GENERAL DATA PROTECTION REGULATION (GDPR)

DAMREV (Pty) Ltd “DAMREV",

Registration Number 2023/162999/07

DAMREV Token Proprietary Limited with Registration Number 2024/356679/07 is a wholly owned subsidiary of DAMREV Proprietary Limited. Collectively, these entities constitute "**DAMREV**."

DAMREV is a leading FinTech service provider specializing in ISO 20022 Blockchain Tokenization and Smart Contract Development. The company focuses on Security Token Offerings (STOs) and employs the Stellar Blockchain to tokenize real-world assets.

DAMREV reserves the right to update, revise, or modify the contents of this document at any time without prior notice. The information contained herein is provided "as is" and DAMREV makes no representations or warranties, express or implied, regarding the accuracy, completeness, or reliability of the information.

Any references to third-party products, services, or information are not intended to constitute an endorsement or recommendation by DAMREV. All third-party trademarks, service marks, logos, and trade names used in this document are the property of their respective owners.

For permissions, inquiries, or further information, please contact the DAMREV compliance team at: compliance@damrev.com.

VERSION HISTORY.

Version	Release Date	Notes
1.0	24 June 2024	Original Published Version

TABLE OF CONTENTS.

1. INTRODUCTION TO THIS GDPR POLICY.

This GDPR policy ensures DAMREV:

- Complies with data protection law and follows good practice;
- Protects the rights of staff, clients, and partners;
- Is open about how it stores and processes individuals' data;
- Protects itself from data protection risks such as breaches of confidentiality, failure to offer choice, and reputational damage.

This GDPR policy applies to:

- The DAMREV offices;
- All staff of DAMREV;
- All contractors, suppliers, and other people working on behalf of DAMREV.

The General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998 from 25th May 2018. It applies to both data controllers and data processors, who have day-to-day responsibility for data protection.

2. PRINCIPLES OF GDPR.

Article 5 of the GDPR

Under the GDPR, the data protection principles set out the main responsibilities for organizations. The principles are similar to those in the Data Protection Act, with added detail at certain points and a new accountability requirement. Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner in relation to individuals;
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

- 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;
- 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;
- 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, using appropriate technical or organizational measures.

The Accountability Principle

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." The new accountability principle requires organizations to show how they comply with the principles of GDPR. This can be done by:

- Maintaining relevant documentation on processing activities;
- Implementing appropriate technical and organizational measures that ensure and demonstrate compliance;
- Implementing internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- Implementing measures that meet the principles of data protection by design and data protection by default.

Data Protection By Design

Data protection by design is an approach that promotes privacy and data protection compliance from the start. Privacy and data protection should be a key consideration in the early stages of any project, and then throughout its life-cycle. For example when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy, or strategies that have privacy implications;
- Embarking on a data sharing initiative;
- Using data for new purposes.

3. LAWFULNESS OF PROCESSING CONDITIONS.

Under the GDPR, there is a requirement to have a valid lawful basis in order to process personal data. There are six available lawful bases for processing set out in Article 6 of the GDPR:

- Consent: the data subject has given clear unambiguous consent for their personal data to be processed for a specific purpose;
- Contract: processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
- Legal obligation: processing is necessary for compliance with a legal obligation;
- Vital interests: processing is necessary to protect the vital interests of a data subject or another individual;
- Public task: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Legitimate interests: processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject.

4. OUR LAWFUL BASES FOR PROCESSING.

Our lawful basis for processing the personal data of clients is that processing is necessary to perform or enter into the contract we have with them to undertake email infrastructure and related services, as outlined in their engagement letter and the terms of business.

Our lawful basis for processing the personal data of employees is that processing is necessary to perform or enter into the employment contract we have with them.

Our lawful basis for processing the personal data of employees in relation to PAYE, pension contributions, and other personal data shared with HMRC is that processing is necessary for compliance with the law.

Our lawful basis for holding the personal data of potential employees/candidates is that we have a legitimate interest in deciding whether to recruit them. Should a candidate be unsuccessful, this legitimate interest will cease to exist and any personal data held on unsuccessful candidates must be deleted/destroyed within three months, as agreed by the directors.

We will only process personal data in relation to marketing activities if we have clear consent from the data subject. This covers contacting clients regarding:

- Networking and similar events;
- Newsletters and updates;
- Additional products/services we can offer such as fee protection;
- Cloud-based software and other applications that we believe could be of interest to you.

