS AGAINST THE RIGHTS OF INDIVIDUALS

Responding to a DSAR may involve providing information that relates both to the individual making the request and to another individual(s). Under data protection law, Dornan is not required to disclose information that would reveal another person's personal data, unless:

- The other individual has given explicit consent; or
- It is otherwise lawful to do so.

Dornan must always protect the privacy of third parties. If disclosure is being considered, the matter must be reviewed and approved by the DPO through the exception process.

6. PROCEDURE STAGES

6.1. STEP 1 – RECOGNISE

DSAR

Also referred to as a Subject Access Request, any individual has the right to ask Dornan for a copy of the personal data being held on them. This right extends to include:

- Being told if any of their personal data is being processed by Dornan.
- Being given a description of the personal data, the reasons it is being processed and advising if it will be shared with any other entities.
- Being given a copy of their personal data.

RTBF Instruction

Under the GDPR, individuals also have the right to erasure. The same identification process and procedural steps for a DSAR, apply when responding to an RTBF request, with the difference that data must be destroyed rather than shared with the data subject, if the request meets all applicable criteria.

Note:
Remember, when delivering the information to the requester (or confirming its destruction), it is important to document the actions taken to meet the GDPR's accountability requirements. It is the responsibility of the Data Protection Department to retain the documented actions.

6.1.1. IS IT A DSAR?

Any request from an individual seeking access to their personal data constitutes a DSAR. Such requests may fall into two categories:

Routine Enquiries

Requests that can be resolved quickly in the normal course of business without accessing multiple systems or sensitive records. Examples include:

- Confirmation of the amount on the most recent invoice.
- Provision of a customer reference number.

Formal DSARs

Requests that require retrieval of personal data from multiple sources or involve sensitive information. These must be handled under the DSAR & RTBF Procedure. Examples include:

- An employee requesting a copy of their personnel file.
- A solicitor acting on behalf of a client requesting access to the client's records.
- A request from law enforcement for personal data.

All formal DSARs, RTBF requests, and any law enforcement requests must be escalated immediately to the Legal, Compliance & Data Protection Department for processing. Contact: dpo@dornangroup.com.

6.2. STEP 2 – INFORM

Once an individual makes a request for their personal information, the DPO (dpo@dornangroup.com) must be informed so that they can commence a process to determine the applicability of the request, how all the personal data can be collated and inform all necessary parties.

Dornan may request only the information needed to locate the personal data, but this does not extend the one-month deadline for fulfilling the request.

If the request does not specify clearly what information is being requested, ask them promptly for the other information you reasonably need so you can find the information they want.

6.3. STEP 3 – VERIFY

Dornan must ensure that sufficient information is obtained from the requester to confirm their identity before releasing any personal data. This safeguard is essential to prevent the accidental or unauthorised disclosure of personal information to the wrong individual.
Verification measures must be proportionate and reasonable. Additional identification must not be requested where the requester's identity is already clear, such as when there is an ongoing business relationship or the individual is otherwise readily identifiable from existing records.

Consider this:
You have received a written DSAR from a current employee and have even had a phone conversation with them about the request. Although Dornan's position is to verify the individual's identity by asking for forms of identification, it would be unnecessary to do so in this case, as you can verify their identity using the information you already hold on the individual's personnel file.

If Dornan cannot confirm the requester's identity based on information already held, the individual must provide two forms of identification:

- One photographic ID (for example, passport, driver's licence, national ID card), and/or

One proof of address (e.g., utility bill, bank statement, official government correspondence).

6.3.1. RESPONDING TO A REQUEST MADE ON BEHALF OF ANOTHER PERSON?

A third party may submit a DSAR on behalf of an individual, such as a solicitor acting for a client or a relative acting for a family member. Before processing such a request, DPO must ensure that the individual has provided clear and explicit consent for the third party to act on their behalf.
This consent must be documented in the form of an authority letter that is duly signed and dated by the data subject. The letter must clearly state the name of the authorised third party, their address and confirm their authority to make the request on the individual's behalf.

6.4. STEP 4 – ACKNOWLEDGE/REFUSE

Dornan must respond back to either a request for information or an instruction to delete information **without undue delay or, at the very latest, within one calendar month**. The timeline for fulfilling the request remains within one calendar month, from the date the request was first received.

6.4.1. ACKNOWLEDGE

If a data subject has been verified/identified, then Dornan must contact them to confirm that the request is being processed and that, in line with the regulation, their request will be

completed within the one calendar month window enforced upon Dornan by the regulation. In this instance, the procedure will continue to Step 5.

