OpenBlue Companion

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.

2. Overview of OpenBlue Companion

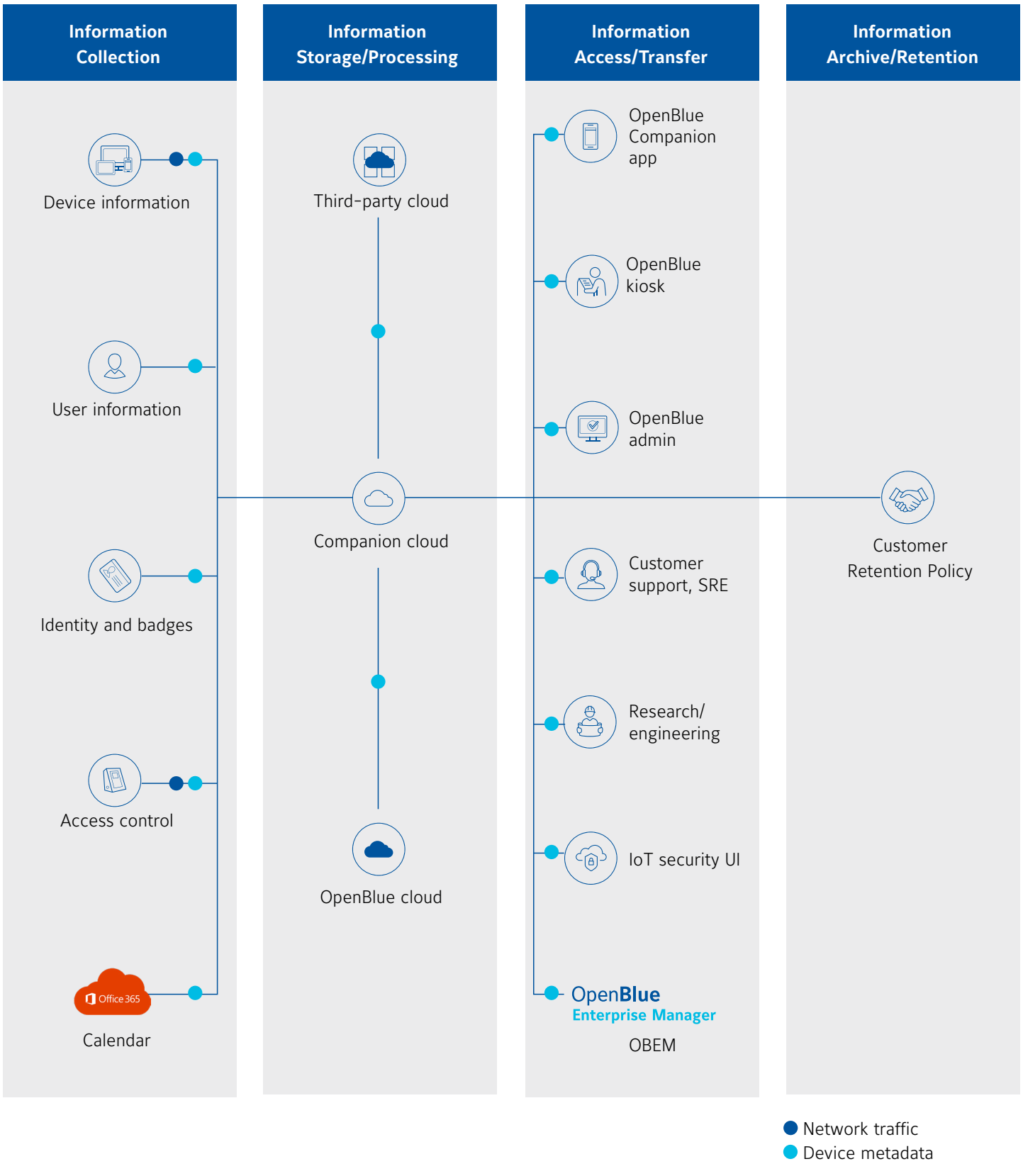
OpenBlue Companion (Companion) is a dynamic application that provides amazing, seamless experiences for occupants while also delivering on the goals of building managers and owners. Companion brings dynamic collaboration and work spaces to life with an intuitive and personalized mobile interface that optimizes your built environment.

For occupants, Companion anticipates needs and integrates features to foster productivity, connecting people to spaces like never before. Go beyond comfort for flexible space booking, navigation, and seamless access control experiences that attract and retain talent. And when it comes time to find and refine a hybrid remote work plan, Companion has rich features to support your strategy as it evolves.

Companion makes the most out of your people and spaces, powered by purpose-driven IoT and AI technology personalized to meet your goals and your investments. You can create your smart building one use case at a time.

3. Information flow map for OpenBlue Companion

Please see below the information flow map for Companion, 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.



