Data Privacy Sheet

Computer Vision Analytics

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.

Data Privacy Sheet

2. Overview of Computer Vision Analytics

The innovative computer vision technology by Sensormatic Solutions delivers retail operational insights based on best-in-class deep learning artificial intelligence (AI) models. Computer Vision Analytics automates tasks and derives meaningful information from video footage in real time. Computer Vision Analytics help strengthen loss prevention efforts, gather insights for improved shopper experiences, and maintain a safe environment for both shoppers and associates.

Easy to deploy and powerful, Computer Vision Analytics leverage existing video infrastructure and a smart hub appliance to tap into data, opening up a world of problem-solving solutions. All analytics are presented in a one-stop, consolidated dashboard for easy access to key metrics.

Measurable loss prevention outcomes

Computer Vision Analytics can play an important role in loss prevention and in keeping an environment safe and secure. Computer Vision Analytics are developed specifically to address some of the most critical loss prevention issues today.

Examples of some of the analytics available to help strengthen loss prevention activities include:

- Group detection alert
- Loitering monitoring
- Shelf sweep detection
- Slip and fall detection
- Vehicle alert

Meaningful shopper insights

Our growing list of Computer Vision Analytics can help you get a better handle on shopper traffic patterns, path to purchase, and demographics and sentiment of shoppers. Some of the Computer Vision Analytics include:

- Audience demographic measurement
- Dwell time measurement
- PPE mask detection and social distancing monitoring
- Queue wait time management and early warnings
- Occupancy tracking
- Traffic pattern insights
- Associate engagement

Measurable loss prevention outcomes

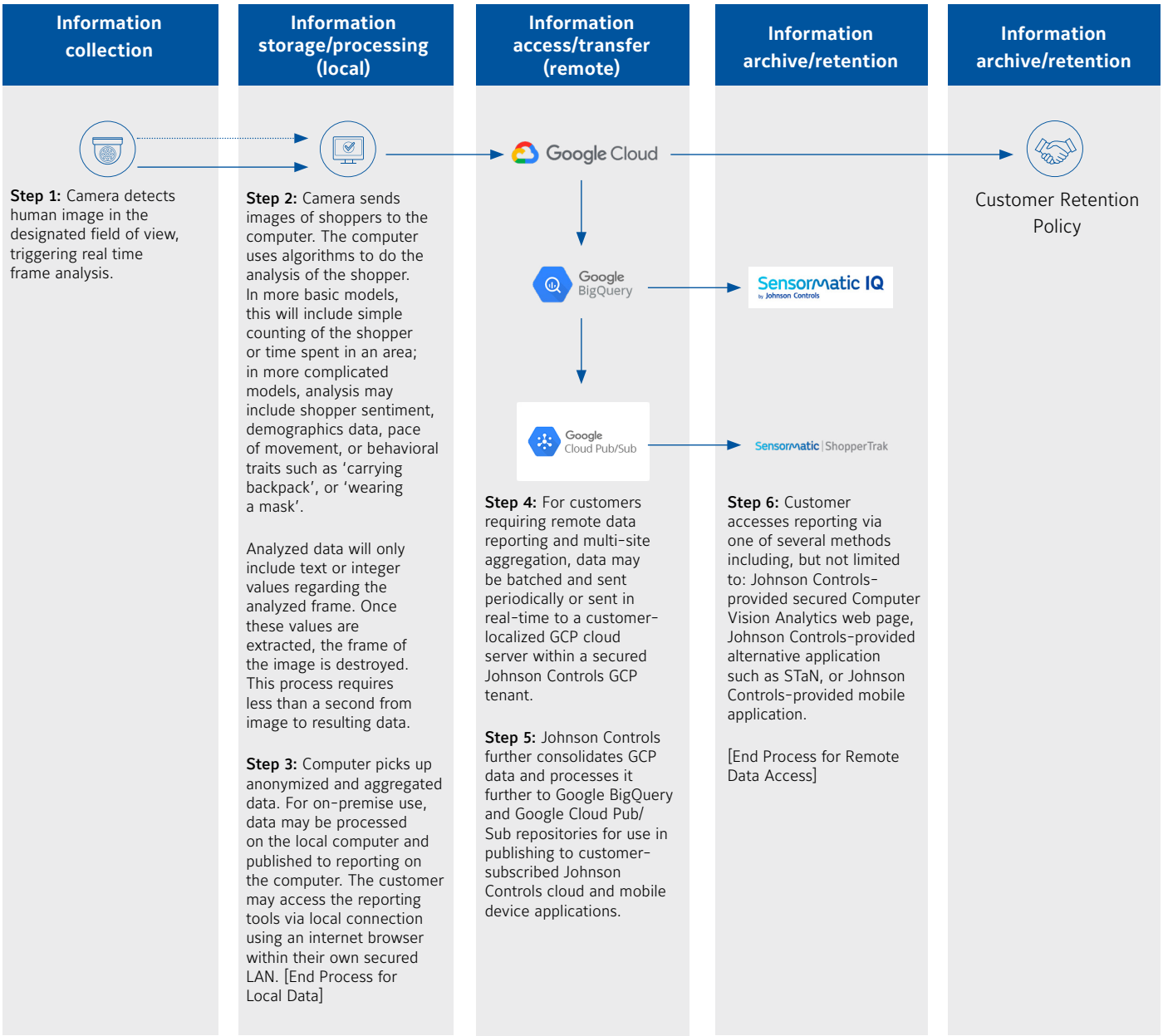
With shrink and organized retail crime (ORC) activity on the rise, retailers are looking for ways to combat these threats while optimizing in-store labor usage. Computer Vision Analytics can play an important role in loss prevention and in helping to keep an environment safe and secure. Computer Vision Analytics are developed specifically to help address some of the most critical loss prevention issues today.

