THE TIMKEN COMPANY
Global Data Privacy Policy

Data privacy commands increasing attention as a compliance obligation around the world. The concern people have over the privacy of their personal data has strengthened as technology has advanced and the world has grown more connected. Governments around the world have responded to these concerns with laws designed to protect personal data and to limit the ways in which personal data may be used. Timken is committed to respecting those concerns and complying with those laws.

This policy prescribes the basic rules that all Timken associates must follow, regardless of their roles in the company. Associates whose job duties more directly involve the collection, use, and protection of personal data, or who have responsibilities for deciding how to use and protect that data, will have additional obligations, which are identified and explained in other materials available from the Global Data Privacy Office.

What is data privacy?

Data privacy – sometimes called data protection – is the compliance area designed to protect **personal data** about **individuals** from **improper use** and from **unauthorized loss or disclosure**.

Personal data – sometimes called personal information – is any item of information, in any format (electronic, paper, sound or image), that can be used, alone or with other information, to *either*

- identify an individual, such as name, identification number, email address, or photograph, or
- learn, record, or decide something about an individual, such as a work or education history, a record of communications, financial account information, or a criminal record.

Privacy/Protection. An obvious purpose of data privacy laws is to protect personal data from **unauthorized loss or disclosure**. But those laws are also designed to protect personal data from **improper use**.

What are your obligations under this policy?

You play an important role in furthering Timken's commitment to data privacy. You can do your part by following these rules:

1. Understand and apply the data privacy principles. It is important that you understand the data privacy principles (these are discussed later), even if your job duties do not involve the regular and systematic use of personal data. All of us come into contact with some personal data, such as names and contact information of our fellow associates or persons associated with our customers, vendors, and other business partners. You should consult with your supervisor, the Global Data Privacy Office, or other Timken reporting resources if you have any questions about how to follow the principles and this policy.

2. Respect and protect the personal data you encounter. These general obligations and prohibitions apply to all Timken associates with respect to the personal data they encounter as part of their job duties.

DO:

- be aware of and follow all information security policies and access rules,
- use reasonable care to protect personal data from inadvertent or unauthorized loss, misuse, or disclosure to persons – even other Timken associates – who are not authorized to view the personal data,
- conduct periodic review of emails and documents you maintain on your computer and mobile devices and on network storage locations over which you have control, and delete items containing personal data that are no longer required to be kept pursuant to applicable data retention policies or our business needs, and
- report violations of this policy of which you become aware.

DO NOT:

- use the personal data of others except as part of your legitimate duties with Timken,
- attempt to obtain access to personal data not necessary for the type and scope of your assigned duties, or retain access to any personal data you might obtain inadvertently, or
- make personal data available to any person or company, whether inside or outside of Timken, other than as part of your job duties and as authorized by the rules governing the business activity in which the personal data is used.

3. Report a personal data breach. You must report a suspected personal data breach as soon as possible. This is extremely important, because many laws require that we report certain personal data breaches within a very short time – as few as 72 hours under some laws.

A **personal data breach** is any situation that **has resulted in** or that **appears might result in** a breach of security leading to the **accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to**, personal data.

4. Follow specific requirements that apply to your job duties. Some associates' job duties will require them to take additional actions arising from the data privacy principles and laws. For example, Timken associates working in an HR role will routinely work with the personal data of Timken associates and must take all of the actions prescribed by their organization for the use of and protection of that personal data. These associates and their supervisors must be sure those specific actions are made a part of the business activity, communicated to all associates working in the activity, and regularly tested for effectiveness. Additional tools and support are available through the Global Data Privacy Office.

What are the data privacy principles?

Our data privacy compliance is built around a set of generally accepted data privacy principles. Although these principles are stated and organized in various ways by different organizations, Timken uses the following seven principles. These principles are explained further in Timken's Data Privacy Principles guide, available at the Timken Ethics and Compliance section of TimkeNet.

1. Lawful, Fair, and Transparent. Personal data must be processed (used) lawfully, fairly, and in a transparent manner in relation to the data subject.

2. Purpose Limitation. Personal data must be collected for specified, explicit and legitimate purposes and not further processed (used) in a manner that is incompatible with those purposes.

3. Minimization. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the information is processed (used).

4. Accuracy. Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed (used), is erased or rectified without delay.

5. Retention Limitation. Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (used).

6. Integrity and Confidentiality - Security. Personal data must be processed (used) in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing (use) and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. Accountability. A company that processes (uses) personal data must be responsible for, and be able to demonstrate compliance with, the other data privacy principles.

How does this policy apply?

Associates. This policy applies to all associates of The Timken Company and its global affiliates for the collection, processing, use, dissemination, transfer and storage of personal data of individuals with whom Timken comes into contact in the conduct of its business. The policy imposes common rules for all Timken associates and affiliates in all countries, even those countries or political subdivisions (such as individual states within the U.S.) that do not have stringent data privacy laws. Some countries and political subdivisions impose a higher burden than the norm, and Timken associates in those countries or political subdivisions are required to follow the stricter rule.

Affiliate Leadership. Associates who have management responsibility for the activities of individual Timken affiliates or groups of related affiliates must ensure that sufficient and qualified personnel and resources are deployed to achieve an appropriate level of compliance with the data privacy principles and laws and that each business activity or process that uses personal data takes the specific actions required by those laws, as suggested by the Global Data Privacy Office. Timken affiliates may not adopt policies or practices that are inconsistent with this policy, except with the approval of the Global Data Privacy Office, or as required by local law upon notice to and consultation with the Global Data Privacy Office.

Interpretation and Enforcement. This policy is issued by Timken's Ethics and Compliance Office, which is responsible for its interpretation. This is a policy with obligations for the global Timken workforce. Violations of the policy could subject an associate to discipline, up to and including termination of employment. This policy may be amended only by the Ethics and Compliance Office, as approved by executive management.

What resources are available to help with compliance?

Global Data Privacy Office. Timken has established a Global Data Privacy Office within our Ethics and Compliance Office. The Global Data Privacy Office provides oversight, support, expertise, and coordination to the processing activity leaders and manages certain common data privacy compliance tools and processes. The office is led by a Global Data Privacy Compliance Lead (Global DPCL). The contact information for the Global Data Privacy Office is:

Timken Data Privacy Office
Mail Code WHQ-02
4500 Mount Pleasant St NW
North Canton, OH 44720 U.S.A.
DataPrivacyOffice@timken.com
+1 234 262 2207
866 846 5369 (toll free in U.S.)

Ethics and Compliance Reporting Resources. You may report concerns to any of these ethics and compliance reporting resources:

- your manager or supervisor
- your HR representative
- any member of management
- the Ethics and Compliance Office at ethics@timken.com
- the Timken Helpline at www.Timkenhelpline.com

Referenced and Related Policies

- Timken Standards of Business Ethics
- Global Information Security Policies
- HIPAA Privacy Manual – Policies and Procedures