GLOBAL EMPLOYEE PRIVACY NOTICE

Last updated: 10 June 2025

Johnson Controls International plc and its affiliated companies (collectively, **Johnson Controls**) care about your privacy and are committed to processing your Personal Information in accordance with fair information practices and applicable data privacy laws.

As a sign of our commitment to privacy, we have adopted a set of Binding Corporate Rules ("BCRs"). These contain our global privacy commitments, including our policy on transfers of personal information and associated individual privacy rights, with the aim of ensuring that your Personal Information is protected while processed by our affiliates around the world. These BCRs have been approved by the European Data Protection Authorities. You can consult our BCRs on the Privacy Center.

1. Scope

This global notice explains how Johnson Controls handles the personal information of employees, applicants, interns, former employees, dependents, beneficiaries, contractors, consultants and temporary agency workers in the course of its activities.

Personal Information means any information relating to an identified or identifiable natural person; one who can be identified, directly or indirectly, by reference to an identifier such as 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.

Special Categories of Personal Information (also known as Sensitive Personal Information) means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, genetic data or biometric data.

2. Identity of Data Controller

Generally, the Johnson Controls entity responsible for the processing of your personal information (often referred to as a 'data controller'), is the Johnson Controls entity with which you have an employment relationship (or, where you are not an employee, the Johnson Controls entity responsible for your work). If you are in any doubt you can contact the Human Resources Department or contact the Privacy Office (privacy@jci.com).

3. Categories of Personal Information

In the normal course of human resources and business activities, we collect and process the following categories of Personal Information:

Personal identification information	Information such as your name, place of birth, home address, date of birth, gender, work-related photographs, home phone number and personal email address.
Government-issued identification numbers	Passport number, Social security number and/or national ID number,
Right-to-work information	Details of your immigration status, right-to-work and residence status.
Family and emergency contact details	The name(s) and contact details of your family members and / or emergency contacts.

Employment-related information	Information relating to your employment/work for Johnson Controls, such as years of service, work location, employment ID, work record, vacation absences, and contract data.
Educational and training information	Information relating to your education and training, such as your educational awards, certificates and licenses, vocational records and in-house training attendance.
Recruitment and performance-related data	Information such as career objectives, ratings, comments, feedback results, career history, work equipment, career and succession planning, skills and competencies and other work- related qualifications and background information.
Information related to your usage of Johnson Controls' assets	Information relating to your usage of, in particular, Johnson Controls' computers, mobile devices, and telecommunication systems, and traffic generated via the Internet.
Information collected by mobile device management software	The information collected by Johnson Controls' mobile device management software, including your name, mobile number, business e-mail address, country of your mobile provider and information contained in corporate applications installed on your device.
Compliance and risk management information	Information required for compliance and risk management, such as disciplinary records, background check reports and security data.
Payroll and payment or benefits related information	Information such as marital status, salary and insurance information, details of dependents, government identifier or tax numbers, bank account details, and employment related benefits information, family and dependent information.
Location and attendance information	Information related to location and time and attendance management.
Travel and passport information	Information related to [employment-related] travel you have undertaken, including passport information.
Business-related voice/video recordings	Business-related voice/video recordings, for example, of meetings and/or presentations you have attended.

In addition, we may process Special Categories of Personal Information, for example:

Health and sickness information	This may include information such as health conditions, symptoms, diagnosis, treatment and medication where necessary, medical certificates and workplace injury and illness information.
Occupational health and safety information	Information relating to occupational health and safety.
Race and nationality	This information may be collected where required or permitted by law.
Biometric data	This may include facial recognition information where our locations operate such systems, in compliance with applicable law.
Precise geographic location data	We may process this information in situations where your role requires it and where permitted by law, including where you operate one of our vehicles.
Trade union membership	Details of any trade union memberships you hold.

Criminal record information	Criminal convictions and prosecutions and other background check information, where permitted by law.
[Certain jurisdictions] **Passport number, social security or national identification number**	In certain jurisdictions, your passport number, social security number or national identification number are classified as Special Category and/or Sensitive Personal Information
[India only] **Passwords and financial information**	In India, passwords and financial information (such as bank account, or credit or debit card, or other payment instrument details) are considered Sensitive Personal Information.

