The GDPR: A New Standard of Care for Personal Data

Written by
Sam Pfeifle
Content Director, International Association of Privacy Professionals (IAPP)

Published by
SecurityFirst™
Protecting Critical Data

SecurityFirst
Protecting Critical Data

The GDPR

A New Standard of Care for Personal Data

Perhaps the most impactful global regulation since the Sarbanes-Oxley Act of 2002, the European Union's (EU) General Data Protection Regulation (the GDPR), which came into force on May 25, 2018, represents a new era in data governance. With its mandates for the protection of personal data and the new rights it grants to those residing in the EU, it changes the way any company does business with Europeans.

Sam Pfeifle
Content Director, IAPP

SCOPE

Not only European-based companies must comply, but any company around the world that gathers the personal data of a person residing in the EU falls under the GDPR's jurisdiction. Even if you simply have employees in Europe.

NEW RIGHTS

Data subjects, as the GDPR calls people, now have the right to request you delete their data, amend their data, provide a record of all the data you hold about them, even require you to provide their data in a machine-readable format so they can give it to one of your competitors.

NEW SECURITY MANDATE

For the first time, the GDPR introduces the concept of "adequate" security in the European Union, and provides important incentives for using encryption and other methods of protecting data.

DATA BREACH NOTIFICATION

For the first time, the EU now has a member-wide mandate to notify regulators and data subjects in case of a data breach. Further, the definition of data breach is significantly expanded. Again, there are important incentives to make sure lost data can't be read by unauthorized people, including hackers.

PENALTIES

Finally, the penalties for not complying with the GDPR are significant, to say the least. Fines can be as high as 4 percent of global revenues for the organization as a whole, or 20 million euros – whichever is higher. The definition of personal data is broad, the new rights for data subjects are significant, and the penalties for not complying are steep indeed. *Ignore the GDPR at your peril.*

The GDPR:
A New Standard of Care for Personal Data

The General Data Protection Regulation (the GDPR) replaced the European Union's (EU) Data Protection Directive 95/46/ec (the Directive) effective May 25, 2018. The GDPR is a wide-ranging and complicated law that, as a regulation instead of a directive, is directly applicable in each of the EU's 28 Member States. It is broken down into Articles and Recitals designed to bring a greater degree of data protection law harmonization across EU nations, in line with the Digital Single Market initiative that aims to make e-commerce easier in the EU.

Although many companies doing business in the EU or with EU citizens have already adopted privacy processes and procedures consistent with the Directive, the GDPR contains a number of new protections for EU data subjects and threatens significant fines and penalties for non-compliant data controllers and processors.

In this paper we'll focus on the new standard of care the GDPR creates for personal data. Because of its jurisdictional scope, any company that markets to or employs people residing in the EU, or even a non-EU resident who happens to be there for a visit, falls under its mandate whether the organization is headquartered on EU soil or not.

And if you violate those mandates? The GDPR allows for very large fines. An organization can be fined as much as 4 percent of total annual revenue (referred to as "turnover" in the GDPR) or 20 million euros, whichever is larger.

Therefore, the GDPR's new obligations for data breach notification, allowing data subjects to access and delete the data you hold, facilitating the transfer of personal data to another company in a machine-readable format, and making sure data subjects can exercise their rights must be accounted for by just about any company doing business on the Internet and welcoming European business.

Collecting and storing sensitive data in clear text, for example, was already a bad idea. It is now essentially illegal and a threat to business integrity.

Under the GDPR, data subjects have gained new rights that must be clearly explained to them using plain language even minors (if included among the expected data subjects) can understand. They must be informed what data is being collected, how it will be processed, and how long it will be retained. Organizations are further obligated to protect that data using appropriate safeguards while it remains in their possession. Collecting and storing sensitive data in clear text, for example, was already a bad idea. It is now essentially illegal and a threat to business integrity.

Central to compliance with the GDPR is the idea of "accountability," which is a fancy way of describing the ability to demonstrate, on demand, that your organization complies with the GDPR. To simply avoid breaking the law is no longer adequate.

One important point before moving on to Chapter 1: The GDPR makes a distinction between organizations based on their relationship to the personal data in question. "Controllers" are organizations that have the relationship with the data subject. They likely collected the data, obtained the consent, or have the business relationship with the customer. "Processors" are generally vendors, such as cloud service providers, that process data on behalf of the controller.

