OpenBlue
Active Responder

Data privacy sheet

1. Introduction to the Johnson Controls Global Privacy Office and Global Privacy Program

Johnson Controls has a Global Privacy Office and a Global Privacy Program, involved at the beginning and throughout the design and development of our processes, activities, products, services, and solutions, in accordance with internationally accepted principles of Privacy by Design.

The Johnson Controls Global Privacy Office is led by the Chief Privacy Officer, and supported by Global Privacy Counsel, Global Privacy Professionals, Global Privacy Champions, analysts, and support staff.

The Johnson Controls Privacy Program is designed with the most stringent global privacy and data protection laws in mind, including the General Data Protection Regulation (GDPR) of the European Union (EU), Brazil's Lei Geral de Proteção de Dados (LGPD), Singapore's Personal Data Protection Act (PDPA), and California's Consumer Privacy Act (CCPA).

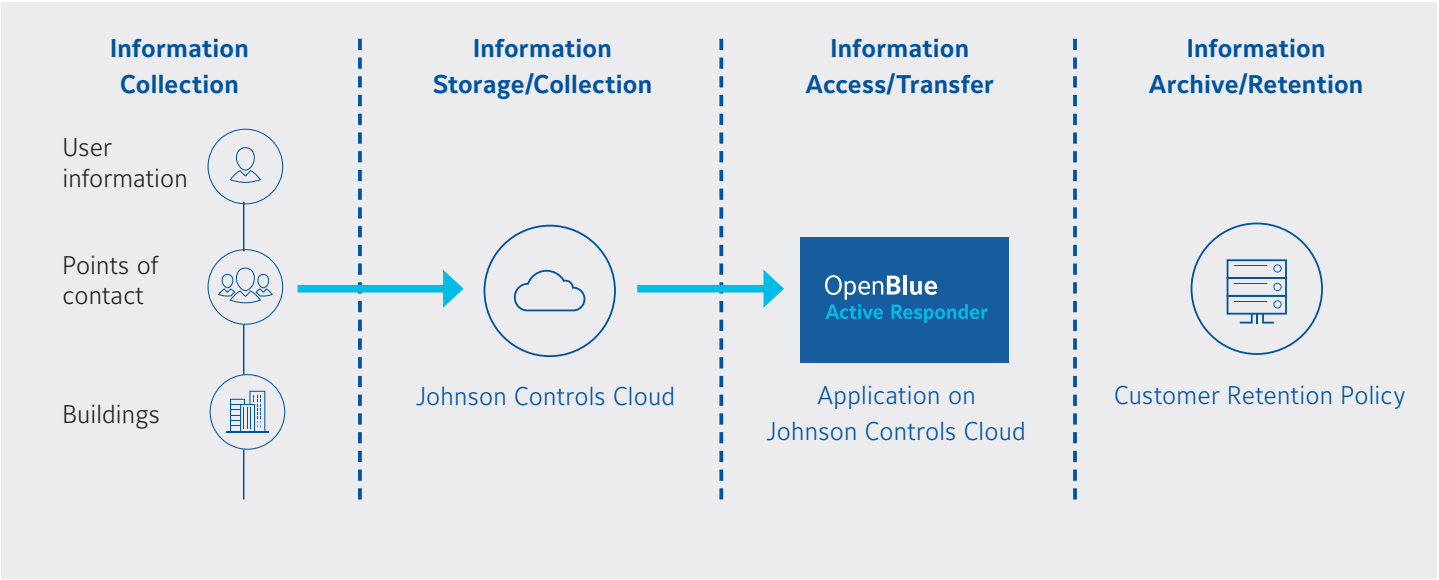
For more information on the Johnson Controls Global Privacy Office and Global Privacy Program, please visit www.johnsoncontrols.com/privacy.

2. Overview of OpenBlue Active Responder

Johnson Controls OpenBlue Active Responder (Active Responder) is a modelling tool that uses Business Process Model and Notation (BPMN) to easily create and execute standard operating procedures (SOPs). Active Responder allows your paper-based SOPs to be transformed into standard-based workflows that digitize user interactions and task behaviour. Operators are guided to perform required workflow tasks to increase consistency, efficiency, and outcome quality. With Active Responder you can manage reviews, approvals, and deployments of SOPs to streamline the governance and roll-out of SOP improvements to your Security Operations Center (SOC) team.

3. Information flow map for Active Responder

Please see below the information flow map for Active Responder that identifies where information is collected, stored and processed, and accessed and transferred. Please note the specifics of this flow depends on the components chosen by our customer and deployed.



4. Personal data processing details of Active Responder

See below details on each category of personal data processed by Active Responder, types of personal data within each category, and the purpose of processing each type.

S. No.	Personal Data Category	Types of Personal Data	Purpose of Processing
1	User Account Information	· First Name · Last Name · Username · Email address	· Required to access the Active Responder application · Required for user notifications · SOPs are associated with user assignees and owners · Required to report on user activity with respect to SOP usage
2	Points of Contact Information (User Work Location and Contact Deatils)	· First Name · Last Name · Role · Phone · Email address	· POCs are associated with one or more buildings · Buildings are associated with one or more SOPs · POC contact details are displayed when an SOP is associated with a building, which in turn is associated with the POC
3	API Connectors (Credentials)	· API Credentials	· Required to access the third-party API connector
4	SOP Creation Details (UNknown)	· Free form	· Users creating and modifying SOPs can add free-form notes and input data according to the design of the SOP (customer created). This may contain PII.