6.4.2. REFUSE

There may be circumstances in which Dornan possesses valid reasons for declining to fulfil a DSAR. In this instance, Dornan is required to communicate to the requester that their request will not be processed and provide the justification for this decision. It is deemed best practice to provide the requester with the details required to lodge a complaint to the supervisory authority for data protection. These details can be found in our Data Privacy Notice online. The DPO will be responsible for issuing this communication.
Grounds for refusal of a DSAR can include:

- The requester has not provided sufficient evidence to prove their identity and has not complied with a request for further identification.
- Dornan does not hold the data (it may be that the information has never been held by Dornan or has already been destroyed in accordance with Dornan's data destruction/retention policy).
- Dornan has a lawful reason for refusing to act on the request.
- A requester has provided multiple or unreasonable requests – Dornan may re-provide the full file of papers in its entirety and charge a reasonable administration fee. For multiple requests (more than two within a 3-month timeframe), Dornan may provide the personal data that has been gathered since the most recent request was fulfilled. Administration fees will be collected by Dornan prior to the release of information requests.

Consider this:
You have received a request for access from an employee who left Dornan 10 years ago. Dornan enforce a data retention policy in which employee data is kept for no longer than 7 years after termination of the employment contract. In this instance, the organisation has no information to provide the requester and Dornan must respond to the individual within one calendar month to advise that the organisation cannot act on their request, outlining the above reason for this refusal to act.

6.5. STEP 5 – ENGAGE WITH REQUESTOR

Once a decision has been made on whether Dornan will acknowledge the request for access or reject the request and regardless of the medium in which the DSAR has been received, communication to the requester must be formal and sent either on official Dornan headed letter or via email explaining the decision made regarding their request. This communication must be issued and signed by the Data Protection Officer.

6.6. STEP 6 – PLAN/FIND/RETRIEVE

Once a request is received, it will be the responsibility of the Data Protection Department to co-ordinate the gathering of the data requested. It is the responsibility of each department to work with the DPO and provide all data requested. Once a DSAR has been verified, the DPO will be able to assess which departments and processors will need to be contacted to obtain the data required by email dpo@dornangroup.com.

During this step, analysis on the locations of personal data and the Records of Processing Activities (ROPA) must be utilised to quickly identify and discover the locations of personal data. The ROPA will be the most efficient method of tracking personal data whilst devising the plan for retrieving this information.

Consider this:
Ongoing enforcement of Dornan policies and adherence to Dornan processes relating to management and handling of personal data will ensure the minimisation of personal data to what is strictly necessary, thereby making the process of finding and retrieving data far more efficient

6.7. STEP 7 – PRODUCE DATA/DESTROY DATA

The necessary steps in this phase will depend upon the nature of the request. The production of data will be required in completing a DSAR, whereas the destruction of the information will be required as part of the RTBF instruction.

6.7.1. REDACTION OF DATA

Documents containing personal information will need to be reviewed in detail to redact (block out) personal data relating to individuals other than the requestor, before sending the documents to the requestor. These documents must be approved by the DPO before issuing.

6.7.2. PRODUCTION OF DATA

Documents containing personal information will come in multiple formats which will need to be taken into consideration when responding to a DSAR. This can include, but is not limited to:

- Physical paper files
- Electronic files
- CCTV / pictorial data files

Consider this:
It is likely that you will need to provide information to a data subject in multiple formats: **Always ensure** that you have been provided with correct and accurate contact details that give you the ability to send information in either hard copy or soft copy.

Once you have located and retrieved the personal data that is relevant to the request, you must communicate it to the requester in an intelligible form. In most cases you can comply with this requirement by supplying a photocopy, print-out or pdf of the relevant information. When providing information on an electronic format, you must ensure that this is provided in an "open reusable format" so the data subject can easily use the data provided to them.

Consider this:
Documents under consideration during a subject access request must be checked to ensure they do not include information on another data subject(s) or any sensitive Dornan information. Ensure that you check the document's classification (as per the Dornan policy) before you share it.

6.7.3. DESTRUCTION OF DATA

Dornan has provided instruction on the secure methods of destroying all types of data (physical and electronic) and guidance on the retention periods for information held by Dornan. Please refer to these documents when destroying personal data as part of a RTBF.

6.8. STEP 8 – DOCUMENT/LOG ACTIVITIES

It is best practice to ensure that a log of the DSAR is stored and maintained. Dornan must log a receipt of any received DSAR and update it to monitor progress as the request is processed.

The log will include copies of information supplied during the request together with an explanation on why the information is held and dated (along with the recorder and/or data owner).

Similarly, it is important that Dornan retain a log with the minimum amount of personal data possible, to verify that a RTBF request has been actioned.

It is the responsibility of the DPO to maintain this Log.

7. BREACHES OF POLICY

Dornan must take appropriate measures to remedy any breach of this procedure through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

8. DOCUMENT OWNER AND APPROVAL

The DPO is the owner of this document and is responsible for ensuring that this policy document is on a regular basis. For queries around any aspect of this document email dpo@dornangroup.com.