SIA: General Data Protection Regulation (GDPR) Fact Sheet 2: Operational Privacy

July 2018

Produced Exclusively for the Security Industry Association

Table of Contents

Operational Privacy for Security Services – GDPR Fact Sheet 2

GDPR puts in place many requirements that impact the delivery of identity and security systems. From an operational perspective, privacy and operational security have independent and dependent relationships. Security has a role to secure sensitive personal information in the same way that security protects people, proprietary information, communications and other assets. Security and privacy need to meet operational requirements in the enterprise (including external supply chain and customer-facing requirements) and, as a result, our everyday lives. Developing the operational requirements for security, including risk assessment and mitigation, is more established and practiced than for privacy.

There may seem to be conflicts. Traditionally, security services have not had or wanted transparency of security infrastructure and services. In contrast, transparency is a design rule as it is mandated for personal data processing.

In the newly enforceable GDPR[i], operational privacy is required to be open and available, even for security services and systems. Security service providers and manufacturers who are not in the EU have requirements to support systems and services in the EU that manage personal data.

These requirements are specified according to the authority being used for the lawful processing of personal information. This requires privacy notices and responses with high availability to perform specific data control functions. Notice and receipts also facilitate policing, are available for gathering as evidence and can administer justice or provide access control when fit for purpose specified. Operational privacy puts in place privacy rights that work in conjunction with the purpose of the (security and surveillance) service.

How does the GDPR affect security providers and practitioners not based in the European Economic Area (EEA)?

The GDPR focuses on the use and control of individuals' personal information (data subjects) in the EU (whether a person is an EU citizen or not). Companies outside of the EU still have to comply with the regulation as long as they offer goods and services to citizens presiding in the EU or if they monitor their behavior.[ii]

- This means that if your organization or the technology services you use are in the EEA or your services involve transfer of employee's or customers' data from the EU to services outside of the EU, then the GDPR applies.
- In some circumstances under international public law, for diplomatic services, the GDPR applies in other countries.
- The GDPR also extends to tracking people in the EU on the internet with website cookies and similar tracking technologies: there is an additional EU law delayed until 2019 referred to as the ePrivacy Directive (ePD), which will impact electronic communications, cybersecurity and the

marketing industry. This law revises a 2002 law previously revised in 2011[1] that is intended to work in parallel with the GDPR.

For security providers and practitioners provisioning security services that operate outside the EEA dealing only with non-EU citizens and services, the GDPR does not directly apply.

In the wake of the Court of Justice European Union (CJEU) Google Spain decision on the liability of search engines and the 'right to be forgotten' in May 2014, along with the CJEU's decision in Weltimmo in October 2015[2], this indicates that increasing regulator activism means that global businesses should take note of how their processing activities may bring the supply of security technology and services within the scope of the regulation, even if it appears that a non-EU based part of their business is involved in different services from EU operations.

In the U.S., there are specific contexts where international public law will provide for the application of the GDPR; for example, diplomatic purposes and services, or where big data use may implicate surveillance technologies and security services. This is in addition to the grey areas of international spaces, like airports, where privacy notice is required and privacy risks are communicated to the unsuspecting European visitor as fair and reasonable.

What are the lawful justifications for security and surveillance of people?

Where the GDPR is applicable, the regulation provides a framework for privacy rights and privacy processing transparency that in all contexts is privacy by default, unless explicitly specified otherwise. There are 6 justifications for lawful processing of personal data[iii]

Which are,

- the data subject has given consent
- processing is necessary for the performance of a contract
- processing is necessary for compliance with a legal obligation
- processing is in the legitimate interest of the controller
- processing in the vital interest of the data subject
- processing in the public interest or in the exercise of official authority vested in the controller.

The justification being used for processing, and the purpose of the processing determines which rights and notices should be available, transparent and presented to the data subject (natural person).

For the purpose of safety, security and surveillance, the justifications are often in the public interest by a public authority, which includes policing, national security, criminal investigations and judicial process.

