**DEFENCE FORCES TRIBUNAL OF INQUIRY**

**DATA PROTECTION POLICY**

| | |
|---|---|
| **Version Number:** | 0.1 |
| **Date:** | 15 April 2026 |

## CONTENTS

**Section** **PAGE**

**Version Control and Responsibility for Maintaining the Data Protection Policy**

The following people are responsible for maintaining this Data Protection Policy:

Data Protection Officer – Final Approval of all Revisions

Data Protection Officer – Providing Updates

**Version Control**

| Version Number | Purpose/Change | Date Adopted |
|---|---|---|
| 0.1 | Initial Draft | 15 April 2026 |

## Section 1 - General

### 1. About this Policy

1.1 The purpose of this policy is to outline the obligations of the Tribunal of Inquiry (the "**Tribunal**") under applicable Data Protection Law, and to describe the steps to be taken to ensure compliance with those obligations. The Tribunal is charged with investigating the matters which are provided for in its Terms of Reference from 1 January 1983 to the date of its establishment by Statutory Instrument [SI 304 of 2024], 20 June 2024. The Tribunal is tasked with inquiring, urgently, into a range of matters pertaining to the effectiveness of the complaints processes and the culture within the Defence Forces relating to complaints of abuse made by former or current members, civilian employees and civil servants of the Defence Forces. Further, it is tasked with investigating the nature and performance of the statutory role of the Minister for Defence/Department of Defence in the systems and procedures for dealing with complaints of abuse. The complaints involved are, principally, complaints of abuse which are defined in the Tribunal's Terms of Reference. Additionally, the Tribunal is to investigate the response to complaints in respect of the use of hazardous chemicals, within Air Corps' headquarters at Casement Aerodrome, Baldonnel, and to consider the adequacy of the complaints processes in light of such response.

1.2 This document should be read in conjunction with related policies or procedures (including those referenced in this policy) that the Tribunal maintains regarding compliance with applicable Data Protection Law.

1.3 This policy applies to the Tribunal and each of (i) the Tribunal's sole member, (ii) the registrar to the Tribunal, (iii) a person appointed by the Tribunal in accordance with section 6 of the Tribunals of Inquiry (Evidence) (Amendment) Act 2002 (No. 7 of 2002) to be an investigator, (iv) the Tribunal's employees/members of staff, (v) Counsel to the Tribunal, (vi) Solicitor to the Tribunal and (vii) any other person who is subject to the Tribunal's supervision and control (which may include consultants, advisors, temporary employees or officers of affiliates or other persons that are designated accordingly) (collectively, "**Covered Persons**") in their activities in so far as those activities relate to the processing of personal data.

1.4 It is the responsibility of all Covered Persons to comply with this policy. Failure to comply with this policy may result in the defaulting Covered Person being subject to disciplinary action, up to and including summary dismissal or termination of contract, as applicable.

1.5 If a Covered Person has any queries in relation to this policy, including regarding the scope of the policy and/or any related policies or procedures, they should contact the Tribunal's Data Protection Officer.

### 2. General Policy Statement

2.1 Data Protection Law confers rights on individuals regarding their 'personal data' and imposes obligations on persons who process personal data. In the course of its work, the Tribunal processes personal data relating to various categories of individuals, including Covered Persons, complainants, individuals who give statements to the

Tribunal, and those in respect of whom allegations have been made. In all such circumstances, it is the Tribunal's policy to ensure that it processes such personal data in accordance with relevant laws, including Data Protection Law, and the terms of this policy.

2.2 This policy relates to 'personal data'. Personal data is information relating to an identified or identifiable natural person (such as a name or an identification number). The legal definition of 'personal data', together with definitions of other key terms as adopted in the applicable Data Protection Law, are set out in Appendix 1 to this policy.

2.3 Personal data shall have the meaning ascribed to it by Article 4(1) of the General Data Protection Regulation and may include, but is not limited to, the names, email addresses and other contact details of individual Covered Persons or individuals with whom the Tribunal deals. Such personal data as is collected, stored or otherwise processed by the Tribunal shall be used only for those purposes necessary for the conduct of the Tribunal's work.

## 3. Data Protection Law in Ireland

3.1 Data Protection Law in Ireland is governed primarily by the General Data Protection Regulation (EU/2016/679) (the "**GDPR**") and the Data Protection Act 2018 (as amended). These laws impose compliance obligations on "controllers" such as the Tribunal, and the Tribunal could be subject to significant penalties for non-compliance with such obligations. As such, all Covered Persons should be mindful of their data protection obligations when carrying out their activities and interacting with personal data.

