

The Timken Company Applicant/Recruitment Privacy Notice

The Timken Company and its global group companies (“we”, “us”, or “our”) are committed to being transparent about how we collect and use your personal data and to meeting our data protection obligations. It is important that you read this Privacy Notice (“**Notice**”) so that you are aware of how and why we will use your personal data 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 on data protection and privacy applicable for within the European Union (“**EU**”) and the European Economic Area (“**EEA**”) (“**GDPR**”). Those portions will be identified as only applying as required by law.

WHO COLLECTS THE INFORMATION?

The controller for the personal data you submit as part of the application and recruitment process through the Timken Careers web portal will be The Timken Company, an Ohio corporation having its global headquarters at 4500 Mount Pleasant Street NW, North Canton, Ohio 44720 USA, and the Timken group company that will be the employer for the position. If you are using our portal, you can determine the Timken group company that will be the employer from the job listing itself. If you are applying directly to a Timken group company and not through the portal, the controller will be that Timken group company and, when that Timken group company enters the personal data into the Timken global system, The Timken Company. A controller of personal data is responsible for deciding how they hold and use personal data about you and for notifying you of the information contained in this Notice.

FROM WHOM DO WE COLLECT THE INFORMATION?

Most of the personal data about you that we collect for recruitment purposes comes from you during the application process. But we also receive information from recruiters and online recruitment sites, such as LinkedIn, Indeed, CareerBuilder, etc. Those online sites will likely have their own privacy notices, which you should consult to understand how those companies will use your personal data. And as described more below, we may receive personal data about you from other sources at later stages of the recruiting process.

WHAT INFORMATION DO WE COLLECT?

To decide whether to shortlist you as an applicant and to contact you in relation to your application, we will collect the following information about you, unless local law places restrictions on our ability to do so:

- a) your name and contact details, for example, address, home and mobile phone numbers, and email address;
- b) your curriculum vitae/resume;
- c) further details of your qualifications, experience, employment history, professional certifications and memberships, language skills, geographic relocation preferences, etc.; and
- d) whether or not you have a disability for which the organization needs to make reasonable adjustments during the recruitment process.

We will not be able to process your application without the items of information identified in a) and b) above.

Further, some job postings have specific qualification requirements, and if the answers you provide do not align with those requirements, your application automatically will not be considered further. If this occurs, you will be given instructions on how to contest the automatic decision.

If you are shortlisted for a role, we may collect additional information about you to decide whether to make a conditional offer of employment to you and to assess whether the offer conditions have

been met. This may include additional information about your previous academic and employment history, details of any conduct, grievance or performance issues, appraisals, and time and attendance, and information from persons you provide as references. To the extent *permitted* by applicable law we may, or when *required* by local law we will, collect the following additional information, either directly from you or from third parties, such as background check agencies:

- information regarding your criminal record;
- your nationality and immigration status and information contained on related documents, such as your passport or other identification and immigration information;
- a copy of your driving licence, in order to comply with our legal obligations; and
- to promote equal opportunities, information about your gender, ethnic origin, health, religion, and, in some countries, sexual orientation.

For example, in many countries we are legally obligated to collect from you information and documents confirming your nationality, immigration status, and right to work in that country.

When we require this information, we will inform you at the appropriate time in the application process and, where required by law, we will provide you with further details.

For some roles in some countries, we seek information about criminal convictions and offenses. Where we seek this information, it is because the personal data is necessary for us to carry out our obligations in relation to employment, because the checks we carry out are necessary and proportionate to the role applied for, because, in some cases, the check is required by local law, or because of our legitimate interests in the security of our information and workplaces. We do not seek this information where the local law does not allow us to do so. If we intend to perform a criminal records check, we will inform you in advance and provide you with any further information required by law, such as the type of offenses we need to know about and the consequences if relevant offenses are discovered.

Except where we specifically require, we do not want you to volunteer any sensitive personal data – what the GDPR calls special categories of personal data – which includes your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life and sexual orientation, and health, genetic and biometric data. And, again, unless we specifically require, we do not want you to provide information about your criminal record.

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

We, and the third party service providers we use in the recruitment process, will use your personal data to process your application, to contact you for further information or to update you on the status of your application, to evaluate your suitability for the position, to support any offer of employment or engagement, and to form the beginning basis of your employment record.

If your application is successful, where required by law (such as the GDPR), further details about how we will process your personal data pursuant to your employment will be provided in our Employee Privacy Notice.

As long as you maintain a profile on our Timken Careers web portal, we will use your personal data to send you information about new job postings that fit the interests you select in your profile. You may remove your profile at any time to stop receiving these notices.

We only process personal data about applicants where the processing has a legitimate basis and is in compliance with local law. Under the GDPR, for example, this will usually be where the processing is necessary:

- to take steps toward entering into and performing the employment contract;
- to ensure compliance with our legal obligations as a potential employer, for example, to ensure that you have the right to work; or

- for our legitimate interests, such as the recruitment, employment, and management of qualified individuals, and maintaining the workforce needed to meet our business objectives, provided your interests and fundamental rights in a particular case do not override those interests.

We may also need to process personal data from job applicants to respond to and defend against legal claims.

The laws in some countries (such as the GDPR) impose additional conditions on our use of sensitive or special categories of personal data. Where GDPR applies, we usually only process such information in the following circumstances:

- with your explicit written consent, but only where permitted by law, in which case further details about the processing of such data will be provided to you at the time such consent is requested;
- where it is necessary for the purposes of performing obligations or exercising rights under local employment laws, for example, if we are obligated to make reasonable adjustments to the recruitment process for candidates who have a disability, or where we process information about ethnic origin, gender, health, religious or philosophical beliefs, or sexual orientation in order to fulfil legal obligations under equal opportunities regulations; or
- where it is necessary in order to establish, exercise, or defend potential legal claims.

