

SAI360°



Compliance and Benefits, Not
Liability and Penalties: Finding
the GDPR's Hidden Treasure

Table of contents

PART 1: APPLICABILITY

Does the GDPR apply to your organization?	4
Third- and fourth-party liability	7
What you can do	7
What the regulation says	7

PART 2: LIABILITY

When are you liable for an infringement?	8
Notification	8
What you can do	8
What the regulation says	10

PART 3: PENALTIES

How are penalties determined?	12
What are the penalties?	12
Lower-level penalties	12
Higher-level penalties	13
Other penalties	13
What you can do	13
Use the GDPR to create competitive advantage	14
What the regulation says	15

Introduction

The European Union's General Data Protection Regulation (GDPR) presents businesses and other organizations around the world with a stark choice: will they view it as a compliance burden to be minimized, avoiding liability with as little disruption and cost as possible? Or instead, will they seize the opportunity to be proactive, reaching beyond bare compliance for the financial, reputational and operational advantages it can bring?

There's no prize for guessing which approach we advocate, and the reasons are simple. *The Harvard Business Review* has noted that when compliance programs fail, it's often due to ineffective data collection and analysis: Firms cannot design effective compliance programs without effective measurement tools... Put simply:



“Better compliance measurement leads to better compliance management.”

Why Compliance Programs Fail, *Harvard Business Review*,
March–April 2018

The GDPR mandates comprehensive data tracking, record-keeping and notification systems, even for non-European Union (“Union”) organizations. Most organizations based in the Union will already have systems and protocols in place to manage data; the clever ones will use the need for GDPR compliance to build a stronger, more proactive, risk-savvy culture that will not only ensure compliance and avoid penalties, but also provide positive business benefits.

This ebook focuses on the penalties, liability and requirements arising from the GDPR, and how you can address them. It outlines the key steps your organization must take to avoid liability; conveniently, **these are also a handy guide to creating just the kind of business-positive compliance culture described above.**

There's no doubt that the penalties imposed by the GDPR are a big stick – but we urge your partners to regard the potential benefits as an even bigger carrot.

Part 1: Applicability

In this section we discuss whether and how the GDPR's provisions apply to your organization, and what actions you can take to ensure you're well-positioned for compliance.

DOES THE GDPR APPLY TO YOUR ORGANIZATION?

If your organization handles the data of European Union citizens, the answer is most likely yes, regardless of whether you have established operations within the Union itself.

The GDPR is concerned with the safety, security and handling of *personal data*. **Personal data** is information that could be used to identify a data subject, either an identifier (such as a name, address, email address or GPS location data) or a factor relating to the person's identity (including physical or health data, political or religious affiliations, sexual identity or activity, or criminal records).

The regulation specifies two categories of organization that handle such data: *controllers* and *processors*.

Controllers are people or organizations that determine what personal data will be used for and how it will be processed. **Processors** are people or organizations that process personal data on behalf of a controller.

In terms of geographical scope, the Regulation broadly applies to the processing of any Union citizen's personal data. More specifically, it applies to the processing of personal data.

- By a controller or processor established in the Union, regardless of where the processing takes place;
- By a controller or processor not established in the Union that is offering goods and services to, or tracking the behavior of, data subjects in the Union
- By a controller not established in the Union but in a place where Member State law applies.

Any data subject who thinks their rights under the Regulation have been infringed can bring a complaint to the *relevant supervisory authority* (usually a national government body or department). The organization committing the infringement does not have to be established in the Union, meaning the **Regulation has global reach**.

Note that simply moving user profiles from one legal entity to another (as Facebook has done) is no protection against incurring a penalty. As noted above, the relevant test is not the controller's or processor's location or jurisdiction; rather, it is whether a data subject's rights regarding their personal data have been infringed.

Importantly, the Regulation also requires controllers and processors to have measures in place to ensure the safety, security, and integrity of any personal data they handle.



You must ensure all your third- and even fourth-party suppliers are compliant.



THIRD- AND FOURTH-PARTY LIABILITY

Note that controllers are liable for their processors' compliance or noncompliance – that is, if a processor commits a breach, its controller will also be held liable.

