SIA: General Data Protection Regulation (GDPR) Fact Sheet 1

July 2018

Produced Exclusively for the Security Industry Association

Table of Contents

GDPR Overview

On May 25, 2018, the GDPR[i] came into force for 28 European countries, and after July 20, three more countries will join for a total of 31[1].

The GDPR impacts the security industry with a mandate that security technologies be used to ensure data protection and rights. This mandate brings with it the expectation that practitioners, manufacturers and software developers within the security industry take a proactive and visible approach to mitigating privacy risk.

The Global Impact of the GDPR

The GDPR is the first multi-jurisdictional privacy enforcement framework that harmonizes privacy laws, unifies a digital single market and enforces an international standard in privacy amongst its members. The regulation is designed to require data controllers to consider privacy risk in order to implement proportional privacy practices[2]. In this regulation, privacy risk is based on the purpose for processing personal data, whether special categories of data are involved, the volume and frequency of personal data processing and how personal data is treated. Both the moral[3] and physical detriments of non-compliance are measured when a privacy complaint is made to a regulator, which can result in the most serious offenders facing up to a maximum fine of 4 percent of their annual global turnovers or €20 million[ii] for each infraction. As a result, knowing the privacy profile of the security implementation is the first step towards being able to identify and quantify the privacy risks involved.

The GDPR has evolved from Fair Information Practices Principles (FIPPs) first created in the United States and other best practices, standards and law in the European Union (EU) and around the world[4].

The regulation aims to operationalize privacy rights (or data control and access permissions) at scale across the EU and, by so doing, drive privacy rights internationally. Already the GDPR is having a global impact, with many different countries enacting privacy legislation in order to establish GDPR compliance. Recent privacy law in the U.S., the California Consumer Privacy Act (CCPA)[5] establishes GDPR-styled legislation further establishing the growing set of global requirements.

Questions & Answers

---

[1] Three new member states joining the EU July 20, 2018, are Iceland, Liechtenstein and Norway
[2] (GDPR, Recital 4)
[3] Note: Moral privacy harms as cited in UK Court of Appeal; *Google Inc v. Vidal-Hall & Ors* **[2015] EWCA Civ 311**
[4] 127 countries with the latest country Brazil passing privacy GDPR-styled (consent-based) privacy law on July 10, 2018.
[5] The CCPA was passed into law on June 29, 2018; it comes into force Jan. 1, 2020

What impact does the GDPR have on the security industry?

Security suppliers and manufacturers of security products provide technologies that are used for a number of purposes, which themselves process or generate personal data.

In general, the GDPR requires an extension of the functionality currently delivered by security systems to accommodate personal data processing. [iii] Depending on the purpose of processing (e.g. public safety, national defense, criminal proceedings, industrial security, marketing or customer behaviour) a range of notices, user controls, data storage and erasure requirements are now by necessity system features, functions and components that are needed to mitigate privacy risk.

How does the GDPR translate to security suppliers?

In the regulation, there are two key roles with defined obligations: the data controller[iv] and the data processor[v].

From a security supply chain perspective, the end users are data controllers. If the end user is also the operator of the security system, then they are the data processor as well. In some cases, a system integrator maintains the data processor security systems and services can come into contact with (or close proximity to) sensitive information, will need to support the data processor and can inherit responsibility for these obligations.

In the context where security technology or a system is provided as a service, then the service supplier becomes the data processor. If this is not the case, system integrators are still supplying systems that are expected to meet privacy requirements of the data processors or data controller. In all of these scenarios, there are additional operational privacy requirements for security services.

What is privacy risk?

A key concern for data controllers is understanding the privacy risk and management of the liability inherent to the provision of services from data processors. **A data controller is liable for the purpose for processing and all third-party (data processor) services and the sub-processors of those services downstream.** This is why the GDPR stipulates that a contract with model contractual clauses and clear chain of data transparency is required throughout the supply chain.

If a system implementation uses a third-party service, this increases the privacy risk in the privacy profile of a security implementation. The GDPR requires that data controllers and third-party data processors manage these risks by adopting model clauses that have been approved by data protection authorities or similar when drawing up contract agreements.

The GDPR requires documenting privacy risk by stating how data and *personal data categories*[vi] are used. If your system is comprised of products and services that can be resold to people in the EU, it should have accompanying privacy documentation as best practice, even if it is just to indicate that this product or service is not used to process personal data.

