Chinese Simplified (汉语)
Chinese Traditional (繁體中文)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
French (Français)
German (Deutsch)
Indonesian (Bahasa Indonesia)
Italian (Italiano)
Japanese (日本語)
Korean (한국어)
Polish (Polski)
Portuguese (Português)
Spanish (Español)
Thai (ภาษาไทย)
Turkish (Türkçe)

Whistleblowing & Privacy Notice for Johnson Controls Integrity Helpline

Last revised: July 26, 2024

This Johnson Controls Integrity Helpline (the "Integrity Helpline") is provided by Johnson Controls International plc (hereafter referred to together with its subsidiaries as "**JCI**"). It allows you to report alleged or suspected misconduct, irregularities, or other noncompliance connected to JCI business practices and processes (as described in the next section and as further detailed in Schedule 1). You may report via the internet at JohnsonControlsIntegrityHelpline.com; by telephone (go to JohnsonControlsIntegrityHelpline.com or the employee portal for toll-free numbers); or, when so provided by applicable law, via an in-person meeting. The Integrity Helpline is operated by JCI's independent service provider, One Trust, formerly Convercent, established at 3858 Walnut Street, Suite #255, Denver, CO 80205, USA ("**Convercent**").

This Notice sets out the rights that apply to individuals (i.e., whistleblowers) who use the Integrity Helpline to report their concerns. This Notice also provides information about how the Integrity Helpline works, including when and how it may be used. Rights and practices may vary per country in which JCI operates to reflect local practices and legal requirements.

The use of the Integrity Helpline is voluntary. The Integrity Helpline is available 24 hours a day, 7 days a week, 365 days a year for you to ask questions or report compliance-related concerns.

Concerns That May be Reported Through the Integrity Helpline

Anyone who suspects or observes misconduct, including potential violations of the Johnson Controls Code of Ethics, Company policy, or the law, is encouraged to use the Integrity Helpline globally for reporting their concerns. Note that you can also report your concerns through other reporting channels, such as your supervisor or manager, a member of the Human Resources, Compliance or Legal teams, or other dedicated individuals. In some countries, if you report a concern, you may be entitled to be protected as a whistleblower under that country's law. For more information about the scope of reportable concerns through the Integrity Helpline under EU and EU Member State laws, see Schedule 1 of this Notice ("*Scope of reportable concerns in EU Member States*").

While we do encourage you to identify yourself when making a report to the Integrity Helpline, you are not always obligated to do so. JCI will accept anonymous reports to the extent permitted by applicable law.

Johnson Controls - © 2024 - All Rights Reserved

Collection of Information

JCI normally collects the following information through the Integrity Helpline: your name, title and contact details; the names of and other information about individuals that are named in your report; a description of the conduct at issue in your report, including date, location, and other pertinent information for the investigation at hand; and any questions you may have. JCI may also collect information from other sources (such as your colleagues and publicly available sources) during any subsequent investigation.

JCI may use the information mentioned above because we have to either comply with a legal obligation imposed on JCI or we have a legitimate interest to investigate the report that you submitted to us.

Processing Information and Access to Information

When you call into the Integrity Helpline, a representative from Convercent will answer your telephone call. Convercent does not capture the telephone number of any incoming calls so that your call-in information can remain anonymous. Convercent also does not record the calls. You will speak with a Communication Specialist who will ask you for information, document your input, and ask follow-up questions to clarify information. Please note that the Communication Specialist is not able to answer any questions about ethics or policy and cannot advise you on any course of action.

If provided by applicable law, for example in the EU, you can ask for an in-person meeting to report your concern.

After the initial report or inquiry is made, a detailed record is prepared and recorded by Convercent directly into the Integrity Helpline system. This record is accessed by trained JCI personnel responsible for administering the Integrity Helpline, who assign it to the appropriate Investigation Team. Depending on the nature of the concern, it may be assigned to Forensics, Human Resources, Enterprise Security, or a member of the Legal or Compliance teams (collectively, the "**Integrity Helpline Investigation Team**"). The assigned investigator reviews the concern and conducts an investigation.

