Johnson Controls

CYBERSECURITY AND DATA PRIVACY SHEET

# OpenBlue Companion

## A comprehensive approach to keeping your business safe

**Gain peace of mind with cyber-resilient systems and solutions which protect your data. Security is designed into all Johnson Controls products, hardware, hosted services and software. The OpenBlue Companion security features listed below enable you to unlock the value in your building knowing that your systems are protected.**

### Data encryption

AES-256 encryption protects data-at-rest and TLS-1.2 for data in transit

### User management

Integrates with Active Directory/ Entra ID to manage users and enforce password policies

### Role-based access control (RBAC)

Assigns permissions according to authorized roles

### Network security

Web Application Firewall (WAF) protects against sophisticated attacks

### Validated authentication

Multi-Factor Authentication (MFA) enhances access control by requiring additional proof of identity

### Vulnerability monitoring

The OpenBlue environment is continuously monitored for cyber events using automated tools

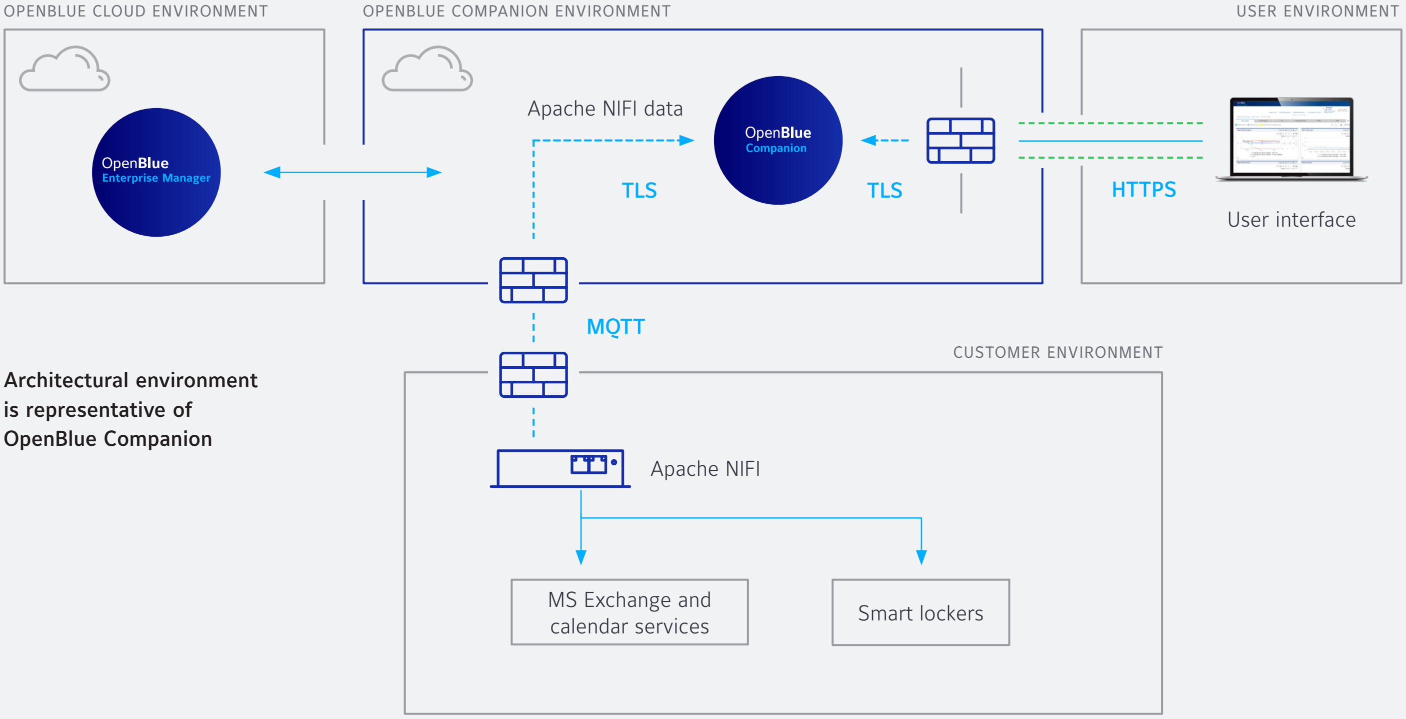
### About OpenBlue Companion

OpenBlue Companion is a dynamic application that provides seamless experiences for occupants while also delivering on the goals of building managers and owners.

