Subject Access Request Policy

Purpose

To provide guidance to all employees involved in the handling and processing of "Subject Access Requests" (SAR's) received under the GDPR. A Subject Access Request is made by an individual or employee to see all personal information the company holds about them.

Scope

All personal data processed by Trident Consulting is within the scope of this procedure.

Data subjects are entitled to obtain:

- confirmation as to whether Trident Consulting is processing any personal data about that individual;
- access to their personal data; and
- any related information;

Policy Statement

Trident Consulting is committed to protecting and respecting personal data. We wish to be transparent on how we process personal data and demonstrate that we are accountable with the GDPR in relation to not only processing personal data but ensuring that any subject access requests are dealt with in a timely and appropriate manner.

Subject Access Requests are to be made by email to john@tridentconsulting.ie.

Roles and Responsibilities

The Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting to management regarding Subject Access Requests (SARs). The Data Protection Officer is responsible for handling all SARs.

Data Subject

A data subject is the individual (living) on whom we have collected and processed personal data. Data subjects have the right under GDPR to request a copy of the personal data we hold on them. However, in order to further protect the data subject to ensure that the request is valid we will request the data subject:

- to provide us with evidence of their identity in the form of a current passport/driving licence; and
- the signature on the identity must be cross-checked to that on another appropriate document.

The data subject may stipulate the specific sets of data held by Trident Consulting on their Subject Access Request email (SAR).

Alternatively, the data subject can request all data held on them.

Data Collection Process

Once received, the SAR application is immediately forwarded to the Data Protection Officer who will ensure that the requested data is collected within the specified time frame, where possible.

The Data Protection Officer, or their nominee, will

- ⇒ record the date that the identification checks were conducted, and the specification of the data sought (on the SAR Record).
- ⇒ collect the data specified by the data subject, and or search all databases and all relevant filing systems (manual files) in Trident Consulting, including all back up and archived files (computerised or manual) and all email folders and archives.
- ⇒ provide the requested information to the data subject within **one month** from this recorded date. Under the GDPR Article 12(3), that period may be extended by two further months where necessary, considering, the complexity and number of the requests received.
- ⇒ inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.
- ⇒ where the data subject makes the request by electronic form, provide the information by electronic means where feasible unless otherwise requested by the data subject.

The Data Protection Officer should maintain a data map that identifies where all data in Trident Consulting is stored. It is essential therefore, that the Data Protection Officer understands the data mapping and data inventory of the entire organisation.

The Data Protection Officer will maintain a record of requests for data and of its receipt, including what identification checks made, what files/databases were searched, response dates, if the response will take longer than one month, and why and how the personal data was supplied (by electronic form or otherwise).

The Data Protection Officer reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National Security
- Crime and taxation
- Health
- Education
- Social Work
- Regulatory work
- Journalism, literature and art
- Research, history and statistics
- Publicly available information
- Corporate finance
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Management forecasts

- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

In the event that a data subject requests us by email to provide them with the personal data stored by us, we will provide the data subject with the requested information by email, unless otherwise specified.

All the items provided to the data subject should be clearly listed along with the data subject's name and the date on which the information is delivered to (and received by) the data subject.

Should a data subject request whether or not personal data concerning him or her is being processed by us, and where this is the case, we will provide the data subject with the following information:

- Purpose of the processing;
- Categories of personal data;
- Recipient(s) of the information, including recipients in third countries or international organisations;
- How long the personal data will be stored;
- The data subject's right to request rectification, erasure, restriction or objection, relative to their personal data being processed; and
- Their right to lodge a complaint with the supervisory authority (Data Protection Commission);
- Information on the source of the personal data if it has not been collected from the data subject;
- The existence of any automated decision-making; and
- If, and where, personal data has been transferred and information on any safeguards in place.

Subject Access Requests and Children

The Data Protection Officer will review Subject Access Requests received from a child. Prior to responding to a SAR in the case of a child, the Data Protection Officer will consider their responsibilities by carefully explaining any implications of sharing their personal data.

Note

- A child has a right of access to the information held about them.
- In most cases, these rights are likely to be exercised by those with parental responsibility for them. However, before responding to a SAR for information held about a child, the Data Protection Officer will consider whether the child is mature enough to understand their rights.
- It is reasonable, in most cases, for a child that is aged 13 years or more, to have the capacity to make a subject access request.
- The implications of sharing their information with others will be clarified as it should be considered that they may not fully understand the information they have been given.

Contacts

John O'Connell, Data Protection Officer (DPO)

Policy Review

Policy Prepared For:	**Trident Consulting**
Approved by Board/Management On:	**31 March 2026**
Policy Became Operational On:	**31 March 2026**