When investigating your report, which may, for example, include speaking to the individuals implicated in your report and other witnesses, the Integrity Helpline Investigation Team will make all reasonable efforts to protect your identity and treat your report as confidential. Additional information and clarifications may be necessary as the investigation progresses, in which case you will be contacted again. Where necessary, the Integrity Helpline Investigation Team may also need to notify members of HR, Legal, Compliance, or management of any finding of violation for purposes of transparency, determining any disciplinary action, and developing a remediation plan. The information may also be shared with JCI's external advisers (such as lawyers and/or auditors) or other third parties whose input is relevant for the purpose of our investigation, and competent authorities (such as regulators and/or police), as allowed or required by applicable law.

You will be informed about the progress of the investigation at reasonable intervals as appropriate, or otherwise within the timeframes prescribed by applicable laws.

Please note that the information you supply may result in decisions that affect JCI employees and other third parties involved in the relevant incident. We therefore ask you to provide only information that you have reasonable grounds to believe is accurate. Knowingly providing inaccurate or misleading information may result in disciplinary action or even civil or criminal liability.

Retaliation against any JCI employee or any individual who seeks advice, raises a concern, reports misconduct, or cooperates with an internal investigation in good faith is strictly prohibited. In such cases, JCI will take appropriate action, even if it later turns out that the employee or individual was mistaken in reporting the matter. If you think that you or anyone else has been retaliated against for raising a concern, you should promptly report it to the Integrity Helpline.

Information Use, Retention, and Data Transfer

JCI has contracted with Convercent to protect the confidentiality and security of your personal information, and Convercent is only permitted to use your personal information for the provision of the Integrity Helpline. Your report will be stored in a Convercent database. Convercent will share the reports with us so that we can review and investigate your concern. We will store the relevant information on secure servers managed by JCI with appropriate access controls in place.

Beyond Convercent, as JCI is a global organization with offices in multiple locations around the world, we may transfer your personal information to JCI in the United States, to any JCI entity worldwide, or to third parties and business partners who are located in various countries around the world. The global nature of our organization means your personal information may be sent to countries that have different data protection rules than are found in the country where you work or are from. We have implemented measures to safeguard your personal information should it be transferred to another country, which include the following:

- **Standard Contractual Clauses**: We use contracts, such as the Standard Contractual Clauses published by the European Commission, to help protect your personal information when it is transferred outside Europe.
- **Binding Corporate Rules**: 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 our Privacy Center.
- **EU-US Data Privacy Framework (EU-US DPF), UK Extension to the EU-US DPF and the Swiss-US Data Privacy Framework (Swiss-US DPF) (together, the "Data Privacy Framework Program"):** JCI has certified to the US Department of Commerce that it adheres to the principles set out in the Data Privacy Framework Program with regard to the processing of personal information received from the European Union, the

United Kingdom (and Gibraltar), and/or Switzerland. For further details, please read the Data Privacy Framework Program section on our Global Privacy Notice here.

- **APEC Cross Border Privacy Rules System ("CBPR")**: JCI privacy practices, described in this 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.

If you are in Japan, please be aware that we may jointly use and share your personal information within the JCI group to the extent needed for the purposes set out in this Notice. Johnson Controls K.K. and Hitachi-Johnson Controls Air Conditioning, Inc. are responsible for the management of the personal information that is jointly used.

Information relating to a report made via the Integrity Helpline will be archived or deleted when the investigation has been closed and no further action is needed, when the period for any relevant litigation has lapsed, and when our obligations for record keeping relating to investigations have lapsed.

Questions & Complaints

If you would like to request to access, correct, update, suppress, restrict, or delete personal information; object to the processing of personal information (to the extent these rights are provided to you by applicable law); or ask a question regarding processing of your personal information you may contact us at privacy@jci.com. We will respond to your request consistent with applicable law.

You can contact the relevant Data Protection Officer, where appointed, at privacy@jci.com. Subject to applicable law, you may also lodge a complaint with a data protection authority where you have your habitual residence or place of work or where an alleged infringement of applicable data protection law occurs (see here for the list of EEA authorities and here for the UK Information Commissioner's Office's contact details).