Organizations and people can have a legitimate interest to use surveillance technology to process personal data, but this comes with additional requirements to ensure data subject rights in the

[1] The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

2 The CJEU's decision in Weltimmo in October 2015, stipulating that a multi-national organization with head offices outside of the EU can be liable in each member state

processing of personal and sensitive data.

What privacy rights apply to security and surveillance?

The GDPR rights specified in the regulation include:

- Right to Be Informed
- Right to Complain
- Right to subject access and rectification
- Right to Data Portability
- Right to Restrict Processing
- Right to Erasure
- Right to Object
- Right to Withdraw Consent
- Rights in Regard to Automated Decision Making and Profiling

In all circumstances, the data subject has the right to be informed. (Although the timing of the information may vary depending on the jurisdiction).

Are the privacy rules different for policing and national security services?

The General Data Protection Act is part of the EU data protection reform package that included The Data Protection Directive for Police and Criminal Justice Authorities 2016/680.

The GDPR sets the framework for rights, the right to object, the right to information, access and correction, as well as the principles which operate in the privacy regulation. The directive provides the governance while the GDPR provides the governance framework.

The regulation stipulates that the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority.

The directive includes protecting personal data when being used by police and criminal justice authorities (from 2018)

The Data Protection Directive for Police and Criminal Justice Authorities, Directive 2016/680, also provides the governance framework for confidentiality that details and protects the personal data of different categories of individuals involved in criminal proceedings, such as witnesses, informants, victims, suspects and accomplices.

Police and criminal justice authorities are obliged to comply with the directive's provisions whenever they process personal data for law enforcement purposes, within both the personal and the material scope of the directive.[iv]

Are security and video surveillance systems exempt from consent?

There are many legal bases that can be used, and explicit consent is not the only option for all processing operations. Security integrators, suppliers, manufacturers and software vendors should understand the privacy profile for their technology in order to understand which requirements and exemptions apply. For example, GDPR provides an exemption from GDPR rights requirement, including explicit consent, for surveillance and security services in the following areas:[3]

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests; in particular, economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

Even with exemptions, all processing requires notice (and associated privacy policy) that provides operational information for access to privacy rights, that is suitable to context and audience. For example, in addition to the ability to use rights to restrict, block or object to processing video surveillance in the EU, there is also a requirement for a CCTV sign used at the perimeter of the surveillance, which displays the purpose, the data controller identity and contact information.

People in the EU have the right to ask for an explanation for any processing involving automatic decision making. They also have the right to access and correct their personal data in addition to the right to ask for privacy information and to make a complaint. This applies to video analytics and particularly facial recognition or other automated identification and profiling processes.

Regardless of whether explicit consent is the basis for the processing of personal information, privacy notices and policies are required for all contexts, necessarily providing access to all applicable privacy rights.

For example, security software solutions should be packaged with a mandatory privacy notice that not only specifies the identity and contact of the controller, but also specifies the purpose and the personal data categories that are disclosed and length of data retention in an accompanying policy.

[3] Exemptions as advised by the UK Information Commissioner can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

What if security software transfers personal data out of the EU into the U.S.?

If your product or service is used to transfer personal data outside of the EU to the U.S., then there are a number of mechanisms beyond explicit consent or the performance of a contract that are considered to be equivalent of GDPR privacy protections.

- Binding Corporate Rules (BCRs) for multi-national enterprise
- Standard Contractual Clause approved by the European Commission (EC)
- Codes of Conduct adopted or authorised by Data Protection Authorities (DPA)
- Privacy Shield, which is an adequacy framework (see appendix)

As a security service provider, can my customer make me liable?

As a processor of personal data, supplier or manufacturer, your organization can be operationally dependent on the instructions from the controller. In some cases, security system providers have no visibility into their customers (the controllers)' data, and unable to assess the nature of the risk. In other cases, the security service provider does have visibility into system and personal information. This means a data processor may be required to develop security requirements and place obligations on security technology providers or their customers to assess, at a minimum, the level of security and privacy controls required for information processing.

