The remedies matrix: a framework for assessing remedies

European Union General Data Protection Regulation

What are the highest-level policy goals of the regime?

There are three main policy goals of the European Union's General Data Protection Regulation (GDPR):

1. Ensure the protection of the fundamental privacy rights of data subjects, such as the security and confidentiality of personal data, the guarantee of notice, choice, right of access, rectification and erasure, and more.
2. To update privacy laws to reflect the latest technology.
3. To unify the 28 disparate privacy laws of the European Union's member states.

GDPR makes it easy for EU citizens to see how their data is being used and raise complaints if necessary. Its supranational nature allows citizens to defend their rights even if the violation does not "originate" from the country in which they reside.

Deterrence: How does the regime seek to deter bad behavior? Options may include direct punishment (fines), redress of harms (compensation), denial of benefits (disgorgement of profits or other benefits), and cost imposition (e.g., a tax or fee).

Direct punishment, such as fines paid to the government

GDPR fines are applied **in addition to, or instead of,** further remedies or corrective powers, such as injunctions, instructions to adjust data processing, and/or a temporary or definitive limitation on an entity's data processing rights. Data processors may be subject to these sanctions by themselves, or alongside data controllers, or both.

GDPR fines are determined with the help of a statutory catalog with clearly defined criteria. Intentional infringement, failure to mitigate, or lack of collaboration with authorities may increase the penalty.

Especially severe violations, defined in Article 83(5), may warrant fines of up to 20 million euros or, in the case of an undertaking, up to 4% of the annual global turnover the preceding fiscal year, whichever is higher. An "undertaking" is defined by the Treaty of the Functioning of the European Union (TFEU), which states that "the concept of an undertaking encompasses every entity engaged in an economic activity, regardless of the legal status of the entity or in the way in which it is financed." Undertakings can therefore be comprised of several corporate entities. In other words, even if only one business unit of a large corporate group commits a GDPR violation, the "percentage of annual turnover" may be assessed on the large corporate group's turnover. For less severe violations, defined in Article 83(4), there is a fine cap of 10 million euros or, in the case of an undertaking, up to 2% of the annual global turnover the preceding fiscal year, whichever is higher.

Redress remedies to individuals (which may include restitution or other money damages)

· According to Article 82(1), an EU person "who has suffered material or non-material damage as a result of an infringement this Regulation [GDPR] shall have the right to receive compensation from the controller or the processor for the damage suffered." Court proceedings for exercising this right "shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)." Article 79(2) states that "proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment," or "where the data subject has his or her habitual residence." This second option of filing a formal complaint in the Member State of habitual residence is unavailable when the data controller or processor is a public authority of an EU Member State exercising its public powers.

Denial of benefits (such as disgorgement of profits or data deletion)

There does not appear to be a 'disgorgement of profits' mechanism in GDPR. The fines stated above are the sole monetary penalties.

Under Article 17, data subjects have the 'right to erasure.' Individuals may demand for their data to be erased if the data in question is no longer necessary to the purposes for which they were collected or processed, if the data subject withdraws consent on which the data processing is based and there are no other legal grounds for processing, if the data subject objects to the processing, and if local Member State laws require for that data to be deleted. Article 17(1)(d) does specifically state that "unlawfully processed" personal data must be erased as well.

Cost imposition (including taxes or fees)

There is no systematic or intentional cost imposition under GDPR.

Does the regime include a mechanism to hold the bad actors' assets at risk?

In the past, several companies have refused to turn over employee data to European investigators, claiming that the GDPR makes it illegal to disclose such personal data to government informational requests. In November 2018, the European Data Protection Supervisor, an independent supranational body that oversees European institutions' data privacy practices, stated that if a company has an obligation to provide personal data to European institutions, then Article 6(1)(c) permits them to do so. This personal data transfer is also lawful if the company voluntarily hands over personal data to assist an ongoing investigation on "legitimate interest" grounds.

It does not appear that GDPR regulators may "seize" the assets of potential violators to prevent further wrongdoing.

Does the regime contemplate the problem of over-deterrence?

Not formally. There have been informal concerns, but nothing in GDPR itself.

Is there a market for noncompliance?

It does not appear so.

Are attorney fees available to successful plaintiffs?

No. While European Data Protection Authorities (each Member State has a DPA) are the only entities with the authority to assess GDPR penalties and fines, they cannot award compensation. When data subjects exercise their right to compensation under GDPR, they do not necessarily have to make a court claim. An organization may simply agree to pay. However, if the

organization refuses, then the complainant may file a court claim, and if the court agrees with the complaint, then it will decide whether the organization shall pay compensation.

How does the regime seek to compel good behavior (carrots or sticks)?

