The Top 10 Operational Impacts of the EU's General Data Protection Regulation

www.iapp.org
IAPP - International Association of Privacy Professionals

The Top 10 Operational Impacts of the EU's General Data Protection Regulation

The new General Data Protection Regulation (GDPR) is set to replace the Data Protection Directive 95/46/EC, effective May 25, 2018. The GDPR is directly applicable in each Member State and will lead to a greater degree of data protection harmonization across EU nations.

Although many companies 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 once it comes into force.

With new obligations on such matters as data subject consent, data anonymization, breach notification, cross-border data transfers, and appointment of data protection officers, to name a few, the GDPR requires companies handling EU citizens' data to undertake major operational reform.

In this 10-part series, IAPP Research Director Rita Heimes, CIPP/US, and Westin Research Fellows Gabriel Maldoff, CIPP/US, and Anna Myers, CIPP/US, explore the major issues with which organizations will have to grapple as they bring themselves into compliance with the world's most impactful privacy law.

Table of Contents

1 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 Directive 95/46/EC, the GDPR imposes stricter obligations on data processors and controllers with regard to data security while simultaneously offering more guidance on appropriate security standards. The GDPR also adopts for the first time specific breach notification guidelines.

Security of data processing standards

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, similarly 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 pseudonymisation 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 regularly 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, respectively — may use these tools to demonstrate compliance with the GDPR's security standards.

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.

"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.

"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 leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." 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.

In the event of a personal data breach, data controllers must notify the supervisory authority "competent in accordance with Article 55," which is most likely (looking to Article 56(1)) the supervisory authority of the Member State where the controller has its main establishment or only establishment, although this is not entirely clear. 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.

> *Notice must be provided "without undue delay and, where feasible, not later than 72 hours after having become aware of it."*

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 to the rights and freedoms of natural persons," a phrase that will no doubt offer data protection officers and their outside counsel opportunities to debate the necessity of notification.

A notification to the authority must "at least": (1) describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected; (2) provide the data protection officer's contact information; (3) "describe the likely consequences of the personal data breach"; and (4) describe how the controller proposes to address the breach, including any mitigation efforts. If not all information is 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.

If the controller has determined that the personal data breach "is likely to result in a high risk to the rights and freedoms of natural persons," it must also communicate information regarding the personal data breach to the affected data subjects. Under Article 34, this must be done "without undue delay."

The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances: (1) the controller has "implemented appropriate technical and organizational protection measures" that "render the personal data unintelligible to any person who is not authorized to access it, such as encryption"; (2) the controller takes actions subsequent to the personal data breach to "ensure that the high risk to the rights and freedoms of data subjects" is unlikely to materialize; or (3) when notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

Assuming the controller has notified the appropriate supervisory authority (commonly known as a "data protection authority" or DPA) of a personal data breach, its discretion to notify data subjects is limited by the DPA's ability, under Article 34(4), to require notification or conversely to determine it is unnecessary under the circumstances.

Harmonization

Data breach notification law is possibly most mature in the U.S., relative to other nations and regions. There, "reasonable" security standards are still being defined and nearly every U.S. state has a different breach notification law, which has led to some consternation among privacy professionals. The GDPR's uniform application across EU Member States should at least provide predictability and thus efficiencies to controllers and processors seeking to establish compliant data security regimes and breach notification procedures across the entirety of the 28 Member States. Nonetheless, the GDPR's reference to a "competent supervisory authority" suggests notification may need to be made to more than one supervisory authority depending on the circumstances, and the ambiguity of a number of terms such as "undue delay," "likelihood of risk to rights and freedoms," and "disproportionate effort" all remain to be further clarified and defined in practice.

2 The Mandatory DPO

A huge number of data controllers and processors alike must designate a data protection officer to comply with the GDPR. Under Article 37, data protection officers must be appointed for all public authorities, and where the core activities of the controller or the processor involve "regular and systematic monitoring of data subjects on a large scale" or where the entity conducts large — scale processing of "special categories of data" (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and the like, defined in Article 9). Although an early draft of the GDPR limited mandatory data protection officer appointment to companies with more than 250 employees, the final version has no such restriction.

Article 37 does not establish the precise credentials data protection officers must carry, but does require that they have "expert knowledge of data protection law and practices." The GDPR's recitals suggest the level of expert knowledge "should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."

The data protection officer's tasks are also delineated in Article 39 of the Regulation to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits.
- Advising with regard to data protection impact assessments when required under Article 35.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

These responsibilities mirror those of privacy professionals elsewhere around the globe and signal a growth spurt for the profession in the EU. In fact, the GDPR borrows some concepts from Germany's Federal Data Protection Act, which already requires a data protection officer to

be appointed by firms with at least nine people employed in the automated processing of personal data, or at least 20 people who are engaged in non — automated data processing. Under German law, data protection officers must be suitably qualified and are protected against dismissal except for severe breach of their duties. Many firms out-source the data protection officer responsibilities to specialized agencies or law firms. Failure to comply with Germany's compulsory data protection officer requirements can lead to significant fines.

Under the Regulation, moreover, data protection officers have many rights in addition to their responsibilities. They may insist upon company resources to fulfill their job functions and for their own ongoing training. They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line "to the highest management level" of the company. Data protection officers are expressly granted significant independence in their job functions and may perform other tasks and duties provided these do not create conflicts of interest. Job security is another perk; the GDPR expressly prevents dismissal or penalty of the data protection officer for performance of her tasks and places no limitation on the length of this tenure.

> *The GDPR expressly prevents dismissal or penalty of the data protection officer for performance of her tasks.*

A company with multiple subsidiaries (a "group of undertakings") may appoint a single data protection officer so long as she is "easily accessible from each establishment." The GDPR also allows the data protection officer functions to be performed by either an employee of the controller or processor or by a third-party service provider, creating opportunities for consulting and legal firms to offer outside DPO services.

Regardless of who fills these roles both inside and outside of the EU, there ought to be considerable competition for talented and trained DPOs. The IAPP recently released a study showing demand for at least 28,000 data protection officers by the spring of 2018.

3 Data Subject Consent

Consent remains a lawful basis to transfer personal data under the GDPR; however, the definition of consent is significantly restricted. Where Directive 95/46/EC allowed controllers to rely on implicit and "opt-out" consent in some circumstances, the GDPR requires the data subject to signal agreement by "a statement or a clear affirmative action." The new law maintains the distinct requirements for processing "special categories of personal data" that were present in the Directive, but it expands the range of what is included in those special categories. Finally, the GDPR introduces restrictions on the ability of children to consent to data processing without parental authorization. This chapter addresses each of these GDPR consent provisions in turn.

GDPR mandates affirmative consent for data processing

Under the GDPR, consent must be "freely given, specific, informed and unambiguous." There was uncertainty leading up to this final draft whether the EU would settle on "unambiguous" consent as required by the Directive, or the higher standard of "explicit" consent. The final draft has staked out a middle position, on the one hand opting for unambiguous consent, while on the other hand requiring such consent to be expressed "by a statement or by a clear affirmative action." Recital 32 clarifies that an affirmative action signaling consent may include ticking a box on a website, "choosing technical settings for information society services," or "another statement or conduct" that clearly indicates assent to the processing. "Silence, pre-ticked boxes or inactivity," however, is presumed inadequate to confer consent.

