A Guide to GDPR and Intelligent Video

MARCH networks®

Introduction

Over the past several years, data protection, privacy, and cybersecurity have moved from behind the scenes activities to front page news, emerging as a strategic priority for every company that handles personal customer data. As data breaches and cybercrimes increase in number and scale, governments are stepping in to create and enforce regulations that data 'collectors' and data 'processors' must meet in order to do business. While video surveillance technology has long been subject to retention and privacy restrictions in certain countries and regions, the requirements have varied widely.

The most recent and thorough legislation to tackle data protection and privacy is the European Union's General Data Protection Regulation (GDPR), which comes into effect on May 25, 2018. Although GDPR is being driven by the European Union (EU), its impact extends well beyond, applying to any organization that collects or processes the personal data of individuals within the EU borders, regardless of where that organization is located.

When applied to video, personal data is any information that can be used to uniquely identify an individual.

GDPR and Surveillance Video

GDPR defines personal data as any information relating to an identified or identifiable individual, such as (but not limited to) his or her name, home or email address, banking details, posts on social networking sites or computer IP address. Personal data also includes information collected using point of sale (POS) applications or analytic-driven applications such as face or license plate recognition software, with some exceptions. When applied to video surveillance, personal data is essentially any information that can be used to uniquely identify an individual.

Read March Networks President and CEO Peter Strom's article on Understanding GDPR and its impacts on video security to learn more.

Importantly, while GDPR mandates that video data must be protected, it does not precisely outline how that must be achieved. The regulation is focused on mandates around data privacy and protection that need to be equally applicable today and years from now, and therefore does not include detailed requirements or checklists for technologies that are currently available, including video technologies. As a result, there is no exact definition of what would constitute video data compliance, and interpretations are varying. Similarly, no bodies have been accredited under the regulation* to certify video solutions with the European Data Protection Seal.

*As of May 2018

How March Networks Solutions Support GDPR

As a global provider of intelligent video solutions, March Networks has been following GDPR requirements closely. In early 2017, we proactively engaged an external European data privacy consultant to independently audit our product portfolio against the regulation's overarching video surveillance guidelines.

As expected, many features already built into our products to help customers meet existing regulations, including the EU's previous data protection directive 95/46/EC, are applicable to GDPR. These include:

Authentication features that enable customers to tightly control and restrict who has access to recorded video data. Because our enterprise-class systems support large deployments with hundreds or thousands of users, we incorporate features to help safeguard data, including: fully configurable access rights (down to specific cameras); optional verification access with smart card asymmetric encryption keys; auditing logs and reports capabilities; and LDAP integration so that all user account information (e.g. privilege levels, passwords and domains) can be applied directly from an organization's corporate network directory, if preferred.

Anonymization features that allow customers to apply fixed privacy masks to conceal the unique identity of individuals captured on surveillance video unintentionally, such as someone walking on a sidewalk outside of a bank or retail store, or the license plates of cars driving alongside a public transit bus. March Networks systems support configurable privacy masking that remains intact in both live and recorded video, ensuring that customers can effectively avoid collecting and storing this identifiable data. See how our privacy masking feature works.

Encryption and Anti-tampering features, to assure customers that the video data they are collecting is being transported securely over the network. Our systems use TLS 1.2, an industry-standard protocol designed to protect the privacy of information over the Internet. In addition, we apply a secure hash algorithm (SHA-256) to exported video, which provides an anti-tampering function by preventing any modified exported video from being authenticated.

Retention features, which can be configured to delete recorded video automatically after a maximum retention time period. Our systems also enable authorized users to delete select recorded video manually. While GDPR does not set specific limits on the length of time an organization can archive its surveillance video, it does note that the data should not be stored for longer than necessary for its defined 'original purpose', so flexibility here is important, given different customer or country requirements.

Video streaming features, including support for multiple video streams, each with configurable resolutions. While GDPR does not specify a set video image resolution, the same restriction that requires organizations to limit data processing to no more than a defined 'original purpose' is applicable here. With multiple video streaming capabilities, customers can flexibly customize different video streams and resolutions to meet their exact applications.

As part of our GDPR audit, March Networks also identified areas where we believed further functionality would be beneficial. We added those features to our product roadmap and are now confident in our ability to support our customers and ensure they are well-prepared to meet GDPR legislation.

Designing inherently secure, data-protected solutions is part of March Networks' DNA, tracing back to our deep roots in information technology and networking

In addition, we continue to add new privacy-focused features into our product roadmaps, such as capabilities to further strengthen password management and user rights configuration. While these capabilities go beyond what may be considered GDPR legislated, they reflect our company's dedication to delivering secure solutions that make it easier for organizations to achieve their business objectives and remain compliant with existing and emerging security and privacy requirements.

A Comprehensive Approach to Data Privacy and Cybersecurity

March Networks has always been committed to providing organizations with secure video surveillance and video-based business intelligence products. We have spent more than 15 years delivering enterprise-class solutions to leading financial, retail and commercial customers worldwide, and following privacy-by-design principles that guide how our solutions capture, integrate and store video and business data. From the launch of our first Financial and Retail Transaction Integration (FTI/RTI) offerings a decade ago, we have worked closely with our customers, partners and privacy experts to understand and address varying data privacy requirements around the world.

Designing inherently secure, data-protected solutions is part of March Networks' DNA, tracing back to our deep roots in information technology and networking. Our holistic approach to cybersecurity involves a 360° view of all aspects of our business, encompassing our products, the people who build them, and the processes that guide us. Our company has participated in extensive security audits with Fortune 500 customers, examining everything from the security of our Network Operations Center to how we control and protect our software code.

We also work with a community of experienced systems integrators and arm them with the information and tools they need to ensure our customers' video systems are well protected. March Networks was the first in the industry to introduce a purpose-built mobile security audit tool in our GURU Smartphone App, and one of the first to create a proactive, transparent Security Updates and Advisories program to keep partners and customers informed about potential security vulnerabilities via email alerts and on our website. Most recently, we've achieved Cyber Essentials certification, recognizing us as a cybersecure business.

March Networks Security and Data Protection

A 360° Approach

March Networks is committed to helping our customers understand and address GDPR as it relates to video surveillance and video-based business intelligence, and to delivering products and solutions developed with a complete approach to cybersecurity.

People

- Deep heritage in information technology and networking
- Background checks on developers working with product code in the company's Canadian R&D Center of Excellence
- Secure, access-restricted Network Operations Center (NOC)
- Corporate offices and R&D labs access card protected

Products

- Extensive list of product features and capabilities to support video data authentication, anonymization, encryption and anti-tampering, flexible retention, multi-video streaming and configurable resolution
- Solutions already compliant with the European Union's previous data protection directive 95/46/EC
- Interactive Security Audit tool via our free GURU Smartphone App
- Product hardening guide

Processes

- Follow security-by-design principles in our product development and business systems
- Participate in extensive security audits with Fortune 500 customers
- Operate an extensive Security Updates and Advisories program; proactive, transparent and available to all customers and partners via our website
- Conduct annual penetration testing of internal business systems
- Cyber Essentials Canada certified, designating March Networks a cybersecure business

Questions? Contact Us

Should you have additional questions about any of our products, please contact your March Networks sales representative, call us at +1 613 591 8181 or email us at info@marchnetworks.com.

North America	1 800 563 5564
Latin America	+5255 5259 9511
Europe	+39 0362 17935
Asia	+65 6818 0963
Australia and New Zealand	+61 1300 089 419
Middle East and Africa	+971 4 399 5525

marchnetworks.com