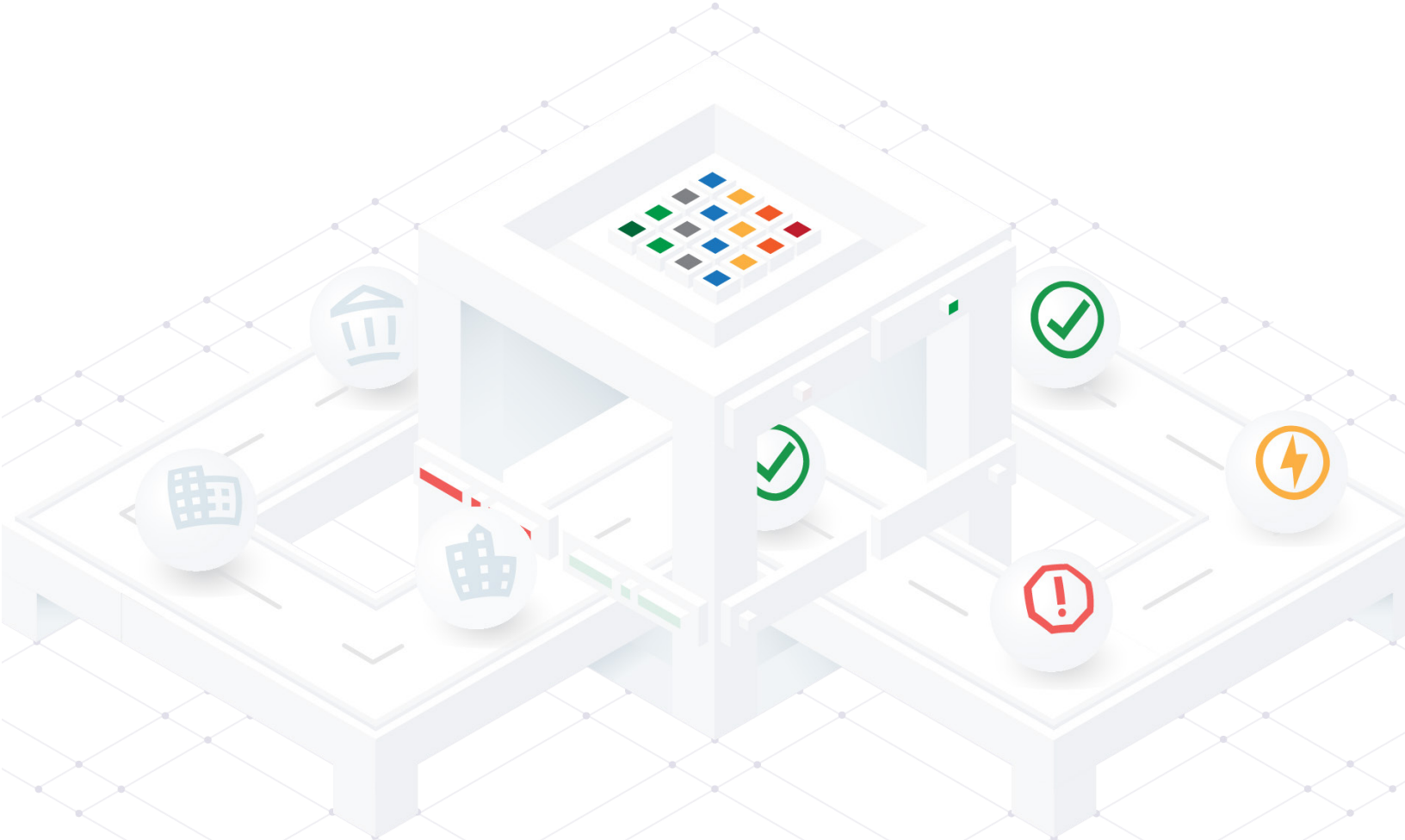
riskrecon

GDPR for Third-party Risk Management

Everything you need to know to stay compliant



RiskRecon.com
sales@riskrecon.com

Salt Lake City, UT
Draper, UT
Boston, MA
(801) 758 - 0560

Table of Contents

GDPR: How Organizations Go From Violations to Fines

Europe's GDPR is widely-discussed in today's news cycles and for good reason. The regulation impacts many organizations throughout the world, and violations of the regulation can result in material fines. One aspect that isn't widely discussed but an organization facing the possibility of a GDPR fine would want to know is how violations are identified and fines decided upon. In other words, what's the enforcement framework for GDPR?