Meaningful shopper insights

To stay ahead of the competition and provide shoppers with an outstanding in-store experience, retailers are always looking to better understand shopper behavior and the shopper journey. With this information in hand, retailers can create the ideal environment and develop appropriate marketing plans that ultimately lead to increased sales. Computer Vision Analytics can help you better understand shopper traffic patterns, path to purchase, merchandising/assortment A/B testing, and even demographics and sentiment of shoppers.

3. Information flow map for Computer Vision Analytics:

Please see below the information flow map for Shopper Demographics, identifying where information is collected, stored and processed as well as 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 Computer Vision Analytics

Most types of Computer Vision Analytics include some type of detection, timestamping, count increment (+1), and aggregation of those counts. Other capabilities may include the detection of directional movement or behavioral detection including movement of hands, selection of items, etc. These types of calculations do not require processing of personal data at any point.

See below details on each category of personal data processed by Computer Vision Analytics, types of data within each category, and the purpose of processing each data type.

S.	Personal Data Category	Types of Personal Data	Purpose of Processing
1	Shopper Demographics	· Detection of gender (male/female) · Detection of approximate age (absolute number)	· Allow creation of demographic profile of store shoppers (e.g. "32% are middle-aged female shoppers")
2	Employee/customer	· Detection of employee vs customer	· Allow accurate counts of customer traffic within specified area as opposed to counting employees multiple times to avoid inaccuracy
3	Unique ID	· For each person detected the system creates a vector and that vector is assigned a random Globally Unique Identifier (GUID). This GUID is used as a unique ID from facial analysis. · Unique ID feature does create a biometric template, but this template is not only transient but encrypted and stored as an alphanumeric or binary vector in such a way that, as raw data, it cannot be extrapolated in any way and the Unique ID cannot be inferred or reconstructed to aid identification in any way. · This embedding vector will be used to identify if a person matches a previous vector using facial analytics. This random unique GUID will be the only information used in data reporting as no photos or images are collected or stored. · The vector resides only on local device memory and cannot be queried or shared with any other camera or database on the network. The biometric template will reside in local memory for 120 minutes then deleted.	· Identify people as unique individuals to allow for distinct counting or matching of the person across disparate cameras on the same network LAN within a pre-defined timeframe · Disallow double-counting of the same individual in multiple areas of the same store or when returning to the store within the 120-minute defined time period
4	Protective mask	· Protective mask (Y/N)	· Allow detection and alerting for safety and corrective follow-up actions

S.	Personal Data Category	Types of Personal Data	Purpose of Processing
5	Clothing/accessory articles	· Detection of specific clothing type such as business suit, formal dress, ball cap to derive or assume interest in specific items or environmental adjustments · Detection of specific clothing type and color within limited search parameter and limited duration · Detection of accessory or carried items such as large handbags or backpacks	· Allow the triggering of environmental adjustments (audio programming, fragrance emission) based on presumed interest. Offer customer service fitting to shopper's perceived interest type (business or pleasure, etc.) · Enable the searching and identification of a lost person, missing child, etc. within a store or mall premises for a specific duration (120 minutes, etc.) · Allow the notification of a store employee to provide customer service for shopper to store their bag or otherwise intervene to ensure customer use of the carried item does not result in a loss event within the store
6	Vehicle license plate	· Detection of customer-provided vehicle license plate · Detection of suspect vehicle included in formal criminal complaint · Detection of suspect vehicle included in retailer's own or fellow retailer's BOLO alert ("Be On Lookout")	· Enable detection and automated notification of customer arrival for order delivery in offerings of omnichannel sale, BOPAC, etc. · Enable detection and automated notification of suspect vehicle attached to retailer criminal complaint involving same potential subject · Enable detection and automated notification of subject vehicle attached to own retailer or fellow retailer's BOLO alert regarding documented suspicious behavior such as shoplifting