3.2 In addition to the GDPR and the Data Protection Act 2018, the Tribunal is also subject to specific regulations made under the Data Protection Act 2018, as follows:

(a) The Data Protection Act 2018 (Section 38(4)(b)) (Defence Forces Tribunal Of Inquiry) Regulations 2024 (S.I. No. 624 of 2024) which is designed to ensure a legal basis for processing personal data (see Section 2, paragraphs 2.5 and 2.6 for further details);

(b) The Data Protection Act 2018 (Section 51(3)) (Defence Forces Tribunal Of Inquiry) Regulations 2024 (S.I. No. 623 of 2024) which is designed to ensure a legal basis for processing special categories of personal data and Article 10 data (see Section 2, paragraphs 2.11 to 2.13 for further details); and

(c) The Data Protection Act 2018 (Section 60(6)) (Defence Forces Tribunal of Inquiry) Regulations 2025 (S.I. No. 338 of 2025) (the "**Section 60 Regulations**") which sets out Tribunal specific exemptions from data subject rights (see Section 2, paragraphs 10.2 to 10.5 for further details).

3.3 The GDPR and the Data Protection Act 2018 are supplemented by guidance published by competent supervisory authorities such as the Data Protection Commission and the European Data Protection Board. This policy is kept under review and updated in light of such legislation and guidance as and when it is published or becomes applicable.

## Section 2 – Data Protection Principles

### 1. Data Protection Principles

1.1 As a controller, the Tribunal must comply with the following key data protection principles in relation to personal data:

(a) Obtain and process personal data lawfully, fairly and in a transparent manner;

(b) Process personal data for only specified, explicit and legitimate purposes;

(c) Ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) Keep personal data accurate and, where necessary, keep it up to date;

(e) Retain personal data for no longer than is necessary for the purpose or purposes for which it is acquired;

(f) Keep personal data safe and secure;

(g) Be responsible for, and be able to demonstrate compliance with, obligations under applicable Data Protection Law; and

(h) Comply with requests from data subjects to exercise their data protection rights (subject to applicable exemptions which are set out in this Policy).

1.2 Details on how the Tribunal complies with these principles in practice are set out below.

### 2. Process personal data lawfully

Legal Bases Relied on for Processing of Personal Data

2.1 For personal data to be processed lawfully, the Tribunal must have a lawful basis as set out under relevant Data Protection Law. In relation to its data processing activities regarding personal data, the Tribunal relies on the following legal bases:

- **'Compliance with a legal obligation' basis (Article 6(1)(c) GDPR)**

2.2 In respect of personal data processed by the Tribunal in order to satisfy its legal obligations, the Tribunal relies on Article 6(1)(c) of the GDPR in combination with the text of the relevant law imposing the obligation by which the Tribunal is bound (as required by Article 6(3) GDPR).

2.3 In particular, in respecting the constitutional right to fair procedures of data subjects, the Tribunal may be required to disclose personal data to third parties.

2.4 The processing of personal data in this manner shall be subject to the provisions of this policy as well as the following supplementary measures:

(a) Only personal data the sharing of which is strictly limited to what is necessary in order to vindicate the right to fair procedures shall be disclosed to third parties;

(b) Such disclosures will be made strictly to third parties who:

(i) who are called for interview as part of the Tribunal's investigative phase;

(ii) who provide legal representation to parties participating in the Tribunal's processes; or

(iii) whose reputations are impugned in materials received by the Tribunal from complainants and who are entitled to be informed of and/or to respond to allegations made against them.

(c) In circumstances where the Tribunal discloses personal data to third parties pursuant to paragraph 2.3 above (i.e. disclosures required to ensure the constitutional right to fair procedures), the Tribunal will issue a clear notice to such third parties, which includes the following details:

(i) the purposes for which the personal data is being disclosed;

(ii) that such third parties are subject to data protection obligations in their own right, as separate and independent controllers, in respect of their use of such personal data;

(iii) that such third parties should only process the personal data to the extent reasonably required to vindicate their right to fair procedures and deal with investigations carried on by the Tribunal;

(iv) that such third parties should not use, disclose or otherwise process the personal data for any other purpose, should keep the data confidential and should not retain the data for any longer than is strictly necessary;

(v) that failure by such third parties to comply with their data protection and confidentiality obligations could result in material adverse consequences for such third parties, including but not limited to an investigation by the Data Protection Commission and enforcement notices, adverse decisions and/or administrative fines levied by the Data Protection Commission as well as potential action by an affected data subject seeking appropriate judicial remedies.

The current version of this notice is set out in Appendix 3 to this Policy.

- **'Performance of a task carried out in the public interest or in the exercise of official; authority' basis (Article 6(1)(e) GDPR)**

2.5 In relation to personal data processed for the purpose of carrying out the Tribunal's functions, the Tribunal generally relies on the lawful basis furnished by Article 6(1)(e) of the GDPR as supplemented by the Data Protection Act 2018 (Section 38(4)(b))

(Defence Forces Tribunal Of Inquiry) Regulations 2024 (S.I. No. 624 of 2024) (as to which, see below) and in accordance with the requirements of Article 6(3) GDPR.

