LGL-POL-10

Torus Group Data Protection Policy

February 2025

0.	DOCUMENT CONTROL
0.1	SUMMARY
	The Subject of this document is the Data Protection Policy

0.2 DOCUMENT INFORMATION

Role	Name/Position	Date
Author	Andrew Wisedale (DPO)	Feb 2025
Approved by	Torus Group Board	Feb 2025
Document Reference	LGL-POL-10	

0.3 DOCUMENT STATUS HISTORY

Version	Date	Change owner	Reason for Update
1.	Nov 2018	Eric Summers	New Policy for "New Torus"
2.	Nov 2019	Ronnie Clawson	Annual Review
3.	Apr 2021	Ronnie Clawson	Annual Review
4.	June 2022	Stella Redford	Appendix added
5.	April 2024	Stella Redford	Review
6.	February 2025	Andrew Wisedale	General Review in line with best practice

0.4 DOCUMENT REVIEW DATE

Review Due	April 2026
Responsible Officer	DPO

0.5 DISTRIBUTION

Name / Department	Title
Torus	All staff
Torus	Initial EIA - All Staff

0.6 ASSOCIATED DOCUMENTS

Ref: ICT-POL 07 01	**Title: Information Security Management Policy**
Ref: LGL PRC 02 04	**Title: Data Breach Notification Procedure**
Ref: LGL PRC 04 05	**Title: Data Subject Rights (SAR) Procedure**

Ref: LGL PRC 05 01	**Title: Data Protection Impact Assessment (DPIA) Procedure**
Ref: GOV POL 07 02	**Title: Data Retention and Disposal Policy**
Ref: LGL-PRC-08-02	**Title: Group Data Sharing Procedure**
Ref - tbc	**Title: Appropriate Policy Document – Processing of Special Categories Personal Data and Criminal Offence Data**
Appendix 1	**Title: Glossary**
Appendix 2	**Title: Website Customer Privacy Notice**

Content Page

1. *Scope* 5
2. *Policy Statement* 6
3. *Roles and Responsibility* 6
4. *Equality and Diversity* 7
5. *Monitoring & Review* 7
6. *Appendix 1 Glossary* 7

1. Scope

1.1 This policy applies to all processing of personal data by, within, or on behalf of Torus Group and any members of the Group including: Torus62 Limited; Torus Foundation, Torus62 Developments Limited and Housing Management Solutions Limited (collectively referred to as Torus').

1.2 The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person. Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

1.3 Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

1.4 This policy provides a framework for ensuring that Torus meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). It applies to all the processing of personal data carried out by Torus including processing carried out by joint controllers, contractors, and processors. Torus complies with data protection legislation guided by the six data protection principles.

1.5 In summary, they require that personal data is:

- Processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

1.6 In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes the overarching Associated Documents listed above.

2. Policy Statement

2.1 Torus is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about customers, staff or those who work or interact with us.

2.2 Information Asset Owners – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with a network of teams and staff with information management responsibilities aid Torus in managing personal data and its associated risks.

2.3 Privacy Notices - we publish a privacy notice on our website and provide timely notices where this is required. We also publish an employee privacy notice and keep it up to date.

2.4 Training - we require all staff to undertake mandatory training on information governance and security which they re-take every year. In addition, all staff are required to complete a more detailed data protection training module as part of their induction.

2.5 Breaches - we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.

2.6 Information Rights - we have a dedicated team and clear processes to handle subject access requests and other information rights requests.

2.7 Data Protection by Design and Default - we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

2.8 Records of Processing Activities (ROPAs) - we record our processing activities and publish our policy document on processing of special category data.

2.9 Policies and Procedures - we produce policies and guidance on information management and compliance that we communicate to staff.

2.10 Communications - We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

2.11 Contracts - Our procurement department oversee that our contracts are compliant with UK GDPR.

3. Roles and Responsibility

3.1 We have an established Risk Management Framework that ensures the risk to personal data across the Torus is identified and appropriately managed. This network's detailed roles and responsibilities comprises:

3.2 Data Protection Management Group (DPMG) is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Chief Financial Officer, Executive Management Team (EMT) and Group Audit & Risk Committee on information governance with data protection and compliance decisions.

3.3 Data Protection Officer (DPO) The Torus Data Protection Officer (DPO) is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance. The Torus DPO can be contacted at DPO@torus.co.uk

3.4 The Chief Financial Officer, EMT, owns the overall risk arising from the processing personal data by Torus.

3.5 Other roles Specific roles are assigned throughout our corporate hierarchy to manage personal data we process and the associated risks in terms of responsibilities, decision making and monitoring compliance.

3.6 Information Asset Owners (IAOs): IAOs have local responsibility for data protection compliance in their area/directorate.

3.7 Information Asset Managers (IAMs): support IAOs in complying with their duties regarding the processing of personal data.

3.8 Local Information Management Officers (LIMOs/ Data Champions): advise their departments on information management and carry specified information management tasks.

3.9 Several teams are responsible for issuing, reviewing and communicating corporate information management standards and procedures. The teams also advise on compliance with data protection and implement IT solutions to ensure we take privacy by design approach.

4. Equality and Diversity

Torus is dedicated to fostering an inclusive and diverse environment in all aspects of its operations, including data protection. We are committed to treating all individuals with fairness, dignity, and respect, regardless of their characteristics or backgrounds. Our data protection practices align with the principles of equality and diversity, aiming to eliminate discrimination and ensure equitable treatment. We recognise the importance of diversity in decision-making processes and strive to create an atmosphere where all individuals, regardless of race, ethnicity, gender, sexual orientation, disability, age, religion, or any other protected characteristic, feel valued and included.

5. Monitoring & Review

The policy is owned, updated, and reviewed by the Group Data Protection Officer.

The policy will be reviewed every year unless there is a change in legislation which means that it must be amended before that date.

6. Appendix 1 Glossary

Data Protection Legislation	the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018) sets out legal responsibilities on all organisations processing personal data and established rights for individuals whose data is being processed. Penalties can be imposed on organisations processing personal data including fines of up to £ 17,500,000 or 4% of total annual turnover, whichever is higher. There are several criminal offences set out in the Act and individuals can be held accountable and be sentenced by the courts for any offences committed.
Data Controller	Any organisation that determines the purposes and means of the processing of personal data.
Data Processor	This is a third party who collects an/or uses personal data on behalf of the Data Controller (Torus Group). These typically include our outsources third party suppliers, such as suppliers who manage our IT systems, document shredding companies, those who host our application, such as our e-learning platform.
Data subject	an individual whose data is collected, held, and/or processed by a data controller for varying purposes and who can be identified, directly or indirectly, by reference to such personal data.

Personal data	Any information relating to an identified or identifiable natural person, including a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Natural person	A living human being.
Special Categories of Personal Data	means any personal data revealing racial or ethnic origin, political. opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; The processing of this data needs greater protection.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Information Incident	means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information.
Personal Data Breach	means 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.
Risk	The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Corporate Data	Corporate data relates to any sensitive corporate information including meeting schedules, agendas, and minutes of meetings; financial accounts; contracts; and organisational policies and procedures.
Recipient	means a natural or legal person, public authority, agency, or another body, to which the personal data is disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of that data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party	Means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Profiling	Is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.
Consent	Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which the person, by way of a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
Data Protection by design and default	The UK GDPR requires organisations to integrate data protection concerns into every aspect of their processing activities. This approach is 'data protection by design and by default'. It is a key element of the UK GDPR's risk-based approach and its focus on accountability, i.e. An Organisation's ability to demonstrate how you are complying with its requirements.