GDPR Policy

Policy Statement:

Transwaste is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets forth the expected behaviors of Transwaste employees and third parties in relation to the collection, retention, transfer, disclosure and destruction of any personal data belonging to a Transwaste contact.

Personal data is any information (including opinions and intentions) which related to an identified or Identifiable Natural Person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data.

Transwaste is fully committed to ensuring continued and effective implementation of this policy and expects all Transwaste employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction. This policy applies to all processing of personal data in electronic form or where it is held in manual files that structured in a way that allows ready access to information about individuals.

Policy Dissemination & Enforcement

Transwaste will ensure that all employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, Transwaste will make sure all third parties engaged to process personal data on their behalf are aware of and comply with the content of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Transwaste.

Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Transwaste entities in relation to this policy, we will carry out annual data protection compliance audits, each audit will, as a minimum, assess:

- The assignment of responsibilities
- Raising awareness
- Training for employees
- The effectiveness of data protection related to operational practices including data transfers, incident management, complaints handling
- The level of understanding of data protection policies and privacy notices

Data Protection Principles

Transwaste has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

1. **Lawfulness, Fairness and Transparency** – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, Transwaste must tell the data subject what processing will occur, the processing must match the description given to the data subject and it must be for one of the purposes specified in the applicable data protection regulation.
2. **Purpose Limitation** – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner this is incompatible with those purposes. This means Transwaste must specify exactly what the personal data collected will be used for a limit the processing of that personal data to only what is necessary to meet the specified purpose.
3. **Data Minimisation** – Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Transwaste must not store any Personal Data beyond what is strictly required.

4. **Accuracy** – Personal data shall be accurate and kept up to date. This means Transwaste must have in place processed for identifying and addressing out of date, incorrect and redundant personal data.
5. **Storage Limitation** – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means Transwaste must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.
6. **Integrity & Confidentiality** – Personal data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. Transwaste must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.
7. **Accountability** – The data controller shall be responsible for and be able to demonstrate compliance. This means Transwaste must demonstrate that the data protection principles outlined above are met for all personal data for which it is responsible.

Data Processing

Transwaste uses the personal data of its contacts for the following broad purposes:

- the general running and business administration of Transwaste entities
- to provide services to Transwaste customers
- the ongoing administration and management of customer services

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained before processing may commence.

Digital Marketing

As a general rule Transwaste will not send promotional or direct marketing material to Transwaste contact through digital channels such as mobile phones, email and the internet, without first obtaining their consent. Any Transwaste entity wishing to carry out a digital marketing campaign without obtaining prior content from the data subject must first have it approved by the data protection officer. It should be noted that where digital marketing is carried out on a 'business to business' context there is no legal requirements to obtain an indication of content to carry out digital marketing to individuals provided that they are given the opportunity to opt- out.

Data Retention

To ensure fair processing, personal data will not be retained by Transwaste for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which Transwaste entities need to retain personal data is set out in the Transwaste Control of Documents Procedure. This takes into account the legal and contractual requirements that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Each Transwaste entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorized alteration, access or processing and other risks to which it may be exposed by virtue of human action or the physical or natural environment. The minimum set of security measure to be adopted by each Transwaste entity is provided in the Transwaste Cyber Security Policy.

Data Subject Requests

If an individual makes a request Transwaste will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data subjects are entitled to obtain, based upon a request made in writing and upon successful verification of their identity, the following information about their own personal data:

- the purposes of the collection, processing, use and storage of their personal data
- the source of the personal data, if it was bot obtained from the data subject
- the categories of personal data stored for the data subject
- the recipients or categories to whom the personal data has been or may be transmitted, along with the location of those recipients
- the envisaged period of storage for the personal data or the rationale for determining the storage period
- the use of any automated decision-making, including profiling

Law Enforcement Requests & Disclosures

In certain circumstances it is permitted that personal data is shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- the assessment or collection for a tax or duty
- by the order of a court or by any rule of law

If a Transwaste entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any Transwaste entity receives a request from a court or any regulatory or law enforcement authority for information relating to Transwaste you must notify the data protection officer immediately who will provide comprehensive guidance and assistance.

Complaints Handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to the data protection officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. If the issue cannot be resolved through consultation between the data subject and the data protection officer then the data subject may at their option seek redress through mediation, binding arbitration, litigation or via complaint to the Data Protection Authority within the application jurisdiction.

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Office of Data Protection providing a description of what occurred.

Mark Hornshaw
Managing Director

01/10/20

Information Notification to Data Subjects

The table below outlines the various information elements that must be provided by the data controller to the data subject depending upon whether consent has been obtained from the data subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the data controller and where applicable of the data controllers' representatives	✓	✓
The original source of the personal data, and if applicable whether it came from a publicly accessible source		✓
The contact details for the data protection officer where applicable	✓	✓
The purposes and legal basis for processing the personal data	✓	✓
The categories of personal data concerned	✓	✓
The recipients or categories of recipients of the personal data	✓	✓
Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was originally collected, the data controller shall provide the data subject prior to that further processing with information on that other purpose.	✓	✓
Where the data controller intends to transfer personal data to a recipient in a third country, notification of that intention and details regarding adequacy decisions taken in relation to the thirds country must be provided	✓	✓
The period for which the personal data will be stored, or if that is not possible the criteria used to determine that period	✓	✓
Where applicable the legitimate interests pursued by the data controller or by a third party	✓	✓
The existence of data subject rights allowing them to request from the data controller – information access, objection to processing, objection to automated decision making and profiling, restriction of processing data portability, data rectification and data erasure.	✓	✓
Where processing is based on consent the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal	✓	
The right to lodge a complaint with a Data Protection Authority	✓	✓
Whether the provision of personal data is a statutory or contractual requirements a requirement necessary to enter into a contract as well as whether the data subject is obliged to provide the personal data and if so the possible consequences of failure to provide such data	✓	✓