

# Quantum's Personnel Data Privacy Policy

EU Data Privacy Directive  
Safe Harbor Compliance

Copies of this policy may be downloaded internally from [myQ](#) and externally from [www.Quantum.com](http://www.Quantum.com) .  
Additional information about the Safe Harbor principles and certification process can be found at  
<http://www.export.gov/safeharbor/>



Quantum Corporation (“Quantum”) is committed to the protection of personal information transferred from Quantum’s subsidiaries and location in the EU and Switzerland (referred to as “Personnel Data”) to the U.S. The company has certified its participation, and compliance with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the transfer of Personnel Data from European Union member countries and Switzerland to the U.S. The principles of Safe Harbor compliance are notice, choice, onward transfer, security, data integrity, access, and enforcement.

#### **SCOPE**

Personnel Data includes your name, address, contact information, compensation, benefits and any other information provided by you or collected in connection with your employment at Quantum. This Personnel Data Privacy Policy (the “Policy”) applies solely to Quantum in its processing of Personnel Data received from Quantum’s subsidiaries and locations in the EU and Switzerland.

This policy is to be used in conjunction with Quantum’s High Road and IT Computing Security and Usage Policy.

#### **PRINCIPLES**

This Policy sets forth Quantum’s procedures for complying with the Safe Harbor Framework in regard to Personnel Data transferred from EU/Swiss subsidiaries and locations to the U.S. This Policy, including the procedures discussed below, will be communicated to all employees of Quantum’s European subsidiaries and locations and to all Quantum employees in the U.S. that process or otherwise have access to the “Personal Data” discussed below.

***Compliance with this Policy is mandatory, and any employee failing to comply will be subject to disciplinary action, up to and including termination of employment.***

#### **1. What information do we collect?**

From time to time, Quantum receives personnel data regarding employees of its European subsidiaries and locations for the purposes of (a) general employment purposes (specifically, providing compensation, health and welfare benefits and related services, keeping updated organizational information, making employment-related decisions, and employee training) and (b) processing and investigating reports under Quantum’s High Road Ethics Program. For example, Personnel Data could include one or more of the following: name, address, job title and other job information, location, compensation information, identification number (including, in some cases, national insurance number), employment history, and copy of employment agreement. Additionally, in the case of reports under Quantum’s High Road Ethics

Program, Quantum may receive information about an employee's actions or inactions relative to a legal requirement or other legal or ethical issue covered by Quantum's Code of Conduct, High Road/Ethics Program, or other Quantum policy. Personnel Data is transferred only to third parties acting as agents of Quantum for the purposes described above (i.e., general employment purposes or processing of reports under Quantum's High Road/Ethics Program). In no case does Quantum transfer Personnel Data for any purpose not compatible with these purposes without first notifying the data subject. And, except in limited and permissible circumstances, Quantum does not transfer to third parties Personnel Data deemed "sensitive" under the Directive. Examples of circumstances in which the transfer of sensitive

Personnel Data is permissible include where the transfer is (a) in the vital interests of the data subject or another person; (b) necessary for the establishment of legal claims or defenses; (c) required to provide medical care or diagnosis; (d) necessary to carry out Quantum's obligations in the field of employment law; or (e) expressly permitted by an employee for a specific purpose.

## **2. Choice**

Quantum gives employees the opportunity to choose not to have his or her Personnel Data transferred to third parties for use in a manner incompatible with the purpose for which it was originally collected. An employee may not opt out of the transfer of his or her Personnel Data which is transferred by Quantum to a third party for the purpose of (1) meeting applicable legal requirements or (2) permitting the legitimate interests of Quantum in making promotions, appointments, or other employment decisions. For certain more sensitive Personnel Data (which might include race, gender, religion, medical information, etc), explicit (opt in) choice is sought if the information is to be disclosed to a third party for use in a manner incompatible with the purpose for which it was collected.