And when you see that word "process" don't think that it means you have to do something with the data. In the EU, simply possessing data is the same as processing it.

TABLE OF CONTENTS

The GDPR enhances data security and breach notification standards

Data security plays a prominent role in the GDPR, reflecting its symbiotic relationship with modern comprehensive privacy regimes. Compared to the Directive, the GDPR imposes stricter obligations on data processors and controllers (we'll explore this distinction further in Chapter 3) with regard to data security, while offering more guidance on appropriate security standards. The GDPR also adopts for the first time specific breach notification guidelines.

The GDPR separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide sufficient guarantees to implement appropriate technical and organizational measures to meet the GDPR's requirements and protect data subjects' rights. Processors must also take all measures required by Article 32, which delineates the GDPR's "security of processing" standards.

Under Article 32, similar to the Directive's Article 17, controllers and processors are required to implement appropriate technical and organizational measures, taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and

severity for the rights and freedoms of natural persons." Unlike the Directive, however, the GDPR provides specific suggestions for what kinds of security actions might be considered appropriate to the risk, including:

- The pseudonymization and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or an approved certification mechanism — as described in Article 40 and Article 42 — may use these tools to demonstrate compliance with the GDPR's security standards. While no codes of conduct have yet to be approved, it may be the case that something like ISO 27001 will be approved by the newly created European Data Protection Board, for example. Demonstrable compliance with such a globally recognized standard may very well become part of an organization's accountability program.

For additional guidance on security standards, controllers and processors may consider the Recitals, in particular Recitals 49 and 71, which allow for processing of personal data in ways that may otherwise be improper when necessary to ensure network security and reliability. If you are collecting personal data — log files of IP addresses or multiple location points for specific customers to ensure proper authentication — it is important for you to demonstrate the necessity of those actions for the proper functioning of your security program.

There are, however, important carve outs if you've taken good security precautions and both encrypted the data and retained encrypted back-ups.

Personal data breach notification standards

Unlike the Directive, which was silent on the issue of data breach, the GDPR contains a definition of "personal data breach," and notification requirements to both the supervisory authority and affected data subjects. There are, however, important carve outs if you've taken good security precautions and both encrypted the data and retained encrypted back-ups.

Personal data is defined in both the Directive and the GDPR as any information relating to an identified or identifiable natural person (data subject). Under the GDPR, a personal data breach is a breach of security, whether accidental or due to bad actors, leading to:

- Destruction of personal data.
- Loss of personal data.
- Alteration of personal data.
- Unauthorized disclosure of, or access to, personal data.

This broad definition differs from that of most U.S. state data breach laws, for example, which typically are triggered only upon exposure of information that can lead to fraud or identity theft, such as financial account information.

Regardless, if you've exposed the personal data of data subjects and "bad things" might happen, this notice must be provided without undue delay and, where feasible, not later than 72 hours after having become aware of it.

In the event of a personal data breach that stands to threaten the rights and freedoms of the data subjects involved, data controllers must notify the supervisory authority, also known as data protection authorities or data protection regulators, "competent under Article 55," which is most likely the supervisory authority of the Member State where the controller has its main establishment or only establishment, although this is not entirely clear. For example, if your EU office is in the UK, the Information Commissioner's Office will be your lead authority — at least until Brexit happens.

What if you don't have any physical location in the EU whatsoever? You'll have to identify a lead authority and create a relationship, though they are likely to encourage some sort of physical presence in the EU.

Regardless, if you've exposed the personal data of data subjects and "bad things" might happen, this notice must be provided without undue delay and, where feasible, not later than 72 hours after having become aware of it. If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

Anyone with experience in information security knows this is a short amount of time. Sometimes, it can take days, weeks, or months to fully understand the nature of a cyberattack or breach and just how much information has been accessed.

However, not fully understanding the nature of the breach may actually be a proper justification for delaying notice. According to guidance released by the Article 29 Working Party, which is the collection of EU data protection authorities that will be replaced by the European Data Protection Board under the GDPR, a controller becomes aware of a data breach when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."