Because the European Union (EU) is a union and not a federal government, its laws and regulations are directly enforced by its Member States. GDPR has required each Member State[1] to establish at least one independent supervisory authority (commonly referred to as data protection authorities, or DPAs), and these entities have responsibility to enforce GDPR in their respective Member State[2].

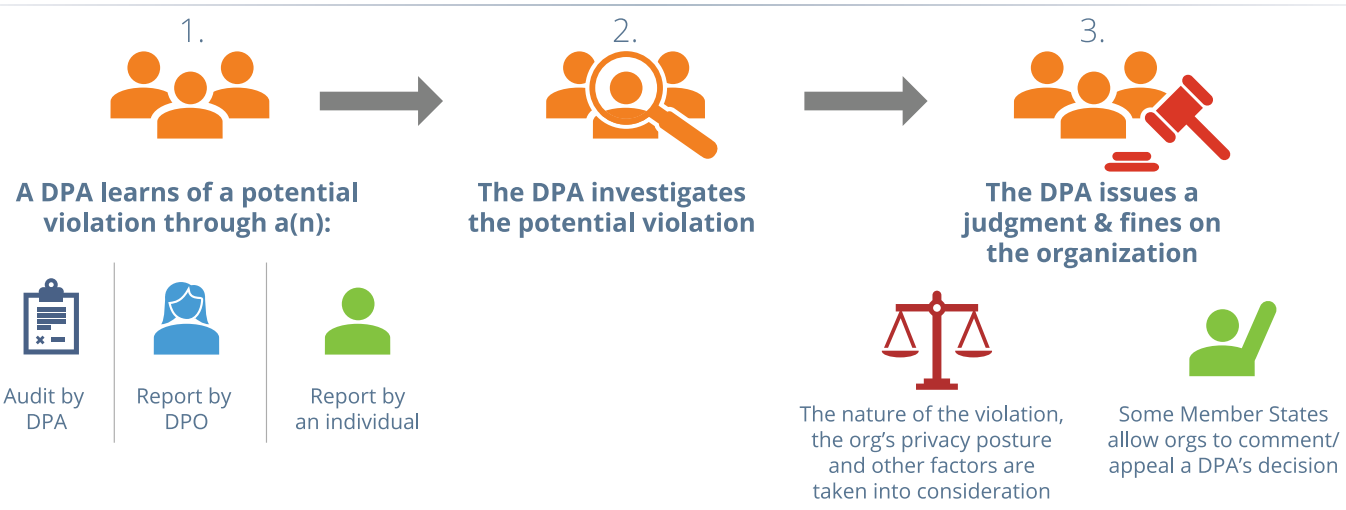


Figure 1: GDPR's Enforcement Process

Before the regulation can be enforced, a DPA must first find out that if an organization has potentially violated GDPR. This discovery occurs in one of three ways:

1. A DPA conducts an audit of an organization
2. An organization reports a violation through its appointed data protection officer (DPO)
3. A complaint is lodged by an individual against an organization

When a potential violation has been identified, the DPA begins investigation to determine if a violation has actually occurred and if it has, its impact (if a violation impacts individuals residing in more than one Member State, the DPA of the Member State whose residents were most affected takes the lead role).

Once an investigation has concluded, the (lead) DPA may issue the violating organization a monetary fine. We'll discuss fines in our next article, but know for now that fines are to be "effective, proportionate and dissuasive" while taking into account the following (Article 83):

- The violating organization's:
  - Size
  - Posture towards privacy
  - Attempts to mitigate the effects of violations
  - (If applicable) Previous GDPR violations
- The types of data involved
- The type of the violation, such as a(n):
  - Unapproved data transfer
  - Data breach

From here, the process differs by each Member State, which are instructed by GDPR to create their own laws that govern how their respective DPAs may exercise authority. For example, the United Kingdom's DPA (called the ICO) generally:

- Issues a preliminary findings and monetary fine
- Allows the organization & affected individuals to comment on the findings and fine
- Delivers a final decision

Regardless of if an appeal process exists in a given Member State, once a fine has been issued, the violating organization will have to pay that fine.

[1] As of July 2019, the EU Member States are (listed alphabetically): Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Spain, Sweden and the United Kingdom

[2] DPAs have other responsibilities as well, but this article focuses solely on DPA's enforcement responsibilities

GDPR Fines: What They Mean For Your Organization and What You Can Do

Until July 8 & 9, 2019, the median GDPR fine was €5,000. On those two days, two fines in the hundreds of millions of euros were announced for GDPR violations. In this article, we'll talk about what this change in enforcement posture means for your organization.