The GDPR, therefore, creates additional hurdles for consent over what was required by the Directive. As interpreted by the Article 29 Working Party's Opinion 15/2011 on the definition of consent, the Directive required the controller to provide "accurate and full information on all relevant issues," including the nature of the data that will be processed, the purposes of processing, the identity of the controller, and the identity of any other recipients of the data. Consent had to be specific to the processing operations and the controller could not request open-ended or blanket consent to cover future processing. Significantly, while consent could be satisfied by an express statement, it also could be inferred from an action or inaction in circumstances where the action or inaction clearly signified consent. Thus, the Directive left open the possibility of "opt-out" consent.

The GDPR removes that possibility by requiring the data subject to make a statement or clear affirmative action. In particular, the GDPR includes three additional requirements:

First, Article 7(3) of the GDPR gives data subjects the right to withdraw consent at any time and "it shall be as easy to withdraw consent as to give it." Controllers must inform data subjects of the right to withdraw before consent is given. Once consent is withdrawn, data subjects have the right to have their personal data erased and no longer used for processing.

Second, in Recital 43, the GDPR adds a presumption that consent is not freely given if there is "a clear imbalance between the data subject and the controller, in particular where the controller is a public authority." Importantly, a controller may not make a service conditional upon consent, unless the processing is necessary for the service.

Third, the GDPR adds that consent must be specific to each data processing operation. To meet the specificity requirement under Article 7, a request for consent to data processing must be "clearly distinguishable" from any other matters in a written document, and it must be provided "in an intelligible and easily accessible form, using clear and plain language." However, the law exempts controllers from obtaining consent for subsequent processing operations if the operations are "compatible." Recital 50 states that compatibility is determined by looking at factors including the link between the processing purposes, the reasonable expectations of the data subject, the nature and consequences of further processing, and the existence of appropriate safeguards for the data.

Importantly, a controller may not make a service conditional upon consent, unless the processing is necessary for the service.

Under Article 5(1)(b), additional processing for archiving in the public interest (as defined by the Member State), statistical purposes, or scientific and historical research generally will be considered compatible, and, therefore, exempt from specific consent. These exceptions are potentially quite broad. Where they apply, under Article 89 controllers will not have to erase or rectify data after the data subject has withdrawn consent. The exceptions also impact restrictions on processing, data portability and the data subject's rights to object to and to be notified of processing operations. (The broader contours of these exceptions are discussed in an article on "How GDPR changes the rules for research.")

Although the GDPR removes the possibility of "opt-out" consent by forbidding silence, inactivity, and pre-ticked boxes as a means of providing consent, Recital 32 states that the data subject may consent by "choosing technical settings for information society services." It remains to be seen how this provision will be interpreted, but the language may leave intact the provisions of the e-Privacy Directive relating to cookies and other tracking technologies. Specifically, Article 5(3) of that Directive states that, generally, a data subject must provide specific, informed consent to the use of cookies or comparable tracking technology. However, Recital 66 provides an exception where cookies are "strictly necessary for the legitimate purpose of enabling the use of a specific service requested by the subscriber or user." It also provides that "the user's consent to processing may be expressed by using the appropriate settings of a browser or other application." Under the Article 29 Working Party's interpretation of this provision, the browser settings exception applies only

if the browser's default rejects the placement of cookies, thereby requiring the user to actively opt-in to receiving cookies. This interpretation may accord with the GDPR's language requiring "a clear affirmative action."

Whenever a controller relies on consent as a basis for processing, under Article 7(1), the controller bears the burden of demonstrating that consent was obtained lawfully according to the principles above.

GDPR requires explicit consent for special categories of personal data

GDPR Article 9 requires a higher level of consent – "explicit" consent – for the processing of "special categories of personal data." These special categories relate to personal data that are "particularly sensitive in relation to fundamental rights and freedoms" and, therefore, "merit specific protection." They include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

The standard for explicit consent likely remains the same as under Directive 95/46/EC, which also required controllers to obtain explicit consent for processing special categories of personal data. Under the Directive, the Article 29 Working Party defined explicit consent as "all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing." Thus, a user's conduct or choice of browser settings probably will not be sufficient to meet this high bar. The GDPR also allows Member States to enact laws that restrict the processing of some categories of data even if the data subject explicitly consents.

The only distinction between the Directive and the GDPR on this issue is that the GDPR expands the definition of sensitive data to include genetic data, biometric data (in some cases), and data concerning sexual orientation. Genetic data is defined, under Article 4, as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question." Biometric data is personal data that identifies an individual based on the "specific technical processing" of the individual's physical or behavioral characteristics. Recital 51 notes that photographs will qualify as biometric data only when they are processed "through a specific technical means allowing the unique identification or authentication of a natural person."

GDPR requires parental consent for processing children's personal data

In Article 8, the GDPR introduces specific protections for children by limiting their ability to consent to data processing without parental authorization. Previous drafts of the Regulation set

the age of consent at 13 years old, which would have been consistent with the age of consent set by the Children's Online Privacy Protection Act (COPPA) in the U.S. However, a last-minute proposal aimed to raise the age of consent to 16 years old. After the last round of trilogue negotiations, the final draft opted for the age of consent to be set at 16 years, but it allows Member States to set a lower age not below 13 years. Thus, unless otherwise provided by Member State law, controllers must obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16. They also must make "reasonable efforts" to verify that a parent or guardian has provided the appropriate consent. Differing rules on the age of consent in EU Member States, as well as between the EU standard and the COPPA age 13 rule applicable in the U.S., could create significant challenges for companies that offer international services. It is unclear whether Member States will act together on this issue. At this time, at least one Member State, the U.K., has vowed to lower its age of consent to 13.

Other Provisions

Consent features in a variety of other sections of the Regulation. For example, under the right to erasure, in Article 17, the data subject has the right to have the controller erase her data if she withdraws consent and the processing had been based on her consent. Under Article 18, where the data subject exercises her right to restrict data processing, the controller may only continue to process the data if it obtains the data subject's consent or if processing is necessary for a legal claim. Article 20 grants the data subject the right to receive all the personal data about her in the controller's possession where the processing is based on her consent. In these circumstances, the required level of consent is "unambiguous" consent.

The GDPR requires the data subject's explicit consent in two other circumstances. Under Article 22, controllers need to obtain explicit consent to make decisions about the data subject "based solely on automated processing, including profiling," when the processing produces legal effects or "similarly significantly affects" the data subject. Controllers also must seek explicit consent, under Article 49, to authorize transfers of personal data to countries that do not provide an adequate level of protection, if no other transfer mechanism is in place.

Penalties

The GDPR provides for two different levels of administrative penalties. Some violations are subject to fines up to 10,000,000 EUR or up to two percent of global annual turnover, while for other violations, those maximums are doubled to 20,000,000 EUR or 4 percent of global turnover. Violation of the rules around consent generally subject controllers to the higher level of fines, but violations of the rules concerning age of consent are subject to the lower level of penalties.

4 Cross-border Data Transfers: Adequacy and Beyond

The GDPR permits personal data transfers outside of the EU subject to compliance with set conditions, including conditions for onward transfer. Similar to the framework set forth in the Directive, the GDPR allows for data transfers to countries whose legal regime is deemed by the European Commission to provide for an "adequate" level of personal data protection. In the absence of an adequacy decision, however, transfers are also allowed outside non-EU states under certain circumstances, such as by use of standard contractual clauses or binding corporate rules (BCRs). Derogations are also permitted under limited additional circumstances.

Important distinctions between the GDPR and the Directive bear noting, however. In particular, the GDPR explicitly acknowledges as valid the current requirements for BCRs for controllers and processors, which will be helpful for data transfers involving those Member States that do not as yet recognize BCRs. Standard contractual clauses, which prior to the GDPR required prior notice to and approval by data protection authorities, may now be used without such prior approval. Further, a newly introduced scheme in Article 42 allows for transfers based upon certifications, provided that binding and enforceable commitments are made by the controller or processor to apply the appropriate safeguards.