During its initial investigation of the incident, which should begin as soon as possible, the controller is not considered to be aware. Whether it is immediately clear that personal data was compromised or this conclusion requires some time to reach, however, the emphasis should be on prompt action to investigate an incident to determine whether personal data has indeed been breached. Once the short period of investigation has passed and the controller has identified the incident, it is considered "aware" and notification to the supervisory authority is then required if this presents a likely risk to individuals.

In fact, Article 33(1) contains a key exception to the supervisory authority notification requirement: Notice is not required if the personal data breach "is unlikely to result in a risk for the rights and freedoms of natural persons," a phrase that will no doubt offer Data Protection Officers (DPOs) and their outside counsel ample opportunities to debate the necessity of notification.

For example, if a data breach involved personal data that was already publicly available, further disclosure of such data would not constitute a likely risk. Another example would be the theft of securely encrypted data for which the confidentiality of the key remained intact or uncompromised by the breach. As such, data would be unintelligible to unauthorized parties, this type of breach would be unlikely to result in a risk to individuals. If, on the other hand, the encrypted data was lost or there was an availability breach (i.e., the controller had no back-up), this could entail adverse consequences for individuals and would require notification.

Further, one must consider the sensitivity of the data. It may be that the nature of the data is so sensitive, such as genetic information or data surrounding lifestyle choices, that even well-encrypted data with a back-up might still require notification, as the risk is so great, even if the possibility of a true breach is very low.

This is where security, privacy, and legal teams have to be in close communication. All three parties will bring vital information to the table as you decide whether notification is legally necessary. Should you deem notification necessary, it must at least:

- Describe the nature of the personal data breach, including the number and categories of data subjects, and personal data records affected.
- Provide the data protection officer's contact information, assuming the organization has one.
- Describe the likely consequences of the personal data breach.
- Describe how the controller proposes to address the breach, including any mitigation efforts.

If all information is not available at once, it may be provided in phases.

When a data processor experiences a personal data breach, it must notify the controller, but otherwise has no other notification or reporting obligation under the GDPR. The controller takes on all those notification obligations and has to do the same calculations as to whether notification is necessary.

If the controller thinks that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals," it must notify the data subjects, in addition to the Data Protection Authority (DPA), whether the breach was the processor's fault or not. The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances:

- The controller has implemented appropriate technical and organizational protection measures that "render the data unintelligible to any person who is not authorized to access it, such as encryption."
- The controller takes actions subsequent to the personal data breach to ensure the high risk for rights and freedoms of data subjects is unlikely to materialize.
- When notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

Encryption is now clearly the standard of care for personal data. Store it in plain text at your peril.

Assuming the controller has notified the appropriate supervisory authority of a personal data breach, it may find the DPA makes the decision on notifying the data subjects.

Regardless, the direction is clear. If you hold personal data, you should encrypt it, both at rest and while in transit. Further, you should have a back-up that is kept separately and is also encrypted.

However, encryption is now clearly the standard of care for personal data. Store it in plain text at your peril.

GDPR compliance checklist

- [ ] 1. Identify any EU citizen personal data.
- [ ] 2. Pseudonymize and encrypt that data.
- [ ] 3. Appoint a DPO as applicable.
- [ ] 4. Select an EU supervisory authority.
- [ ] 5. Allow data subjects to request private data.
- [ ] 6. Establish ability to delete private data upon request.

The new rights to be forgotten and to data portability

Perhaps more than anything else, the GDPR seeks to provide data subjects with as much control over how their data is collected, used, handled, and destroyed as possible. Relatively long-standing rights to know what data an organization holds about a data subject, to have that data corrected, and to withdraw consent for the use of that data have been strengthened and made universal across the EU.

In addition, as part of its effort to expand individual control over the use of personal data, the GDPR introduces two new rights. First, it codifies a "right to be forgotten". This right allows individuals to request the deletion of personal data, and, where the controller has publicized the data, to require other controllers to also comply. Second, the "right to data portability" requires controllers to provide personal data to the data subject in a commonly used format and to transfer that data to another controller if the data subject so requests.

The data subjects' right to object to processing is broader than under the Directive, moreover, allowing them to object to processing at any time, unless the controller has compelling legitimate grounds.