For occupants, Companion anticipates needs and integrates features to foster productivity, connecting people to spaces like never before. 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 build one use case at a time.

Learn more here

## OpenBlue Companion architectural and data flow



**Architectural environment is representative of OpenBlue Companion**

### ISASecure® Security Development Lifecycle Assurance (SDLA) certified

All Johnson Controls global development locations comply with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customer commitment to provide cyber-resilient solutions that follow best-in-class industry practices.

### SOC 2 Type II report compliance

An SOC 2 Type II audit is an evaluation of an organization's information systems and controls based on the criteria outlined in the Trust Service Criteria. It focuses on security, availability, processing integrity, confidentiality and privacy. The Type II indicates that the audit covers a specified time period (usually a minimum of six months) to assess the effectiveness of the controls in place.

### ISO27001 certification

ISO/IEC 27001:2013 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization's overall business risks. The standard provides a systematic approach to managing sensitive information, ensuring its confidentiality, integrity and availability.

ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

SOC 2 Type II report compliance*

ISO27001 certification*

* For OpenBlue Companion, the US instance has successfully undergone SOC 2 Type II audit and ISO/IEC 27001:2013 certification. Non-US instances have substantially similar controls and protocols.

## Data privacy

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 Program is led by our privacy experts and designed in accordance with global privacy and data protection laws. In addition to product-related information provided in this section, please visit **www.johnsoncontrols.com/trust-center/privacy** for more details on our Global Privacy Program.

**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:**

| Personal data category | Type of personal data | Purpose of processing |
|---|---|---|
| User and account information | · First name, middle name, last name<br>· User login ID<br>· User email ID<br>· Business contact number<br>· User profile image (optional)<br>· Preferred language<br>· POD (people of determination) status<br>· Mobile number<br>· Vehicle registration number<br>· Government ID type (only for visitors)<br>· Government ID number (only for visitors) | · Required to run an active subscription<br>· Required for licensing<br>· Required for user notifications<br>· Required for getting parking and for availing carpooling feature<br>· Required for visitor authentication – Government ID number is one field which is getting passed to third party visitor management system from Companion<br>· Vehicle registration number is a field getting passed to third party parking management system and access control system from Companion |
| User access and location details | · User access card badge details<br>· User badge details<br>· Location services<br>· Phone BLE (Bluetooth and location data)<br>· Badge in and badge out<br>· Nearest home boarding point<br>· Nearest work boarding point | · Required for activating user location in facility for navigation and access<br>· Required for carpooling feature. These are not the actual home address and work address but the nearest common boarding where people who are going to use carpooling can gather together |
| User work location | · Work location<br>· Business unit | · Required for user access to location assigned<br>· Required for managing schedule of the user to access work location |
| User reservations | · User workstation<br>· User roster schedule (optional)<br>· User schedule/calendar<br>· Favorite spaces<br>· Gym reservation<br>· Parking reservation<br>· Meeting room reservation<br>· Locker reservation | · Required for indoor navigation reservations<br>· Required for user reservations (space, workstations, etc)<br>· Required for user calendar schedule<br>· Required for space performance analytics |
| Notifications | · Device ID | · Required for user communications<br>· Required for internal communications<br>· App notification (bell and push) on mobile<br>· App notification (bell only) on web |
| User facility access clearance | · Clear/no clear status | · Required for user access to facility based on clearance |
| Alerts and acknowledgement | · SOS incidents<br>· “I am safe” acknowledgement | · Required for user alerts and notifications |

| Personal data category | Type of personal data | Purpose of processing |
|---|---|---|
| General | · User feedback<br>· Help and support tickets | · Required for app feedback, space feedback and collecting issues |
| System configuration and access | · Persistent access badge IDs<br>· Email and/or mobile number<br>· 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<br>· Essential for security processing in order to detect unauthorized access/movement<br>· Email and/or mobile number used for sending alerts from the system to select individuals<br>· Username and password is required for system access |

## Retention and deletion of personal data

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 deletion of data Johnson Controls is processing. The Global Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.

