Becoming GDPR Compliant with Avigilon

The General Data Protection Regulation (GDPR) is a new regulation under European Union (EU) law regarding data protection and privacy for all individuals within the EU and individuals whose personal data is processed by EU-established organizations. The new regulation imposes new obligations on those who collect, store, and process such data. The GDPR went into effect in all EU countries on May 25th, 2018.

While the GDPR was not written expressly with video in mind, video is considered personal data of the subjects captured on camera, and therefore the regulation implies that those who own and operate video surveillance systems must carefully consider, document, and manage the privacy impact of their video surveillance systems.

Although technology (such as Avigilon Control Center (ACC) video management software) cannot itself be GDPR compliant, all technology providers must consider how their products and solutions can assist enterprises in deploying and operating a GDPR compliant system. Avigilon has taken care to ensure that its video security solutions include features and functionality that will support GDPR compliance.

This document provides a simple framework based on five basic principles of the GDPR to help support compliance of a **Data Controller's** video system. Additionally, it highlights the specific capabilities within Avigilon's video security solutions that will help enable an organization to be compliant.

5 Basic Principles of the GDPR

- **Clearly Justified Purpose** All organizations must have a valid lawful basis for collecting and processing personal data.
- **Privacy by Design** The GDPR mandates that privacy must be a priority throughout system design and commissioning. The approach taken with respect to data privacy must be proactive, not reactive. Risks should be anticipated and the objective must be preventing events before they occur.
- **Right to Access** Under Article 15, the GDPR gives individuals control over their personal data including the right to see that data.
- **Right to be Forgotten** Under Article 17, the GDPR gives individuals control over their personal data including the right to have their personal data erased if it is no longer necessary for the intended purpose of the system.
- **Security** The GDPR requires organizations have comprehensive policies and procedures ensuring personal data remains within control of the organization at all times. Additionally, personal data breaches must be reported within 72 hours to the competent supervisory authority appointed by their country's government.

PRINCIPLE	VIDEO SYSTEM IMPLICATIONS	SUGGESTED ACTIONS TO PROMOTE COMPLIANCE	RELATED AVIGILON FEATURES AND FUNCTIONALITY
Clearly Justified Purpose	Documented description of: the purpose of the video system, what information is collected, what it will be used for, by whom, and for how long. In specific cases deemed high risk of encroaching on privacy, a formalized data privacy impact assessment (DPIA) is required.	Ensure signs are posted including details on where data subjects can find more information. Assure information is available to any data subject on: purpose of data gathering, type of processing done (e.g. live or recorded), data retention time, etc. Consider whether a DPIA is required.	None. These procedural based requirements are the Data Controller's responsibility.
Privacy by Design	Organizations must carefully consider and document how systems are designed to stay within the stated objectives. Care must be paid to not capture personal data of subjects who fall outside of the domain of the system (e.g. adjacent public areas). Careful consideration of who needs to see what information (e.g. live/recorded, timeframe, resolution) and who can access what features (e.g. search).	Use the Avigilon System Design Tool (SDT) to document resolution at different points in the camera scene, intended retention, etc. Review roles and responsibilities for operators, investigators, system administrators and others with access to the system. Consider restricting access to groups tasked with investigations for cameras that are specifically positioned to capture identity (e.g. faces of people entering a store). Consider restricting access to recorded video for operators, either completely, to only the video recorded since they last logged on, or only with dual authorization. Ensure the administrator account password is known only by specified people and that this account is used only for administrative tasks.	SDT is useful in planning a system before installation and helping to ensure that coverage, resolution, and retention are properly considered. ACC™ offers control over user permissions, ensuring security personnel can only access the video data that they need to do their job. ACC will control the resolution of the video displayed based on user permissions. ACC requires explicit user permissions to access search functionality that uses personally identifiable information such as personal appearance, access control identity cards, license plates or point-of-sale information.

PRINCIPLE	VIDEO SYSTEM IMPLICATIONS	SUGGESTED ACTIONS TO PROMOTE COMPLIANCE	RELATED AVIGILON FEATURES AND FUNCTIONALITY
Right to Access	Upon request, organizations need to deliver to a data subject all the personal data collected about them, including video collected by a video surveillance system. When delivering video to a data subject, other people appearing in the video must be masked or otherwise anonymized.	Ensure formal procedures and policies are created for handling right to access requests.	ACC enables the bookmarking and export of video. Avigilon Appearance Search™ technology is also featured in ACC, which enables users to locate, bookmark, and export recorded video of a specific individual. Appearance Search results can be exported by ACC while anonymizing images of all other subjects in the video.
Right to be Forgotten	Since deleting a specific subject from video is not practical, data-processors must strictly limit how long video is retained in accordance with the documented purpose of the system.	Review retention time for all cameras and ensure it is set in accordance with the documented system purpose.	ACC strictly enforces end-user specified limits on retention time per camera and license plate captures.
Cyber-Security	Take all appropriate organization and technical measures to protect against compromising personal data. Strictly adhere to GDPR guidelines on reporting breaches should they occur.	Review security policies around password control and account use. Consider setting minimum password strength requirements for all groups. Consider setting stronger requirements for administrative accounts. Have processes in place to audit protection status and detect breaches. Ensure users do not share accounts, whether by sharing passwords or by not logging off/on at the end/start of their shift. Maintain a documented policy and procedure governing appropriate actions in the event of data breach.	ACC employs security measures including strong password enforcement, connection authentication, and data encryption. ACC provides activity logs for all user actions to enable auditors to see who accessed what resources when.

Additional Resources

ICO.org Guide to the General Data Protection Regulation

EU Data Protection Supervisor, “The EDPS Video-Surveillance Guidelines” (PDF)

EU Data Protection Supervisor, “Article 13 – Information to be provided where personal data are collected from the data subject,”

EU Data Protection Supervisor, “Article 25 – Data protection by design and by default,”

EU Data Protection Supervisor, “Article 15 – Right of access by the data subject,”

EU Data Protection Supervisor “Article 33 – Notification of a personal data breach to the supervisory authority,”

North America: +1 888-281-5182 | International: +1 604-629-5182 | asksales@avigilon.com | avigilon.com

Global Headquarters | 555 Robson Street, 3rd Floor | Vancouver, British Columbia V6B 1A6 | Canada

L1018