As well as collecting Personal Information directly from you, we may also collect your Personal Information from other sources, including:

- Government organisations, health providers and benefits providers;
- Service providers e.g. companies that perform background checks;
- Your supervisors, colleagues or nominated referees; and
- Publicly available information.

4. Purposes of Processing and legal bases for processing

We collect and process Personal Information for the purposes listed below. Where we are required by law, we will rely on one or more legal bases, which may include your prior consent. For the purposes of European data protection law we will rely on the legal bases listed in the table below (see "Legal basis relied upon for this processing").

Purpose for processing Personal Information	**Personal Information processed for this purpose**	**Legal basis relied upon for this processing**
Human resources and employment: This includes workforce administration, payroll, compensation and benefit programs, performance management, learning and development, advancement and succession planning.	Personal identification information Government-issued identification numbers Right-to-work information Family and emergency contact details Employment-related information Educational and training information Recruitment and performance-related data Payroll and payment or benefits related information Location and attendance information	The processing is necessary for us to perform our contract with you, such as to pay you and manage your employment relationship with us.

	Special Categories of Personal Information Health and sickness information Occupational health and safety information Biometric data Precise geographic location data Trade union membership Race and nationality	The processing is necessary for the purposes of carrying out obligations and exercising rights in relation to employment law. Where race is used for diversity and inclusion we may rely on explicit consent.
Workforce planning and recruitment	Personal identification information Government-issued identification numbers Right-to-work information Employment-related information Educational and training information Recruitment and performance-related data **Special Categories of Personal Information** Race and nationality	The processing is necessary for us to perform our contract with you, such as to manage the employment relationship with you and allocate work. The processing is necessary for us to take steps to enter into a contract with you. For example, if you apply to work for us. Where race is used for diversity and inclusion we may rely on explicit consent.
Mergers, acquisitions and divestitures	Personal identification information Employment-related information Payroll and payment or benefits related information *Depending on the nature of the merger, acquisition or divestiture, potentially other categories of Personal Information listed in Section 3.*	The processing is necessary for the purposes of our legitimate interests in connection with undertaking mergers, acquisitions and divestitures.
Legal compliance, including corporate management, compliance with government authority requests for information, liens, garnishments and tax compliance	Personal identification information Right-to-work information Employment-related information	The processing is necessary for compliance with a legal obligation to which Johnson Controls is subject.

	Payroll and payment or benefits related information *Depending on the nature of the compliance obligation, potentially other categories of Personal Information listed in Section 3.*	
Workplace management, such as travel and expense programs and internal health and safety programs	Personal identification information Employment-related information Travel and passport information Payroll and payment or benefits related information **Special Categories of Personal Information** Health and sickness information Occupational health and safety information	The processing is necessary for us to perform our contract with you, such as to manage our workforce and deliver travel, expense, and health and safety programs to our employees. The processing is necessary for the purposes of carrying out obligations and exercising rights in relation to employment law.
Internal reporting and audit	Personal identification information Employment-related information Payroll and payment or benefits related information Information needed for compliance and risk management *Depending on the nature of the report or audit, potentially other categories of Personal Information listed in Section 3.*	The processing is necessary for the purposes of our legitimate interests in carrying out internal reporting and conducting audits.
To protect Johnson Controls, its workforce, and the public against injury, theft, legal liability, fraud or abuse or other injury	Personal identification information Right-to-work information Family and emergency contact details Information related to your usage of Johnson Controls' assets Information collected by mobile device management software Information needed for compliance and risk management	The processing is necessary for our legitimate interests in protecting Johnson Controls, its workforce, and the public against injury, theft, legal liability, fraud or abuse or other injury. The processing may also be necessary for compliance with a legal obligation to which Johnson Controls is subject.

