



DATA PROTECTION POLICY



Contents

- 1. PURPOSE AND POLICY STATEMENT 3
- 2. SCOPE OF APPLICATION 3
- 3. DEFINITIONS 3
- 4. PRINCIPLES 4
- 5. DATA COLLECTION AND PROCESSING 4
- 6. RIGHTS OF DATA SUBJECTS..... 5
- 7. SECURITY CONTROLS 5
- 8. NOTIFICATION OF BREACHES 5
- 9. TRANSFER OF DATA 6
- 10. DOCUMENTATION 6
- 11. RESPONSIBILITIES..... 6
- 12. SPEAK UP 6
- 13. DISCIPLINARY ACTION 7
- 14. REVIEW PROCESS 7

1. PURPOSE AND POLICY STATEMENT

Fast exchange of large volumes of data is now essential to modern societies and businesses, including us at QTerminals. Unfortunately, data in the globalised world creates not only opportunities but also threats, especially in relation to Personal Data where misuse can lead to violation of fundamental rights and freedoms.

QTerminals considers safeguarding Personal Data to be part of our social responsibility and is committed to manage data responsibly. With this policy, QTerminals establishes a framework for the handling of Personal Data to ensure its lawful protection and responsible processing.

2. SCOPE OF APPLICATION

The Policy applies globally to all Employees. This Policy does not replace any national or international law. In case legislation requires stricter standards or higher level of protection of Personal Data, it must take precedence over this Policy.

3. DEFINITIONS

Personal Data means 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.

Data Subject means any natural person whose Personal Data is processed in the context of this Policy.

Processing means any operation or set of operations performed on 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 of Personal Data.

Controller means the authorised personnel which alone or jointly with others determines the purposes and means of the Processing of Personal Data, for example a HR coordinator who is responsible for processing the employment contract.

Consent means freely given, specific, informed, and unambiguous indication of the Data Subject's wishes to agree to the Processing of Personal Data relating to him or her.

Employees means all QTerminals' employees (including contracted workers), officers, and directors.

Ethics Review Panel (ERP) means a multidisciplinary body within QTerminals committed to reviewing all reported alleged unethical matters, misconduct and wrongdoings in a timely manner and deciding on the respective disciplinary action. ERP members are selected on a case-by-case basis by the Group Legal and Compliance Director, depending on the nature and criticality of the alleged misconduct and/or wrongdoing.

Line Manager is a person with direct managerial responsibility for a particular Employee.

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.

QTerminals means Qterminals W.L.L. and its controlled subsidiaries, affiliates, and joint ventures.

4. PRINCIPLES

In Processing Personal Data, we follow the foundational principles set out below:

- **Lawfulness:** Personal Data should be collected and processed only based on adequate legal basis.
- **Fairness and Transparency:** Personal Data should be handled with respect and Data Subjects should be made aware in intelligible, easily accessible, and clear form about how their Personal Data is managed and for what purpose.
- **Purpose Limitation:** Personal Data should be processed only for legitimate purposes that are explicitly disclosed at the time of collection of Personal Data. Personal Data cannot be processed in a manner that is incompatible with those purposes.
- **Data minimisation:** Collection and Processing of Personal Data should be limited to what is strictly necessary for the defined legitimate purposes.
- **Storage limitation:** Personal Data should be stored for no longer than necessary to achieve the purpose for which the data is processed.
- **Accuracy:** Personal Data should be accurate and, where necessary, kept up to date. Reasonable steps should be taken to erase or rectify incorrect data.
- **Integrity and Confidentiality:** Personal Data should be protected against unauthorised or unlawful processing, accidental loss, destruction, or damage. Appropriate technical and organisational measures need to be introduced and followed to ensure secure and confidential storage and processing of Personal Data.
- **Accountability:** Clear governance and effective processes should be put in place to ensure adherence to principles and provisions of this Policy. Relevant records and documentation should be maintained to be able to demonstrate compliance with the requirements of this Policy.
- **Access Control:** Access to personal data should be on a need-to-know basis and restricted to the authorised persons only.

5. DATA COLLECTION AND PROCESSING

Collection, Processing, and use of Personal Data is permitted only under certain circumstances in accordance with applicable laws, including the following:

- Prior consent of the Data Subject.
- Fulfilment of a contract concerning the Data Subject.
- Obligation imposed by law.
- Protection of vital interests of individuals.
- Performance of task in public interest or national authorities' functions.
- Legitimate interest of QTerminals or a third party.

Consent of the Data Subject and the fulfilment of a contract are two primary grounds for Processing Personal Data at QTerminals. In case data is processed based on Consent, the Data Subject should receive information about data Processing in concise, transparent, intelligible, and easily accessible form and in clear language. Data Subject should be informed prior to giving consent at least about:

- Purpose and legal basis for processing Personal Data.
- Identity and contact details of Controllers who will have access to the Personal Data.
- Comprehensive and accurate description of Processing activities.
- Recipients or categories of recipients.
- Storage period of Personal Data, or if that is not possible, the criteria used to determine that period.
- Rights of Data Subject.
- Existence of automated decision-making, including profiling.

Personal Data that relates to ethnic origin, children, health, physical or psychological condition, religious creeds, marital relations, and criminal offenses, is considered as sensitive. Responsible Controllers should at all times follow local legislation in relation to Processing of sensitive Personal Data.