We are under legal obligation to hold company and accounting records (on behalf of our clients) for 6 years from the end of the last company financial year they relate to, or longer if:

- They show a transaction that covers more than one of the company's accounting periods;
- The company has bought something that it expects to last more than 6 years, like equipment or machinery.

We therefore have a legal obligation to hold personal data relating to these company records for approximately 7 years. We may keep these records for longer than 7 years if we have a legitimate interest to do so. Payroll records will be kept for 7 years, as agreed by the directors.

5. DATA CONTROLLERS & DATA PROCESSORS.

The GDPR applies to data controllers and data processors. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

Obligations as the Data Controller

When processing personal information for email infrastructure and related services, DAMREV acts as the data controller and will therefore comply with the following obligations:

- Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected;
- Whenever the data controller uses a data processor, it needs to have a written contract in place;
- The data controller must ensure written contracts between data controllers and processors comply with GDPR. Contracts must include the following details:
    - The subject matter and duration of the processing;
    - The nature and purpose of the processing;
    - The type of personal data and categories of data subject;
    - The obligations and rights of the controller;
    - The obligations of the processor.
- As a matter of good practice, contracts should state that nothing within the contract relieves the data processor of its own direct responsibilities and liabilities under the GDPR;
- As a matter of good practice, contracts should reflect any indemnity that has been agreed;
- Data controllers must record and report any serious data breaches to the Information Commissioner's Office (ICO);
- Controllers have a legal obligation to give effect to the rights of data subjects.

Obligations as the Data Processor

For services such as Email Infrastructure Resellers/Partners where DAMREV processes personal data on behalf of its client, the company acts as the data processor and the client acts as the data controller. DAMREV will therefore comply with the following obligations placed on it as the data processor, under the GDPR:

- The data processor must have adequate security measures in place for processing personal data;
- The data processor must only act on the documented instruction of the data controller unless required by law to act without such instruction;
- The data processor must ensure that the people processing the data are subject to a duty of confidence;
- The data processor will only engage a sub-processor with the prior consent of the data controller and a written contract;
- The data processor will assist the data controller in meeting their GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments;
- The data processor must maintain records of personal data and data processing activities;
- The data processor must inform the data controller if it becomes aware of any breach of personal data;
- The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.

6. DESCRIPTION OF OUR PROCESSING ACTIVITIES

Each controller must keep records of its processing activities, including:

- The contact details of the controller/representative;
- The purposes of the processing;
- The categories of data subjects and personal data processed;
- The categories of recipients with whom the data may be shared;
- Information regarding Cross-Border Data Transfers;

- The applicable data retention periods; and
- A description of the security measures implemented in respect of the processed data.

Upon request, these records must be disclosed to data protection authorities.

DAMREV processes personal information in order to:

- Provide email Infrastructure-related services;
- Maintain its own accounts;
- Support and manage its employees.

The company processes personal information about customers and clients, advisers and other professional experts, and employees.

This information may include:

- Personal details;
- Family, lifestyle, and social circumstances;
- Goods and services;
- Financial details;
- Education details;
- Employment details.

DAMREV also processes sensitive classes of information that may include:

- Physical or mental health details;
- Racial or ethnic origin;
- Religious or other beliefs;
- Trade union membership.

DAMREV's processing activities do not involve automated decision making or profiling.

Sharing Personal Information

The company may need to share the personal information it processes with the individual themselves and also with other organizations. Where this is necessary, the company is required to comply with all aspects of the GDPR. Where necessary or required, the company shares information with:

- Business associates, professional advisers;
- Family, associates, and representatives of the person whose personal data is being processed;
- Suppliers;
- Local and central government;
- Financial organizations;
- Ombudsmen and regulatory authorities;
- Credit reference and debt collection agencies;
- Healthcare professionals, social, and welfare organizations;
- Current, past, or prospective employers;
- Examining bodies;
- Service providers.

Transferring Personal Information Overseas

It may sometimes be necessary to transfer personal information overseas. When this is needed, information is only shared within the European Economic Area (EEA). Any transfers made will be in full compliance with all aspects of the GDPR.

Retention of Personal Data

It has been agreed that personal data held on clients, including data within billing and usage, will be kept by the company for 7 years after:

- The date at which the client ceases to be our client.

After this, the records will be deleted/destroyed.

The company may, however, keep clients' records for longer than 7 years, where it believes it has a legitimate interest/reason to do so.