5. Data retention and deletion

Johnson Controls has a global Records Management Program, which includes a Global Records Retention policy and procedures. The purpose of our Records Management Program is to detail the responsibilities and working instructions necessary for the use, maintenance, retention or destruction of data and to assign appropriate responsibilities to the right individuals.

When Johnson Controls processes personal data for our own purposes, the Johnson Controls Records Management Program applies to all records, on all media, and must be maintained in accordance with the Johnson Controls Records Retention Policy and Records Retention Schedule for the specific country and business in which the record has been stored. The Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.

Similarly, when Johnson Controls processes personal data on behalf of a customer, or when our products are operating on customer sites, those offerings can be configured to meet customer data retention periods.

See below the default retention periods applied to Active Responder:

S. No.	Data Category	Retention Period	Reason for Retention
1	User Account Information · First Name · Last Name · Username · Email address	10 years as per Johnson Controls Records retention policy or Customer Data Retention Policy agreement at time of signing	· Required to access the Active Responder application · Required for user notifications · SOPs are associated with user assignees and owners · Required to report on user activity with respect to SOP usage
2	Points of Contact Information (User Work Location and Contact Deatils) · First Name · Last Name · Role · Phone · Email address	10 years as per Johnson Controls Records retention policy or Customer Data Retention Policy agreement at time of signing	· POCs are associated with one or more buildings · Buildings are associated with one or more SOPs · POC contact details are displayed when an SOP is associated with a building, which in turn is associated with the POC
3	API Connectors	10 years as per Johnson Controls Records retention policy or Customer Data Retention Policy agreement at time of signing	· Required to access the third-party API connector
4	SOP Creation Details (UNknown)	10 years as per Johnson Controls Records retention policy or Customer Data Retention Policy agreement at time of signing	· Users creating and modifying SOPs can add free-form notes and input data according to the design of the SOP (customer created). This may contain PII.

6. Sub-processors for Active Responder

Please see below the list of current sub-processors utilized for Active Responder:

Sub-Processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Microsoft Azure Cloud	• First Name • Last Name • Username • Email address • POC Role • POC Phone • API credentials • SOP-related data entry	Third-Party Cloud Hosting	• United States • Asia-Pacific • UAE • Canada • LATAM	• Managing compliance in the cloud • Compliance offerings for Microsoft 365, Azure and other Microsoft services • Service Trust Portal

7. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organisation, Johnson Controls has substantive experience in dealing with cross-border transfer issues and restrictions. When Johnson Controls processes personal data for our own purposes or on behalf of a customer, we utilize the following transfer mechanisms that can assist our customers.

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection for personal data no matter where in world it is processed by Johnson Controls. With respect to the European Union (EU), the Johnson Controls BCRs have been specifically approved by the European Union Data Protection Authorities (DPAs) for transfer of EU personal data globally within Johnson Controls.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification that demonstrates Johnson Controls complies with internationally recognized data privacy protections and is the framework approved for the transfer of personal data by Johnson Controls between participating APEC member economies: United States of America, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei, and the Philippines.
EU Standard Contractual Clauses (SCCs)	Johnson Controls incorporates the EU's approved standard contractual clauses, also referred to as the "Model Contract", into the Johnson Controls Data Protection Agreement located at www.johnsoncontrols.com/dpa to afford the contractual protection under the SCCs to our customers.
EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework	Johnson Controls was and continues to be certified under the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework. Although the Privacy Shield Framework has been invalidated by the Court of Justice of the European Union (CJEU), Johnson Controls intends to continue to maintain its certification for the foreseeable future, until a replacement framework is created.

8. Privacy certifications

Johnson Controls has substantive experience with global privacy issues, and has achieved the below global privacy certifications, which demonstrate our commitment to creating solutions that respect global fair information practices and Privacy by Design.

Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP certification enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program, and to transfer data processed on behalf of our customers (including our cloud solutions) between the USA, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory for more information.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification that demonstrates that Johnson Controls complies with internationally recognized data privacy protections. Please see the CBPR Compliance Directory and the Johnson Controls CBPR TRUSTe validation page for more information.
TRUSTe Enterprise Seal	The Johnson Controls TRUSTe Privacy Certification Seal demonstrates our responsible data collection and processing practices consistent with regulatory expectations and external standards for privacy accountability. Please see the Johnson Controls TRUSTe validation page for more information.

Please note this document is for customer guidance purposes only and is not legal advice. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law, implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

About OpenBlue

OpenBlue is a complete suite of connected solutions that serves industries from workplaces to schools, hospitals to campuses, and beyond. This platform includes tailored, AI-infused service solutions such as remote diagnostics, predictive maintenance, compliance monitoring, advanced risk assessments, and more. A dynamic new space from Johnson Controls, OpenBlue is how buildings come alive.

HQ2109023 - AR