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 Computer Vision Analytics:

S.	Data Category	Retention Period	Reason for Retention
1	Demographics: · Gender · Age	· 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. · With respect to the reporting level data there is no single process for deletion as the information retained is anonymized and aggregated data.	· No retention of the images of shoppers. · Data is retained to provide historical evolution of data for three years (four years of data available).
2	Employee/customer	· 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. · With respect to the reporting level data there is no single process for deletion as the information retained is anonymized and aggregated data.	· No retention of the images of shoppers. · Data is retained to provide historical evolution of data for three years (four years of data available).
3	Unique ID	· Unique ID or the biometric template resides only on local device memory for 120 minutes (two hours) then deleted and cannot be queried or shared with any other camera or database on the network.	· Unique ID or the biometric template is retained to check a new face detected by the camera and avoid duplications when counting the people in the store within two hours after being created. Unique ID data cannot be extrapolated and cannot be inferred or reconstructed to identify people in any way.
4	Protective mask	· Once an analysis on a frame of video is conducted on premises and protective mask usage is detected, the frame is destroyed. This takes less than a second. · With respect to the reporting level data there is no single process for deletion as the information retained is anonymized and aggregated data.	· No retention of the images of shoppers · Data is retained to provide historical evolution of data for three years (four years of data available).

S.	Data Category	Retention Period	Reason for Retention
5	Clothing/accessory articles	· Once an analysis on a frame of video is conducted on premises and a clothing article is detected, the frame is destroyed. This takes less than a second. · In the context of active search for certain garment color, etc. for public safety search, analysis will continue for the duration of the limited search. Matching frames will be retained temporarily for the purposes of verifying the subject of the search, if the frame is not verified as a subject, the frame will be destroyed immediately. Matching and verified frames are subject to the customer's data retention policy with regard to safety or security incidents or investigations on their premises. · Once an analysis on a frame of video is conducted on premises and an accessory or carried item such as a large handbag or backpack is detected, the frame is destroyed. This takes less than a second.	· No general retention of the images of shoppers · Images of subjects matching search criteria may be retained as needed per customer's data retention policy regarding public safety incidents. · Allow the notification of a store employee to provide customer service for shopper to store their bag or otherwise intervene to ensure customer use of the carried item does not result in a loss event within the store.
6	Vehicle license plate	· Once an analysis on a frame of video is conducted and vehicle license plate does not match the customer-provided vehicle license plate, the frame is destroyed. This takes less than a second. · Matching license plate images for the purposes of delivery, BOPAC will be deleted upon detection and notification alert. This takes less than a second. · Matching license plate images for the purposes of criminal complaint suspect vehicles may be retained by the customer per customer's data retention policy with regard to safety or security incidents or investigations on their premises. · Matching license plate images for the purposes of retailer's own or fellow retailer's BOLO alert suspect vehicles may be retained by the customer per customer's data retention policy with regard to safety or security incidents or investigations on their premises.	· No general retention of license plate images · Retention of license plate images matching license plate descriptions within criminal complaints or retailer's own or fellow retailers' BOLO alerts subject to the customer's own data retention policy related to safety or security incidents or investigations.

Data Privacy Sheet

6. Sub-processors for Computer Vision Analytics:

Please see below the list of current sub-processors utilized for Computer Vision Analytics:

Sub-Processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Sensormatic uses Google Cloud as primary hosting of data	Only anonymized and aggregated data regarding: • Age • Gender	Third-party cloud hosting	Google cloud physical location (country by country) ensures that data residency is assured. Please see link for physical locations: https://cloud.google.com/about/locations	For information regarding Google Cloud security see: https://cloud.google.com/security

7. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organisation, 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 world it is processed by Johnson Controls. With respect to the European Union, 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 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 USA, 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 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 USA, 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.

© 2022 Johnson Controls. All rights reserved.