

THE TIMKEN COMPANY PRIVACY NOTICE VENDOR MANAGEMENT AND ADMINISTRATION

The purpose of this Privacy Notice (“**Notice**”) is to inform you about how and why we use your personal information as part of the management and administration of our relationships with vendors. This Notice applies (1) to individuals who are employed by or who are otherwise acting on behalf of vendors of good or services to The Timken Company and any of its global affiliates (“**we**”, “**us**”, or “**our**”) and (2) to vendors who are individuals or equivalent organizations, such as sole proprietorships or certain partnerships; in both cases limited to vendors to those global Timken affiliates that use the Ariba system. It is important that you read this Notice so that you are aware of how and why we will use your personal information and how we will treat it.

Most of this Notice applies globally, but some portions apply only where specifically required by local law, for example, the General Data Protection Regulation 2016/679, a regulation of the European Union on data protection and privacy for all individuals within the European Union (“**EU**”) and the European Economic Area (“**EEA**”) (“**GDPR**”), and the California Consumer Privacy Act (“**CCPA**”). Those portions will be identified as only applying as required by law.

WHO COLLECTS THE INFORMATION?

The controller for the personal data is The Timken Company and any of our global affiliates with which you conduct business. Contact details for The Timken Company are provided at the end of this Notice. A controller of personal data is responsible for deciding how they hold and use personal information about you and for notifying you of the information contained in this Notice.

WHAT INFORMATION DO WE COLLECT?

For individuals employed by or associated by our vendors, we collect and use your name and the business contact information that you provide or that has been provided to us by your employer. If you use the Ariba system, we will generate and store log-in credentials.

In addition, for a vendor that is an individual or equivalent organization:

- We collect from you name and contact information, information about your business and quality capabilities, bank account information, and applicable government issued tax or other identification numbers.
- We may collect creditworthiness information from publicly available sources or from references you provide.
- In the United States only, we may collect from you demographic information and information about racial or ethnic origin, to satisfy government requirements for equal opportunity efforts and reporting.
- During the course of our relationship, information about our transactions (such as ordering, delivery, quality and payment history) will be generated in the ordinary course.

WHY DO WE COLLECT YOUR PERSONAL DATA AND ON WHAT BASIS?

We collect this information in order to carry on our business relationship with our vendors, for example to communicate with our vendors, place orders, make payments, perform periodic performance reviews, etc.

Where required, such as where the GDPR applies, we will only process personal information about you where we have a lawful basis to do so. For the purposes of vendor management and

administration, it is in our legitimate interests to process your personal data as described above so that we can acquire for quality goods and services necessary to run our business.

WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA AND WHERE WILL IT BE STORED?

We use the Ariba platform for collecting and storing the personal information. Ariba is operated by Ariba, Inc., an SAP company headquartered in California, USA. Employees and contractors of Ariba may have access to the personal information in their role as a system administrator. Ariba, Inc. is contractually bound to protect your personal data and to only act on behalf of and upon instructions from Timken, or as may be required by law.

Your personal data will be accessed by employees of The Timken Company in the U.S. and any global affiliate with which you or your employer is engaging in business. Those employees may be in departments such as supply chain, purchasing, manufacturing, accounts payable, IT, and internal audit. These Timken personnel may be located in a country other than your country, including in the United States.

Your personal information may be accessed by employees at other Timken global affiliates that use the Ariba system, except that bank account and tax ID information is accessible only by necessary accounts payable personnel and personnel providing system administration support.

Personal information within email and other communications with Timken personnel is stored on servers and on personal computers protected with appropriate security measures, including encryption of personal computers.

We may disclose your personal information to the purchaser of all or a portion of the business of Timken or one of its group companies. We may disclose your personal data when we have a legal duty to do so, to enforce or apply our agreements, and to protect the rights, property, or safety of Timken, our applicants, employees, customers, and providers.

HOW DO WE PROTECT YOUR PERSONAL DATA?

Timken has implemented an information security program that includes physical, technical and organizational measures to protect your personal data from unauthorized disclosure or access, unlawful processing, and accidental or unlawful loss, destruction, or alteration.

We will keep the personal information that we obtain about you for as long as we need to manage our relationships with vendors to deal with any complaints or other issues that arise or to assert or defend our legal rights, and comply with applicable laws and regulations.

WHAT ARE YOUR RIGHTS UNDER GDPR?

Where the GDPR applies, you have a number of rights, which are subject to certain conditions and exemptions under the GDPR and its local implementing laws. These rights include the right to:

- request access to your personal information, which enables you to receive a copy of personal data we hold about you and to check that we are lawfully processing it;
- require us to correct incorrect or complete incomplete data we hold about you;
- request erasure of your personal information, which, when applicable, enables you to require us to delete or to remove your data, for example where the data is no longer necessary for the purposes of processing;

- request the transfer of your personal information to another party; and
- request the restriction of processing of your personal information, for example if you want to establish its accuracy or the reason for processing it.

You also have the right to object to the processing of your personal information where we are relying on our legitimate interests (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground.

You will not usually have to pay a fee to access your personal information or to exercise any of the other rights. However, we may charge a reasonable fee if your request is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

If you wish to exercise any of these rights, please contact us using the contact details set out in the “Contacting Us” section of this Notice.

We strive to process your personal data in accordance with the applicable legal obligations, but if you have a complaint in that regard, please address your complaint using the contact details set out below.

If you are a data subject under GDPR, you also have the right to lodge a complaint with a supervisory authority if you are not happy with how we handle your personal data and we could not provide you with a satisfactory resolution to your request.

CONTACTING US

To contact us, please contact the Data Privacy Office at The Timken Company as follows:

The Timken Company
Data Privacy Office/Legal
4500 Mount Pleasant Street NW
North Canton, Ohio 44720 USA
DataPrivacyOffice@Timken.com
+1 234.262.2207