This means you must ensure all your third- and even fourth-party suppliers are compliant.

A fourth-party is any organization providing services to a third party. It can include individual subcontractors as well as organizations like internet service providers and cloud service providers.

What you can do

We recommend this process to determine your potential liability:

- Determine whether any of your operations involve the personal data of data subjects.
- Understand whether you are a controller or a processor.
- Identify all the processors you engage (if you are a controller).
- Conduct risk assessments/audits of relevant internal systems and demand evidence of the same from your providers or vendors.
- Ensure your providers audit their supply chains so you're not exposed to fourth-party risks.

What the regulation says

GDPR [*Article 3 Territorial scope*](#) provides that the Regulation applies to the *processing of personal data* by controllers and processors established in the Union; in places where Member State laws apply; or where data subjects are offered goods and services or are monitored.

GRPR [*Article 4 Definitions*](#) provides detailed definitions of terms including data subject, personal data, controller, processor, relevant supervisory authority and more.

GDPR [*Article 32 Security of processing*](#) mandates that controllers and processors implement *technical and organizational measures* to ensure appropriate security, including: pseudonymization and encryption; measures to ensure systems' *confidentiality, integrity, availability* and resilience; the ability to restore availability and access to personal data in a timely manner; and processes for *regularly testing, assessing and evaluating* their security.

Part 2: Liability

In this section we discuss what constitutes an infringement of the Regulation, and how you can prepare and respond.

WHEN ARE YOU LIABLE FOR AN INFRINGEMENT?

Data controllers and processors are liable when data is improperly handled: lost, altered, disclosed, transmitted, stored, or processed without the relevant data subject's authorization.

Further, processing must be secure, meaning data must be anonymized and encrypted, and the data's confidentiality, integrity, and availability must be maintained. In the event of an infringement, access must be restored in a timely manner, and organizations must be able to demonstrate a process for regularly testing the above.

NOTIFICATION

Importantly, the relevant supervisory authority must generally be notified *within 72 hours*. Affected data subject(s) must be notified *without undue delay*, though in some cases there is no requirement to notify data subjects (e.g. if the data breached was unreadable).

More specifically, you must notify the affected data subjects if the data protection impact assessment's (DPIA) result regarding the processing activity in question indicated that a high risk was imposed on the rights and freedoms of the natural persons involved in the breach.

What you can do

Ultimately, the regulation requires you to have a clear understanding of the likely points of weakness or vulnerability in your system. Thorough record-keeping is critical, and you must be able to answer the following questions about your processes:

- Where, how, and when do you process data?
- Who has access to this data, and with whom do you share it?
- Do you have data hygiene and security systems in place?
- Do you have a risk-aware compliance culture?
- If you are a controller, are your processors similarly able to identify their systems?

Most importantly, you must put in place robust systems to detect possible infringements, both internally and externally. And if you are a controller you are liable for your processors, which means your liability extends to third and even fourth parties.

Finally, you must put in place procedures to notify the relevant authorities and individuals within the necessary time frames (72 hours is a good standard to adopt for both). This includes systems for handling group notifications and timeline monitoring in the event of a wide-reaching infringement.

An effective compliance regime can be not only a strong defense against a breach, but also a mitigating factor if one occurs.



What the regulation says

GDPR [Article 32 Security of processing](#) mandates that controllers and processors implement technical and organizational measures to ensure appropriate security, including: pseudonymization and encryption; measures to ensure systems' confidentiality, integrity, availability and resilience; the ability to restore availability and access to personal data in a timely manner; and processes for regularly testing, assessing and evaluating their security.

