Cloudvue

Privacy by Design | GDPR

For over 20 years, Cloudvue has leveraged its device management and video services expertise to create and implement industry-leading secure software development, operational management, and threat mitigation practices. Our surveillance systems may at times capture video footage that contains different forms of personal data such as a person's face or other personally identifiable visual or personal information. We recognize the importance of this data and stand committed to protecting its security and integrity.

Global privacy laws, including the General Data Protection Regulation (GDPR) of the European Union (EU) are important and complex. Johnson Controls has solved for this by designing and developing solutions using Privacy by Design (PbD).

How does Johnson Controls implement Privacy by Design (PbD)?

- Privacy by Design (PbD), by way of Privacy Impact Assessment (PIA), identifies potential privacy issues in the use of our solutions at an early stage to prevent them in the long run, allowing our products and services to be used by our customers ethically and in compliance with law as it applies to that customer.

- The Johnson Controls Privacy by Design process embeds privacy-enhancing functionality and controls into the design and architecture of our solutions in the early phases of a project and throughout the entire engineering development and testing process.

- Using solutions built with Privacy by Design, like Johnson Controls' solutions, can assist our customers with their obligations under GDPR, and other global privacy laws.

Johnson Controls

The power behind **your mission**

Privacy by Design features in the Cloudvue solution include:

- Transparency: The Cloudvue Terms of Service and EULA recommends users of its services post public notice of the use of video surveillance.

- Role Based Access: Cloudvue supports the use of multiple roles and permissions to ensure that only authorized people have access to data as determined by its customers.

- Data Minimization: Cloudvue only collects, processes and maintains personal data only for the purpose of making our services available to our customers. Cloudvue only saves, manages or processes data that is related to the required operations of the service. We also use this data to improve the performance and security of the services and to contact customers for important service notices such as upgrades and requests for feedback.

- Accuracy and integrity: Cloudvue encrypts data once captured and cannot independently edit the data with the customer's permission. It also provides the facility to delete all video and personal data from its platform.

- Storage Limitation: Cloudvue offers video data retention options from no storage to five years in the cloud and multiple options for internal storage within cameras and gateways. Cloudvue also provides the facility to delete all video and personal data from its platform. Additional features allow for the limitation of internal storage within cameras and gateways.

- Security: Cloudvue has leveraged a decade of expertise to create and implement industry-leading secure software development, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance. For a detailed technical brief of security and frequently asked questions, visit our Cloudvue Security site.

- Protection at Scale: Cloudvue has a demonstrated history of successfully operating at a large scale uploading, storing and securing 72M minutes of video surveillance daily and over 52B minutes of cloud stored video surveillance.

- In-Country Hosting: Cloudvue operates a dedicated UK server option and continues its expansion into other countries worldwide in its drive to provide the highest level of performance and data privacy.

- Infrastructure: The Cloudvue infrastructure runs exclusively on a third party cloud, provided by a global leader in data security.

- Auditing: The Cloudvue Manager service supports robust auditing and reporting on system access and configuration changes.

- Authentication: Cloudvue improves security of its services utilizing technologies such as two factor authentication (2FA) and biometric authentication (fingerprint) among other technologies.

- Encryption: Cloudvue data is encrypted at capture, in transport and at rest (in storage). The platform leverages outbound communications and TLS 1.3 for end to end encryption of data. Cloudvue utilizes port 443 for data communications.

- Firmware Updates: Cloudvue automatically updates cloud and gateway firmware to ensure the latest in privacy and cyber security protection.

How does Johnson Controls manage its own compliance with privacy laws, including the GDPR?

- Johnson Controls has a Global Privacy Program built on global privacy principles, which include accountability, transparency, integrity and security of data, underpinned by our Controller Binding Corporate Rules (BCR). It is this Program which governs the Privacy by Design process, together with all Johnson Controls obligations as both Controller and Processor of personal data.

The Cloudvue Commitment

Cloudvue is committed to making your world a safer place and assisting you *with* keeping your data secure through investments in and regular upgrades to its privacy and cyber security technologies. For additional information about Cloudvue, please visit us at Cloudvue.ai.

Additional References: White Paper regarding GDPR Impact on Video Surveillance