What is operational privacy for video surveillance?

The most intense topic in privacy is surveillance. As security and safety technology advances, so does surveillance. The UK arguably has the most mature governance framework for CCTV and video surveillance in the world. The UK has been an early adopter of video surveillance at scale and, as a result, now has a surveillance commissioner and a surveillance code of practice.[v]

The code provides a governance framework and guiding principles which can be used as short guide, providing high quality awareness for system operators and manufacturers.

Video system operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted, and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorized access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement, with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system that compares against a reference database for matching purposes should be accurate and kept up to date. [vi]

GDPR Acronyms

Binding Corporate Rules (BCRs)

California Consumer Privacy Act (CCPA)

Court of Justice European Union (CJEU)

Data Protection Authorities (DPA)

Data Protection Impact Assessment (DPIA)

Data Protection Representative (DPR)

Data Protection Officer (DPO)

ePrivacy Directive (ePD)

European Commission (EC)

European Economic Areas (EEA)

Fair Information Practices Principles (FIPPs)

International Organization for Standards (ISO)

National Institute of Standards and Technology (NIST)

Video Management System (VMS)

Appendix: Privacy Shield Considerations

Should my organization be registered with the EU-U.S. Privacy Shield?

For those practitioners in the U.S., the EU-U.S. Privacy Shield framework ***currently*** provides a recognized level of adequacy from the EU for the transfer of personal data to the U.S. and is required for services that transfer the data of people in the EU to the U.S. most commonly with explicit consent or a contract. (The lack of a) Privacy Shield registration is one of the key items in an organization's public privacy profile. Beyond the reputational damage, organizations that transfer personal data to the U.S. are liable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) as well as other laws or regulations prohibiting such acts.

Is a Privacy Shield registration enough to protect my cloud service?

Even with Privacy Shield registration, the privacy compliance and rights requirements for security and surveillance technologies vary greatly depending on the purpose and the sensitivity of personal information. Privacy Shield does not require many aspects of the GDPR, so it is not a good technical reference even if at present it may be a legal one.

For example, the GDPR refers to special categories of data that require additional considerations not considered in Privacy Shield. In the GDPR and CCPA (the recent California legislation) the privacy and security of children's data is most strongly emphasized, especially when this sensitive data is profiled and used for automatic decision making. The GDPR requires that rights are operationally usable. For example, explicit consent from a parent before transferring children's data is needed. This requires consent and identity record keeping, logging changes to policy and notice and obtaining further consent prior to any material changes in the purpose of personal data processing. Depending on the purpose and privacy profile, these GDPR requirements can apply for example to security systems in primary education and day-care.

Note: There are expected changes to the status and or the operation of the Privacy Shield framework Sept. 1, 2018.[4]

[4] Note: There are expected changes to the status and or the operation of the Privacy Shield framework, which is used as a consent framework to provide adequate privacy rights for the transfer and use of personal information. The European Commission has ruled on the adequacy of privacy shield and issued a resolution that unless changes are made, the Privacy Shield will be suspended Sept.r 1, 2018. [http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2018-0305&language=EN]

[i] The Council of the European Union, May 24, 2016 **The General Data Protection Regulation (GDPR),** https://ec.europa.eu/info/files/regulation-eu-2016-679-protection-natural-persons-regard-processing-personal-data-and-free-movement-such-data_en

[ii] ibid.,1 Article 3(2)

iii ibid., 1 Article 6 (1)

[iv] ibid., 1 Article 2 (1), The Council of the European Union, April 27, 2016 DIRECTIVE (EU) 2016/680 Data Protection Directive for Police and Criminal Justice Authorities http://eur-lex.europa.eu/legal-ontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

[v] UK Surveillance Commissioner, June 2013, **Surveillance Camera Code of Practice**, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

[vi] ibid., vi