The Breaches and The Fines

In the fall of 2018, British Airways and Marriott International, Inc. notified the public that they had experienced data breaches involving sensitive customer data. At British Airways, an injection vulnerability was exploited in Sep. 2018 by hackers who scraped 500,000 individuals' credit card and other personal information. And in 2016, Marriott acquired Starwood Hotels, but unbeknownst to Marriott or Starwood, Starwood had been experiencing an undetected security breach since 2014. This breach, finally uncovered in Sep. 2018, exposed the personal details of over 300 million individuals, including over 5 million unencrypted passport numbers.

On July 8 and 9, 2019, the UK's GDPR enforcement agency (the ICO) announced that they intend to fine[1] British Airways and Marriott £183.39 million ($204 million) and £99 million ($110 million) fines, respectively, for these breaches[2].

What These Fines Mean For Your Organization

When announcing the two intended fines, the UK's ICO Commissioner, Elizabeth Denham, stated that:

"People's personal data is just that — personal. When an organization fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights."

This statement and the size of the fines make it clear that European officials intend to more strictly enforce GDPR going forward (keep in mind that fines can be up to €20 million or 4 percent of annual, global revenue, whichever is greater).

To protect your organization from potential material fines, it can take the following steps to ensure it's GDPR compliant:

- If you haven't already, determine how GDPR applies to your organization

You'll need to assemble the appropriate parties (e.g., legal counsel, information security, etc.) to determine how it applies to your organization. In short, though, if your organization targets or has data on individuals in Europe (regardless of their citizenship), your organization is required to comply with GDPR and protect that personal data.

- Establish a mature security program

Article 32 requires organizations to implement information security measures that are commensurate to the risk associated with the personal data that the organization processes, including:

- Pseudonymization (i.e., anonymization) and encryption of personal data
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems/services
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

If your organization is looking for a place to start, there are many industry standards that can guide you in implementing a mature program. ISO 27001 and NIST's security framework are two such standards.

- Sign data protection agreements with all of your vendors who will handle personal data originating from Europe

If you transfer personal data to any of your vendors, your organization needs to create and sign data protection agreements with them that contractually obligate them to fully comply with GDPR and only process the data per your organization's instructions.

- When making acquisitions, conduct a thorough security & privacy assessment of the organization you're wanting to acquire

As Marriott learned the hard way, your organization assumes full responsibility for any GDPR violations that the company you acquire may be committing. If a process is not already in place, be sure to conduct a thorough security & privacy assessment when acquiring companies. Be aware that other GDPR-like privacy regulations exist, and more are coming

Many countries around the world are actively adopting privacy regulations similar to GDPR, and it's likely that the United States will enact its own federal privacy regulation in the coming years. California has already passed the California Consumer Privacy Act, which in a simplified way, is a less-strict version of GDPR. Additionally, the European Union has stated that any country wanting to sign a trade deal with the bloc will be required to comply with GDPR as a part of the agreement.

To ensure you're complying with all of these regulations, consult with your organization's legal counsel to obtain a full list of which regulations apply to your organization.

How Can I Stay Updated On New GDPR Fines?

In addition to news announcements, http://www.enforcementtracker.com/ maintains a list of all GDPR fines.

[1]As we discussed in-depth in our previous article, The UK's ICO first announces fines, gives the fined organizations time to respond, and then issues a final fine.

[2]The differences in breach amounts were likely due to the number of individuals residing in Europe for each breach.

GDPR: Third-party Risk Management Obligations

Historically, organizations have sometimes been able to shift some liability for data breaches to their third-parties, if not all liability (this has been especially true for payment data breaches).

Under GDPR, however, organizations are held responsible for all of their third-parties' actions and can even be held responsible for fourth-parties' actions if the organization doesn't adhere to GDPR's requirements. In this article, we'll discuss what these requirements are and what your organization can do to comply with them.

This article is organized as follows (includes links to article destinations):

Definitions

Before we dive into the requirements, there are four terms that are vital to understand when dealing with GDPR and third/fourth-party risk management:

1. Controller
2. Processor (i.e., third-party)
3. Sub-processor (i.e., fourth-party)
4. Processing

1. **Controller:** When many people hear the word controller in a compliance situation, they are often thinking of someone who ensures their organization's policies are properly implemented and followed. GDPR's definition of a controller, however, is completely different. Under the Regulation, a controller is any entity (a person or organization) that decides how personal data is to be processed.