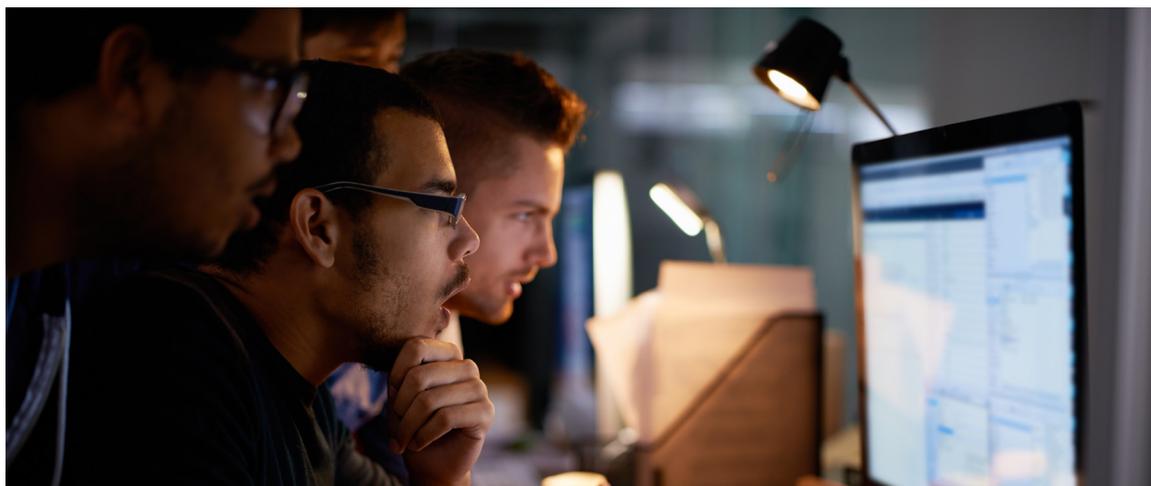
GDPR [Article 33 Notification of a personal data breach to the supervisory authority](#) specifies that controllers must notify supervisory authorities without undue delay and, where feasible, not later than 72 hours after becoming aware of a breach.

GDPR [Article 34 Notification of a personal data breach to the data subject](#) specifies that controllers must notify the data subjects without undue delay.

GDPR [Article 35 Data protection impact assessment](#) describes when a DPIA is required, what it should contain, how it should be created, and various other details.

GDPR [Article 77 Right to lodge a complaint with a supervisory authority](#) provides that data subjects may lodge a complaint if they consider that the processing of personal data relating to him or her infringes this Regulation.

GDPR [Article 79 Right to an effective judicial remedy against a controller or processor](#) notes that each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed.



Part 3: Penalties

In this section we discuss the penalties that can be imposed. As noted, they can be severe. The Regulation's governing principle is that they should be *effective, proportionate, and dissuasive*.

HOW ARE PENALTIES DETERMINED?

Ten criteria are used to determine the penalties imposed on a noncompliant organization:

- **NATURE:** How many data subjects were affected, what damage did they suffer, what was the processing's purpose?
- **CHARACTER:** Was the infringement negligent or intentional?
- **MITIGATION:** What action has been taken to mitigate the damage?
- **PREPARATION:** Did the organization have technical and organizational safeguards in place?
- **HISTORY:** Has the organization infringed before?
- **COOPERATION:** Has the organization cooperated with the supervisory authority?
- **CATEGORIES:** Did the breach involve personal data, sensitive personal data, or both?
- **NOTIFICATION:** Did the organization notify the supervisory authority directly and within 72 hours, and data subjects if required?

- **CERTIFICATION:** Have the organization's systems been certified, and are codes of practice in place?
- **OTHER:** Are there any other aggravating or mitigating factors, such as financial losses or benefits?

Note that if an organization infringes more than one Article, it will be fined only for the most serious breach.

If more than one controller and/or processor is liable, all will be penalized. No organization may take recovery action against another until it has paid its fine. This is critical, as it reinforces controllers' liability for their processors, and it means payment of fines cannot be delayed while liable organizations litigate responsibility.

What are the penalties?

There are three categories of penalty: for low-level breaches, generally relating to lapses in obligations and processes; for high-level breaches, generally relating to more serious breaches of personal data; and other penalties imposed by Member States.

LOWER-LEVEL PENALTIES

Up to €10 million, or 2% of the prior year's annual global revenue, whichever is higher. This applies to infringements relating to obligations of controllers and processors, certification bodies, and monitoring bodies.

HIGHER-LEVEL PENALTIES

Up to €20 million, or 4% of the prior year's annual global revenue, whichever is higher. This applies to infringements relating to basic principles for processing, data subjects' rights, transfers of personal data, obligations pursuant to Member State law, and noncompliance with orders imposed by supervisory bodies.