## **3. Onward Transfer of Personnel Data**

In addition to the limitations of the transfer of Personnel Data discussed above, Quantum transfers Personnel Data only to those third parties who (a) have agreed in writing to provide at least the same level of privacy protection to the Personnel Data as is required under the Directive or the Safe Harbor Principles and/or (b) adhere to the Safe Harbor Principles. Exceptions to this limitation on onward transfer include where an employee has granted Quantum express permission to transfer his or her data to the third party or where such transfer is necessary for the purpose of meeting a legal requirement.

## **4. How do we safeguard personal information?**

Quantum takes every reasonable precautions to protect Personnel Data from loss, misuse, or unauthorized access, disclosure, alteration or destruction. Personnel Data is maintained in secure electronic and manual files at Quantum, and access to these files is limited to Quantum employees for whom access is necessary to properly process the Personnel Data consistent with the stated purposes. Personnel Data that is transferred to third parties is done so by methods designed to reasonably reduce the risk that the Personnel Data is lost, stolen, or inadvertently sent to a person or organization other than the intended recipient. Quantum retains Personnel Data only as long as is necessary for its intended use, after which time the Data is deleted, destroyed, or returned. Quantum employees who are authorized to access the files for the stated purposes are trained periodically on this Personnel Data

Privacy Policy, with emphasis on the need to keep Personnel Data private and secure and the potential disciplinary consequences for the failure to do so.

### **5. Ensuring Data Integrity**

Quantum's US personnel coordinate closely with personnel from Quantum's European subsidiaries and locations (in particular the Compliance, Information Technology, Human Resources and Legal Departments) to ensure that Personnel Data is up-to-date, accurate, complete, and reliable for its intended use.

### **6. Access to Personnel Data**

You may request access to your Personnel Data for the purpose of correcting, amending, or deleting data that is inaccurate. Quantum may require information confirming the identity of anyone requesting access to Personnel Information. In such cases, Quantum will comply with an access request within 40 days of receipt of the request, in most cases sooner. Quantum may deny an employee's request to access his or her Personnel Data where the rights of persons other than the requesting employee would be violated.

### **7. Verification of Compliance**

To verify its compliance with the Safe Harbor Principles, Quantum periodically (at least once a year) conducts a self assessment to ensure that (a) this EU Personnel Data Privacy Policy is accurate, comprehensive, prominently displayed, completely implemented and accessible, and conforms to the Safe Harbor Principles; (b) employees are informed of the internal arrangements for handling complaints and the independent mechanisms through which they may pursue complaints; and (c) Quantum has in place procedures for training the appropriate employees on the implementation of this Policy and disciplining those who fail to comply.

### **8. Questions and Complaints**

To access your information, ask questions or raise a concern about the collection, use or disclosure of Personnel Data, please contact Quantum's International Privacy Officer in the first instance:

**Tara LaBree**, International Privacy Officer  
Manager, Risk and Compliance (Worldwide)  
10125 Federal Drive  
Colorado Springs, CO 80908  
Phone: +1 (719) 536-6397  
(E-mail address: [internationalprivacyofficer@quantum.com](mailto:internationalprivacyofficer@quantum.com))

If a complaint, access request or inquiry is not resolved to your satisfaction, you may report complaints to the **U.S. Federal Trade Commission** ("FTC") or the applicable EU **Data Protection Authority** ("DPA"). Quantum will cooperate with the DPA in investigation and resolution of any complaints brought under the Policy.



Copies of this policy may be downloaded internally from [myQ](#) and externally from [www.Quantum.com](http://www.Quantum.com) . Additional information about the Safe Harbor principles and certification process can be found at <http://www.export.gov/safeharbor/>.

The following forms may be requested by contacting **Quantum's International Privacy Officer**

- Request For Access To Personnel Data
- Request Form To Correct Personnel Data
- Complaint Form

**Quantum reserves the right to revise or amend this policy at any time.**

Reissued: 29 October 2009