GDPR Personal

Data Protection Policy

Version: 2.0

Date: 01/10/2022

Document Control

1.	**Document Title**	**GDPR Personal Data Protection Policy (GDPR PDPP)**
2.	Document Code	TV-GDPR-PDPP-01
3.	Date of Release	01/10/2022
4.	Document Superseded	NA
5.	Version No.	2.0
6.	Document Owner	Security Team
7.	Document Author(s)	DPO
8.	Document Location	
9.	Last Review	January 2022
10.	Next Review	June 2023

Document Approvers

Name	**Title**	**Date of Approval**	**Version No**

Version History

Version No	**Version Date**	**Author**	**Summary of Changes**
1.0	01/10/2022	CISO	First Issue
2.0	02/15/2022	CISO	

Table of Contents

Introduction

In its everyday business operations Tovie AI Limited, hereinafter referred to as the «Company», makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Consumers, customers, suppliers, business partners
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Tovie AI Limited is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization’s information systems, including board members, directors, employees, suppliers and other third parties who have access to Company systems.

The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is a standout amongst the most noteworthy bits of enactment influencing the way that Company does its data preparing exercises. Huge fines are relevant if a break is esteemed to have happened under the GDPR, which is intended to secure the individual information of nationals of the European Union. It is Company strategy to guarantee that our consistence with the GDPR and other important enactment is clear and verifiable consistently.

GDPR Fundamental concepts

The most important concepts from GDPR regulation that are consistent within our organization and apply properly for this policy are the following:

Personal data is defined as:

any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'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;

'controller' means*:*

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Principles relating to processing of personal data

As per GDPR regulation, 2016 version, there are 7 principles involving personal data and how companies should treat these aspects. These are as follows, as per Chapter II, Article 5.1

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Company complies with these principles by using business workflows based on technology that use metadata in order to search, discover, classify, label, protect and apply actions at all levels of personal data. Also, Operational Security Procedures

defined support and provide the specific guidelines for all teams involved including IT Support, Customer Support or Line of Business

Our staff responsibilities

Any staff member of ***Company*** who is involved in the collection, storage or processing of personal data has responsibilities under the legislation.

Any staff member involved in the processing/storing of personal data should make sure;

- to obtain and process personal data fairly.
- to keep such data only for explicit and lawful purposes.
- to disclose such data only in ways compatible with these purposes
- to keep such data safe and secure.
- to keep such data accurate, complete and up-to-date.
- to ensure that such data is adequate, relevant and not excessive.
- to retain such data for no longer than is necessary for the explicit purpose.

Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Company that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown below:

Data Subject Request	**Deadline**
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Consent

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In case of children below the age of 16 parental consent must be obtained. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data are not obtained directly from the data subject then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

Privacy by Design

Company has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation should be considered where applicable and appropriate.

Transfer of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an

appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, ***Company*** require a Data Protection Officer to be appointed.

Breach Notification

It is Tovie AI Limited policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our *Information Security Incident Response Procedure* which sets out the overall process of handling information security incidents.

Addressing Compliance to the GDPR

The following actions are undertaken to ensure that Tovie AI Limited complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place

- Personal data retention schedules
- Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management review process of the information security management system.

Our Obligations as a Cloud Service Provider

In addition to holding personal data on our own account, Tovie AI Limited also stores and processes the personal data of our cloud customers. In doing so, there are a number of additional obligations that must be fulfilled to allow our customers to stay within the law. Our policy in this area is informed by *ISO/IEC 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* which, as well as recommending specific enhancements to ISO/IEC 27001 controls, also provides the following policy guidance:

- We provide our customers with the facilities to meet their obligations under law in activities such as accessing, amending and erasing individuals' PII
- We only use the cloud customer's PII for their purposes, not our own
- The customer is informed if we are required by law to disclose any of their data, unless we are prohibited from doing so
- Details of disclosures are recorded
- We tell our customers if we use sub-contractors to process their PII
- We tell our customers if their PII is subject to unauthorized access.

------ End of the Document ------