Open**Blue**
Plant Simulator

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 Central Utility Plant (CUP) Plant Simulator
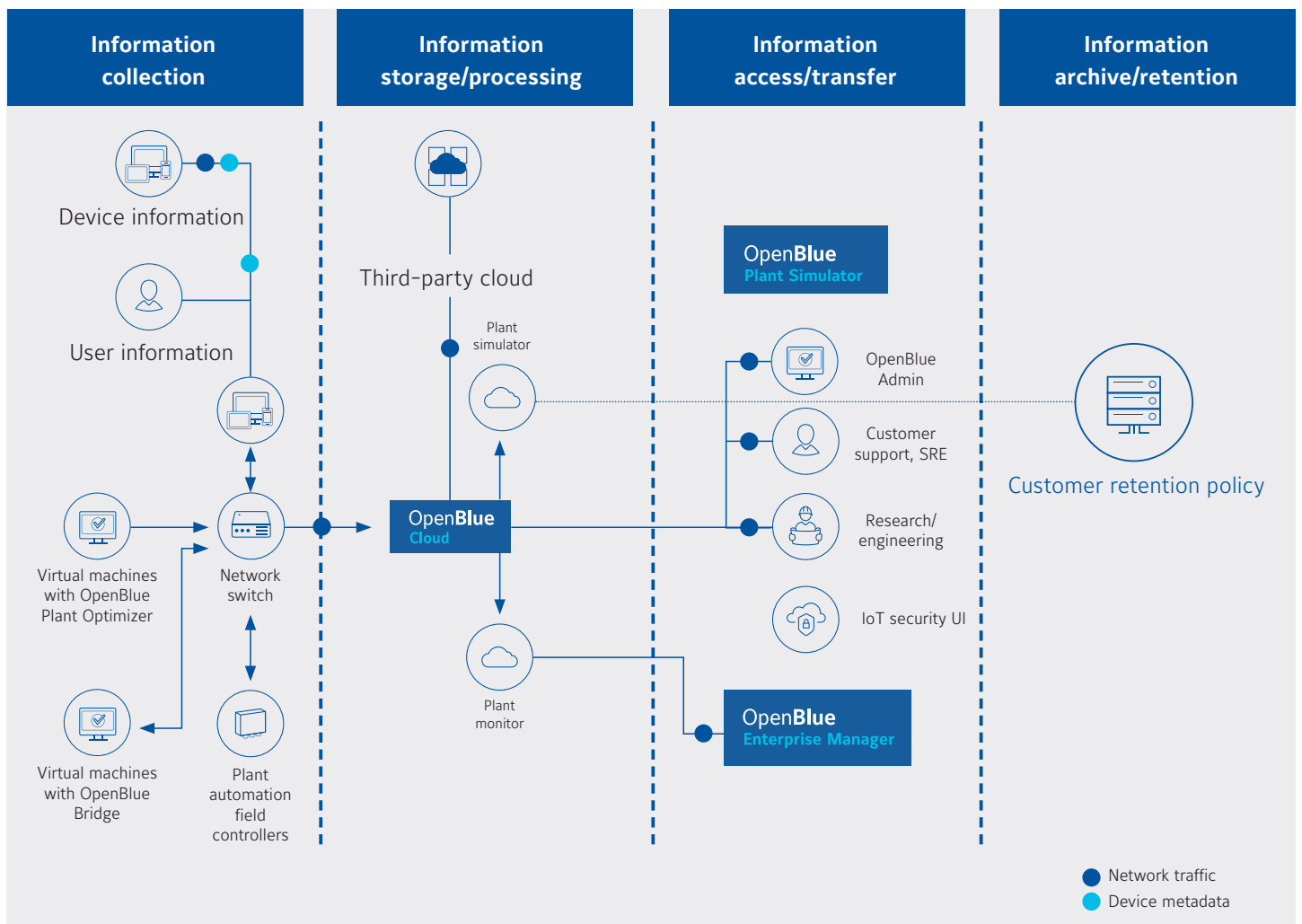
Johnson OpenBlue Central Utility Plant (CUP) is a solution package of software applications that use real-time information to reduce energy use and operating cost, without sacrificing reliability, in central utility plants that produce cooling, heating, and electricity for a campus. One such application is the OpenBlue Plant Simulator.

The power behind **your mission**

The OpenBlue Plant Simulator application assists plant engineers in making plant design decisions. Plant Simulator can be used to:

- aid design of new central plants to compare different configurations, technologies, and equipment sizes. Model the annual utility cost impact for "what-if" scenarios such as upgrades to an existing plant, assuming Optimization control is in effect
- plan for capacity limitations of future load growth scenarios
- forecast utility budgets and perform sensitivity analysis for different assumptions
- evaluate the cost savings potential and return on investment (ROI) for future central plant expansions, adding load, adding new equipment, or connecting multiple plants
- model scenarios to determine when to schedule equipment for preventative maintenance to minimize the utility cost impact or ability to meet critical loads
- support utility supplier rate negotiations by estimating the impact different types of rate structures, or model the potential benefit of participating in market-based demand curtailment programs

3. Information flow map for OpenBlue Plant Simulator

Please see below the information flow map for OpenBlue Plant Simulator, identifying where information is collected, stored and processed, and accessed and transferred. Please note the specifics of this flow depend on the components chosen by our customer and deployed.

Information collection	Information storage/processing	Information access/transfer	Information archive/retention

Device information

User information

Virtual machines with OpenBlue Plant Optimizer

Network switch

Virtual machines with OpenBlue Bridge

Plant automation field controllers

Third-party cloud

Plant simulator

Open**Blue** Cloud

Plant monitor

Open**Blue** Plant Simulator

OpenBlue Admin

Customer support, SRE

Research/ engineering

IoT security UI

Open**Blue** Enterprise Manager

Customer retention policy

● Network traffic
● Device metadata

4. Personal data processing details of OpenBlue Plant Simulator

See below details on each category of personal data processed by OpenBlue Plant Simulator, 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 • User login ID • User email ID • Language preference	• Required to run an active subscription • Required for licensing • Required for user notifications

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 site, those offerings can be configured to meet customer data retention periods.

See below the default retention periods applied to risk insight:

S. No.	Data Category	Retention Period	Reason for Retention
1	User account information • First name, last name • User login ID • User email ID • Language preference	10 years as per Johnson Controls Records Retention Policy or Customer Data Retention Policy agreement at time of signing subscription.	• Required to run an active subscription • Required for licensing • Required for user notifications
2	General • User feedback • Help and support tickets	Three years as per Johnson Controls Records Retention Policy or as per Customer Data Retention Policy agreement at the time of signing subscription.	• Required for app feedback and collecting usability issues

6. Sub-processors for OpenBlue Plant Simulator

Please see below the list of current sub-processors utilized to provide OpenBlue Plant Simulator:

Sub-Processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Microsoft Azure Cloud	• First name, last name • User email ID • Language preference	Third-party cloud hosting	• United States • Asia-Pacific • UAE • Canada	For information regarding Microsoft Azure see www.microsoft.com/en-ie/trust-center/compliance/compliance-overview which includes Audit reports and https://docs.microsoft.com/en-GB/compliance/regulatory/offering-home for comprehensive compliance information

7. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organization, 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 the 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 which demonstrates that 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 which 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 that 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.

 Follow us on twitter or visit johnsoncontrols.com

HQ2202015 - PS