

## Johnson Controls Binding Corporate Privacy Rules

### Contents

1. Introduction
2. Scope and Application
3. Transparency and Notice
4. Fairness and Purpose Limitation
5. Data Quality and Proportionality
6. Rights of Individuals
7. Compliance with Local Law
8. Automated Decision Making
9. Direct Marketing
10. Security, Confidentiality and Use of Third Parties
11. Cross-border Transfers and Transfers outside of Europe
12. Monitoring Compliance through Audits
13. Cooperation with Data Protection Authorities
14. Conflicts with National Law
15. Complaints and Inquiries
16. Specific Rights for European Individuals
17. Effective Date and Changes and Publication of the Rules

## 1. Introduction

These Binding Corporate Privacy Rules (“Rules”) outline how the Johnson Controls group treats personal data of current, past and prospective employees and contractors, customers, consumers, suppliers and vendors (“Individual(s)”) and set out its approach to privacy and data protection compliance. An overview of the Johnson Controls group members that have committed to respect these Rules (collectively referred to as “JCI”, “We”, “Our” or “JCI Companies”, and each individually as “JCI Company”) can be found in Annex I to these Rules.

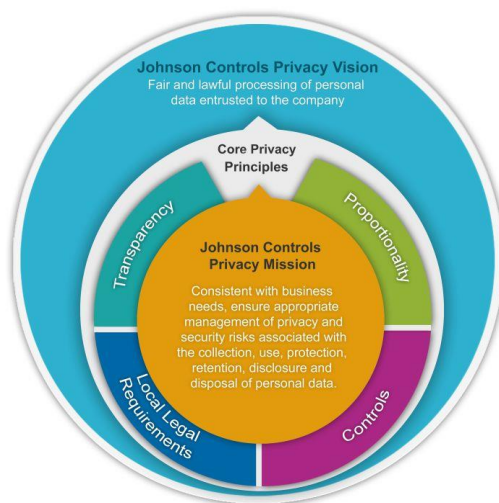
All JCI Companies and their employees must comply with these Rules when processing and transferring personal data. Personal data is any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

JCI’s privacy mission is:

**Consistent with business needs, ensure appropriate management of privacy and security risks associated with the collection, use, protection, retention, disclosure and disposal of personal data (“Processing”, “Process” or “Processed”).**

That mission in turn supports the JCI’s privacy vision:

**Fair and lawful Processing of personal data entrusted to the company.**



JCI has a Privacy Office that is comprised of a multi-disciplinary team that is active throughout the world. The Privacy Office is tasked with the enforcement of these Rules and ensures effective communication mechanisms are maintained to allow consistent governance of these Rules across JCI, regardless of business unit or geography. JCI maintains a privacy communications and awareness program to train Our employees globally and across all lines of businesses. We also conduct trainings aimed at certain functions that access personal data, are involved in its collection, or in the development of tools or systems used in Processing.

## 2. Scope and Application

As a global company, JCI Processes and transfers personal data between JCI Companies for normal business purposes, including workforce planning, talent acquisition, on-boarding, performance management, succession planning, learning and development, compensation and benefits, payroll, maintenance of employee data and other HR operational processes. Additionally, JCI Processes customer, consumer, supplier and vendor data for relationship management and the administration of its contractual obligations. JCI will also Process personal data to fulfil its reporting duties and facilitate internal communications.

JCI will respect these Rules when Processing and transferring personal data of Individuals regardless of the location. This ensures that personal data receives the same level of protection when it is transferred between JCI Companies across the world. These Rules also apply when a JCI Company Processes personal data on behalf of other JCI Companies.

Johnson Controls International NV/SA, a Belgian public limited company, acts as the affiliate with delegated data protection responsibility and is responsible for taking the necessary actions to ensure compliance with the Rules by JCI Companies.

### **3. Transparency and Notice**

We maintain and provide transparent notices to Individuals about why and how We collect and Process their personal data. These notices include clear information on the use of personal data, including the purposes for which personal data is Processed. Consistent with applicable legal requirements, notices will also include any other information to ensure that Processing is fair such as the identity of the JCI Company using the personal data, other recipients, rights and practical means for Individuals to contact us or exercise their rights. If We do not provide notice at the time of collection, We will do so as soon as possible thereafter, except if there is an exemption under applicable law for not doing so.

### **4. Fairness and Purpose Limitation**

Personal data will be Processed in a fair and lawful manner.