To keep up with the augmented rights under the GDPR, data controllers must implement processes for handling and documenting requests from data subjects.

A right to erasure and the right to be forgotten

In a significant departure from the Directive, under Article 17 of the GDPR, controllers must erase personal data without undue delay if the data is no longer needed, the data subject objects to the processing, or the processing was unlawful.

Recital 65 explains that this right is especially relevant when a child consents to processing and later wants to remove the information, even if he is no longer a child. However, the right is not unlimited. It must be balanced against freedom of expression, the public interest in health, scientific and historical research, and the exercise or defense of legal claims.

The "right to erasure" extends additional obligations to any controller that makes personal data public, especially online. Where a data subject requests the erasure of data that has been made public, the controller must take "reasonable steps" to inform other controllers processing the data about the person's objection, unless it would require "disproportionate effort." Any controller processing the data must then erase copies of it or links to it. Whether the steps taken are reasonable will depend on the available technology and the cost of implementation.

When a data subject requests the restriction of processing, the controller should temporarily remove the data from a general filing system or from a public website so as to avoid further processing. Recital 67 specifies that controllers should flag the restricted data in a way that makes clear that processing is restricted.

For many organizations, this will prove difficult to accomplish and here's why:

- Can you readily find all of the places where information regarding a certain customer or contact is located?
- Do you have a database separate from your main database where such information could be quarantined?
- Do you have a way to attach metadata to certain personal information to indicate what consent is attached to it and the fact that certain consent has been revoked?

If so, you're ahead of the game.

A new right to data portability

One of the responses of the GDPR to the so-called "Big Data" trend is the creation of a new right to data portability that aims to increase user choice of online services.

Where controllers process personal data through automated means, Article 20 grants data subjects the right to receive the personal data concerning them. Controllers must provide the data in a commonly used and machine-readable format, and data subjects have the right to transmit that data to any other controller.

Where feasible, the controller may even be required to transmit the data directly to a competitor. However, Recital 68 specifies that it does not impose an obligation for controllers to adopt processing systems that are technically compatible.

The right to data portability applies only when processing was originally based on the user's consent or on a contract. It does not apply to processing based on a public interest or the controller's legitimate interests.

Your organization must figure out how it will segregate this data that might be subject to data portability so you can easily identify it and provide it to the data subject for portability on demand.

As an example, the Article 29 Working Party writes in guidance on data portability, "the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party."

Your organization must figure out how it will segregate this data that might be subject to data portability so you can easily identify it and provide it to the data subject for portability on demand. This can require both new policies and processes and new technologies, like software that allows you to easily attach metadata or keep one set of data apart from another, even though you want to use both sets of data and have them available at the same time.

Enhanced rights to notice, access, rectify, and to object to processing

Under the Directive, controllers had to provide data subjects with certain minimum information before collecting personal data. These disclosures included the identity of the controller, the purposes of processing, and any recipients of personal data. The Directive also provided data subjects with a right of access to data, which required controllers to confirm what data they were processing and the logic involved in any automatic processing operations. If a controller processed information in violation of the Directive, data subjects could block the processing and request the erasure or rectification of the data. Data subjects could also object in narrow circumstances where they could demonstrate compelling legitimate grounds or where the data was used for direct marketing.

The new Regulation increases the number of disclosures a controller must make before collecting personal data. In addition to the identity of the controller, the purposes for processing, and any recipients of personal data, Article 13 requires controllers to address with data subjects:

- How long the data will be stored.
- The right to withdraw consent at any time.
- The right to request access, rectification, or restriction of processing.
- The right to lodge a complaint with a supervisory authority.

Furthermore, these disclosures must be intelligible and easily accessible, using clear and plain language that is tailored to the appropriate audience.

Article 15 establishes a right of access that is more robust than what was required by the Directive. Users have a right to request a copy of their personal data undergoing processing, and they may also request to know the consequences of any profiling. Controllers must set up processes for responding for access requests and, in particular, for verifying the identity of a data subject who requests access. Recital 63 recognizes, however, that the right of access needs to be balanced against other rights, such as intellectual property, trade secrecy, and copyright protections for software.