	Special Categories of Personal Information Occupational health and safety information Biometric data Criminal record information	The processing is necessary for the purposes of carrying out obligations and exercising rights in relation to employment law.
Training and product demonstrations	Personal identification information Educational and training information Business-related voice/video recordings	The processing is necessary for our legitimate interests in providing training and conducting product demonstrations.
Product development that would involve or relate to employees	Personal identification information Employment-related information *Depending on the nature of the product development, potentially other categories of Personal Information listed in Section 3.*	The processing is necessary for our legitimate interests in developing new products and assessing their efficacy.
Monitoring and filtering the use of devices, our network, and internet traffic for lawful business purposes, and in particular for: • Ensuring adequate Information Systems integrity and detecting and preventing criminal activity, including cyber-crime; • Protecting information, including, but not limited to, personal information, confidential information, and high-value business information against destruction, loss, alteration, unauthorized access, disclosure or hacking; • Securing the effective operation of its Information Systems; • Ensuring compliance with applicable regulatory and self-regulatory obligations; • Detecting instances of non-compliance with Johnson Controls' policies on internet use and the Code of Ethics.	Personal identification information Information related to your usage of Johnson Controls' assets Information collected by mobile device management software Information needed for compliance and risk management	The processing is necessary for our legitimate interests in ensuring the integrity of our information systems. The processing may also be necessary for compliance with a legal obligation to which Johnson Controls is subject.

Please note: Where mobile device management software has been installed on your personal device (in order for you to access Johnson Controls e-mail, network services and data), Johnson Controls may need to make changes to the device's security configuration in order to comply with Johnson Controls mobile security requirements. Any monitoring and/or filtering of usage of this device, for the above mentioned purposes, is limited to corporate applications. For more information please see 'How to contact us' below.		

5. Recipients of Personal Information

Category of recipient	Purpose for disclosing Personal Information
Other Johnson Controls entities	We may disclose Personal Information to other Johnson Controls entities who perform services on our behalf for the purposes listed in Section 4.
Joint ventures, subcontractors, vendors or suppliers	We may disclose Personal Information to joint ventures, subcontractors, vendors or suppliers who perform services on our behalf for the purposes listed in Section 4.
A newly formed or acquiring organization	If Johnson Controls is involved in a merger, sale or a transfer of some or all of its business, Personal Information may be disclosed to the newly formed or acquiring organization.
Third party service providers	Personal Information may be shared with third party service providers who help us carry out our business activities, for example, IT providers, benefits providers, payroll service providers, and advisers (such as lawyers, accountants and auditors).
Recipients we are [legally] required to disclose Personal Information to	We may disclose Personal Information in order to comply with a legal obligation Johnson Controls is subject to, such as complying with an applicable court order or law.
Recipients you have consented to us disclosing Personal Information to	We may disclose Personal Information to recipients where you have consented to this disclosure, for example, where disclosure is necessary for employment verification checks.
Recipients who may receive Personal Information in an life-threatening emergency	Where reasonably necessary in the event of a life threatening emergency, we may disclose Personal Information to third parties, for example, to ensure emergency care can be provided.

6. International Transfers

The third parties, subsidiaries and affiliates to which your Personal Information can be disclosed may be located throughout the world, including the United States, India, Slovakia and Mexico; therefore information may be sent to countries with different privacy laws than your country of residence. In certain circumstances, courts, law enforcement agencies, regulatory agencies or security authorities in those other countries may be entitled to access your Personal Information. As required by applicable law, we take measures to ensure that your Personal

Information receives an adequate level of protection, which include our Binding Corporate Rules, setting forth our high standards for processing personal information, and Standard Contractual Terms. Where required, in accordance with local law, we may request your consent.

APEC Cross Border Privacy Rules System (CBPR): Johnson Controls privacy practices, described in this Privacy Notice, comply with the APEC Cross Border Privacy Rules System. The APEC CBPR system provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. More information about the APEC framework can be found here. Click here to view our APEC CBPR certification status.

For transfers from the European Economic Area ("EEA"), the UK, and/or Switzerland: Some jurisdictions outside of the EEA/UK/Switzerland are recognized by the European Commission, the UK government, and/or the Swiss government as providing an adequate level of protection according to EEA/UK/Swiss standards: the list of the EEA's adequate jurisdictions is available here, the list of the UK's adequate jurisdictions is available here, and the list of Switzerland's adequate jurisdictions is available here. For transfers from the EEA, the UK, and/or Switzerland to countries not considered adequate by the European Commission, the UK government, or the Swiss government (as applicable), we have put in place adequate measures, such as standard contractual clauses adopted by the relevant authority, to protect your Personal Information. Employees in the EEA, UK, and Switzerland may obtain a copy of these measures by contacting us in accordance with the "How to Contact Us" section below

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at: https://feedback-form.truste.com/watchdog/request.