In addition to facilitating international data transfers through new mechanisms, the GDPR also makes clear that it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country. It also imposes hefty monetary fines for transfers in violation of the Regulation.

Transfers with an adequacy decision

Chapter V of the GDPR (Articles 44 through 49) governs cross-border transfers of personal data. Article 45 states the conditions for transfers with an adequacy decision; Article 46 sets forth the conditions for transfers by way of appropriate safeguards in the absence of an adequacy decision; Article 47 sets the conditions for transfers by way of binding corporate rules; Article 48 addresses situations in which a foreign tribunal or administrative body has ordered transfer not otherwise permitted by the GDPR; and Article 49 states the conditions for derogations for specific situations in the absence of an adequacy decision or appropriate safeguards.

These articles mirror the data controller's or processor's menu choices for GDPR-compliant personal data transfers in descending order of preference and likely in ascending order of expense. In other words, only if data is transferred to a country not deemed "adequate" does the controller or processor turn to the other options.

Under the Directive, only approved third countries were appropriate to receive personal data transfers outside the Member States. The GDPR allows transfers not only to third countries, but also to a territory or a specified sector within a third country, or to an international organization, provided they have been awarded the Commission's adequacy designation. Once the Commission confers (or retracts) an adequacy designation, the decision binds all EU Member States.

The Schrems case (C-362/14) raised the bar required for an adequacy decision to "essential equivalence." Recital 104 confirms that a Commission adequacy decision means that the third country or specified entity ensures "an adequate level of protection essentially equivalent to that ensured within the [European] Union." The Commission considers myriad factors in determining adequacy, including the specific processing activities, access to justice, international human rights norms, the general and sectoral law of the country, legislation concerning public security, defense and national security, public order, and criminal law.

Transfers to an "adequate" third country or entity may take place without further authorization by the Commission or Member States. Adequacy decisions are also subject to periodic review, at least every four years, to determine whether the third country or entity still ensures an adequate level of data protection (Article 45(3)). In the periodic review, the Commission consults with the third country of entity, considers relevant developments and information from other relevant sources such as the findings of the European Parliament or Council (Recital 106).

Transfers by way of appropriate safeguards

Similar to the Directive, the GDPR provides mechanisms for cross-border data transfers in the absence of an adequacy designation if the controller or processor utilizes certain safeguards. Under Article 46, appropriate safeguards include:

- Legally binding and enforceable instrument between public authorities or bodies.
- Binding corporate rules in accordance with Article 47.
- Standard data protection contractual clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).
- Standard data protection contractual clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2).

- An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

- An approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Standard data protection contractual clauses

Changes to the requirements for standard data protection contractual clauses reduce their administrative burden. Under the GDPR, these clauses do not require prior authorization of supervisory authorities and such clauses can be adopted by the European Commission as well as by national supervisory authorities. Existing standard contract clauses may remain valid, but the GDPR leaves open the possibility of their repeal.

Ad hoc contractual clauses may also be used for GDPR compliance, although they must receive prior supervisory authority approval and thus are potentially a less attractive option for controllers.

Codes of conduct and certification mechanisms

In Article 46, the GDPR lists two new appropriate safeguards — codes of conduct and certification mechanisms — that have general application to both controllers and processors.

Codes of conduct resemble the self-regulatory programs used elsewhere to demonstrate to regulators and consumers that a company adheres to certain information privacy standards. Under the GDPR, such codes may be prepared by associations or other bodies representing controllers or processors, and may be drawn up to address many aspects of the GDPR including international data transfers. Adherence to these codes of conduct by controllers or processors not otherwise subject to the Regulation, but involved in the transfer of personal data outside the EU, will help a regulated controller demonstrate adequate safeguards. Draft codes of conducts must be submitted to the appropriate supervisory authority for approval pursuant to Article 40. An accredited and competent body may, under Article 41, monitor compliance with a code of conduct.

Changes to the requirements for standard data protection contractual clauses reduce their administrative burden.

Data protection certification, seals, and marks may be developed, ideally at the Union level, to demonstrate a controller's or processor's adherence to certain standards. Like codes of conduct, certification is available to controllers and processors outside the EU provided they demonstrate, by contractual or other legal binding instruments, their willingness to adhere to the mandated data protection safeguards. As further described in Articles 42 and 43, the certification mechanisms, seals, and marks require further action by the European Data Protection Board, which may develop a common European Data Protection Seal and which will also be responsible for publishing information about certification registrants in a common and publicly available directory.

BCR-specific provisions

The GDPR — unlike the Directive — explicitly lists BCRs as an appropriate safeguard in Article 46 and provides detailed conditions for transfers by way of BCRs in Article 47. Those provisions specify that BCRs require approval from a supervisory authority in accordance with the consistency mechanism in Article 63 and govern what must be included in BCRs at a minimum, such as structure and contact details for the concerned group, information about the data and transfer processes, how the rules apply general data protection principles, complaint procedures, and compliance mechanisms.

BCRs are a favored mechanism in practice because of their flexibility, and their lower administrative burden once implemented. Article 4(20) and Recital 110 also allow a corporate group or group of enterprises engaged in joint economic activity to use the same BCR structure for international data transfers.

Derogations for specific situations

Article 49 sets out the derogations or exceptions from the GDPR prohibition on transferring personal data outside the EU without adequate protections. The derogations generally parallel those in the Directive along with a new derogation for acceptable transfers for the "compelling legitimate interests" of the controller. The derogations apply when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.

- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.

- The transfer is necessary for important reasons of public interest.

- The transfer is necessary for the establishment, exercise or defence of legal claims.

- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

- The transfer is made from a register that, according to EU or Member State law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

A final derogation allows for the greatest flexibility but also, like the GDPR regime generally, requires careful and consistent internal documentation. It provides that where a transfer could not be based on standard contractual clauses, BCRs, or any of the other derogations, a transfer to a third country or an international organization may take place only if the transfer is "not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data."

Such language is subject to broad interpretation by the data controller and regulators alike, suggesting data protection officers and supervisory authorities should work together to develop examples that will guide controllers in their documentation and decision-making.

From unambiguous to explicit consent

In these derogations above, the GDPR shifted from the Directive's "unambiguous consent" to a higher standard of "explicit consent." Unambiguous consent allows the data subject to express her wishes either by a statement or by a clear affirmative action (Article 4(11)). The standard for explicit consent, which likely carries over the definition applied under the Directive, requires a data subject to "respond actively to the question, orally or in writing" as defined the Article 29 working party.

Notice

Pursuant to Article 13, controllers must provide certain information to data subjects when their information is obtained. This explicitly includes (a) that the controller intends to transfer personal data to a third country or international organization; and (b) that such transfer is pursuant to an adequacy decision by the Commission; or (c) reference to the appropriate or suitable safeguards and the means for the data subject to obtain them. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and as otherwise required by Article 12.

Monetary Fines

Perhaps one of the most significant implications of the GDPR is that, unlike under the Directive, failure to comply with the GDPR's international data transfer provisions may result in hefty fines.

Violations of the data transfer provisions in Articles 44-49 are subject to the steeper of the two administrative fine provisions in the GDPR. Such violations may result in "administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher." Under Article 83(2), the factors considered for imposing this fine include the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct, and any other aggravating or mitigating factor.