2.6 The Data Protection Act 2018 (Section 38(4)(b)) (Defence Forces Tribunal Of Inquiry) Regulations 2024 (S.I. No. 624 of 2024) provides for the processing by the Tribunal of personal data which is necessary and proportionate for the performance of its tasks. It also states that the circumstances in which personal data may be processed include the performance by the Tribunal of such relevant tasks as the Tribunal considers necessary and proportionate to enable the Tribunal to perform its functions under the Tribunals of Inquiry (Evidence) Acts 1921 to 2011. The impact of these provisions is to ensure that the Tribunal has an appropriate legal basis under Article 6(1)(e) of the GDPR for processing personal data which is necessary and proportionate for the performance of its functions. The foregoing is a summary of these Regulations. Covered Persons should, however, read the full text of these Regulations for further details.

- **'Processing necessary for the performance of a contract' basis (Article 6(1)(b) of the GDPR**

2.7 For data which are processed in an employment context by the Tribunal, a legal basis relied on is Article 6(1)(b) of the GDPR (that the processing is necessary for the purposes of the performance of the employment contract).

- **'Consent of the data subject' basis (Article 6(1)(a) of the GDPR)**

2.8 In limited circumstances, the Tribunal may rely on the consent of a data subject to particular processing as the legal basis for such processing. However, such consent must be freely given, fully informed and capable of withdrawal, so the Tribunal will usually rely on alternative grounds for processing as set out in this Section 2, paragraphs 2.1 to 2.7.

**<u>Legal Bases Relied on for Processing of Special Category Data and Article 10 Data</u>**

2.9 The GDPR specifies certain "special categories of personal data" which attach discrete and strictly construed legal basis for their processing.

2.10 Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data and data concerning health, sex life or sexual orientation are considered special category personal data.

2.11 The Tribunal generally relies on Article 9(2)(g) and the Data Protection Act 2018 (Section 51(3)) (Defence Forces Tribunal Of Inquiry) Regulations 2024 (as to which, see below) to justify the processing of special categories of personal data.

2.12 In addition, the Tribunal may only process personal data relating to criminal convictions or offences when authorised by law (Article 10 of the GDPR).

2.13 The Data Protection Act 2018 (Section 51(3)) (Defence Forces Tribunal Of Inquiry) Regulations 2024 (S.I. No. 623 of 2024) provides that the processing by the Tribunal of (i) special categories of personal data and (ii) personal data relating to criminal convictions and offences is permitted where such processing is necessary for, and

proportionate to, the performance by the Tribunal of its functions (as specified in the resolutions passed by Dáil Éireann on 24 January 2024 and by Seanad Éireann on 30 January 2024 as a matter of urgent public importance and for which the Tribunal was appointed to inquire into, report and make such findings and recommendations as it sees fit to the Taoiseach under the Tribunals of Inquiry (Evidence) Act 1921 (Appointment of Tribunal) Instrument 2024 (S.I. No. 304 of 2024)). The foregoing is a summary of these Regulations. Covered Persons should, however, read the full text of these Regulations for further details.

2.14 The Tribunal may also rely on Section 49(b) of the Data Protection Act 2018. This is on the basis that, subject to suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects, the processing of special categories of personal data shall be lawful where the processing respects the essence of the right to data protection and is necessary and proportionate for the performance of a function conferred on the Tribunal by or under an enactment or by the Constitution.

2.15 The impact of the above Regulations and statutory provisions is to ensure that (i) the Tribunal is in a position to rely on Article 9(2)(g) as the relevant legitimising condition for processing special categories of personal data and (ii) the processing by the Tribunal of personal data relating to criminal convictions and offences is compliant with Article 10 of the GDPR. In certain limited contexts, the Tribunal may rely on explicit consent where data subjects have explicitly consented to the processing of their personal data by the Tribunal pursuant to Article 9(2)(a). Consent under this legal basis cannot be imputed, implied or inferred and may be withdrawn at any time.

2.16 For data which are processed in an employment context by the Tribunal the legal basis relied on is Article 9(2)(b) (that the processing is necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment and social security and social protection law).

2.17 The Tribunal further relies on Article 9(2)(c) where the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Article 9(2)(c)).

**3. Processed fairly and in a transparent manner**

3.1 For personal data to be processed fairly and in a transparent manner, data subjects must be provided with certain information about how their data will be processed and for what purpose.

3.2 In general, this information will be provided at the time at which the personal data is obtained (or within one month where the personal data in question was obtained from a third party).

