

# Data Privacy Sheet

## Shopper Demographics



### 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).

# Data Privacy Sheet

## 2. Overview of Shopper Demographics

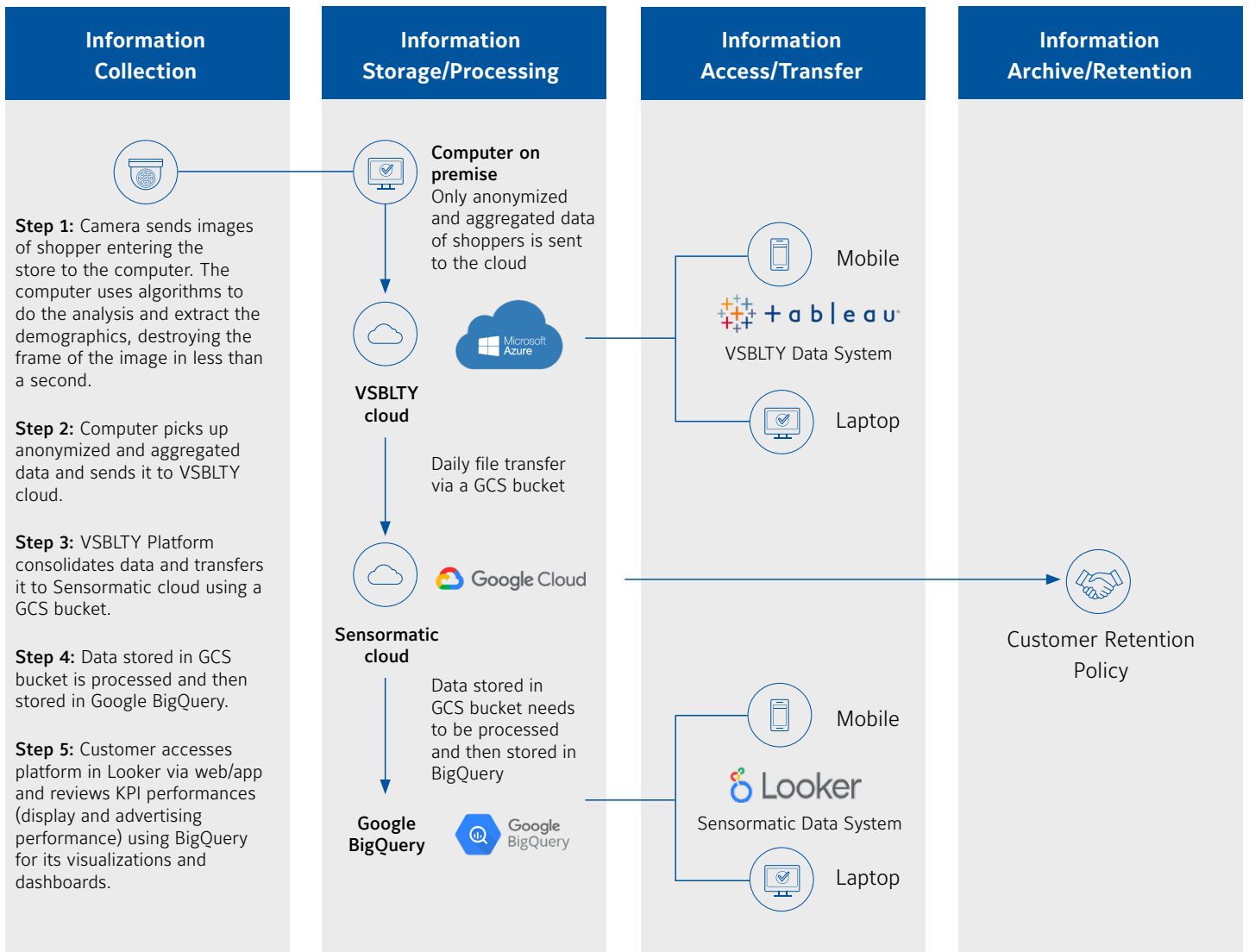
A set of cameras and sensor technology with facial recognition, machine learning and computer vision at the entrance of the store(s) to provide the demographic profile of the visitors and how this profile evolves over time in terms of gender, age and sentiment (neutral, happiness, sadness, surprise or anger)

Use cases:

- provide the profile and the evolution of visitors and shoppers in brick-and-mortar stores as well as theme parks, casinos and shopping malls
- provide power hours by gender and age
- evaluate the effectiveness of marketing campaigns to drive store traffic by gender and age

## 3. Information flow map for Shopper Demographics

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



# Data Privacy Sheet

## 4. Personal data processing details of Shopper Demographics

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

S.	Personal Data Category	Types of Personal Data	Purpose of Processing
1	Shopper Demographics	<ul style="list-style-type: none"><li>Gender (male/female)</li><li>Age (absolute number)</li></ul>	<ul style="list-style-type: none"><li>Create the demographic profile of visitors</li></ul>

## 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 Shopper Demographics:

S.	Data Category	Retention Period	Reason for Retention
1	Demographics: <ul style="list-style-type: none"><li>Gender</li><li>Age</li></ul>	<ul style="list-style-type: none"><li>Once an analysis on a frame of video is conducted on premise and the gender and age defined, the frame is destroyed – this takes less than a second.</li><li>With respect to the reporting level data there is no single process for deletion as the information retained is anonymized and aggregated data</li></ul>	<ul style="list-style-type: none"><li>No retention of the images of shoppers</li><li>Data is retained to provide historical evolution of data for three years (four years of data available)</li></ul>

# Data Privacy Sheet

## 6. Sub-processors for Shopper Demographics

Please see below the list of current sub-processors for Shopper Demographics:

Sub-Processor	Personal Data	Service Type	Location of Data Center	Security Assurance
VSBLTY uses Microsoft Azure as a primary hosting provider	Only anonymized and aggregated data regarding <ul style="list-style-type: none"> <li>• Age</li> <li>• Gender</li> </ul>	Third-party cloud hosting	Microsoft Azure physical location (country by country) ensures that data residency is assured. Please see link for physical locations: <a href="https://azure.microsoft.com/en-us/global-infrastructure/data-residency/#select-geography">https://azure.microsoft.com/en-us/global-infrastructure/data-residency/#select-geography</a>	For information regarding Microsoft Azure security see: <a href="https://azure.microsoft.com/en-us/overview/security/">https://azure.microsoft.com/en-us/overview/security/</a>
Sensormatic uses Google Cloud as primary hosting of data	Only anonymized and aggregated data regarding <ul style="list-style-type: none"> <li>• Age</li> <li>• Gender</li> </ul>	Third-party cloud hosting	Google Cloud physical location (country by country) ensures that data residency is assured. Please see link for physical locations: <a href="https://cloud.google.com/about/locations">https://cloud.google.com/about/locations</a>	For information regarding Google Cloud security see: <a href="https://cloud.google.com/security">https://cloud.google.com/security</a>

## 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 that can assist our customers:

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection of 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 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 <a href="#">Johnson Controls PRP TRUSTe validation page</a> 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 <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.

# Data Privacy Sheet

## 8. Privacy certifications

Johnson Controls has substantial experience with global privacy issues, and has achieved the below global privacy certifications that 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 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 <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.