The right to object to processing is significantly expanded under Article 21. Whereas under the Directive, data subjects could only object to processing where they could demonstrate compelling and legitimate grounds, the GDPR flips the burden, allowing a

data subject to object any time processing is based on public interest or the legitimate interests of the controller, unless the controller demonstrates compelling grounds.

Collect less, authenticate more

In the process of heightening user control over data, these expanded rights have created new challenges for controllers to implement systems that are responsive to user requests concerning their data. To this end, Article 12 requires controllers to provide "modalities" to facilitate the exercise of data subject rights. These modalities can include new user interfaces and customer support services.

Controllers should communicate with data subjects in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Where a data subject seeks to exercise one of the above rights, the controller must take the appropriate action without undue delay, or at the latest within a month of the request. The controller may, however, seek an extension where necessary because of a high number of requests. If the controller opts not to grant the request, it must explain its decision to the data subject within one month. All these services must be free of charge, unless the requests are "manifestly unfounded or excessive."

Controllers will face new changes in trying to authenticate users to process their requests. Article 12 provides that a controller may refuse to act on a request if it demonstrates that it is not in a position to identify the data subject. On the other hand, if it has reasonable doubts about the identity of the person making a request, it can ask the person for additional information to confirm his or her identity.

Controllers must face a difficult challenge in trying to authenticate users to process their requests.

Controllers must be thoughtful in implementing systems that, on the one hand, minimize the collection of data while, on the other hand, ensure accurate authentication to avoid abuse.

The GDPR requires companies that engage in regular and systematic monitoring of data subjects on a large scale to appoint DPOs with responsibility for overseeing these systems.

For these companies, managing access requests and the right to be forgotten represent a major focus for their new DPOs.

Controllers, processors, and vendor management

In its effort to protect and expand the rights of data subjects, the GDPR creates clear lines of accountability over data processing. This is especially evident in the way it delineates responsibilities between “controllers” and “processors” for handling personal data. As a reminder, controllers are essentially those organizations that have the relationship with the data subject. Processors are generally vendors, such as cloud service providers, that process data on behalf of the controller.

Burden on controllers

The GDPR makes it vital that you have tight control on the personal information you provide to vendors and other third parties.

Article 24 makes controllers responsible for ensuring that any processing activities are performed in compliance with the GDPR. Controllers must implement appropriate technical and organizational measures not only to ensure compliance, but also to be able to demonstrate the measures that they have in place.

Controllers also have specific responsibility for:

- Carrying out data protection impact assessments when the type of processing is likely to result in a high risk to the rights and freedoms of natural persons and implementing appropriate technical safeguards.
- Assuring the protection of data subject rights, such as erasure, reporting and notice requirements, and maintaining records of processing activities.
- Duties to the supervisory authority, such as data breach notification and consultation prior to processing.

The GDPR also encourages controllers to implement the principles of data protection by design and by default, where feasible. In essence, this means that controllers should design products with privacy in mind, rather than tacking it on as an afterthought, and that privacy-protective settings should be the default in any product.

While the GDPR imposes these heightened requirements on controllers, it is important to note that it also relaxes one of the requirements that existed under the Directive. Controllers are no longer required to register their processing activities with a DPA in each Member State. Instead, the GDPR imposes strict requirements on controllers to maintain their own detailed records of processing.

The GDPR allows controllers to demonstrate their compliance by adhering to codes of conduct and certifications that were approved by DPAs in the relevant Member States.

The GDPR also encourages controllers to implement the principles of data protection by design and by default, where feasible. In essence, this means that controllers should design products with privacy in mind, rather than tacking it on as an afterthought, and that privacy-protective settings should be the default in any product.

Selecting processors

Controllers are liable for the actions of the processors they select and responsible for compliance with the GDPR's personal data processing principles; however, if a processor acts as a controller or outside the scope of authority granted by a controller, then the Regulation treats the processor as a controller for the relevant processing and it becomes subject to the provisions regarding controllers.

When selecting a processor, controllers must only use processors that provide sufficient guarantees of their abilities to implement the technical and organizational measures necessary to meet the requirements of the GDPR. For example, if a controller uses binding corporate rules or standard contractual clauses as an appropriate safeguard for cross-border data transfers, controllers should bind processors they select to those rules or terms.