3.3 It is the Tribunal's policy to provide this information by setting out the relevant information in an appropriately worded data protection/privacy notice and to provide this/make this available to data subjects at the time that data is first processed, where it is possible to do so.

3.4 The information to be provided to data subjects includes: the identity and contact details of the controller; the purposes and legal basis for the processing activities; the recipients of personal data; and, where the personal data may be transferred to a non-EEA country, the safeguards which have been adopted in relation to such transfer. Covered Persons should contact the Data Protection Officer for further information in the event that they require a data protection notice.

**4. Processed only for specified, explicit and legitimate purposes**

4.1 The Tribunal only processes personal data for specific, lawful and clearly stated purposes.

4.2 Covered Persons are reminded that they should not collect or engage in the processing or further processing of information about individuals routinely and indiscriminately without having a clear legal basis, and corresponding justification, for doing so.

4.3 Where Covered Persons obtain personal data for a particular purpose then, subject to limited exceptions, the data should not be further processed for any other purpose, or for any purpose that is incompatible with that for which it was originally obtained. Exceptions to this include where such further processing is permitted by law.

**5. Ensure that processing is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed**

5.1 Personal data should not be processed if it is not needed and/or on the basis that there is a possibility that a use might be found for the data in the future.

5.2 The Tribunal's practice is to ensure that it processes only such personal data as is necessary for the purposes set out in its data protection/privacy notices (see paragraph 3 above).

5.3 The type of personal data which the Tribunal processes is periodically reviewed to ensure compliance with this requirement. See Section 4 – Documenting and Monitoring Compliance, for further details.

**6. Ensure personal data are accurate, complete and up-to-date**

6.1 The Tribunal will seek to ensure that the personal data it holds are accurate, complete and up to date.

6.2 The Tribunal will request data subjects to notify it of changes to their personal data (e.g. upon a change of address).

6.3 The Tribunal will take every reasonable step to ensure that personal data that is inaccurate, including having regard to the purposes for which it is processed, is erased or rectified without delay in accordance with the procedures set out in Section 4 – Documenting and Monitoring Compliance.

**7. Retain personal data for no longer than necessary given the purpose(s) for which it is processed**

7.1 The GDPR provides that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed.

7.2 However, personal data provided to and processed by the Tribunal is subject to the National Archives Act 1986 and Part 15 of the Civil Law (Miscellaneous Provisions) Act 2011, as amended, which provides that no Tribunal record (subject to limited exceptions) may be disposed of without authorisation from the Director of the National Archives.

7.3 In light of these requirements, the Tribunal will only delete data where instructed or authorised to do so by the Director. Covered Persons should therefore retain and securely store personal data which are relevant to and necessary for the work of the Tribunal and should consult with the Data Protection Officer in circumstances where any deletion of data is being considered.

**8. Keep personal data safe and secure**

8.1 The Tribunal will ensure that personal data is 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.

8.2 The Tribunal's practice is to ensure that Covered Person access to personal data which is held by the Tribunal is restricted on a 'need to know' basis.

8.3 To the extent that any third party processes personal data on behalf of the Tribunal, the Tribunal will ensure that there is a written agreement in place which includes, among other things, appropriate security obligations regarding such personal data (see Section 3 – Dealing with Third Parties).

8.4 The security of the Tribunal's IT systems is under the overall responsibility of the Office of the Government Chief Information Officer.

8.5 All Covered Persons who have access to the Tribunal's IT systems are subject to security and acceptable use policies which outline their responsibilities in using the Tribunal's IT Systems. Further details regarding the technical and security measures that are implemented by the Tribunal are set out in the Data Security Sub-Policy.

**9. Be responsible for, and be able to demonstrate compliance with, obligations under applicable Data Protection Law**

9.1 The Tribunal takes its responsibility for complying with applicable Data Protection Law seriously and maintains this policy and the practices referred to in this policy for this purpose.

9.2 The Tribunal also ensures that it can demonstrate its compliance with its obligations under applicable Data Protection Law.

9.3 The Tribunal achieves this by maintaining the records, policies and procedures referred to in Section 4 – Documenting and Monitoring Compliance and listed in Appendix 2.

**10. Comply with requests from data subjects to exercise their data protection rights**

10.1 Under Data Protection Law, individuals have the following rights in relation to the processing of their personal data (subject to certain limited exceptions as provided in law):

(a) The right to access personal data. Data subjects have the right to be provided with a copy of their personal data along with certain details in relation to the processing of that personal data.

(b) The right to information. Data subjects have the right to be provided with certain information, generally at the time at which their personal data is obtained. The Tribunal complies with this obligation via its data protection/privacy notices.

(c) The right to rectification. Data subjects have the right to have inaccurate personal data that a controller holds in relation to them rectified.