Any personal data held on potential employees/candidates, which prove unsuccessful, will be deleted/destroyed within three months.

Retention periods for personal data held on employees vary according to the category of data. Retention of personal data held on employees is not outlined in this policy document but details can be obtained from the board.

7. THE RIGHTS OF DATA SUBJECTS.

The GDPR provides the following rights for individuals:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

The Right to be Informed

We are obliged to provide ‘fair processing information’, typically through a privacy notice or policy document. The information that must be supplied includes:

- Identity and contact details of the data controller;
- Purpose of the processing and the lawful basis for the processing;
- The legitimate interests of the controller;
- Any recipient or categories of recipients of the personal data;
- Retention periods;
- The rights of the data subjects;
- The existence of any automated decision making and profiling.

If the data is obtained directly from the data subject, the information should be provided at the time the data is obtained. If the data is not obtained directly from the data subject, the information should be provided:

- Within one month of obtaining the data;
- When the first communication takes place;
- Before the data is disclosed to another recipient if disclosure to another recipient is envisaged.

The information we supply individuals about the processing of personal data must be:

- Concise, transparent, intelligible, and easily accessible;
- Written in clear and plain language;
- Free of charge.

Right of Access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

The company must provide a copy of the information free of charge. However, it can charge a ‘reasonable fee’ when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Information must be provided without delay and at the latest within one month of receiving the request. The company will be able to extend the period of compliance by a further two months where requests are complex or numerous.

The company must verify the identity of the person making the request, using ‘reasonable means’. If the request is made electronically, the company should provide the information in a commonly used electronic format.

Where requests are manifestly unfounded or excessive, the company can:

- Charge a reasonable fee based on administrative costs; or
- Refuse to respond.

If the company refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If the company has disclosed the personal data to others, it must contact each recipient and inform them of the rectification unless this proves impossible or involves disproportionate effort.

A request for rectification must be responded to within one month. This can be extended by two months where the request is complex.

Right to Erasure / Right to be Forgotten

The right to erasure enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data has to be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and the company can refuse to deal with a request. This is where the personal data is processed:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research, or statistical purposes; or
- For the exercise or defense of legal claims.

If the company has disclosed the personal data to others, it must contact each recipient and inform them of the erasure of the personal data unless this proves impossible or involves disproportionate effort.

Right to Restrict Processing

Individuals have a right to ‘block’ or suppress processing of personal data. When processing is restricted, the company is permitted to store the personal data, but not further process it. The company can retain just enough information about the individual to ensure that the restriction is respected in the future.

The company will be required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, the company should restrict the processing until it has verified the accuracy of the personal data;
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the company is considering whether its legitimate grounds override those of the individual;
- When processing is unlawful and the individual opposes erasure and requests restriction instead;

- If the company no longer needs the personal data but the individual requires the data to establish, exercise, or defend a legal claim.

If the company has disclosed the personal data to others, it must contact each recipient and inform them of the restriction on the processing of the personal data unless this proves impossible or involves disproportionate effort. The company must inform individuals when it decides to lift a restriction on processing.

Right of Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The company must provide the personal data in a structured, commonly used, and machine-readable form. This should enable other data controllers to use the data.

The information must be provided free of charge. The company must respond without undue delay, and within one month.

Right to Object

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

Individuals must have an objection on “grounds relating to his or her particular situation”.

The company must stop processing the personal data unless:

- It can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or
- The processing is for the establishment, exercise, or defense of legal claims.

The company must inform individuals of their right to object “at the point of first communication” and in their privacy notice. This must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

The company must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

If the company’s processing activities are carried out online, it must offer a way for individuals to object online.

Rights in Relation to Automated Decision Making & Profiling

The GDPR has provisions on automated decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

Organizations can only carry out this type of decision-making where the decision is:

- Necessary for the entry into or performance of a contract; or
- Authorized by Union or Member state law applicable to the controller; or
- Based on the individual’s explicit consent.

DAMREV confirms its processing activities do not involve automated decision making or profiling.

8. OUR RESPONSIBILITIES.

Everyone who works for or with DAMREV has some degree of responsibility for ensuring data is collected, stored, and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. The board of directors is ultimately responsible for ensuring that DAMREV meets its legal obligations.