Preapprovals (permits, licenses)

A recently added "feature" of GDPR is the *GDPR Certification.* Entities may now receive certification from approved GDPR certification bodies to demonstrate their compliance with GDPR.

Injunctive relief

GDPR itself does not preclude the possibility of injunctive relief, but whether it is possible can depend on local Member State rules and regulations.

Safe harbors

Yes. Article 83(2) states that fines and penalties are to be determined with the violator's degree of cooperation with the supervisory authority taken into account. Their adherence to approved codes of conduct as outlined in Article 40 or certification pursuant of Article 42 are also considered.

Role of Gatekeepers and Third Parties

Does the ecosystem for the sector/practice include gatekeepers (e.g., third party service providers) who regulate conduct?

If a company's core activities involves processing sensitive personal data at scale or process data with far-reaching consequences for data subjects, then the company is required to appoint a Data Protection Officer (DPO), regardless of its size. Public bodies must always appoint a DPO. An undertaking, such as a group of corporate entities house under one group, may appoint a single DPO. Even if a DPO is not required, companies may voluntarily appoint one to handle data compliance work.

Companies have two options to meet their DPO obligations. They may either name an internal employee or hire an external person. Conflicts of interest must be resolved. DPOs are responsible for ensuring the company's compliance with data protection laws, employee awareness raising, and collaborating with supervisory authorities. DPOs are not to be penalized or dismissed for conducting their tasks. Companies are ultimately responsible for compliance with data protection laws.

How does the regime address third parties who are involved in the underlying unwanted behavior?

Under GDPR, when data processing is outsourced, the outsourcer becomes a "data controller," and the entity to which the data is outsourced becomes a "data processor." The responsibility of determining what data is processed and the lawful basis for doing so lies with the data controller. Data controllers and data processors are responsible for their own compliance with GDPR. Contracts are required to be clearly written so that the data processor will only act on the instructions provided by the data controller, will not outsource data processing further, and will delete all data provided by the data controller by the end of the contract.

Other Issues

How does the regime address the problem of guile?

One of GDPR's strategic goals is to "deter opportunism and guile," according to Professor Chris Hoofnagle. It accomplishes this by making data processing illegal unless justified. GDPR's "legitimate interests" legal ground for processing is counterbalanced by the "fundamental rights and freedoms of the data subject," so data subjects may object if their wish. GDPR also deters consent by using many requirements to meet the condition of "consent," with the burden being on the data controller to prove the consent's validity.

How does the regime address collective wrongs (small injuries to many people)?

Class actions. In the fall of 2020, two of the world's largest data brokers, Oracle and Salesforce, were served with GDPR class action lawsuits. The claimants in that case argue that Oracle and Salesforce engaged in mass surveillance of internet users to conduct its real-time bidding ad auctions, which violates GDPR's requirement of consent.

How does the regime address power differentials among victims and wrongdoers?

Special oversight authority given to each EU Member State Data Protection Authority and class action lawsuits.

How does the regime respond to technological change?

The European Union's executive branch, the European Commission, is responsible for amending and updating GDPR as time passes. For example, in 2021, the European Commission introduced a broader definition of a joint controller, removed the EU-US Privacy Shield, addressed cookie walls, and updated standard contractual clauses.

Regulatory Structures

Is the regime complemented by an agency and what are that agency's powers?

Yes. The GDPR established the European Data Protection Board (EDPB) as its enforcement agency. The powers and responsibilities of the EDPB are laid out in Article 70 of the Regulation, such as issuing guidelines, updating regulations, communicating with the European Commission, and ensuring the consistency of GDPR's application across member states.

Member States themselves have some room to adapt GDPR to their local environment. Each of the 28 EU Member States have a supervisory authority, known as a Data Protection Authority (DPA). DPAs monitor local GDPR compliance, receive and investigate complaints, and cooperate with other GDPR agencies.

Monitoring or investigation?

Both.

Overall Assessment of Efficacy

Does the regime achieve desired policy outcomes?

As the largest legislation of its kind in the world, it has led the charge on data protection. The large amount of GDPR complaints raised to supervisory authorities demonstrate that these issues

are top-of-mind for EU citizens. According to DLA Piper, between January 2020 and January 2021, GDPR fines rose by nearly 40%, indicating a clear adjustment to sufficiently deter GDPR violations. Numerous large companies, such as Google, H&M, Telecom Italia, British Airways, and Marriott have been served with multimillion dollar fines, though many argue that these fines are a mere “slap on the wrist” for companies of their size. Most notable is the $888 million fine Amazon received on July 16, 2021, for processing personal data in violation of GDPR. Companies, to avoid these fines, have spent millions to be GDPR-compliant, so it is likely that there has been a material increase in privacy and data protections for data subjects. Given the newness of this regulation, it may take a few more years to realize its potential, or show that it sufficiently stifles innovations to outweigh the privacy gains.