(d) The right to object to and restrict processing. Data subjects have the right to require that a controller restricts its processing of their data in some circumstances and have the right to object to the processing of their data in certain circumstances.

(e) The rights in relation to automated decision making. Data subjects have the right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, unless one of a limited number of exemptions applies.

(f) The right to be forgotten/the right to erasure. Under certain circumstances a data subject has the right to request the erasure of their personal data.

(g) The right to data portability. Under certain circumstances, data subjects are entitled to receive a copy of their personal data in a structured, commonly used and machine readable format.

10.2 The Data Protection Act 2018 (Section 60(6)) (Defence Forces Tribunal of Inquiry) Regulations 2025 (S.I. No. 338 of 2025) (the "**Section 60 Regulations**") set out Tribunal specific exemptions which may have an impact on the data subject rights set out above. For example, data subject rights are restricted to the extent that such a restriction is:

(a) necessary, and only for so long as is necessary, to safeguard a relevant objective (as defined in the Section 60 Regulations), and

(b) proportionate to the need to safeguard that relevant objective,

including, but not limited to, where the exercise of the right or compliance with the obligation, as the case may be, would:

(i) obstruct or otherwise prejudice, in whole or in part, the performance by the Tribunal of a relevant function (as defined in the Section 60 Regulations),

(ii) disclose that the Tribunal is performing a function in pursuit of a relevant objective, in a case in which such disclosure would be obstruct or otherwise prejudice the achievement of the relevant objective, or

(iii) prevent the Tribunal processing personal data to which the Section 60 Regulations apply for a period of time, in a case where any delay to the processing would obstruct or otherwise prejudice the achievement of a relevant objective.

10.3 Matters which are relevant in determining whether a restriction of a right or obligation is necessary to safeguard a relevant objective, and is proportionate to the need to safeguard that relevant objective are set out in Regulation 7(2) of the Section 60 Regulations.

10.4 The Section 60 Regulations also establish what the Tribunal must do where a right or obligation is restricted under their terms including in circumstances where the Tribunal does not have to notify a data subject about such restrictions.

10.5 Where data subject rights are not restricted by the Section 60 Regulations (or do not benefit from other exemptions under applicable Data Protection Law), the Tribunal is obliged to comply with the data subject rights as provided under Data Protection Law.

10.6 If a Covered Person receives a data subject request it should notify the Data Protection Officer without delay in order to facilitate the fulfilment of the data subject rights invoked by the data subject within the applicable timeline as provided in Data Protection Law.

## Section 3 – Dealing with Third Parties

### 1. Engaging Processors

1.1 A processor is a third party that processes personal data on behalf of the Tribunal.

1.2 If the Tribunal provides access to personal data to a third party, but that third party uses the personal data for its own purposes, this will be a controller to controller transfer (see below for further details).

1.3 The Record of Processing Activities (ROPA) sets out details of the processors that are engaged by the Tribunal. The details of processors in the ROPA must be kept up to date in accordance with the procedure set out in Section 4 – Documenting and Monitoring Compliance.

1.4 Prior to engaging processors, the Tribunal will:

(a) undertake due diligence to ensure that it is appropriate to engage the processor (and, if the processor is engaged will conduct a periodic review of the processor and its security and other relevant items from time to time); and

(b) ensure that it puts in place a written agreement with the processor that complies with the requirements under applicable Data Protection Law.

1.5 Details of arrangements that the Tribunal has in place with third party processors will be kept by the Data Protection Officer.

1.6 For further details of the records the Tribunal retains in relation to its dealings with third party processors, see Section 4 - Documenting and Monitoring Compliance.

### 2. Controller to Controller Transfers

2.1 In certain circumstances the Tribunal transfers personal data relating to Covered Persons to third parties, or allows third parties to have access to such personal data, on a controller to controller basis. This means that the third party will process such personal data for their own purposes and not on behalf of the Tribunal. By way of example, this will occur in the following circumstances:

(a) Pensions – When Covered Person data is provided to a pension service provider, the trustee(s) of the pension will be a controller in relation to such data. This data is then processed by the pension trustees (or the pension service provider) for the purposes of administering the pension;

(b) Health Insurance – When Covered Persons are provided with health insurance, the health insurance provider will be a controller in relation to the Covered Person data that is used to administer the insurance;

(c) Public Bodies – The Tribunal is required by law to transfer certain personal data to public bodies (e.g. the Revenue Commissioners of Ireland). The public body becomes a controller in relation to any personal data that it receives.

2.2 The Tribunal also transfers personal data related to data subjects other than Covered Persons to third parties, or allows third parties to have access to such personal data, on a controller to controller basis. These transfers are described in the Tribunal's Data Protection Notice.