7. Retention

Your Personal Information will be retained as long as necessary to achieve the purpose for which it was collected, usually for the duration of any contractual relationship and for any period thereafter as legally required or permitted by applicable law. Johnson Controls Records Retention schedules can be found at: https://my.jci.com/Ethics/Pages/RIM.aspx.

8. Protection and Security

Johnson Controls takes precautions to protect Personal Information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. We have taken appropriate technical and organizational measures to protect the information systems on which your Personal Information is stored and we require our suppliers and service providers to protect your Personal Information by contractual and other means.

9. Your Rights

Your rights may depend on local law. Johnson Controls will be guided by local law in responding to privacy rights requests such as those listed below.

- Information and Access: You may request to access your Personal Information, be provided with supplemental information, and be provided with a copy of your Personal Information. The right to Information and Access has some restrictions. For example, access may be denied (i) in the case of recurrent access requests within a short time interval, or (ii) where providing such access or correction could compromise the privacy of another person or unreasonably expose sensitive company information.
- Rectification: You may request to rectify and/or update your inaccurate or out-of-date Personal Information.
- Erasure: You may have the right to have your Personal Information erased. This right is subject to restrictions.

- Restriction: You may have the right to have your Personal Information restricted. Restriction means that your Personal Information is only stored by Johnson Controls, and not further processed, while your complaint is dealt with.
- Object to Processing: You may have the right to object to specific types of processing. These types are direct marketing, processing for research or statistical purposes and processing based on legitimate interests. The right to object to processing based on legitimate interests may be subject to demonstration by Johnson Controls of grounds which override your right to object.
- Data Portability: You may have the right to request Data Portability. Data Portability is the provision of your Personal Information in a structured, commonly used and machine readable form so that it may be transferred by you or by Johnson Controls to another company easily. The right to Data Portability is subject to restrictions. For example, Data Portability does not apply to paper records, and must not prejudice the rights of others, or sensitive company information.
- Right not to be subject to decisions based solely Automated Decision Making: You may have the right not to be subject to decisions based solely on automated processing (i.e. without human intervention), if those decisions produce legal effects or significantly affect you. Automated Processing is Processing of your Personal Information by automated means. If we implement processing that employs automated decision-making which produces legal effects or that significantly affects you, then you shall have the right not to be subject to a decision based solely on automated processing.

You may also have the right to lodge a complaint with a supervisory authority.

You may request to exercise any of these rights through your local Human Resources contact or the Privacy Office at privacy@jci.com.

10. Your obligations

Please keep Personal Information up to date and inform us of any significant changes to Personal Information.

This Privacy Notice also applies to the Personal Information of other individuals which you provide to us. For example, beneficiaries of your employment benefits, such as the individuals who are on your health plan and the beneficiaries of your retirement accounts, as well as your emergency contacts and other dependents. It is your responsibility to inform any such individuals about this Global Employee Privacy Notice and/or provide a copy of this Global Employee Privacy Notice to those individuals and ensure that you have the right to provide their Personal Information to us.

It is also your responsibility to follow applicable law and company policies, standards, and procedures that are brought to your attention when handling any Personal Information to which you have access in the course of your relationship with us. In particular, you should not access or use any Personal Information for any purpose other than in connection with and to the extent necessary for your work with us. You understand that these obligations continue to exist after termination of your relationship with us

11. Consent and Withdrawal of Consent

If consent is the legal basis of the processing of your Personal Information or Special Categories of Personal Information, you may withdraw your consent free of charge, by contacting our Privacy Office at privacy@jci.com (where that withdrawal is required and/or permitted under applicable law).

12. Modifications to our Privacy Notice

We may amend this notice from time to time, should it become necessary to do so. If we propose to make any material changes, we will notify you by means of a notice on this page. This notice may also be supplemented by

other statements as needed to comply with local requirements in the country where you live, or where employee representation agreements exist.

13. Privacy Concerns and How to contact us

If you have any questions about this notice or if you believe that your Personal Information is not handled in accordance with the applicable law or this notice, you have several options:

- Contact the Privacy Office at privacy@jci.com;
- Contact your Data Protection Officer at dpo@jci.com
  - Discuss the issue with your supervisor or another supervisor or manager;
- Contact the Human Resources department; or
- You may also contact Johnson Controls 24-hour Integrity Helpline at: www.johnsoncontrolsintegrityhelpline.com.