OTHER PENALTIES

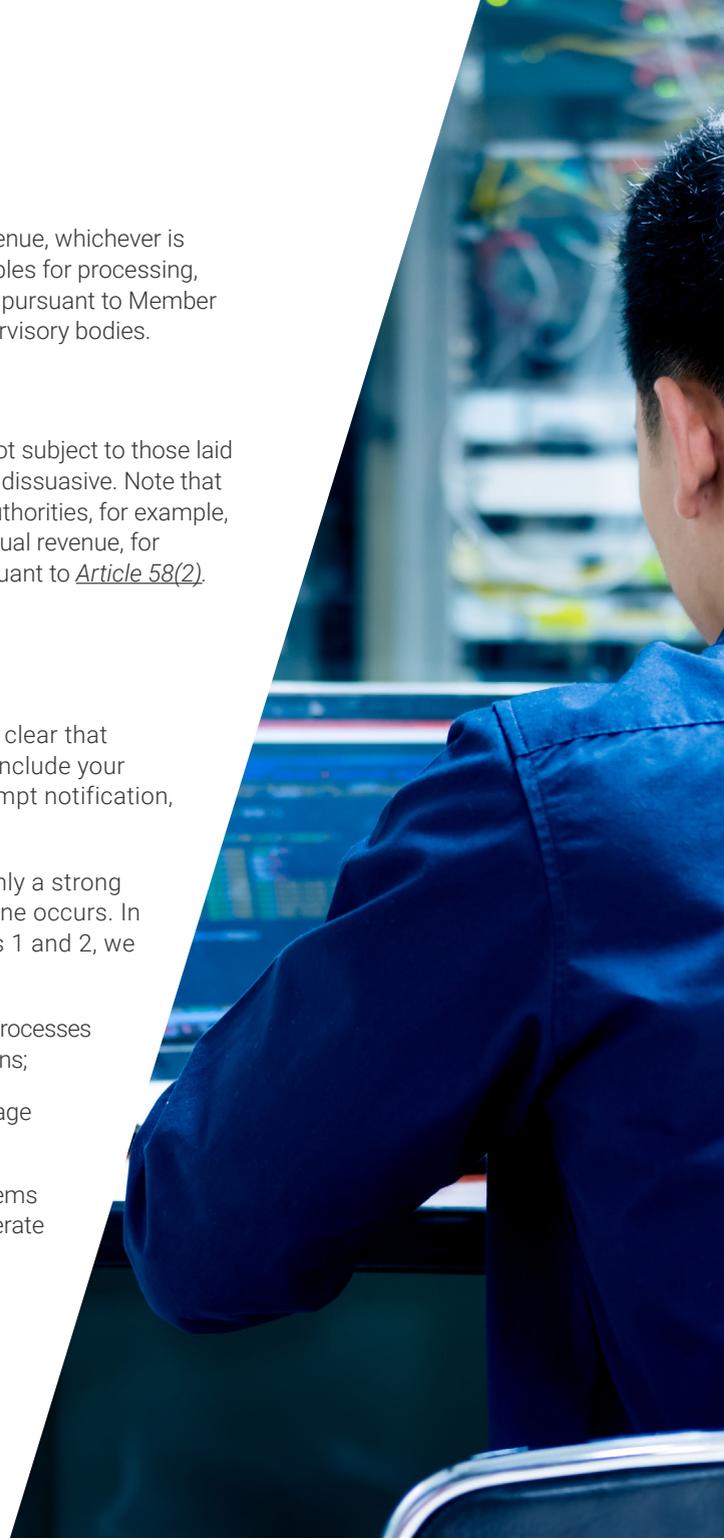
National bodies may impose penalties for other breaches not subject to those laid out in [Article 83](#). These shall be effective, proportionate and dissuasive. Note that these too can be significant; the German Data Protection Authorities, for example, can levy fines up to €20 million, or 4% of the prior year's annual revenue, for non-compliance with an order by the supervisory body pursuant to [Article 58\(2\)](#).