2.3 Where there is a controller to controller transfer, the transferee is primarily responsible for complying with its own data protection obligations (i.e. the Tribunal is not responsible for ensuring that a transferee of personal data complies with that transferee's data protection obligations). Details of controller to controller transfers are set out in the ROPA. In the event that the transfer involves a transfer of data outside of the EEA, paragraph 3 below should be considered.

**3. Transfers of Personal Data Outside the European Economic Area (EEA)**

3.1 Under Data Protection Law, the Tribunal may not (save where one of a limited number of exemptions applies) transfer personal data outside of the EEA to any third country, unless that third country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of personal data.

3.2 This prohibition on transfers outside the European Economic Area will not apply if pursuant to Article 49 GDPR:

(a) The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) The transfer is necessary for the performance of a contract between the controller and data subject, or the implementation of pre-contractual measures taken at the data subject's request;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) The transfer is necessary for important reasons of public interest;

(e) The transfer is necessary for the establishment, exercise or defence of legal claims;

(f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case

3.3 In the alternative, the prohibition on transfers outside the European Economic Area will not apply if, pursuant to Articles 46 or 47 GDPR:

(a) A data transfer is made subject to appropriate safeguards as defined in Article 46(1) GDPR and in accordance with either Article 46(2) or Article 46(3) GDPR; or

(b) The data is transferred subject to a set of "Binding Corporate Rules" governing the transfer of data to third countries and such rules have been approved by the relevant data protection supervisory authorities and comply with Article 47 GDPR.

## Section 4 – Documenting and Monitoring Compliance

### 1. Ensuring Compliance

As noted above in Section 2, paragraph 8, the Tribunal is obliged to put in place policies and procedures to ensure that it can demonstrate its compliance under Data Protection Law. The Tribunal achieves this by maintaining the records referred to in Appendix 2 to this policy, and in accordance with the monitoring of compliance set out in this section.

### 2. Record of Processing Activities (ROPA)

2.2 The Tribunal is required to maintain an inventory of the personal data that it holds. The ROPA must include the following details about the Tribunal's processing of personal data:

(a) details of the controller(s);

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) details of transfers of personal data to a third country, including the identification of that third country;

(f) where possible, time limits for retention; and

(g) where possible, a description of the technical and organisational security measures that are undertaken to protect the data.

2.3 The Tribunal's ROPA is maintained by the Data Protection Officer and reviewed on an annual basis.

### 3. Privacy by Design and Default

3.1 Two of the key principles under Data Protection Law are that data protection compliance shall be implemented by design and by default, this means:

(a) **Data Protection by Design** - Data protection by design is the notion that the means and purposes of the processing of personal data are designed, from the beginning, with data protection in mind. The principle requires the Tribunal to implement both technical and organisational measures that will guarantee and protect the privacy of data subjects. The Tribunal seeks, where possible, to implement and practise methods of data minimisation (which could include, where feasible, the pseudonymisation of personal data). Other methods of data protection by design include staff training and audit and policy reviews in the context of data protection.

(b) **Data Protection by Default** – The Tribunal implements appropriate technical and organisational measures to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and their accessibility. In particular, such measures ensure that by default a data subject's personal data is not made accessible without the data subject's intervention to an indefinite number of natural persons.

3.2 The Tribunal ensures data protection by design and data protection by default through, among other things, following the procedures set out in paragraph 4 below, whenever it implements a new project.

**4. Data Protection Impact Assessments**

4.1 The Tribunal is obliged to ensure that a Data Protection Impact Assessment ("**DPIA**") is undertaken before commencing any processing that is likely to result in a "high risk" to data subject's rights and freedoms. For further details of the circumstances where a DPIA is required and when an alternative approach (privacy impact assessment or compliance paper) will be sufficient (including a template form of DPIA), Covered Persons should consult the Data Protection Impact Assessment Sub-Policy.

**5. Accuracy**

5.1 The Tribunal seeks to ensure that personal data is accurate and kept up-to-date. The Tribunal takes every reasonable step to ensure that any personal data that is inaccurate or out of date, having regard to the purposes for which it is processed, is erased or rectified without delay in accordance with the following procedures:

(a) The Tribunal reviews personal data held in relation to data subjects on a regular basis and updates, rectifies or erases it as necessary; and

(b) The Tribunal reviews its ROPA annually.

**6. Training**

6.1 The Tribunal ensures that Covered Persons whose roles involve the processing of personal data are made aware of and, when necessary, receive training in respect of data protection law and principles. Records of data protection training completed by Covered Persons are maintained by the Data Protection Officer.

**7. Data Minimisation**

7.1 Personal data should be adequate, relevant and limited to what is necessary for the purpose for which it is processed. As such, the Tribunal should only collect and process personal data which is relevant for the performance of its functions.