4. Personal data processing details of OpenBlue Companion

See below details on each category of personal data processed by Companion, types of personal data within each category, and the purpose of processing each type:

S.No.	Personal Data Category	Type of Personal Data	Purpose of Processing
1	User and account information	· First name, middle name, last name · User login ID · User email ID · Business contact number · User profile image (optional)	· Required to run an active subscription · Required for licensing · Required for user notifications
2	User access and location details	· User access card badge details · User badge details · Location services · Phone BLE · Badge in and badge out	· Required for activating user location in facility for navigation and access
3	User work location	· Work location · Business unit	· Required for user access to location assigned · Required for managing schedule of the user to access work location
4	User reservations	· User workstation reservations · User roster schedule (optional) · User schedule/calendar · Favorite spaces · Ergonomic settings for workstations	· Required for indoor navigation · Required for user reservations (space, workstations, etc) · Required for user calendar schedule · Required for space performance analytics · Required for user workstation settings
5	Notifications	· App notifications · Device ID	· Required for user communications · Required for internal communications
6	User facility access clearance	· Clear/no clear status	· Required for user access to facility based on clearance
7	Alerts and acknowledgement	· Social distancing alerts · SoS incidents · Social distance scoring (user and team) · "I am safe" acknowledgement	· Required for user alerts and notifications
8	General	· User feedback · Help and support tickets	· Required for app feedback and collecting usability issues
9	System configuration and access	· Persistent access badge IDs · Email and/or mobile number · Username does not have to be an individual's actual name – the username chosen will be unique to that person and assigned and generated by organization's identity team	· Essential for health and safety features such as contact tracing · Essential for security processing in order to detect unauthorized access/movement · Email and/or mobile number used for sending alerts from the system to select individuals · Username and password is required for system access

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 Global 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 Global 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 Global 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 Companion:

S. No.	Data Category	Retention Period	Reason for Retention
1	User and account information · First name, middle name, last name · User login ID · User email ID · Business contact number · User profile image (optional)	10 years as per Johnson Controls Records Retention Policy or as per customer's data retention policy agreement at the time of signing subscription	· Required to run an active subscription · Required for licensing · Required for user notifications
2	User access and location details · Location services · Phone BLE · Badge in and badge out	10 years as per Johnson Controls Records Retention Policy or as per customer data retention policy agreement at the time of signing subscription	· Required for activating user location in facility for navigation and access
3	User work location · Work location · Business unit	10 years as per Johnson Controls Records Retention Policy or as per customer data retention policy agreement at the time of signing subscription	· Required for user access to location assigned · Required for managing schedule of the user to access work location
4	User reservations · User workstation reservations · User roster schedule (optional) · User schedule/calendar · Favorite spaces · Ergonomic settings for workstations	10 years as per Johnson Controls Records Retention Policy or as per customer data retention policy agreement at the time of signing subscription	· Required for indoor navigation · Required for user reservations (space, workstations, etc) · Required for user calendar schedule · Required for space performance analytics · Required for user workstation settings
5	Notifications · App notifications · Device ID · Organizational news	10 years as per Johnson Controls Records Retention Policy or as per customer data retention policy agreement at the time of signing subscription	· Required for user communications · Required for internal communications
6	User facility access clearance · Clear/no clear status	10 years as per Johnson Controls Records Retention Policy or as per customer data retention policy agreement at the time of signing subscription	· Required for user access to facility based on clearance

S. No.	Data Category	Retention Period	Reason for Retention
7	Alerts and acknowledgement · Social distancing alerts · SoS incident · Social distance scoring (user and team) · "I am safe" acknowledgement	10 years as per Johnson Controls Clear/no clear status or as per customer data retention policy agreement at the time of signing subscription	· Required for user alerts and notifications
8	General · User feedback · Help and support tickets	10 years as per Johnson Controls Clear/no clear status or as per customer data retention policy agreement at the time of signing subscription	· Required for app feedback and collecting usability issues
9	System configuration and access · Persistent access badge IDs · Email and/or mobile number · Username does not have to be an individual's actual name – the username chosen will be unique to that person and assigned and generated by the organization's identity team	10 years as per Johnson Controls Clear/no clear status or as per customer data retention policy agreement at the time of signing subscription	· Essential for health and safety features such as contact tracing · Essential for security processing in order to detect unauthorized access/movement · Email and/or mobile number used for sending alerts from the system to select individuals · Username and password is required for system access

As detailed above, data is deleted from the Companion systems:

1. on customer request
2. on the expiry of the specific retention period configured for the customer
3. on the expiry of the default Johnson Controls data retention period

Personal information will be permanently removed from the Companion system using the Automatic Archival Service.

6. Sub-processors for OpenBlue Companion

Please see below the list of current sub-processors utilized to support Companion:

Sub-Processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Microsoft Azure Cloud	· First name, middle name, last name · User email ID · User access card badge details · User HID badge details · Work location · User alerts · Facility access clearance · SoS incidents	Third-party cloud hosting	· United States · Asia Pacific · UAE · Canada · EU – Germany	· For information regarding Microsoft Azure see www.microsoft.com/en-ie/trust-center/compliance/compliance-overview, which includes audit reports, and 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 substantial 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 which 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 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: the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines.
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 United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe validation page for more information.
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 substantial experience with global privacy issues, and has achieved the below global privacy certifications which demonstrate our commitment to creating solutions which 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 United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe validation page 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, 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.