Editor's Note: This piece was informed in part by a training created by Wilson Sonsini Partner and Brussels Privacy Hub Co-Chair Chrtistopher Kuner for the IAPP's GDPR Comprehensive program held in Brussels, in February 2016.

5 Profiling and the Right to Object

Since the Directive was implemented nearly 20 years ago, technologies have proliferated that allow data controllers to gather personal data and analyze it for a variety of purposes, including drawing conclusions about data subjects and potentially taking action in response to those conclusions such as target marketing, price differentiation, and the like. Although the concepts of "profiling" or "target marketing" appear in the Directive, the precise terms do not. In its sweeping efforts to define and enhance data subjects' rights to control their personal data, the GDPR contains many restrictions on automated data processing – and decisions based upon such processing – to the extent they can be characterized as profiling.

Definition of profiling

A hotly contested provision of the GDPR, the "profiling" restrictions ultimately adopted were narrower than initially proposed.

Under Article 4(4), data processing may be characterized as "profiling" when it involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Specific examples include analyzing or predicting "aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

This definition implicitly excludes data processing that is not "automated."

Further elaboration of this definition may be found in Recital 24, where the GDPR establishes its jurisdiction over non-EU controllers provided they are monitoring "the behaviour of [EU] data subjects as far as their behaviour takes places within the Union." Processing activity involves data subject "monitoring" when "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes." This definition suggests that profiling is not equivalent to tracking, but instead is something more, involving the intention to take decisions regarding a data subject or predict the subject's behaviors and preferences.

That "profiling" requires some sort of an outcome or action resulting from the data processing is underscored by the data subject's rights to be informed of the "consequences" of profiling decisions as discussed in Recitals 60 and 63. Articles 13 and 15, which address information to be provided a data subject upon personal data collection and upon the data subject's request, both require disclosure of "the existence of automated decision-making, including profiling" along with "the significance and the envisaged consequences of such processing for the data subject."

Recital 70 clarifies that data subjects may object to processing for direct marketing as well as to "profiling to the extent that it is related to … direct marketing," further underscoring that profiling is not direct marketing per se but instead is something more.

Finally, Recital 91 describes the obligation to conduct a data impact assessment and characterizes the "profiling of data" as follows: "A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data."

Accordingly, taking all of the definitions and discussions of "profiling" together, they seem to consistently require not simply the gathering of personal data involving personal aspects of natural persons, but the automated processing of such data for the purpose of making decisions about the data subjects.

Controllers must honor data subjects' rights regarding profiling

Data subjects are entitled under the GDPR to a number of rights with regard to profiling, some of which – like notice and access – require procedures similar to non-profiling data processing, but others of which – like the right to object, halt the profiling, and avoid profiling-based decisions – will require special attention and processes for compliance.

Restrictions on profiling-based decisions producing legal effects

Pursuant to Article 22(1) of the GDPR, data subjects have a right not necessarily to avoid profiling itself (e.g. automated processing of personal data for the purpose of making a decision), but rather to avoid being "subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Recital 71 provides as examples the "automatic refusal of an on-line credit application or e-recruiting practices without any human intervention."

> *Data subjects are entitled under the GDPR to a number of rights with regard to profiling, some of which will require special attention and processes for compliance.*

Article 22(2) clarifies that the decision may nonetheless be made provided it is (a) necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) based on the data subject's explicit consent. Suitable safeguards may include anonymization or pseudonymization as components of profiling-based activities.

In the case of a decision made pursuant to a contract with the data subject or his explicit consent, the controller must still allow the data subject to contest the decision under Article 22(3).

When data is transferred pursuant to binding corporate rules, such BCRs must specify "the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22."

Article 22(4) provides that profiling-based decisions shall not be based on special categories of personal data (e.g. racial, ethnic, or religious information) unless (a) the data subject has given explicit consent to the processing of the personal data for one or more specified purposes, except where prohibited by Union law or Member State law; or (b) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. Even in these circumstances, described more fully in Article 9(2)(a) and (g), the controller must still ensure "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place." Presumably the European Data Protection Board will provide additional guidance on the circumstances under which profiling-based decisions are permissible for special categories of personal data.

For all permissible profiling, Recital 71 compels a controller to use appropriate mathematical or statistical procedures, implement technical and organisational measures to correct personal data inaccuracies and avoid errors, secure all personal data, and minimize the risk of "discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status, or sexual orientation."

Notice and access

In the case of profiling decisions subject to Article 22, Article 13 provides that the controller must inform a data subject at the time data is collected not only of the fact that profiling will occur, but as well "the logic involved" and "the envisaged consequences of such processing." Under Article 15, a data subject may also inquire of a controller and receive confirmation of any such processing, including profiling and its consequences, at any time.

Processing must cease upon data subject's objection

Even when profiling is otherwise lawful, a data subject has the right to object at any time. Pursuant to Article 21, upon the data subject's objection to profiling that is otherwise authorized under Article 6, the processing must cease unless the controller demonstrates "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject."

When processing is for direct marketing purposes, including profiling, the data subject similarly has a right to object but in this case processing must cease and the controller is not authorized to continue under any circumstances.

Data impact assessments for controllers engaged in profiling

One of the triggers requiring a data impact assessment is when a controller engages in "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person." Parsing this language (in Article 35(3)(a)) once again demonstrates that "profiling" involves more than merely automated processing, and that profiling may or may not involve decisions that produce legal effects or significantly affect an individual, but, when it does, the data subject is entitled to many additional rights and remedies.

Controllers will undoubtedly be seeking additional guidance from the European Data Protection Board to determine what automated data processing activities fall within the definition of profiling, and what profiling activities may fall outside the purview of Article 22. Data subjects, on the other hand, will benefit from a broader interpretation of profiling activities in order to be able to avoid profiling-based decisions – even those to which they have given prior explicit consent.

6 The New Rights To Be Forgotten and to Data Portability

As part of its effort to expand individual control over the use of personal data, the GDPR introduces two new rights. First, the Regulation codifies a right to be forgotten, following on the recognition of a similar right in a 2014 case before European Court of Justice. 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 with the request. 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 GDPR also augments the existing rights of data subjects to receive notice about processing activities, gain access to the information that is being processed, and to have the controller rectify inaccuracies. The data subject's right to object to processing is broader than under the Directive, moreover, allowing her to object to processing at any time, unless the controller has compelling legitimate grounds.

To keep up with the augmented rights under the Regulation, data controllers will have to 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 Directive 95/46/EC, the GDPR recognizes a "right to erasure." This right builds on and expands the so-called "right to be forgotten" recognized by the European Court of Justice in its Google Spain v. AEPD and Mario Costeja González ruling in 2014. There, the Court required search engines, upon a person's request, to remove links to webpages that appear when searching that person's name unless "the preponderant interest of the general public" in having access to the information justifies the search engine's refusal to comply with the request.

> *The GDPR for the first time codifies the right to be forgotten and applies it to all controllers.*

The GDPR for the first time codifies the right and applies it to all controllers. Under Article 17, 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 that are 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.

Article 18 establishes a procedure for when there is disagreement over whether the right to erasure applies. The data subject is entitled to seek the "restriction of processing" for the time needed to verify whether information is accurate if she contests its accuracy. The data subject also may request a restriction where the controller no longer needs the data, but the data subject needs it for a legal claim. Finally, he may request a restriction where he has objected to processing but the controller seeks to prove it has compelling legitimate grounds for overriding the objection.

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.

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.