Personal data will be collected for specific and legitimate purposes and not further Processed in a way incompatible with those purposes. In certain cases, additional consent from Individuals may be required. JCI Processes personal data for legitimate business purposes, such as the management and administration of human resources, customers, consumers, vendors and suppliers or to pursue compliance with legal requirements.

### **5. Data Quality and Proportionality**

Personal data Processed by JCI will be:

- Adequate, relevant and not excessive in relation to the purposes for which it is collected and used.
- Accurate, complete and kept up to date, to the extent necessary.
- Not Processed or retained in an identifiable format for longer than necessary to achieve the purposes.

## **6. Rights of Individuals**

In addition to Our commitment to transparency and notice to Individuals, JCI respects and complies with Individuals' rights to access personal data relating to them. This includes confirmation to the Individual as to whether or not personal data relating to him/her is being Processed, the purposes of Processing, categories of personal data concerned, any recipients or categories of recipients to whom the personal data is disclosed, communication to him/her in an intelligible form about the personal data Processed and any available information as to the source. Individuals also have a right to request the correction of inaccurate personal data and, where relevant, obtain the deletion or blocking of their personal data. Individuals can exercise these rights without constraint, at reasonable intervals and without excessive delay or expense. More information on how to contact JCI and exercise these rights can be found in Section 15 of these Rules.

## **7. Compliance with Local Law**

JCI will only use personal data in accordance with the applicable law on personal data, including any additional laws that may relate to the Processing of personal data. Where applicable law requires a higher level of protection of personal data than the Rules, the law will take precedence over the Rules.

Sensitive or special personal data is 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. JCI will only Process sensitive or special personal data with the Individual's explicit consent, unless JCI can rely on an alternative legal basis, permission or requirement under applicable law for such Processing without consent.

## **8. Automated Decision Making**

If JCI implements Processing that employs automated decision-making, it will provide appropriate measures to safeguard Individuals' legitimate interests and will provide Individuals with the opportunity to receive information on the logic involved.

## **9. Direct Marketing**

When Processing personal data for direct marketing purposes, JCI provides measures for Individuals to opt-out from receiving marketing free of charge. This can be done by clicking on relevant website links, following the directions contained in an email or by contacting Our Privacy Office at [privacy@jci.com](mailto:privacy@jci.com).

## **10. Security, Confidentiality and the Use of Third Parties**

JCI applies appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, in particular where personal data is transferred over a network, and against all other unlawful forms of Processing. We maintain a comprehensive information security program that is proportionate to the risks associated with the Processing. The program is continuously adapted to mitigate operational risks and to ensure the protection of personal data taking into account best practices. JCI will also use enhanced security measures when Processing any sensitive personal data.

We conduct third party security reviews to ensure third parties to whom We entrust personal data offer adequate protection. Whenever JCI relies on such third parties that may have access to personal data, We enter into contractual arrangements with them to ensure they provide sufficient technical and organizational measures to protect the security and confidentiality of the personal data. We also require that they only act upon Our instructions.

Where a JCI Company Processes personal data on behalf of another JCI Company it will adhere to these Rules and act only upon the instructions of the JCI Company on whose behalf the Processing is carried out. JCI maintains processes to ensure that prior to the transfer of personal data to another JCI Company, the receiving JCI Company is bound by the Rules and abides by the applicable data privacy laws.

## **11. Cross-border Transfers and Transfers outside of Europe**

JCI maintains an inventory of key processing systems, storage locations, third party service providers and data flows. We ensure this information is kept up-to-date to reflect any change to Processing activities. We also maintain processes to ensure that personal data transferred will be treated in accordance with these Rules, regardless of their location.

Furthermore, when We do rely on third parties outside of JCI, We maintain procedures to ensure protection for personal data and compliance with applicable laws to the personal data transferred. If personal data is disclosed to third parties located outside the European Economic Area and Switzerland (“Europe”), We take measures to ensure that personal data transferred receives adequate protection in accordance with applicable data protection rules, such as through contractual clauses.

#### **12. Monitoring Compliance through Audits**

In addition to the work of Our Privacy Office, We maintain processes with JCI’s internal audit department to regularly audit Our compliance with the BCR. Audit findings are reported to Our management and the Privacy Office, and include follow up on action plans to ensure corrective measures are taken. Audit findings will be made available to the competent data protection authorities upon their request.