Key Areas of Responsibility

- The board must be kept updated about GDPR responsibilities, risks, and issues;
- The company must demonstrate compliance with the data protection principles and GDPR;
- The company should implement appropriate technical and organizational measures to ensure and to demonstrate that processing activities are compliant with the GDPR;
- All data protection procedures and related policies will be reviewed every three years, as agreed by the directors;
- Training and advice on data protection should be arranged for the people covered by this policy;
- The data protection representative, Duane Herholdt, should handle data protection questions from staff and anyone else covered by this policy;
- The organization should deal with requests from individuals such as right of access or right to be forgotten;
- The organization should address any data protection queries from journalists or the media;
- Any third-party services the organization is considering using to store or process data should be evaluated;
- Contracts with third parties and processors that may handle the company's sensitive data should be checked and reviewed;
- All systems, services, and equipment used for storing data must meet acceptable security standards;
- Regular checks and scans should be performed to ensure security hardware and software is functioning properly;
- Data protection statements attached to communications such as emails should be approved and updated when necessary;
- Marketing initiatives should abide by GDPR principles;
- Adequate data protection procedures should be in place for when an employee leaves;

- Data breaches should be recorded, serious data breaches should be reported to the ICO, and high-risk breaches should be reported to the affected data subjects;
- Following any breaches, the company should review the adequacy of its security measures;
- The company should make sure individuals are aware that their data is being processed, how the data is being used, and how to exercise their rights;
- The company must have a lawful basis for all processing activities;
- The company should make sure this policy document is made available to potential and existing clients and employees;
- The company must ensure they continue to be registered as a data controller with the ICO.

9. PRACTICAL SECURITY MEASURES.

Office Building

- The building is alarmed outside of office hours;
- Visitors can only enter with authorization from reception;
- Employees require office keys to enter the building;
- The reception area is not left unattended if there are visitors in the building;
- Cleaners are subject to a duty of confidence and must sign a confidentiality agreement.

General Staff Guidelines

- Employees should keep all data secure by taking sensible precautions and following the guidelines below;
- DAMREV will provide training to all employees to help them understand their responsibilities;
- Employees should request help from the data protection representative, Duane Herholdt, if they are unsure about any aspect of data protection;
- The only people able to access data covered by this policy should be those who need it for their work;

- Personal data should not be disclosed to unauthorized people, either within the company or externally;
- Employees should only process personal data electronically from the company's remote desktop and keep their credentials secure;
- Employees must maintain their duty of confidence as outlined in their confidentiality agreements.

Data Storage

- Servers containing personal data should be sited in a secure location, away from general office space;
- Data should be backed up frequently and these backups should be tested regularly;
- All servers and computers containing data should be protected by approved security software and a firewall;
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts;
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones;
- Employees should not save copies of personal data to their own computers or the normal desktop;
- Payroll details held electronically should be password protected and payroll details held manually should be retained in files within a secure environment;
- Backups transferred to memory sticks should be password protected;
- Employees should keep memory sticks in a secure place when not in use;
- The company should keep account of the number of memory sticks in use; employees should limit how many memory sticks they use;
- Personal data stored on memory sticks should be protected as much as possible;
- Data stored on memory sticks should be cleared regularly;
- Personal data stored or printed out on paper should be kept in a secure location where unauthorized people cannot see it;

- Data printouts should be shredded and disposed of securely when no longer required;
- When working from home or at clients' premises, or if visitors are in the office, employees should ensure computer screens are locked when left unattended;
- Personal data should never be transferred outside of the European Economic Area;
- When using clients' laptops in the office, employees should ensure access is restricted and that laptops are kept locked away overnight;
- When using clients' remote desktops, written consent must be given and access must be restricted;
- When taking files and records containing personal data out of the office, employees should take reasonable measures to ensure the data is protected and that no unauthorized persons access the data;
- Employees should be encouraged to use lockable briefcases to take client's personal files out of the building.

Data Accuracy

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible;
- Staff should take every opportunity to ensure data is updated; data should be updated as inaccuracies are discovered;
- DAMREV must make it easy for data subjects to update their information that is held by the company.

Emailing Personal Data

- In order to increase the security of personal data, the company has agreed that documents containing clients' personal data should not be emailed as email is not considered a secure method of communication;
- Documents containing personal data should be shared between the company and clients through DAMREV's Secure Portal, a cloud application that allows secure file exchange and electronic document approval;

- Clients have their own login and create their own password, making the process more secure;
- If a client wishes to use email communication for sharing such data, they should have a discussion with us;
- Attachments to emails containing personal data should be password protected or encrypted if this is possible.