If you have any questions or concerns about the Integrity Helpline or JCI's compliance program, please contact us at askcompliance@jci.com. Note that you may also have the right to report your concerns about violations of EU laws externally to competent authorities of EU Member States, when EU law applies to your report. You have this right (1) if this Integrity Helpline does not function properly, (2) if your report was not dealt with diligently or within a reasonable timeframe, or (3) if no appropriate action was taken to address your concerns despite the results of the related internal enquiry confirming the existence of a violation of an EU law. We do encourage you to first contact askcompliance@jci.com, who will try to independently resolve your concerns about the effectiveness of the Integrity Helpline and subsequent investigation.

For more information on how JCI processes personal information, please see the JCI privacy notice that applies to you, available at https://www.johnsoncontrols.com/trust-center/privacy/global-privacy-notice (JCI's Global Privacy Notice) and https://www.johnsoncontrols.com/legal/employee-privacy (Employees' Privacy Notice). If

you are uncertain which privacy policy applies to you, please contact privacy@jci.com for clarifications.

Changes

We will update this notice from time to time. Any changes will be posted on this page with an updated revision date.

Schedule 1
Scope of reportable concerns in EU Member States

The EU Whistleblowing Directive ((EU) 2019/1937) applies certain protections to persons who report concerns about issues about public procurement; financial services; products and markets; prevention of money laundering and terrorist financing; product safety; transport safety; public health; protection of the environment; consumer protection affecting the financial interest of the EU or relating to the internal market (e.g., competition and State aid rules); radiation protection and nuclear safety; food safety; animal health and welfare; and protection of privacy, data protection and data security. In addition, the table below sets out the scope of reportable concerns that entitle individuals to protection in EU Member States in addition to the matters set out in the EU Whistleblowing Directive. **If you need any clarification about this scope, please contact askcompliance@jci.com.**

Country	Scope of reportable concerns
1. Austria	The scope is extended to reports covering the criminal corruption offenses set out in Sections 302 to 309 of the Austrian Criminal Code, such as bribery or illegal allocation of advantages/gifts to public officials.
2. Belgium	The scope is extended to reports covering tax and social fraud; social fraud can encompass undue receipt of benefits and other infringements of social laws in Belgium.
3. Czech Republic	The scope is extended to reports covering: • Any criminal offense under national law (such as extortion and physical harm); • Any misdemeanors (i.e., administrative offenses) punishable by a fine of at least CSK 100,000 (such as violations of the Czech Labor Code); and • Any violations of the Czech whistleblowing law.
4. Denmark	The scope is extended to reports covering: • Matters that relate to serious offenses or other serious matters; and • Actions or omissions that make it possible to circumvent the purpose of the provisions of the Danish whistleblowing law.
5. Finland	The scope is extended to reports covering violations of national law, based on the list of matters within the scope of the EU Whistleblowing Directive, and any matters that can seriously endanger the goals and broader aims of such laws.

6. France	The scope is extended to reports covering: • Actual and attempted violations of international law applicable in France; • Crimes or offenses under national law; and • Threats or harm to the public interest.
7. Germany	The scope is extended to reports covering: • All criminal offenses under national law; • Administrative offenses (i.e., violations that are subject to a fine under national law) that serve to protect life, limb, or health of individuals or the rights of employees and their representative bodies (e.g., works councils); and • Concerns about supply chain due diligence.
8. Hungary	The scope is extended to reports covering: • Any illegal or suspected illegal acts, omissions, or other misconduct, provided that the matter is within the scope of the EU Whistleblowing Directive; and • Misconduct and violations of workplace rules that an organization has put in place to protect public interests or overriding private interests for its employees under the conditions set out in Article 9(2) of Act I of 2012 in the Labor Code.