Enhanced rights to notice, access, rectification 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 GDPR 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 disclose how long the data will be stored. Controllers also must inform data subjects of the right to withdraw consent at any time, the right to request access, rectification or restriction of processing, and 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. Thus, policies aimed at children will have to be drafted in a way that children can understand. For controllers that receive the data from a source other than the data subject – from another controller or a public record, for instance – disclosure is not necessary if it would require a "disproportionate effort."

Controllers must inform data subjects of the right to withdraw consent at any time, the right to request access, rectification or restriction of processing, and the right to lodge a complaint with a supervisory authority.

Article 15 establishes a right of access that is more robust than what was required by the Directive. Users will have a right to request a copy of their personal data undergoing processing. They may also request to know the purposes of processing, the period of time for which data will be stored, the identity of any recipients of the data, the logic of automatic data processing, and the consequences of any profiling. Controllers will have to set up processes for responding to 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. In cases where the controller processes "a large quantity of information" about the data subject, it may require the data subject to specify the information or processing activities at issue in the request.

The right to object to processing is significantly expanded under Article 21. Whereas under the Directive, a data subject could only object to processing where she could demonstrate compelling legitimate grounds, the GDPR flips the burden, allowing a data subject to object any time processing is based on public interest (Article 6(1)(e)) or the legitimate interests of the controller (Article 6(1)(f)), unless the controller demonstrates compelling legitimate grounds. This is in addition to the data subject's right to withdraw consent whenever processing is based on consent. Like the Directive, the GDPR also allows a data subject to object to processing for direct marketing at any time and Article 16 grants the right to correct inaccurate information.

Businesses will need to implement effective user interfaces

In the process of heightening user control over data, these expanded rights will create 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 likely will include 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 a difficult challenge 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. Recital 57 lends little in the way of clarity: Controllers are not required to take additional information in order to identify the data subject, but they also should not refuse to take such information if the data subject offers it in the exercise of his rights.

Controllers will have to 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 data protection officers with responsibility for overseeing these systems.

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

7 Clarifying Duties and Responsibilities of Controllers and Processors

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.

Under the Directive, data processors had duties of confidentiality and security. The Directive allowed them to act only with instructions from the controller, under contract, and to provide controllers with assurances of adequate technical and administrative measures to protect personal data.

The GDPR expands significantly upon the controller's responsibility for processing activities and sets out specific rules for allocating responsibility between the controller and processor.

The Regulation's more detailed requirements for controller-processor contracts may compel some data controllers to reassess their vendor agreements to achieve compliance. Processors not only have additional duties under the GDPR, moreover, they also face enhanced liability for non-compliance or for acting outside the authority granted by a controller. Nonetheless, the burden for personal data protection under the GDPR still rests primarily with controllers.

Burden on Controllers

The GDPR defines a controller in Article 4 as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." The controller, therefore, is the entity that makes decisions about processing activities, regardless of whether it actually carries out any processing operations.

Article 24 makes controllers responsible for ensuring that any processing activities are performed in compliance with the Regulation. Controllers must "implement appropriate technical and organisational 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.

While the Regulation 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 will no longer be required to register their processing activities with a DPA in each Member State. Instead, under Article 30, the GDPR imposes strict requirements on controllers to maintain their own detailed records of processing.

The GDPR allows controllers to demonstrate their compliance with the Regulation by adhering to codes of conduct and certifications that were approved by DPAs in the relevant Member States. The Regulation 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. Under the GDPR, the term "processor" means a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." In other words, while the controller is the entity that makes decisions about processing activities, the processor is any entity contracted by the controller for carrying out the processing. If a processor acts as a controller or outside the scope of authority granted by a controller, however, 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 use only 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. Unlike the Directive, which was largely silent on the matter, meeting the "sufficient guarantees" obligation can be accomplished under the GDPR through the use of an approved code of conduct or certification mechanism.

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 data protection authority 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.

Processors' additional duties and restrictions on subcontracting

Article 28 of the GDPR prescribes specific obligations of processors in addition to contract terms between controllers and processors. Processors' duties are primarily to controllers, including requirements to: (a) process data only as instructed by controllers; (b) use appropriate technical and organisational measures to comply with the GDPR; (c) delete or return data to the controller once processing is complete; and (d) submit to specific conditions for engaging other processors.

The processors' restrictions on subcontracting bear special attention. Under the GDPR, processors are prohibited from enlisting another processor without prior specific or general written permission of the controller. In either case, controllers retain the right to object to the addition or replacement of processors. Thus, if a processor enlists a subprocessor based on the controller's general consent, Article 28(4) requires the processor to inform the controller so that it may have the opportunity to object. Sub-processors also are subject to the same requirements under the GDPR and they too are bound by any contracts with the controller.

While the controller is responsible for maintaining records of processing activities, processors are responsible for maintaining records of all categories of personal data processing carried out on behalf of the controller. These records should contain contact information for the processor(s) and the controller(s), the categories of processing carried out for each controller, information on cross-border transfers if applicable, and a general description of the implemented technical and organizational security measures.

Joint controllers

Article 26 provides specific provisions for when "two or more controllers jointly determine the purposes and means of processing." Joint controllers are required to create an agreement determining their respective duties to comply with the Regulation. The agreement must be available to data subjects and may designate one point of contact amongst them for data subjects. Regardless of the allocation of responsibility set out in the contract, data subjects are entitled to enforce their rights against either controller. Therefore, each joint controller is individually liable for compliance with the Regulation.

Data breach responsibilities

In the event of a personal data breach, processors are required under Article 33 to notify the controller without "undue delay" if it happens on the processor's watch. The burden falls on the controller, then, to notify the supervisory authority within 72 hours of becoming aware of the breach. If notification is not made within 72 hours, controllers are required to provide a reasoned justification for the delay. Controllers are also responsible for documenting personal data breaches, including the facts of the breach, its effects, and remedial actions.

Liability and penalties

Controllers are liable under Article 82 for the damage caused by processing "which infringes" the GDPR. A processor, on the other hand, is liable "only where it has not complied with the obligations of [the GDPR] specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller." In other words, parties bringing claims against processors under the GDPR must prove an additional element apart from damage and general noncompliance, namely, that the processors have violated one of their specific legal duties or contractual obligations.

> *Parties bringing claims against processors must prove an additional element apart from damage and general noncompliance.*

When non-compliance is established, the burden shifts to controllers and processors to prove they are not responsible for the damage in any way.

When the controller and processor are joined in the same judicial proceedings, liability for damages may be apportioned among them according to their respective responsibility for the harm, as long as the data subject(s) receive full compensation. Additionally, controllers or processors who have paid the entire compensation may institute proceedings against other controllers or processors involved in the same processing to claim back the portion(s) for which they are not responsible.

8 'Pseudonymization' of Personal Data

The concept of personally identifying information lies at the core of the GDPR. Any "personal data," which is defined as "information relating to an identified or identifiable natural person ('data subject')," falls within the scope of the Regulation. The Regulation does not apply, however, to data that "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital 26).

The GDPR introduces a new concept in European data protection law – "pseudonymization" – for a process rendering data neither anonymous nor directly identifying. Pseudonymization is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. Pseudonymization, therefore, may significantly reduce the risks associated with data processing, while also maintaining the data's utility. For this reason, the GDPR creates incentives for controllers to pseudonymize the data that they collect. Although pseudonymous data is not exempt from the Regulation altogether, the GDPR relaxes several requirements on controllers that use the technique.

What is pseudonymous data?

The GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymize a data set, the "additional information" must be "kept separately and … subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable person." In sum, it is a privacy-enhancing technique where directly identifying data is held separately and securely from processed data to ensure non-attribution.