7.2 To ensure compliance with the principles of Data Protection Law (and any applicable statutory requirements in respect of the retention of records), the Tribunal's practice is to ensure that it collects and keeps only such personal data as is necessary for the purposes set out in its data protection notices.

## Section 5 – Data Security

### 1. Data Security

1.1 The Tribunal implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks to personal data that may arise in connection with the processing activities the Tribunal undertakes. Such measures include:

(a) the encryption and, where appropriate and feasible, pseudonymisation of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.2 In assessing the appropriate level of security, the Tribunal takes account of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

1.3 All Covered Persons who have access to the Tribunal's IT systems are subject to the Data Security Sub-Policy. Further details regarding the technical and security measures, and the organisational security measures, that are implemented by the Tribunal are set out in the Data Security Sub-Policy.

### 2. Data Security Incidents

2.1 Regardless of the measures that are taken in accordance with the above paragraph and related policies, there is always a risk of data security incidents arising. Data security incidents may range from relatively minor incidents, which do not actually result in unauthorised disclosure, loss, destruction or alteration of personal data, to major security incidents, such as the loss or theft of devices, such as laptops, which contain personal data.

2.2 The GDPR defines a 'personal data breach' as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.3 It is essential that all data security incidents are reported to the Data Protection Officer without delay, and that the following procedures are followed.

2.4 The Data Protection Officer shall consider whether the incident constitutes a personal data breach. If the incident does constitute a personal data breach, the Data Protection Officer shall consider whether a notification is required. The Data Protection Officer shall also take such steps as are required to stop, contain or mitigate the effects of the

data security incident and ensure that appropriate steps are taken in response to the incident, including the putting in place of new policies and procedures where necessary.

2.5 Where a personal data breach occurs, it must be reported to the competent supervisory authority without delay and, where feasible, not later than 72 hours after the Tribunal becomes aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

2.6 Where a personal data breach is likely to result in a high risk to the rights and freedoms of affected data subjects, then those data subjects must also be notified without undue delay. This obligation is restricted in certain circumstances set out in the Section 60 Regulations.

2.7 The Data Protection Officer shall also ensure that an appropriate record of the data security incident as well as any associated communications, are maintained in the Data Security Incident Log.

2.8 For further details of the types of personal data breach that are notifiable to supervisory authorities, and the content of notifications, Covered Persons should consult the Data Security Sub-Policy.

## Section 6 – Compliance and Enforcement

### 1. Data Protection Officer

1.1 Certain controllers and processors are required under Data Protection Law to appoint a Data Protection Officer.

1.2 The Tribunal has appointed a Data Protection Officer. Their contact details are:

Email: dpo@toidf.ie

Post: Data Protection Officer, Defence Forces Tribunal, Infinity Building, Third Floor, George's Court, George's Lane, Smithfield, Dublin, D07 E98Y.

### 2. Supervisory Authority

Each country in the EEA has a "Supervisory Authority" that oversees compliance with Data Protection Law. In Ireland, the Data Protection Commission (the "**DPC**") is the relevant Supervisory Authority.

### 3. Enforcement, Sanctions and Penalties

3.1 It is important that all Covered Persons comply with this policy and related policies and procedures, as a breach of Data Protection Law could result in serious consequences for the Tribunal. Such consequences could include the following:

(a) **Investigations, Audits and Criminal Penalties**

The DPC a wide range of investigation and enforcement powers, including the powers to investigate complaints, to carry out an audit of an organisation's compliance with Data Protection Law and the power to issue enforcement notices setting out steps which must be taken to rectify breaches of Data Protection Law. Failure to comply with enforcement actions by the DPC may result in a criminal offence;

(b) **Fines**

As the Tribunal is a public body, in addition to its investigation and enforcement powers, the DPC has the ability to levy fines of up to €1,000,000 for certain breaches of the GDPR.

3.2 All communications from a Supervisory Authority, must be forwarded immediately to the Data Protection Officer.

### 4. Interactions with Supervisory Authorities

All interactions with Supervisory Authorities will be recorded by the Data Protection Officer.

## Appendix 1 - Definitions

The following definitions are, in some cases, modified versions of definitions which are set out in the relevant Data Protection Law. For the exact wording of the relevant definition, please see the relevant Data Protection Law.

**Automated means** is, broadly speaking, processing using a computer or other electronic device.

**Data** means information in a form which can be processed. It includes both data processed by automated means and manual data.

**Controller or data controller** means any person who, either alone or with others, controls the purpose and means of the processing of personal data. Controllers can be either legal entities such as companies, government departments or voluntary organisations, or they can be individuals.

**Processor or data processor** means a person who processes personal data on behalf of a controller, but does not include a Covered Person of a controller who processes such data in the course of his/her employment.