The controller should also consider carrying out a data protection impact assessment prior to selecting a processor. The Recitals suggest that such an assessment is prudent in all cases, but is particularly vital when the parties are handling sensitive personal data. The controller ignores at its peril, signs that using a particular processor may involve high risk to personal data. The best approach if the controller wishes to proceed with that processor, is to consult the relevant DPA first.

Once a processor is selected, the relationship between controller and processor should be governed by a contract or other legal act under Union or Member State law. The contract should contain provisions regarding the tasks and responsibilities of the processor. These provisions include how and when data will be returned or deleted after processing and the details of the processing, such as subject matter, duration, nature, purpose, type of data, and categories of data subjects. The controller and processor may also choose to use standard contractual clauses adopted by the Commission.

Of course, contracts mostly dictate what is supposed to happen and what happens if the contract is breached. Wise controllers will implement technology that binds the hands of their processors in ways a contract cannot.

Consequences for GDPR violations

More than any new substantive right or complex procedure, the new GDPR measure most likely to draw attention from the C-suite is the provision on penalties and fines. In a stark departure from previous privacy legislation in Europe or elsewhere, the GDPR authorizes regulators to levy remarkably steep fines, up to either 20 million euros or 4 percent of annual global turnover (revenue), whichever is higher.

GDPR authorizes regulators to levy remarkably steep fines, up to either 20 million euros or 4 percent of annual global turnover (revenue), whichever is higher.

Specifically, the GDPR empowers supervisory authorities to assess fines that are "effective, proportionate and dissuasive." It sets forth both mitigating and aggravating factors to help DPAs assess the amount of a fine. For example, intentional violations are worse than merely negligent ones. Mitigating factors include adherence to a code of conduct or certification mechanisms, minimizing the use of sensitive categories of data, and employing appropriate technical and organizational safeguards. In the event of non-compliance, moreover, controllers or processors may limit the amount of a fine by mitigating the damaging nature, gravity, and duration of the violation, reporting the violation as soon as possible, and/or cooperating with the supervisory authority.

In guidance documents, the Article 29 Working Party identified four factors for determining the severity of fines and enforcement actions in general:

- **The number of data subjects involved.** As a rule of thumb, the more people affected, the bigger the fine, especially if the number is larger because of repeatedly doing the same thing, rather than a single isolated incident.
- **The purpose of the processing.** DPAs will examine closely how the organization has addressed the purpose limitation principle, in regard to both purpose specification and compatible use.
- **The damage suffered by data subjects.** While DPAs are not competent to award compensation to the data subjects themselves, they are encouraged to consider the damage suffered, or likely to be suffered, as suggested by examples of the "risks to rights and freedoms" in Recital 75.
- **The duration of the infringement.** A long time isn't bad, per se, but may be indicative of willful conduct, failure to take appropriate preventative measures, or an inability to put in place required technical safeguards.

Two "tiers"

The GDPR creates two tiers of maximum fines depending on whether the controller or processor committed any previous violations and the nature of the violation. The higher fine threshold is 4 percent of an undertaking's worldwide annual turnover or 20 million euros, whichever is higher. The lower fine threshold fine is two percent of an undertaking's worldwide annual turnover or 10 million euros, whichever is higher.

These amounts are the maximum, meaning supervisory authorities are empowered to assess lower but not higher fines. Specifically, Recital 148 authorizes a DPA to issue a reprimand in place of a fine in cases of a minor infringement where the fine would constitute a disproportionate burden on a natural person. Additionally, fines are not compounded for multiple violations arising from the same incident; the total fine cannot exceed the fine for the gravest violation.

When fines are imposed on a natural person, as opposed to a corporate controller or processor, their general income level and personal economic situation will inform the appropriate amount of fine.

Higher fine threshold

Fines in the higher threshold are assessed for more serious violations by controllers and processors, such as the violation of a data subject's rights. Specifically, higher fines are assessed for violating:

- Basic principles for processing data, including consent (Articles 5-7, 9).
- Data subjects' rights (Articles 12-22).
- Data transfer provisions (Articles 44-49).
- Obligations to Member State laws including the right to freedom of expression and information, collection and use of national identification numbers, employment processing, secrecy obligations, and data protection rules for churches and religious associations (Chapter IX).
- Non-compliance with an order or a temporary or definitive limitation on processing or suspension of data flows by a supervisory authority (Articles 58(1), 58(2)).