What you can do

Despite the potentially severe penalties, the Regulation is clear that certain factors can be used in mitigation. As noted, they include your organization's efforts around compliance, mitigation, prompt notification, cooperation with authorities, and so on.

To this end, an effective compliance regime can be not only a strong defense against a breach, but also a mitigating factor if one occurs. In addition to the processes and controls discussed in Parts 1 and 2, we recommend putting in place:

- **AUDIT TRAILS** to ensure all your relevant systems and processes are regularly audited by reputable third-party organizations;
- **MITIGATION** plans and processes to ensure the damage inflicted by any breach is minimized;
- **ANALYTICS** to ensure the data gathered by your systems is used to continuously improve compliance and generate usable business intelligence; and
- a **COMPLIANCE CULTURE** to ensure operational compliance and that your systems and processes are being properly used.





Culture's importance cannot be over-stressed in this context. We have seen in the news numerous examples of organizations where a lax or unethical culture has had serious consequences. These include: poor internal security procedures leading to identity theft and data breaches; aggressive, sales-focused cultures leading to fraud and financial misconduct; and even inward-looking cultures leading to deceptive and illegal conduct.

Senior leaders must show the way on culture, by creating a compliance-savvy environment with automated and easy-to-use tools and processes. The data thus collected throughout the organization can then be aggregated and analyzed, predicting risks and identifying opportunities.

USE THE GDPR TO CREATE COMPETITIVE ADVANTAGE

In this way, compliance and risk management become business-positive tools for producing business intelligence and competitive advantage. For example, such tools can help identify the risks associated with a new product. By analyzing them alongside the willingness of a target market to accept them, informed decisions can be made about product design, launch, sales forecasts, marketing programs, staffing and resourcing, and more.

Compliance with the GDPR – and ensuring you are ready to make the most of the mitigating factors available if a breach occurs – will take you a considerable distance down this road. We suggest that wise businesses, charities, government departments, and other organizations of all types and sizes keep traveling.

The GDPR won't just help you avoid dead ends and potholes in the road. It will put you on the high road to success.

What the regulation says

GDPR [Article 58 Powers](#) describes supervisory authorities' investigative, coercive, and authorisation and advisory powers:

- *Investigative powers* include the authority to access information, conduct investigations, review certifications, access premises, data and other information.
- *Coercive powers* include the authority to issue warnings, make orders regarding compliance and communication of data breaches, impose bans, order data erasure, and impose administrative fines.
- *Authorisation and advisory powers* include the authority to issue opinions and certifications, authorize processing and contractual clauses, and approve binding corporate rules.

GDPR [Article 83 General conditions for imposing administrative fines](#) specifies penalties:

Up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements relating to:

- obligations of controllers and processors (Articles 8, 11, 25–39, 42, 43);
- obligations of the certification body (Articles 42, 43); and
- obligations of the monitoring body (Article 41(4)).

Up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements relating to:

- processing, including consent (Articles 5, 6, 7, 9);
- data subjects' rights (Articles 12–22);
- data transfers to third countries or international organizations (Articles 44–49);
- noncompliance with a supervisory body's order (Article 83(6)); and
- obligations pursuant to member state laws (Chapter 9).

GDPR [Article 84 Penalties](#) notes that other penalties for infringements not subject to the fines specified in Article 83 *shall be set down by Member States, and that such penalties shall be effective, proportionate and dissuasive.*

[solutions] to advance confidently

About SAI Global

At SAI Global, we help organizations proactively manage risk to achieve business excellence, growth, sustainability and ultimately, create trust.

Our integrated risk management solutions are a combination of world-class tech platforms, services and advisory capabilities that operate across the entire lifecycle allowing businesses to focus on opportunities presented by uncertainty. Together, these tools and knowledge enable customers to develop a holistic, integrated view of risk. In Australia, we are also a leading provider of settlement-related services; company, personal and property information.

SAI Global's head office is located in Chicago, Illinois. We employ more than 2,000 people across 28 countries and 51 locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

saiglobal.com/sai360



SAI Global ABN 67 050 611 642 © 2018 SAI Global.
The SAI Global name and logo are trademarks of SAI Global.
All Rights Reserved. 129196 1118