**Data Protection Law** means the General Data Protection Regulation (EU Regulation 2016/679) and any implementing or supplementing legislation in Ireland, including the Data Protection Act 2018, the Data Protection Act 2018 (Section 38(4)(B)) (Defence Forces Tribunal Of Inquiry) Regulations 2024, the Data Protection Act 2018 (Section 51(3))) (Defence Forces Tribunal Of Inquiry) Regulations 2024 and the Data Protection Act 2018 (Section 60(6)) (Defence Forces Tribunal of Inquiry) Regulations 2025.

**Data subject** means an individual who is the subject of personal data.

**Manual data** means information that is recorded as part of a 'filing system', or with the intention that it should form part of a 'filing system'. 'Filing system' means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

**Personal data** means data relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental economic, cultural or social identity of a person). This can be a very wide definition, depending on the circumstances.

**Processing** means performing any operation or set of operations on personal data including: (a) recording the data; (b) collecting, organising, structuring, storing, altering or adapting the data; (c) retrieving, consulting or using the information or data; (d) disclosing the data by transmitting, disseminating or otherwise making it available; or (e) aligning, combining, restriction, erasing, or destroying the data.

**Special Categories of Personal Data** means personal data relating to an individual's: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life

or sexual orientation: individuals have additional rights in relation to the processing of any such data.

## Appendix 2 – Related Policies and Procedures

| | **Policy /Procedure** | **Kept by [business unit/location]** |
|---|---|---|
| 1. | Data Subject Rights Sub-Policy | Data Protection Officer |
| 2. | Data Security Sub-Policy | Data Protection Officer |
| 3. | Data Protection Impact Assessment Policy | Data Protection Officer |
| 4. | Record of Processing Activities (ROPA) | Data Protection Officer |

## Appendix 3 – Template Notice Concerning Disclosure of Third-Party Data

In order to respect the constitutional rights of all individuals to fair procedures and in keeping with existing legal principles, the Tribunal may, on occasion, be required to disclose personal data to third parties. Where this is the case, the Tribunal makes such disclosures on the basis of its legal obligation to do so, and in accordance with Article 6(1)(c) of the GDPR ('compliance with a legal obligation').

This Notice is made pursuant to Section 2, paragraph 2.4 (iii) of the Tribunal's Data Protection Policy ('Disclosure Required to Ensure the Constitutional Right to Fair Procedures') to notify you as a third party recipient of personal data of the principles that apply to your processing of that data.

This notice is not exhaustive and does not constitute legal advice. Recipients of data are advised to consult the text of the relevant laws and to seek independent legal advice in respect of their independent data protection obligations should they have queries.

**TAKE NOTICE:**

The purpose for which this personal data is being disclosed to you is to allow you, in accordance with your constitutional right to fair procedures, to address, fully, the issues raised within the documents that accompany this Notice and/or to respond to allegations made against you therein. Some of the documents being shared with you in order to vindicate your constitutional right contain personal data concerning third parties. In light of their competing rights of privacy and data protection, the disclosure of such personal data made by the Tribunal to you has been limited to what is strictly necessary in order to vindicate your right to fair procedures.

Furthermore, the Tribunal is sharing this personal data with you strictly on the following basis:

A. that you are subject to data protection obligations in your own right, as a separate and independent controller, in respect of your use of the personal data disclosed to you. You should read the full text of the GDPR and the Data Protection Act 2018 to understand your obligations in this respect;

B. that you will process the personal data you receive only to the extent reasonably required to vindicate your right to fair procedures and to deal with investigations in respect of the work of the Tribunal;

C. that you will not process or further process the data for any related or unrelated purpose and that you will not disclose it to others beyond what is necessary to vindicate your right to fair procedures in connection with the operation of the Tribunal;

D. that you will keep the personal data confidential and that the data, or any copies thereof, or matters referred to therein, will not be furnished to, distributed, disclosed or in any manner whatsoever disseminated, to any person, body corporate or party save as necessary to vindicate your right to fair procedures in connection with the operation of the Tribunal;

E. that, without prejudice to your obligation to keep the data confidential, you may use the materials shared with you – including any personal data contained therein – in order to obtain legal advice in connection with the operation of the Tribunal;

F. that you will implement appropriate security measures to ensure that the data will not be subject to any unauthorised access or any processing that is incompatible with the purpose for which the data is being shared;

G. that you will not retain the data for any longer than is strictly necessary;

H. that your failure to comply with your data protection and confidentiality obligations could result in material adverse consequences for you, including but not limited to an investigation by the Data Protection Commission and enforcement notices, adverse decisions and/or administrative fines levied by the Data Protection Commission as well as potential action by an affected data subject seeking appropriate judicial remedies.