Lower fine threshold

Fines in the lower tier are assessed on controllers, processors, certification bodies, or monitoring bodies. Violations of most other provisions are subject to the lower fine tiers or penalties. There are some notable obligations that are specifically subject to the lower fines, including:

- Obtaining a child's consent according to the applicable conditions in relation to information society services (Article 8).
- Notifying the supervisory authority of a personal data breach (Article 33).
- Notifying the data subject of a personal data breach (Article 34).
- Designating a data protection officer (and the data protection officer has related obligations to their position) (Articles 37-39).

There are also obligations of certification bodies (Articles 42, 43), and obligations of monitoring bodies (for monitoring of approved codes of conduct) to take appropriate action to enforce code violations (Article 41(4)).

Lead regard supervisory authorities

The GDPR attempts to harmonize administrative proceedings across multiple Member States. Each must appoint their own competent DPAs under Article 55. To avoid multiple parallel administrative proceedings, and to ensure decisions are enforceable, it sets out in Article 51a that each controller or processor will be subject primarily to the authority of a single lead supervisory authority. This authority is the DPA of the Member State where the controller or processor has its main establishment.

Data subjects may file complaints with the DPA of the Member State in which they reside, where they work, or where the alleged infringement occurred. A DPA also may pursue infringement actions on its own accord when there has been an infringement in its Member State or which affects the residents of that State. If the controller or processor subject to the complaint has its main establishment in a Member State other than where the complaint is filed or launched, the original DPA must notify the lead DPA. If the lead DPA declines to take the case, the original supervisory authority is allowed to keep it, subject to the procedures in Articles 61 and 62.

Damages and compensation for data subjects

Similar to the Directive, the GDPR allows data subjects to seek monetary damages in court from controllers who violate their rights and from processors as well if the processors are liable for a data breach, violate the processor-specific provisions of the GDPR, or act outside a controller's lawful instruction.

Under Article 79, data subjects may bring an action for damages or compensation before the courts of the Member State where they reside. They also may bring the action in any Member State where the controller or processor has an establishment. The GDPR encourages courts to stay proceedings in favor of the first-filed case when a controller or processor faces lawsuits in many jurisdictions for the same incident.

Data subjects may ask non-profit public interest organizations to bring an action on their behalf, and such organizations may bring an action independently where permitted by Member State law. Because data subjects have a right to an effective judicial remedy, moreover, the GDPR empowers a data subject to bring an action against supervisory authorities in the courts of their Member State when they do not deal with a complaint or timely inform a data subject of the complaint's progress or outcome.

CONCLUSION

The impetus for data protection

The GDPR empowers data subjects with many new rights and further to seek judicial relief for damages and file administrative complaints with supervisory authorities should those rights be violated. Any organization collecting or processing personal data must specifically provide for its security before the fact and regularly test that these provisions have not become weakened or compromised.

The GDPR's guidance on imposing fines replaces the patchwork enforcement structure of the Directive, while establishing accountability and consistency mechanisms also lacking under the Directive. A new-found consistency in the way that data protection law is implemented throughout the EU will likely soon emerge, even if there are some variations from Member State to Member State.

The hefty fines and penalties for infringement not only encourage accountability, they may be the single most impactful feature of the Regulation, causing multinationals and local companies to invest more in compliance. These penalties have certainly increased interest in data protection. The loss of pseudonymized and/or encrypted personal data can save controllers and processors from many GDPR perils.

The GDPR's consistency mechanisms – encouraging supervisory authorities to cooperate and agree on infringement decisions, empowering the Board for dispute resolution, making final decisions binding – will hopefully ease burdens on controllers and processors doing business across Member State states by offering more efficient enforcement solutions. Of course, most controllers and processers hope never to encounter the enforcement process at all.

The International Association of Privacy Professionals (IAPP) is a resource for professionals who want to develop and advance their careers by helping their organizations successfully manage these risks and protect their data. In fact, we're the world's largest and most comprehensive global information privacy community.

The IAPP is the only place that brings together the people, tools and global information management practices you need to thrive in today's rapidly evolving information economy.