Although Recital 28 recognizes that pseudonymization "can reduce risks to the data subjects," it is not alone a sufficient technique to exempt data from the scope of the Regulation. Indeed, Recital 26 states that "[p]ersonal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person" (i.e., personal data). Thus, pseudonymization is "not intended to preclude any other measures of data protection" (Recital 28).

GDPR creates incentives for controllers to pseudonymize data

The Regulation recognizes the ability of pseudonymization to help protect the rights of individuals while also enabling data utility. Recital 29 emphasizes the GDPR's aim "to create incentives to apply pseudonymization when processing personal data" and finds that "measures of pseudonymization should, whilst allowing general analysis, be possible". These incentives appear in five separate sections of the Regulation.

Pseudonymization may facilitate processing personal data beyond original collection purposes.

The GDPR requires controllers to collect data only for "specific, explicit and legitimate purposes." Article 5 provides an exception to the purpose limitation principle, however, where data is further processed in a way that is "compatible" with the initial purposes for collection. Whether further processing is compatible depends on several factors outlined in Article 6(4), including the link between the processing activities, the context of the collection, the nature of the data, and the possible consequences for the data subject. An additional factor to consider is "the existence of appropriate safeguards, which may include encryption or pseudonymization" (Article 6(4)(e)). Thus, the GDPR allows controllers who pseudonymize personal data more leeway to process the data for a different purpose than the one for which they were collected.

Pseudonymization is an important safeguard for processing personal data for scientific, historical and statistical purposes.

The GDPR also provides an exception to the purpose limitation principle for data processing for scientific, historical and statistical research. However, Article 89(1) requires controllers that process data for these purposes to implement "appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject." Specifically, controllers must adopt "technical and organizational measures" to adhere to the data minimization principle. The only example the Regulation provides is for controllers to use pseudonymization so that the processing "does not permit or no longer permits the identification of data subjects."

Pseudonymization is a central feature of "data protection by design."

The GDPR for the first time introduces the concept of "data protection by design" into formal legislation. At the conceptual level, data protection by design means that privacy should be a feature of the development of a product, rather than something that is tacked on later. Thus, Article 25(1) requires controllers to implement appropriate safeguards "both at the time of the determination of the means for processing and at the time of the processing itself." One way that controllers can do this is by pseudonymizing personal data.

Controllers can use pseudonymization to help meet the GDPR's data security requirements.

Under Article 32, controllers are required to implement risk-based measures for protecting data security. One such measure is the "pseudonymization and encryption of personal data" (Article 32(1)(a)). The use of pseudonymization potentially has profound implications under

this provision. Controllers are required to notify a data protection authority any time there is a security incident that presents "a risk to the rights and freedoms of natural persons" (Article 33(1)). They must, moreover, notify the concerned individuals anytime that risk is "high" (Article 34(1)). Since pseudonymization reduces the risk of harm to data subjects, controllers that use it may be able to avoid notification of security incidents.

Controllers do not need to provide data subjects with access, rectification, erasure or data portability if they can no longer identify a data subject.

Controllers may employ methods of pseudonymization that prevent it from being able to re-identify a data subject. For example, if a controller deletes the directly identifying data rather than holding it separately, it may not be capable of re-identifying the data without collecting additional information. Article 11 acknowledges this situation and provides an exemption from the rights to access, rectification, erasure and data portability outlined in Articles 15 through 20. The exemption applies only if "the controller is able to demonstrate that it is not in a position to identify the data subject" and, if possible, it provides notice of these practices to data subjects. The GDPR does not require a controller to hold additional information "for the sole purpose of complying with this Regulation." If, however, a data subject provides the controller with additional information that allows her to be identified in the data set, she must be permitted to exercise her rights under Articles 15 through 20.

The GDPR encourages controllers to adopt codes of conduct that promote pseudonymization.

The GDPR encourages controllers to adopt codes of conduct that are approved by the Member States, the supervisory authorities, the European Data Protection Board or the Commission. Among other provisions outlined in Article 40, these codes of conduct should promote the use of pseudonymization as a way to comply with the Regulation (Article 40(2)(d)). As further explored in Chapter 9, using codes of conduct allows controllers and processors to demonstrate adherence to the principles of the Regulation, and they may even be used as a mechanism for transferring personal data to third countries.

Pseudonymous data is not anonymous

Much debate surrounds the extent to which pseudonymized data can be reidentified. This issue is of critical importance because it determines whether a processing operation will be subject to the provisions of the Regulation. The GDPR adopts a more flexible approach than the traditional binary of the Data Protection Directive, focusing on the risk that data will reveal identifiable individuals.

Thus, the key distinction between pseudonymous data, which is regulated by the GDPR, and anonymous data, which is not, is whether the data can be reidentified with reasonable effort.

To illustrate the concept of reidentification risk, it is important to distinguish between direct and indirect identifiers. The International Organization for Standardization (ISO) defines direct identifiers as "data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain." They are data points that correspond directly to a person's identity, such as a name, national ID number or contact information.

Indirect identifiers are data that do not identify an individual in isolation but may reveal individual identities if combined with additional data points. For example, one frequently cited study found that 87 percent of Americans can be uniquely identified by combining three indirect identifiers: date of birth, gender and postal code. In other words, while no individual can be singled out based on just a date of birth, when combined with gender and postal code, the lens focuses on a specific identity.

> *The key distinction between pseudonymous data and anonymous data is whether the data can be reidentified with reasonable effort.*

Pseudonymization involves removing or obscuring direct identifiers and, in some cases, certain indirect identifiers that could combine to reveal a person's identity. These data points are then held in a separate database that could be linked to the de-identified database through the use of a key, such as a random identification number or some other pseudonym.

As a result of this process, pseudonymized data, unlike anonymous data, faces the risk of reidentification in two ways. First, a data breach may permit an attacker to obtain the key or otherwise link the pseudonymized data set to individual identities. Alternatively, even if the key is not revealed, a malicious actor may be able to identify individuals by combining indirect identifiers in the pseudonymous database with other available information.

The GDPR addresses the first concern in Recital 75, which instructs controllers to implement appropriate safeguards to prevent the "unauthorized reversal of pseudonymization." To mitigate the risk, controllers should have in place appropriate technical (e.g., encryption, hashing or tokenization) and organizational (e.g., agreements, policies, privacy by design) measures separating pseudonymous data from an identification key.

In Recital 26, the GDPR recognizes the second type of reidentification risk by considering whether a method of reidentification is "reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." Such an analysis is necessarily contextual and "account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

The GDPR acknowledges that re-identification must be "reasonably likely"

Under the Directive, the Article 29 Working Party found that "pseudonymization is not a method of anonymization" because some risks of re-identification remained, even if those risks were very small. Thus, even when controllers deleted all identifying information and could not themselves re-identify a data set, the Working Party found that the data was still covered by the Directive if any third party could conceivably re-identify the data sometime in the future. A controller could escape regulation only by not collecting identifying information in the first place.

In contrast, by focusing on whether re-identification is "reasonably likely," the GDPR may provide greater flexibility than the Directive. For example, where the controller deletes the identification key and the remaining indirect identifiers pose little risk of identifying an individual, the controller may be able to argue that there is no reasonable risk of re-identification. Recital 57 addresses this situation in relation to the data subject's right to access personal data held by the controller. In cases where "the personal data processed by the controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purposes of complying with any provision of this Regulation."

9 Codes of Conduct and Certifications

Confirming each data controller's or processor's compliance with the GDPR's many protections for data subjects would exceed the capacity of any regulator. The GDPR therefore endorses the use of codes of conduct and certifications to provide guidance on the GDPR's requirements, signal to data subjects and regulators that an organization is in compliance with the Regulation, and offer third-party oversight as another check on controllers' and processors' data handling practices.