9. Ireland	The scope is extended to reports covering: • An offense that has been, is being, or is likely to be committed; • A person who has failed, is failing, or is likely to fail to comply with any legal obligation, other than one arising under the worker's contract of employment or other contract whereby the worker undertakes to do or perform personally any work or services; • A miscarriage of justice that has occurred, is occurring, or is likely to occur; • The fact that the health or safety of any individual has been, is being, or is likely to be endangered; • The fact that the environment has been, is being, or is likely to be damaged; • An unlawful or otherwise improper use of funds or resources of a public body, or of other public money, which has occurred, is occurring, or is likely to occur; • An act or omission by or on behalf of a public body that is oppressive, discriminatory, or grossly negligent or constitutes gross mismanagement; • A violation of law that has occurred, is occurring, or is likely to occur; and Information tending to show that any matter falling within the above has been, is being, or is likely to be concealed or destroyed or an attempt has been, is being, or is likely to be made to conceal or destroy such information.
10. Italy	The scope is extended to reports covering: • Administrative, accounting, civil, and criminal offenses; • Unlawful conduct set out in Decree 231/2001 (a law that governs corporate criminal liability); and • Acts or conduct that undermine the object or purpose of the matters within the scope of the EU Whistleblowing Directive.
11. Luxembourg	The scope is extended to reports covering any unlawful act or omission that is contrary to the object or purpose of national or EU law.
12. Netherlands	The scope is extended to reports covering: • Acts or omissions with an impact on the public interest, such as violations or potential violations of internal rules established by an employer; and • Acts or omissions that could pose a danger to public health, to the safety of persons, to the environment, or to the proper functioning of the public service or of an organization.

13. Poland	The scope of the EU Whistleblowing Directive is extended to reports covering: • Violations of constitutional rights and freedoms; • Financial interests of the Treasury of the Republic of Poland, and the local government unit; and • Based on the organisation's discretion, violations of internal regulations or ethical standards applicable to the organisation.
14. Portugal	The scope is extended to reports covering all crimes stated in Crimes under Law no. 5/2002, of 11 January, which are: • Drug trafficking; • Human trafficking; • Terrorism, terrorist organizations, international terrorism, and financing of terrorism; • Weapons trafficking; • Influence peddling / lobbying; • Active and passive corruption, both in public and private sectors and in the international trade, whereby active corruption is when an individual is giving a bribe and passive corruption is when an individual receives a bribe; • Embezzlement; • Economic interest in a business; • Money laundering; • Criminal association; • Child pornography and solicitation; • Forgery; • Solicitation; • Smuggling; • Vehicle theft and trafficking; • Computer and software sabotage and damage; and • Illegitimate access to software.
15. Romania	The scope is extended to reports covering actions or inactions that constitute violations of national law, such as the matters within the scope of the EU Whistleblowing Directive.

16. Slovakia	The scope is extended to reports covering anti-social activities. This may include unethical practices in the workplace or issues that have a negative impact on society. Note that Slovakian law distinguishes between “anti-social activities” and “serious anti-social activities.” Reports about “serious anti-social activities” provide additional protection to whistleblowers, and are defined to include: • Specific offenses under the Slovakian Criminal Code such as criminal offenses damaging the interests of the EU, offenses of deceitful practice in public procurement and public auction, offenses committed by public officials, theft, embezzlement and corruption; • Criminal offenses punishable by a maximum penalty of at least 2 years’ imprisonment in Slovakia; • Administrative offenses for which the upper limit of the fine is determined by a calculation under national law; and • Administrative offenses punishable by a fine in Slovakia of at least EUR 30,000.
17. Spain	The scope is extended to reports covering acts or omissions that may constitute a serious or very serious criminal or administrative offense under national law, such as offenses involving financial loss to the Public Treasury and to the Social Security System, and violations in the area of health and safety at work.
18. Sweden	The scope is extended to reports covering: • Maladministration that is in the public interest to be disclosed; • Acts or omissions contrary to a directly applicable Union act within the scope of the EU Whistleblowing Directive; • Acts or omissions that contravene a law or other provision referred to in Chapter 8 of the Instrument of Government (the Swedish Constitution) and that implement or supplement an act of Union law falling within the scope of the EU Whistleblowing Directive; and • Acts or omissions contrary to the aim or purpose of the provisions of a Union act within the scope of the EU Whistleblowing Directive.