If personal data is transferred to a third country, the level of protection afforded by that third country, referenced to an adequacy framework (e.g., Privacy Shield[6]), or details of the safeguards adopted by controllers in the absence of an adequacy decision is required to be presented in notices and privacy policy.

How do I take a more proactive approach to privacy?

Be aware of the public privacy profile of your product or service and the obligations this privacy profile has for data controllers and data processors that use your service.

If your product or service is used in high-risk data processing, this needs to be identified (and assessed) as a higher privacy risk, and a data protection impact assessment must be conducted in order to have appropriate controls in place. High-risk processing is more likely to attract the regulators, and the inevitable scrutiny from all parties adds to the heightened risk in a profile.

In terms of security and liability, it is a best practice to receive the appropriate policy from the data controller and note what data processing role any data processors and sub-processors have in an integrated system.

If the processing involves automated decision making and/or analytics, information about the logic involved, including privacy risk, should be provided to the individual in a notice.

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:[7]

- National security
- Defense
- Public security
- The prevention, investigation, detection or prosecution of criminal offenses
- 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

[6] For more information on how EU-U.S. Privacy Shield applies see the appendix,
[7] 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/

- Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defense, other important public interests or crime/ethics prevention
- The protection of the individual or the rights and freedoms of others
- The enforcement of civil law matters

Even with exemptions, all processing requires a notice (and associated privacy policy) that provides operational information for access to privacy rights. 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 to display the purpose, 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.

Regardless of whether explicit consent is the basis for the processing of personal information, privacy notices and policies are required for all contexts and 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 data controller, but also specifies the purpose and the personal data categories that are disclosed and length of data retention in an accompanying policy.

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

In the GDPR the focus is on the use and control of personal information of individuals (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 GDPR as long as they offer goods and services to citizens presiding in the EU or if they monitor their behavior.

- Indirectly this means that if your organization or the technology services you use are in the EEA, or if your services involve transfer or customers' data from the EU to services outside of the EU, 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 called the ePrivacy Directive (ePD), which will impact electronic communications,

cybersecurity and the marketing industry. This law revises a 2002 law, previously revised in 2011[8], that is intended to work in parallel with the GDPR.

For security providers and practitioners provisioning security services that operate outside the EEA and 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[9], increasing regulator activism means that each global business should take note of how it may be brought within the scope of the regulation even if it appears that a non-EU-based part of its business is involved in different services from EU operations.

In the U.S., there are specific contexts in which 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 a privacy notice is required and privacy risks communicated to the unsuspecting European visitor are fair and reasonable.

What are key GDPR obligations?

The regulation imposes a number of service and compliance obligations with corresponding sanctions that effect third-party service providers (data processors). This is a significant change, as service providers could not have previously been held directly liable.

- Privacy should be a key item for any new contract renewal with your service. New service acquisitions from companies in the EU will require privacy contract clauses and considerations in order to be future proofed, regardless of what country you are in.
- As a data processor, for example, a VMS operator would need to gain prior written authorization from the data controller before using any sub-processors and will be fully liable for the actions of any sub-processor that it uses to provide its services and required to flow down its obligations under the regulation to the sub-processor.
- In such circumstances, the non-EU based personal data processors must designate an EU representative unless the data processing is occasional, does not involve sensitive data processing or is not high risk to the individual. The data protection representative is mandated to act with or in place of the data controller for all matters relating to data protection and on all issues relating to processing for the purpose of ensuring compliance with the regulation. (Art 27 (4)) [vii]
- Data processors, in addition to data controllers, are directly responsible for implementing appropriate security measures. The regulation includes a positive obligation to consider pseudonymization and encryption, ensure ongoing confidentiality, integrity, availability

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

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

and resilience of systems and services, certified capacity to restore access to data and, when operating a process, regularly test, assess and evaluate the effectiveness of security measures. The processor must also notify a controller without 'undue delay' after becoming aware of a personal data breach.[10]
- Processors must also comply with requests from data controllers to delete personal data, update and correct personal data records and produce a log of such actions upon request.

