

# OpenBlue Cloud

## 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 the California Consumer Privacy Act (CCPA).

For more information on the Johnson Controls Global Privacy Office and Global Privacy Program, please visit [www.johnsoncontrols.com/privacy](http://www.johnsoncontrols.com/privacy).

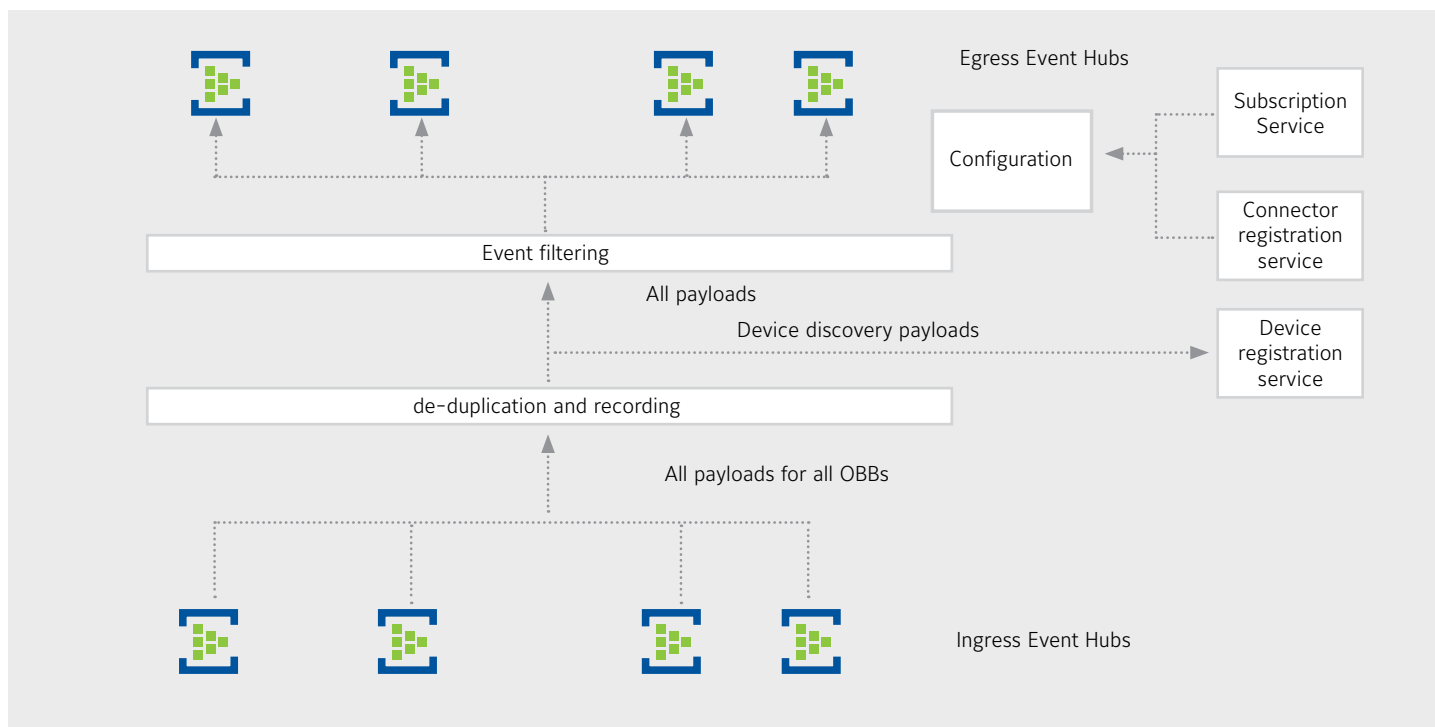
## 2. Overview of OpenBlue Cloud

The OpenBlue Cloud (OBC) is a multi-tenant cloud services platform which provides the following services to subscribed applications (e.g. OBEM, Companion, etc.):

- **Connector Registration Service** - The Connector Registration Service securely stores all connection details to OpenBlue Bridge (OBB) for each tenant.
- **Administration Service** - The Administration Service is responsible for managing and maintaining the end-to-end communication infrastructure between sources and clients. The administration service exposes APIs to manage ingress, source groups, sources, and subscriptions.
- **Subscription Service** - The Subscription Service is responsible for persisting all client subscriptions to OBC for each tenant.
- **Device Management Service** - The Device Management Service is responsible for keeping track of all edge devices and their association with OBB instances. This association is then used by the Command and Control Service to identify where to send command and control (C&C) payloads.
- **Command and Control Service** - The Command and Control Service is responsible for accepting C&C requests from client applications for a given tenant and forwarding them to the correct OBB.
- **Remote Configuration Service** - The Remote Configuration Service is responsible for persisting and retrieving device configurations. For example, it stores the OBB configuration, such as the connection details (connection string or certificate), to OBC.
- **Event Processor** - The Event Processor is responsible for connecting to all OBBs registered in the Connector Registration Service, subscribing for all events, and forwarding them to client applications given the subscriptions specified in the Subscription Service.

### 3. Information flow map for OpenBlue Cloud

Please see below the information flow map for the OpenBlue Cloud (OBC). Information is collected from on-premise gateways (OBBs), as well as cloud-to-cloud connections from certain devices (e.g. IoT Hubs). There is no persistent data storage in the OBC; what data is buffered is used in support of troubleshooting and maintenance of configuration data. There is currently no customer data maintained in the OBC. The data flow for the cloud is consistent across all consuming applications (products) chosen and deployed by our customers.



### 4. Personal data processing details of OpenBlue Cloud

See below for details on each category of personal data processed by OpenBlue Cloud, 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	Login ID Password	The information is used for authentication purposes only.

## 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 a customer's site, those offerings can be configured to meet customer data retention periods.

See below the default retention periods applied to OpenBlue Cloud:

S. No.	Data Category	Retention Period	Reason for Retention
1	User account information	n/a	The information is used for authentication purposes only.

## 6. 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 EU 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 <a href="http://www.johnsoncontrols.com/dpa">www.johnsoncontrols.com/dpa</a> 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.

## 7. Privacy certifications

Johnson Controls has substantive experience with global privacy issues and has achieved the below global privacy certifications, demonstrating 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 is a government-backed privacy certification that 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 and the <a href="#">Johnson Controls PRP TRUSTe validation page</a> for more information.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections. Please see the <a href="#">CBPR Compliance Directory</a> and the Johnson Controls CBPR <a href="#">TRUSTe validation page</a> 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 <a href="#">Johnson Controls TRUSTe validation page</a> for more information.

Please note that this document is for customer guidance purposes only, is not legal advice and is subject to changes from time to time due to modifications of our solutions. 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.