These tools are likely to feature prominently in company plans for legitimate cross-border data transfers. Should they prove effective, moreover, they may underlie global data transfer mechanisms — consistent with systems already used in the U.S. and under the Asia Pacific Economic Cooperative — and lower costs of privacy compliance worldwide.

Codes of conduct and certifications may both be used to demonstrate compliance, but there are subtle differences between them and how the GDPR envisions their deployment. Although codes of conduct were featured in the Directive, they played only a minor role compared to their prominence in the Regulation. Certifications, moreover, are familiar to EU privacy and security regimes, but make their debut in the GDPR as a formal component of data protection regulation.

By officially recognizing these tools, the EU adopts a legal construct more familiar to U.S. privacy law, namely the notion that through regulatory enforcement mechanisms, companies may be held to keep binding promises made to non-governmental third parties. Still, the GDPR maintains a heavy dose of regulatory oversight and guidance into these third-party-managed programs, creating essentially a hybrid co-regulatory public/private system to develop a meaningful, binding and enforceable data protection regime that empowers data subjects, third-party administrators, and regulators alike. Surrounded by these systems, data controllers and processors face opportunities to demonstrate GDPR compliance — as well as potential pitfalls.

Codes of Conduct

What are codes of conduct under the GDPR?

Articles 40 and 41 are the primary sources of authority for establishing approved codes of conduct to serve as compliance-signaling tools for controllers and processors.

Preliminarily, the Regulation directs data protection regulators at all levels — Member States, supervisory authorities, the European Data Protection Board, and the Commission — to encourage development of codes of conduct to assist with the GDPR's "proper application." These codes may be created by the regulators themselves, but the GDPR expressly authorizes "associations or other bodies representing controllers or processors" to draw up codes of conduct or amend existing ones to implement the GDPR's particular requirements. Such codes should address, among other things:

- Fair and transparent processing.
- The legitimate interests pursued by controllers in specific contexts.
- The collection of personal data.
- The pseudonymisation of personal data.
- The information provided to the public and to data subjects.
- The exercise of the rights of data subjects.
- Information provided to and the protection of children and the manner in which the consent of the holders of parental responsibility over children is to be obtained.
- General data protection obligations of data controllers, including privacy by design and measures to ensure security of processing.
- Notification of personal data breaches to supervisory authorities and communication of such personal data breaches to data subjects.
- Transfer of personal data to third countries or international organizations.
- Out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to the processing, without prejudice to the rights of data subjects.

When private associations prepare codes of conduct or amend existing ones for the purposes of allowing members to indicate GDPR compliance, Recital 99 encourages them to "consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations." A draft code must also be submitted to the appropriate supervisory authority to determine whether it provides "sufficient appropriate safeguards" (Article 40(5)). When the draft code relates to processing activities in several Member States, the supervisory authority must, before approval, submit it to the European Data Protection Board for an opinion as to the code's compliance with the Regulation. Thereafter, the European Commission must review it.

Approved codes of conduct will receive publicity from the Commission, and be published in a register created and maintained by the Board.

Up to this point, the procedures in the GDPR are relatively consistent with those of the Directive, which also encouraged preparation and approval of codes of conduct, although the Directive empowered the Article 29 Working Party to approve EU-wide codes.

In what situations are codes of conduct useful?

The GDPR more actively than the Directive incorporates codes of conduct into its compliance and enforcement mechanisms. These codes seem particularly well suited to setting forth and then demonstrating compliance with security risks associated with data processing.

Recital 77 encourages use of approved codes of conduct by both controllers and processors. These codes may demonstrate that a controller or processor has identified any risk related to data processing; assessed the origin, nature, likelihood, and severity of the risk; and determined how best to mitigate the risk. Article 32 expressly acknowledges adherence to an approved code of conduct as one means for demonstrating compliance with the Regulation's data security obligations.

Article 24, which sets forth the controller's primary responsibilities with regard to processing personal data, also encourages codes of conduct to demonstrate GDPR compliance. Article 28 and Recital 81, moreover, expressly provide that a processor's adherence to an approved code of conduct is "an element to demonstrate compliance" with the controller's obligations. Processors eager to keep controllers as clients will therefore soon be in the market to join associations maintaining a GDPR-approved code of conduct.

Adherence to these codes can create market efficiencies. The association creating them conducts extensive reviews of any applicant seeking membership or otherwise desiring to claim compliance with the code. This saves a controller, for example, from having to conduct its own review of a potential data processor's systems. The controller can simply shop for processors who are already deemed to satisfy the code's requirements, and rely on the association to police the processor's compliance.

Cross-border data transfers

Approved codes of conduct will also facilitate cross-border data transfers. Controllers or processors that are not otherwise subject to the GDPR may demonstrate, by adhering to a code of conduct, that they provide appropriate safeguards for personal data transfers to third countries or international organizations.

Under Article 46(2)(e), appropriate safeguards for a controller or processor based outside the EU may include adhering to an approved code of conduct pursuant to Article 30 "together with" making a "binding and enforceable commitment" to comply with the GDPR and respect data subjects' rights.

The GDPR references the "binding and enforceable" nature of codes of conduct only regarding their use for cross-border transfers. The Regulation does not elaborate, but the analog to this situation is of course binding corporate rules. Controllers adopting BCRs must demonstrate their "bindingness" by creating internal compliance obligations for subsidiaries and employees, establishing third-party beneficiary rights for data subjects, accepting liability and submitting to DPA jurisdiction, and confirming sufficient assets to pay damages for a breach.

How is code of conduct compliance enforced and what are the consequences of non-compliance?

The GDPR's key breakthrough with regard to codes of conduct is the notion that they can be made binding and enforceable — rather than merely voluntary and self-regulatory.

This is somewhat analogous to how the Federal Trade Commission (FTC) has viewed third party codes of conduct in the United States, such as adherence by online advertisers to the Network Advertising Alliance (NAI) principles. The FTC, pursuant to its authority under Section 5 of the Federal Trade Commission Act, can bring a deception action against a company that self-certifies under the NAI code but fails to comply. For example, the FTC pursued Google for allegedly misrepresenting its compliance with NAI's code in the "Google Safari Hack" case. The case ultimately resulted in a $22.5 million settlement. The NAI may also refer its members to the FTC if they are in noncompliance with the NAI's codes.

The GDPR similarly requires that approved codes of conduct must enable "the mandatory monitoring of compliance with its provisions." The monitoring body must be accredited by the competent supervisory authority, after demonstrating "an appropriate level of expertise in relation to the subject-matter of the code." Accreditation is available if the body (a) demonstrates "its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority"; (b) "has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation"; (c) has "established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public"; and (d) demonstrates "to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests"(Article 41)(2).

The accredited body shall "take appropriate action" when a controller or processor "infringes" the code of conduct, including suspending or excluding the infringing party from the code. Thereafter the supervising authority must be notified of the infringement proceeding.

Enforcement by the accredited body is "without prejudice to the tasks and powers of the supervisory authority."

When the accredited body or supervisory authority enforces code of conduct infringement, the enforcer's interpretation—and not the drafter's—will prevail. Controllers and processors adhering to an association's code therefore face a risk that the association's approval doesn't guarantee regulatory compliance. NAI, for example, did not bring an enforcement action against Google for violating its standards even though the FTC did.