The GDPR makes it mandatory to appoint a data protection officer (DPO) or data protection representative (DPR) unless exempt. Organizations that process special and sensitive categories of personal data or significant amounts of what is classified as personal data, use surveillance and profiling technologies, perform automatic decision making, transfer personal data out of the EU or have a new technology that can have a significant impact on the privacy of people are not exempt.

What if security software transfers personal data out of the EU into the US?

If your product or service is used to transfer personal data outside of the EU to the U.S., 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)

As a security service provider, am I dependent on my customer and can my customer make me liable?

As a data processor, supplier or manufacturer, your organization is dependent on the instructions from the data controller. In some cases, security system providers have no visibility into their customers' (the controllers') data, so they will be 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.

[10] For regulated security services and federal security systems, privacy and security obligations are consistent with security best practices found in the National Institute of Standards and Technology (NIST) cybersecurity framework or other NIST special publications (insert ref) or security standards and controls from the International Standards Organization.

As a security supplier, what should I do to be prepared for the GDPR?

Dealing with or understanding the impact of the GDPR on your customers, the services you offer or products you develop might at first be quite daunting. The simple approach is to become aware of your own privacy risk and the privacy profile[11] of the systems active data processing activities once it is implemented. Then, with this privacy profile, provide the associated privacy and rights notices.

Privacy Profile Awareness Checklist:

1. Does this privacy profile present a high privacy risk?
    a. Does the implemented systems process personal data on a large scale?
    b. Is there processing of special personal data categories?
    c. Is there profiling? Is there automatic decision making based on personal data?
    d. Does your service transfer personal data out of the EEAs?
    e. What are the categories of personal data that are being processed?
    f. Are special categories (or sensitive categories) processed? What is the quantity and frequency of data processed?
2. What services do you have that process or have access to personal data? How many of these are third-party processors? What is the justification data collection?
3. Are your privacy practices documented?
    a. Has the service description been documented?
    b. Is the purpose definition, the justification[12] (authority for processing personal data), documented and defined?
    c. Are the personal data categories gathered and disclosed?
    d. Are all the data processors and sub-processors involved in the life cycle of the service listed?
4. If you have a high-risk profile: Have you conducted a data protection impact assessment?[13]
5. Manufacturers should provide known privacy risks in a multi-format resource that is operationally usable by the service integrators and the end service user.

---

[11] A privacy profile is determined by the nature of the service, its justification for processing personal data, the purpose for processing, the personal data categories processed, the disclosures of personal data and the associated context. Each profile has applicable rights, required notice and a proportional level of responsiveness for privacy information.

[12] Under the GDPR there are six justifications for processing; fulfillment of a contract, explicit consent, legitimate interest and legal obligation in the public interest or in the vital interest of a data subject

[13] (this is required in the regulation for high-risk data processing, the regulation stipulates that the identified risk should be mitigated, and if mitigation is not feasible, the regulation stipulates that you should contact a supervising privacy authority.)

6. Where possible, use international standards, adhere to industry defined codes of practice and use defined purpose specifications for your industry

Consider Privacy Rights, Notices and Operational Administration

For security practitioners, the GDPR provides operational rights. It sets a maximum response time of one month to privacy information requests and 72 hours[viii] to notify after a data breach, removes the fee for subject access requests and better defines the privacy.

The regulation specifies privacy notices that include the data controller identity, address, contact, purpose and data categories collected and shared to the data subject – including the length of personal data retention so that controllers and processors send a clear operational signal of how long personal data will be processed for, that includes notice for the use of rights. The access to rights and privacy information will be operationally different depending on the justification for processing personal information.

Many security practitioners will operate, or help build, systems that can have exemptions from supporting certain types of rights, require a policy, notice and the operational ability to process privacy requests from people and a record of the notices people have consented to.

Acronyms

Binding Corporate Rule (BCR)
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)

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 reflected in the 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. [14]

---

[14] 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. 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),** [Internet, accessed July 13, 2018] **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 Art 83 (4) & (5)
[iii] ibid., 1 Recital 83
[iv] Data controller (PII controller) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by union or member state law, the controller or the specific criteria for its nomination may be provided for by union or member state law;
[v] Data processor (or PII Processor) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
[vi] Personal data categories: All purpose specifications for the processing of personal data need to specify the categories of personal data that are used.
[vii] ibid., 1 Article 27 (4)
[viii] ibid., 1 Recital (85)