Procedures for & when an Employee Leaves

- Office keys must be returned;
- Office memory sticks must be returned;
- Ensure no files and records are still at the employee's residence;
- Ensure no files are kept on the employee's desktop at home;
- Remove employee access/login to remote desktop;
- Change passwords for portal logins;
- Redirect emails to a director;
- Check the employee cannot access work emails from their phone;
- Remove the employee's CRM login, and remove credentials for any other cloud-based software used for clients' data;
- Remove their GitLab login.

10. RECORDING & REPORTING A DATA BREACH.

What Constitutes a Personal Data Breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Recording a Breach

All data breaches should be recorded internally, using the DAMREV Data Protection Breach Report Form. This form should be completed by the member of staff who discovered the breach, a member of staff who has knowledge of the company's data protection procedures in place, and the decision as to

whether to report the breach must be signed off by the directors. Completing this form will assist the company when and if the breach is reported.

How We Decide Whether to Report a Breach?

Each case must be considered on its own merits. Breaches that are considered by the company to be 'serious' should be reported to the Information Commissioner's Office (ICO). The seriousness of a breach will depend on:

- The potential detriment to data subjects;
- The volume of personal data lost / released / corrupted;
- The sensitivity of the data lost / released / corrupted.

The potential detriment to individuals is the overriding consideration in deciding whether to report a breach of security. Detriment includes emotional distress as well as both physical and financial damage. Where there is significant actual or potential detriment as a result of a breach, whether due to the volume of data, its sensitivity, or the combination of the two, there should be a presumption to report.

There is no need to report a breach if it is "unlikely to result in a risk to the rights and freedoms of natural persons".

How do We Report a Breach?

The company has 72 hours from the time it becomes aware of a reportable breach within which to report it.

Serious breaches should be reported to the ICO using the DPA security breach helpline on 0303 123 1113. To report the breach in writing, use the DPA security breach notification form (found on the ICO website www.ico.org.uk) and send it to casework@ico.org.uk or by post to Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. The ICO will then advise what to do next.

The company has agreed that serious breaches will be reported to the ICO by Duane Herholdt.

Should We Notify the Data Subject(s) Affected?

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the breach must also be reported to the affected individual(s) without undue delay.

The company has agreed that individuals will be notified of a breach in writing by Duane Herholdt.

11. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS).

Purpose of DPIAs

Data Protection Impact Assessments (DPIAs) are a tool used to identify and mitigate data protection risks in new projects. DAMREV will conduct DPIAs for any new processing activities or significant changes to existing processing activities.

When to Conduct a DPIA

A DPIA should be conducted when:

- Introducing new technologies or systems that process personal data;
- Undertaking large-scale processing of sensitive data;
- Processing personal data that is likely to result in a high risk to the rights and freedoms of individuals.

Process for Conducting a DPIA

The DPIA process involves:

- Identifying the need for a DPIA;
- Describing the processing activities;
- Assessing the necessity and proportionality of the processing;
- Identifying and assessing risks to individuals;
- Identifying measures to mitigate the risks;

- Consulting with relevant stakeholders, including data subjects where appropriate;
- Documenting the DPIA and its outcomes.

12. INTERNATIONAL DATA TRANSFERS.

Transferring Data Outside the EEA

When transferring personal data outside the European Economic Area (EEA), DAMREV will ensure that appropriate safeguards are in place to protect the data. This includes:

- Ensuring the recipient country has adequate data protection laws;
- Using standard contractual clauses approved by the European Commission;
- Implementing binding corporate rules for transfers within the same corporate group;
- Obtaining explicit consent from data subjects for the transfer.

Documentation and Records

DAMREV will maintain records of all international data transfers, including the legal basis for the transfer and the safeguards implemented.

13. TRAINING AND AWARENESS.

Staff Training

DAMREV will provide regular training to all employees on data protection and GDPR compliance. Training will cover:

- GDPR principles and obligations;
- Data protection policies and procedures;
- Identifying and reporting data breaches;
- Handling data subject requests;
- Practical security measures.

Awareness Campaigns

DAMREV will conduct awareness campaigns to ensure that all employees understand the importance of data protection and their role in ensuring compliance.

14. REVIEW AND UPDATES.

Regular Reviews

This GDPR policy will be reviewed regularly and updated as necessary to ensure its effectiveness and compliance with applicable laws and regulations. The next review is scheduled for January 2025.

Amendments

Any amendments to this policy will be communicated to all relevant stakeholders, including employees, clients, and partners.