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

Your personal data may be accessed by our human resources administrators, supervisors and other personnel within the Timken group companies as necessary to perform their respective functions with regard to recruitment, human resources management or employment law. Your personal data may also be shared with third party contractors and vendors to perform certain services for the same purposes. Some of these Timken personnel and contractors are located in countries outside the European Economic Area (“**EEA**”) which are not governed by EU data protection laws. However, any transfers of personal data from the EU outside the EEA will be subject to appropriate protections, as further described in the paragraphs below.

If you apply through the Timken Careers web portal, your information will initially be uploaded to servers maintained in the United States by our Human Resource Management system, called MySuccess, which is operated by [Success Factors Inc.](#), a company formed under U.S. laws with a headquarters as of the date of this Notice at 1 Tower Place, Suite 1100, South San Francisco, CA 94080. If you apply directly to the applicable Timken group company, your personal data will initially be stored in paper files or on servers located in the host country and, in some cases, in the United States. At some point during the recruitment process – at least by the offer stage if not earlier – your personal data will be entered into the MySuccess platform.

Service providers with whom we share your personal data are required to protect your personal data and to act only on behalf of and upon instructions from Timken as may be required under law.

Transfers of your personal data outside of the EU/EEA – such as to Timken or MySuccess in the U.S. – are protected by adequate safeguards such as, in the case of Timken group companies and Success Factors, standard contractual clauses¹. A copy of these clauses can be obtained from the contacts identified in the “Contacting Us” section at the end of this Notice. You may view the precedent copy of the standard contractual clauses [at this link](#).

We may disclose your personal data to the purchaser of all or a portion of the business of Timken or one of its group companies, or to the seller of a business that is being acquired.

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.

¹ Reference GDPR Article 46.

If your application for employment is successful, we may then share your data with those former employers about which you have provided details to obtain references for you. If you begin employment with us, we will collect and share additional information and, where required by law, we will provide you with further information about this in our Employee Privacy Notice.

Further information about the recipients of your personal data can be obtained by contacting us using the details set out in the “Contacting Us” section at the end of this Notice.

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. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us. Accordingly, any voluntary transmission by you through the Timken Careers web portal is at your own risk.

We will keep the personal data that we obtain about you for as long as we need to in order to complete our recruitment process for any particular position for which you apply. Thereafter, if you created a profile in the Timken Careers web portal, we will retain your personal data to enable us to update you on current open positions within Timken, unless you delete your profile, which you may do at any time. We will also retain your personal data as long as necessary to respond to challenges about a hiring decision, assert or defend our legal rights, and comply with applicable laws and regulations.

For further information about the retention of your personal data, please contact us using the details provided at the end of this Notice.

If your application is successful, we will keep only the recruitment information that is necessary in relation to your employment in accordance with our practices and, where required by law, as set out in our Employee Privacy Notice and our records retention policy.

WHAT ARE YOUR RIGHTS UNDER GDPR?

Where the GDPR applies – such as where your personal data is processed by a Timken group company located in the EU/EEA – you have a number of rights. These rights are not absolute and may be subject to certain conditions and exemptions under the GDPR and local implementing laws. These rights include the right to:

- request access to your personal data, 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 personal data we hold about you;
- request erasure of your personal data, which, when applicable, enables you to require us to delete your data, for example where the data is no longer necessary for the purposes of processing;
- in certain circumstances request the transfer of your personal data to another party; and
- request the restriction of processing of your personal data, for example if you want to establish its accuracy or the reason for processing it.

You also have the right to object (on grounds related to your personal situation) to the processing of your personal data where we are relying on our legitimate interests or those of a third party.

You will not usually have to pay a fee to access your personal data 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.

Where we rely on your consent to process your personal data, you have the right to withdraw your consent for that specific processing at any time. If we receive notice from you withdrawing your consent, we will stop that specific processing of your personal data unless there is an alternative legal basis to continue such processing.

If you think any information we have about you is incorrect or incomplete, please write to us or email us using the contact details set out in the “Contacting Us” section below and we will correct or update any information as soon as possible.

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.

HOW CAN YOU MAKE A COMPLAINT?

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 GDPR applies to your personal data, you also have the right to lodge a complaint with a supervisory body 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

You may contact us by addressing the question to the location of the local Timken group company that would be the employer for the position for which you applied. You may also contact the main 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

EU/EEA Timken Group Companies

Timken Europe (France)
Timken Europe B.V. (Netherlands)
Timken Espana S.L. (Spain)
Timken GmbH (Germany)
Timken ILS Cheltenham Limited (UK)
Timken Italia S.r.l. (Italy)
Timken Polska SP z.o.o. (Poland)
Timken PWP S.r.l. (Romania)
Timken Romania SA (Romania)
Timken UK Limited (UK)
R+L Hydraulics GmbH (Germany)
Groeneveld s.r.o. (Czech Republic)
Groeneveld Lubrication Solutions S.a.r.l. (France)
Groeneveld Lubrication Solutions GmbH (Germany)
Groeneveld Italia S.r.l. (Italy)

Groeneveld Lubrication Solutions S.r.l. (Italy)
Groeneveld Groep Holding B.V. (Netherlands)
Groeneveld Transport Efficiency B.V. (Netherlands)
Groeneveld Transport Efficiency Nederland B.V. (Netherlands)
Groeneveld Polska SP z.o.o.
Groeneveld Transport Efficiency Iberica S.A. (Spain)
Groeneveld UK Ltd. (UK)
Rollon S.a.r.l. (France)
Rollon GmbH (Germany)
Rollon B.V. (Netherlands)
Rollon UK (UK)
Rollon S.p.A (Italy)
Cone Drive Operations Ltd. (UK)