#### **13. Cooperation with Data Protection Authorities**

JCI will cooperate with the relevant data protection authorities and will respond to requests and questions about compliance with applicable data privacy laws and the Rules. When personal data is transferred between JCI Companies, the importing and exporting entities will cooperate with inquiries and audits from the data protection authority responsible for the exporting entity. JCI will also consider the advice of data protection authorities with competent jurisdiction on data protection or privacy law issues that may affect the Rules. Moreover, JCI will comply with any formal decision on the application and interpretation of the Rules by a data protection authority with competent jurisdiction that is final and to which no further appeal is possible.

#### **14. Conflicts with National Law**

If JCI has reason to believe that there is a conflict between national law and the Rules, which is likely to prevent it from complying with the Rules, the relevant JCI Company will promptly notify the Privacy Office or its local data privacy contact, except where local law prohibits such notification. The Privacy Office or its local data privacy contact will take a responsible decision on what action to take and will consult the competent data protection authorities in case of doubt.

## 15. Complaints and Inquiries

Any Individual whose personal data is subject to these Rules may raise concerns that JCI is not complying with them or applicable data protection law by contacting the Privacy Office to obtain details of JCI's complaint handling processes:

By email to: [privacy@jci.com](mailto:privacy@jci.com)

Or in writing to:

Johnson Controls Privacy Office  
c/o Johnson Controls International NV/SA,  
De Kleetlaan 7b, 1831 Diegem  
Belgium

All complaints will be handled by the Privacy Office in an independent manner. Furthermore, all individuals are welcome to communicate with JCI regarding privacy issues (including questions on how to exercise individual rights of access, rectification, deletion or blocking) or with questions or comments through one of the means above. All JCI employees are responsible for reporting any complaints or privacy incidents that are brought to their attention.

## 16. Specific Rights for European Data Subjects

### Third Party Beneficiary Rights

Individuals whose (i) personal data is subject to EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data or the Swiss Federal Act on Data Protection (as amended or replaced from time to time) and (ii) transferred to a JCI Company outside of Europe (collectively: "Beneficiaries" and individually: "Beneficiary") may seek enforcement of the Rules (other than Section 12 of these Rules covering audits) as third party beneficiaries by:

- lodging a complaint with each JCI Company that Processes their personal data or by contacting the JCI Privacy Office as set forth in Section 15 of these Rules;
- lodging a complaint with a national data protection authority of competent jurisdiction; or



- bringing proceedings against (i) Johnson Controls International NV/SA in the courts in Belgium or (ii) each JCI Company located in Europe that transferred the personal data in their respective jurisdictions.

#### Liability, Jurisdiction & Burden of Proof

As part of the remedies set forth in this Section 16 of these Rules, Beneficiaries may seek appropriate redress from Johnson Controls International NV/SA before the courts in Belgium to remedy any breach of the Rules by any non-European JCI Company and, where appropriate, receive compensation for damages suffered as a result of such breach, in accordance with a decision of a court.

If such Beneficiary demonstrates that he or she has suffered damage and that such damage likely occurred due to a breach of the Rules by a non-European JCI Company, the burden of proof to show that this entity is not responsible for the breach or that no such breach took place will rest with Johnson Controls International NV/SA.

#### **17. Effective Date and Changes and Publication of the Rules**

The Rules became effective on January 6, 2015 and apply to all Processing of personal data by JCI Companies on or after that date. The Rules may be modified as necessary, for example to ensure compliance with changes in local law or regulations, binding formal decisions of data protection authorities, as well as alterations to JCI processes or its internal organization.

JCI will communicate any material change to the Rules to the Belgian Privacy Commission and, where required, any other relevant European data protection authorities on at least an annual basis. Administrative changes or changes resulting from a change in local data protection legislation in any European country will not be reported unless they have a significant impact on the Rules. JCI will communicate any changes to the Rules to JCI Companies bound by them.

JCI will take measures to ensure that new JCI Companies are bound by the Rules and the Privacy Office will maintain an updated list of the JCI Companies. Personal data transfers to new JCI Companies will not take place before they are effectively bound by the Rules and able to comply.

The updated list of JCI Companies will also be communicated to the JCI Companies bound by the Rules and to the data protection authorities at recurrent time intervals where required.

These Rules will be made publicly available. For more information, please see [www.johnsoncontrols.com](http://www.johnsoncontrols.com). Individuals can obtain a copy of the intra-group agreement implementing the Rules by contacting the Privacy Office at the contact details provided in Section 15 above.