When Johnson Controls processes personal data on behalf of a customer, or when products are operating on the customer's site to the extent provided by a product's functionalities and upon a system's configuration, customers may access such data and delete it at any time on their own. The default retention periods as predefined by Johnson Controls apply. See the below table for the default retention periods applied to Companion.

If, during the 90 days following the end of a subscription, Johnson Controls receives from customer a request to export a customer's personal data, Johnson Controls will provide the customer with an export of their personal data in a structured commonly used machine-readable format as reasonably determined by Johnson Controls. Such request must be made to the JCI Digital Customer Support email currently at **openbluetechnicalsupport@jci.com**. If not already deleted by the customer using available internal product deletion features, the customer's personal data will be deleted after such 90-day period or as otherwise agreed. During any retention period, the provisions of the underlying agreement that are applicable to the retention and product of a customer's personal data continue to apply.

**Default retention periods for customer personal data are as set forth in the table below:**

| Data category | Retention period | Reason for retention |
|---|---|---|
| User and account information:<br>· First name, middle name, last name<br>· User login ID<br>· User email ID<br>· Business contact number<br>· User profile image (optional)<br>· Preferred language<br>· POD status<br>· Mobile number<br>· Vehicle registration number<br>· Government ID type (only for visitors)<br>· Government ID number (only for visitors) | · For the period of active subscription +90 days | · Required to run an active subscription<br>· Required for licensing<br>· Required for user notifications |
| User access and location details:<br>· Location services<br>· Phone BLE<br>· Badge in and badge out<br>· Nearest home boarding point<br>· Nearest work boarding point | · For the period of active subscription +90 days | · Required for activating user location in facility for navigation and access |

| Data category | Retention period | Reason for retention |
|---|---|---|
| User work location:<br>· Work location<br>· Business unit | · For the period of active subscription +90 days | · Required for user access to location assigned<br>· Required for managing schedule of the user to access work location |
| User reservations:<br>· User workstation reservation<br>· User roster schedule (optional)<br>· User schedule/calendar<br>· Favorite spaces<br>· Gym reservation<br>· Parking reservation<br>· Meeting room reservation<br>· Locker reservation | · For the period of active subscription +90 days | · Required for indoor navigation<br>· Required for user reservations (space, workstations, etc.)<br>· Required for user calendar schedule<br>· Required for space performance analytics<br>· Required for user workstation settings |
| Notifications:<br>· App notifications<br>· Device ID<br>· Organizational news | · For the period of active subscription +90 days | · Required for user communications<br>· Required for internal communications |
| User facility access clearance:<br>· Clear/no clear status | · For the period of active subscription +90 days | · Required for user access to facility based on clearance |
| Alerts and acknowledgement:<br>· SOS incidents<br>· "I am safe" acknowledgement | · For the period of active subscription +90 days | · Required for user alerts and notifications |
| General:<br>· User feedback<br>· Help and support tickets | · For the period of active subscription +90 days | · Required for app feedback and collecting usability issues |
| System configuration and access:<br>· Persistent access badge IDs<br>· Email and/or mobile number<br>· 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 | · For the period of active subscription +90 days | · Essential for health and safety features such as contact tracing<br>· Essential for security processing in order to detect unauthorized access/movement<br>· Email and/or mobile number used for sending alerts from the system to select individuals<br>· Username and password is required for system access |

## Sub-processors for OpenBlue Companion

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

| Sub-processor | Service type | Location of data center | Security assurance |
|---|---|---|---|
| Microsoft Azure Cloud | · Third-party cloud hosting | · United States<br>· Asia Pacific<br>· UAE<br>· Canada<br>· 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 |

## 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 use 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. |
| US Data Privacy Framework (DPF) | Johnson Controls is certified under the US Data Privacy Framework for transfers of personal data from the EU, United Kingdom and Switzerland to the United States. |

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.

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to deliver smart building solutions.

To learn more, please visit our website at **www.johnsoncontrols.com/trust-center** or contact us at **TrustCenter@jci.com**.

Visit **johnsoncontrols.com** or follow us **@johnsoncontrols**