2. **Processor (i.e., third-party):** A processor is any entity (a person or organization) that actually processes personal data under and per the controller's instructions. Processors are not permitted to use the controller's data in any way except as explicitly authorized by the controller.

3. **Sub-processor (i.e., fourth-party):** While not an official GDPR term, sub-processor is a term that's widely used in practice. A sub-processor is an entity that performs processing activities on behalf of the processor.

4. **Processing:** Processing is a pretty broad term, essentially meaning any interaction with data. The official definition is "any operation performed on personal data (whether automated or not) including adapting/altering, aligning, collecting, combining, consulting, destroying, erasing, making available (e.g., distributing through transmission or dissemination), organizing, recording, restricting, retrieving, storing, structuring and using."

Classifications are Relative

To illustrate this concept, let's consider a fictional scenario from the perspective of each entity.

In this scenario, ABC, Corp. has hired Data Processing, Corp. to process some personal data. Data Processing, Corp. has, in turn, hired a company named Analyze Your Data, Inc. to assist with processing personal data. Analyze Your Data, Inc. has also hired some companies so it can fulfill its contract with Data Processing, Corp.

Classifications from ABC, Corp's Perspective

From ABC, Corp's perspective, the other entities have the following relationships with it:

- Data Processing, Corp - Processor (i.e., third-parties)
- Analyze Your Data, Inc - Sub-Processor (i.e., fourth-parties)
- Other Companies - n/a (i.e., fifth-parties)

Classifications from Data Processing, Corp.'s Perspective

From Data Processing, Corp.'s perspective, the other entities have the following relationships with it:

- ABC, Corp - Controller
- Analyze Your Data, Inc - Processor (i.e., third-party)
- Other Companies - Sub-processors (i.e., fourth-parties)

Classifications from Analyze Your Data, Inc.'s Perspective

- ABC, Corp. - No relationship
- Data Processing, Corp - Controller
- Other Companies - Processors (i.e., third-parties)

Requirements

Now that we understand how organizations are classified and their relationships with one another, let's now discuss each type of organization's responsibilities under GDPR as well as the requirements for entering into data protection agreements and some of GDPR's high-level requirements.

Controllers' Requirements

Controllers are required to:

- Ensure that their processors are able to comply with GDPR, including:
  - Only using processors who provide sufficient guarantees, especially in regards to the following, that the processor can implement appropriate mechanisms that enable compliance with GDPR:
  - Expert knowledge
  - Reliability
  - Resources
- Approve in writing of each of a processor's sub-processors
- Enter into a contract with each processor, commonly referred to as a "Data Protection Agreement"

Processors' Requirements

Processors are required to:

- Process the controller's data only as directed in writing by the controller
- Have all sub-processors approved by the controller:
  - In writing
  - Prior to being been engaged
- Take full responsibility if a sub-processor fails to comply with GDPR
- Ensure that its personnel who will be processing the controller's data are committed to keeping the data confidential
- Assist the controller, when necessary and upon request from the controller, in complying with GDPR by carrying out data protection impact assessments
- After completing the processing activities on the controller's behalf and at the discretion of the controller, return or delete all personal data.
- If a processor is required to store the data to comply with another law, though, it may do so
- Enter into a contract with the controller, commonly referred to as a "Data Protection Agreement"
- Enter into a contract with each of its sub-processors, commonly referred to as a "Data Protection Agreement"

Sub-processors' Requirements

Because GDPR's classification of entities are relative, sub-processors will enter into agreements with the organization hiring them as a processor and the hiring organization as a controller. Each entity will then be subject to those types of entities' requirements.

Data Protection Agreement (DPA) Requirements

DPAs may either be a(n):

- Individual contract
- Standard contractual clause adopted by the European Commission or a Supervisory Authority

DPAs must:

- Bind the processor to the controller
- Specify the:
  - Types of data to be processed
  - Duration of the processing
  - Reasons for the processing
  - Processor's specific tasks & responsibilities
  - Risks to the rights and freedoms of the data subjects
- Require a processor to:
  - Take all measures required in Article 32 (more on this below)
  - Assist the controller in:
    - Fulfilling the controller's obligations to data subjects' rights (more on this below)
  - Complying with Articles 32 - 36 (more on this below)
    - Have all sub-processor approved by the controller
    - Enter into a separate DPA with each of its sub-processors
    - After completing the processing activities on the controller's behalf and at the discretion of the controller, return or delete all personal data (unless required to retain the data by another law)
  - Provide all necessary information to the controller in order:
    - To demonstrate compliance with GDPR
    - For the controller to conduct audits of the processor
  - Inform the controller if, in the processor's opinion, any of the controller's instructions violate GDPR

While not specifically required, most controllers require their processors to inform them of any data breaches within 24 hours of becoming aware of the breach.