6. RIGHTS OF DATA SUBJECTS

In relation to own Personal Data, Data Subjects have right to:

- Be informed of the nature and circumstances of the Processing and Data Subject's rights in this respect.
- Access Personal Data and receive a copy of their Personal Data
- Rectify inaccurate Personal Data.
- Withdraw consent (applicable only if Personal Data is processed based on consent).
- Request to erase Personal Data if the legal basis or purpose have ceased to apply.
- Object and restrict Processing unless Controller has legitimate grounds for Processing.
- Object to and be excluded from direct marketing or automatic profiling.

Data Controllers should assist Data Subjects in exercising their rights upon request.

7. SECURITY CONTROLS

Technical and organisational measures should be implemented to ensure security of Personal Data considering risk for the rights and freedoms of individuals, as well as cost of implementation, scope, and purposes of Processing. The measures should include at least the following:


- Personal Data should be encrypted when transmitted via end-user messaging technologies (e.g., email).
- By definition, Personal Data should be classified as confidential and accessed only on a need-to-know basis.
- Personal Data should be filed and stored in a way that it is accessible only to authorised personnel and transferred only through use of protected means of communication.
- Personal Data should be pseudonymised in case purpose of its Processing can be achieved using pseudonymised data.
- Personal Data should be securely disposed of in line with the "Disposal" section of the Data Retention Policy.
- In case of physical or technical incident, availability to the data should be restored in a timely manner.
- Employees should receive data protection training in case they are involved Processing of Personal Data.

When introducing new processes or significantly changing existing processes, security risks to Personal Data should be considered. In case such changes are likely to result in high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment should be carried out. Results of a Data Protection Impact Assessment should be approved by Compliance team.

The effectiveness of technical and organisational measures for Personal Data protection should be regularly tested and evaluated by Compliance and Internal Audit teams.

8. NOTIFICATION OF BREACHES

Compliance team should be notified immediately in case any breach of Personal Data is suspected. When the breach is likely to result in risk to the rights and freedoms of an individual, Compliance team must inform the Data Subject and supervisory authority of the breach. Controller and Compliance officers should document facts relating to Personal Data Breach, its effects and measures taken to mitigate the risks.



Compliance team should investigate each breach of Personal Data and evaluate the need to add or adjust security controls to prevent or minimise impact of further breaches.

9. TRANSFER OF DATA

Considering potential differences in local legislations, Data Controllers should consult and follow local laws prior to transfer of Personal Data, including both intercompany transfer and transfer to a third party. Personal Data can be transferred only in case the recipients have adequate level of data protection controls and process Personal Data according to local legislation. Unless the transfer is needed to fulfil a contract or for important reasons of public interest, consent of the Data Subject should be received. Transfer of Personal Data to third parties should always be based on specific Data Transfer Agreement or Data Processing Agreement that will specify the legal basis for the transfer and will ensure that the data recipient will adhere to data protection standards.

10. DOCUMENTATION

Written record of all Processing activities of Personal Data should be maintained by the respective Controller. The record should contain contact information of Controller, consent of Data Subject (if applicable), the purposes of the Processing, description of categories of Personal Data and Data Subjects, categories of recipients to whom data will be disclosed or transferred and, where possible, time limits for storage of Personal Data and security measures applied.

11. RESPONSIBILITIES

All Employees are responsible for adhering to this Policy. We expect Employees to read, understand, acknowledge, and adhere to all aspects of this Policy and any supplementary procedures issued by QTerminals. All Employees are encouraged to contact their Line Manager and, if required, HR or the Compliance Officer/Representative to clarify questions, request information or express concerns relating to this topic.

All Line Managers, along with the relevant guidance from Compliance or HR departments, shall ensure that any concerns related to Data Retention of those Employees reporting to them are resolved.

Management of QTerminals is responsible for ensuring that legal requirements and provisions of this Policy are followed. Each managing senior executive of QTerminals at port or terminal level must ensure that the business unit they are responsible for is and will remain fully compliant with this Policy, promoting awareness and understanding of this Policy and ensuring allocation of adequate resources to effectively implement this Policy. Specifically, the Compliance team must ensure that the required processes are in place that enable adherence to this Policy.

12. SPEAK UP

QTerminals promotes an environment of integrity and transparency under which its Employees are encouraged to report any violation or suspected violation of this Policy within QTerminals or at any of the third parties, either by informing their Line Manager, their HR department, their Compliance Officer/Representative or alternatively through the QTerminals Ethics Line, which is available on QTerminals intranet, QTerminals website and as a dedicated phone line.

Additionally, any retaliation against anyone who notices and reports a known or suspected violation of the Policy is strictly prohibited. Anyone proven to have retaliated against a person who has reported a breach

in good faith is to be subjected to disciplinary action. However, any false or malicious allegations may lead to appropriate disciplinary and legal action, up to and including termination of employment.

For more information on the whistleblowing process, please refer to QTerminals Whistleblower and Anti-fraud Procedures.

13. DISCIPLINARY ACTION

At QTerminals, all to whom this Policy applies, as specified in the “Scope of Application” are expected to abide by this Policy. Any violation thereof may result in disciplinary action, termination of employment or legal proceedings.

In case the complaints for wrongdoings warrant an investigation, there will be investigations whose results and proposed corrective actions will be reviewed by the Ethics Review Panel (ERP). The corrective actions will be determined based on the facts and circumstances of the breach of conduct and results of the investigation.

For more information on the process of investigation of alleged misconduct and violations of the Code of Conduct or this Policy, please refer to QTerminals Whistleblower and Anti-fraud Procedures.

14. REVIEW PROCESS

Compliance team is responsible for monitoring risks relating to Data Protection and regularly reviewing, evaluating and improving this Policy. Risks and overall effectiveness of the Policy should be reported to executive management.

Approved By:



Group CEO

Neville Bissett