GDPR Requirements (high level)

Covering GDPR's requirements would take multiple articles, but at a high-level GDPR requires organizations to:

- Respect the privacy rights of persons residing in the EU (not just EU citizens)
- Ensure the confidentiality, integrity, availability and resilience of personal data

In this piece, we referenced several GDPR Articles and the rights of data subjects. At a high level, these requirements are as follows:

- Data Subjects' Rights
  - The Right to Rectification
    - An individual may direct an organization to correct personal information that is incorrect
  - The Right to Be Forgotten
    - An individual may direct an organization to delete any and all of their personal data
  - The Right to Data Portability
    - Personal data must be easily transferable between related services
    - An individual may direct an organization to either provide them with a copy of easy transferable personal data or transfer the personal data to a similar type of service
  - The Right to Object
    - An individual may direct an organization to not process any and all their personal data
  - The Right to the Restriction of Processing
    - An individual may direct an organization to stop processing any and all their personal data

GDPR is a complex piece of legislation, and how an organization is classified is entirely relative. These distinctions are important to know as you enter into contracts with different entities and consider your organization's respective responsibilities.

- The Right of Access
  - An individual may direct an organization to provide them with all of their personal data, including:
    - Data the individual's given to the organization
    - Data the organization has:
      - Collected on the individual
      - Inferred about the individual
- Article 32 - Security of Processing Personal Data
  - Processes and controls must be implemented to ensure that personal data is appropriately secured, depending on the type & sensitivity of the data processed
- Article 33 - Breach Notification to Supervisory Authorities
  - Processors must promptly notify their controllers of any personal data breaches
  - Controllers must notify the appropriate Supervisory Authority that a personal data breach has occurred within 72 hours of becoming aware of the breach
- Article 34 - Breach Notification to Data Subjects
  - Controllers must inform data subjects of any data breach immediately if the data breach is likely to cause a high degree of harm to the data subjects
  - Controllers do not have to inform each data subject impacted by a data breach if any of the following conditions are met:
    - The data was appropriately encrypted
    - The controller has taken appropriate steps to ensure harm to the data subjects resulting from the data breach are no longer likely to occur
  - Doing so would be too time-consuming, costly, etc. In these cases, a public notification is to be made.
  - Supervisory Authorities may require controllers to inform data subjects of any data breaches, regardless of impact on the data subjects

- Article 35 - Data Protection Impact Assessment
  - If processing activities are likely to significantly affect the rights & freedoms of data subjects, controllers must carry out a data protection impact assessment
- Article 36 - Prior Consultation with Supervisory Authorities
  - If a data protection impact assessment finds a high level of risk to data subjects' rights and freedoms without appropriate controls or compensating controls in place, the controller must consult with the appropriate supervisory authority prior to processing the data

What Can Your Organization Do?

To ensure your organization complying with GDPR and to limit its exposure to risk:

- Thoroughly vet all third-parties and fourth-parties that will touch personal data subject to GDPR
- Enter into Data Protection Agreements with each of your third-parties who will be processing personal data subject to GDPR
- For US-based companies, consider becoming US-EU Privacy Shield compliant
- Be compliant with all of GDPR, including respecting the privacy rights of individuals residing in the EU (not just EU citizens)

Sources

GDPR: How Organization Go From Violations to Fines

- https://europa.eu/european-union/about-eu/countries_en
- The GDPR - A Comprehensive Overview by Andrew Sanford (https://drive.google.com/file/d/1s6jc71ghKk7NInz-yci9ALo4uV5JyxMu/view)
- UK's ICO https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach

GDPR Fines: What THey Mean for Your Organization and What You Can Do

- https://news.marriott.com/2016/09/marriotts-acquisition-of-starwood-complete/
- https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
- https://krebsonsecurity.com/tag/starwood-breach/
- https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information
- http://starwoodstag.wpengine.com/wp-content/uploads/2019/05/us-en_Second-Response.pdf
- https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- https://www.iso.org/isoiec-27001-information-security.html
- https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
- https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
- https://www.ft.com/content/e489abba-0dc5-11e8-8eb7-42f857ea9f09

GDPR: Third-party Risk Management Obligations

- Original, full text of GDPR
- GDPR's recitals (i.e., official guiding instructions)
- Personal experience dealing with GDPR