Membership in an association with an enforceable code of conduct may also generate a one-size-fits-all system not compatible with the GDPR's aims. For instance, the European Interactive Digital Advertising Alliance allows consumers to click on an icon used by EDAA members and manage their controls for all EDAA members at once. This may allow broader opt-in features than the GDPR approves. Then again it may conveniently suit a data subject's preferences and foster efficiency.

A supervisory authority can weigh code of conduct adherence in assessing the amount of an administrative fine. Article 83(2)(j) suggests compliance with a code of conduct is a mitigating factor, allowing for a lower penalty. Conceivably, however, non-compliance could be an aggravating one.

Pursuant to Article 83(4)(c), moreover, an accredited monitoring body faces fines up to 10,000,000 EUR for failing to "take appropriate action" when a controller or processor infringes a code of conduct.

Certifications/Seals/Marks

What are certifications under the GDPR?

Certifications are a new feature of formal EU data protection law. Unlike the Directive, the GDPR expressly recognizes certifications (as well as seals and marks) as acceptable mechanisms for demonstrating compliance.

For years, certification marks and seals have served as useful signals for consumers interested in engaging with commercial entities that adhere to certain desirable principles or follow particular manufacturing, harvesting, or sourcing practices. In the food and beverage sector, for example, certifications may indicate "fair trade" or "GMO-free."

In privacy, the EuroPriSe seal has been the principal European certification under the Directive. It aims to foster consumer trust in information-technology tools and services. Manufacturers and vendors of IT products and services undergo independent evaluation of their data privacy and security practices, following which they are eligible to display the EuroPriSe seal for two years before they must re-apply.

In the United States, TRUSTe provides one example of enterprise-level certification. TRUSTe offers compliance assessments with not only U.S. law but also the Directive, and has provided assistance with "Safe Harbor" self-certification with the U.S. Department of Commerce. It also offers APEC certification.

The GDPR provides, in Article 42, that Member States, supervisory authorities, the Board, and the Commission shall all "encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors."

Controllers and processors outside the EU engaging in international personal data transfers may also use such certifications, seals or marks to demonstrate GDPR compliance. As with codes of conduct, non-EU controllers and processors must also make "binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including as regards data subjects' rights." This is reinforced under Article 46(2)(f), which provides that compliant cross-border data transfers may involve an approved certification mechanism but must also involve binding and enforceable commitments "in the third country."

Certifications "shall be voluntary and available via a process that is transparent," and do not serve to "reduce the responsibility of the controller or the processor for compliance" with the GDPR.

Certifications may be issued by either an accredited certification body, "the competent supervisory authority" on the basis of criteria it establishes, or by the Board, which may create a "common certification — the European Data Protection Seal." It will be interesting to see whether controllers and processors favor government-sponsored certifications over private ones.

Controllers and processors outside the EU engaging in international personal data transfers may also use such certifications, seals or marks.

Accreditation is available to a certification body under Article 43 only if it: (a) demonstrates its "independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority"; (b) undertakes "to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63"; (c) establishes "procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks"; (d) establishes "procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public"; and (e) demonstrates "to the satisfaction of the competent supervisory authority that [its] tasks and duties do not result in a conflict of interests."

Accreditation is good for up to five years and may be renewed if the accrediting body maintains compliance with these standards.

Accrediting authority is granted at multiple regulatory levels. Supervisory authorities may create standards, and grant and withdraw accreditation, for certification bodies within their territories. The Board is also empowered to accredit certification bodies and maintain a register of accredited bodies.

When a certification body, supervisory authority, or Board award certification, it lasts for no more than three years at which time it may be renewed if the conditions and requirements are still met. Certification shall be withdrawn by the issuing body where the controller or processor no longer meets the requirements.

The GDPR directs the Board to "collect all certification mechanisms and data protection seals and marks in a register and … make them publicly available through any appropriate means."

In what situations are certifications useful?

Certifications assist controllers and processors in all the situations codes of conduct do, but in addition certifications — but not codes of conduct — may also be used to demonstrate compliance with Article 25, which governs data protection by design and by default.

According to Article 25(1), data controllers are obliged to implement "appropriate technical and organisational measures, such as pseudonymisation" designed to "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." Under Article 25(2), a controller "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."

Approved certification mechanisms may be used to demonstrate compliance with both of these provisions.

How is compliance with a certification enforced, and what are the consequences of non-compliance?

An accredited certification body is responsible for "proper assessment" leading to granting certification, and likewise leading to its withdrawal in the event of noncompliance. The body must inform the supervisory authority, and provide reasons, when it grants or withdraws certification from a controller or processor.

As with codes of conduct, award of certification by an accredited body is a factor to be considered in assessing an administrative fine. Article 83(2)(j) suggests certification adherence is a mitigating factor useful to limiting such fines.

Accredited certification bodies that violate their duties under the GDPR are subject to penalties up to 10,000,000 EUR.

Looking forward

The GDPR's adoption of codes of conduct and certification mechanisms is a welcome development for controllers and processors seeking efficient means for compliance. There are of course upfront administrative burdens of establishing and maintaining compliance with a code of conduct or earning certification status. But these costs are offset by the ease of finding compliant processors, for example, via screening for those adhering to a code or displaying a certification seal. The codes and certifications also may serve as marketing tools, allowing data subjects to choose controllers signaling GDPR compliance via their membership in associations or their certified status. They also will likely play a significant role in facilitating cross-border data transfers.

The GDPR's code of conduct and certification mechanisms create business opportunities for new third-party administrators to establish membership associations or become accredited certification or enforcement bodies. They also represent acknowledgment that such third-party programs can be effective means for establishing binding promises by controllers and processors that regulators can enforce, consistent with regimes familiar to those operating in the U.S. or under the APEC privacy framework. Globally consistent and familiar privacy regimes could ultimately improve the ease of legal compliance and in so doing lower compliance costs.

10 Complex Administrative Procedures and Hefty Fines

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. As noted previously, and in a stark departure from previous privacy legislation in Europe or elsewhere, the GDPR authorizes regulators to levy remarkably steep fines in amounts exceeding 20 million euros or 4 percent of annual global turnover, whichever is higher.

Circumstances giving rise to fines and factors to be considered

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 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 and processors may limit their exposure by mitigating "the damaging nature, gravity and duration of the violation," reporting the violation as soon as possible, and cooperating with the supervisory authority.

Aggravating factors generally include the opposite actions — not seeking to mitigate harm or acting contrary to the mitigating factors.

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 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 2 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.

Obligations of controllers and processors include:

- 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)).

Applicability and consistency of fines in Member States

The national laws of two of the Member States, Denmark and Estonia, do not allow for the imposition of administrative fines as set out in the GDPR. Consequently, Recital 151 provides an exception for those two Member States, allowing competent national courts to impose the fines as criminal sanctions in Denmark and through a misdemeanor procedure framework in Estonia. In those Member States, the supervisory authority refers the case to the relevant courts to initiate the fines. The national courts should, however, "take into account the recommendation by the supervisory authority initiating the fine."

In general, where the Regulation does not impose administrative fines for infringements, or for other special cases such as serious violations, Member States are required to implement a penalty system. Member States must notify the Commission of any legislation or legislative changes adopted to create penalties for violations outside administrative fines. Similar to administrative fines, penalties must be "effective, proportionate and dissuasive." Unlike fines, penalties may be criminal under the national law of a Member State.

Lead and concerned supervisory authorities

The Regulation attempts to harmonize administrative proceedings across multiple Member States, each of which must appoint their own competent supervisory authorities under Article 55. To avoid multiple parallel administrative proceedings, and to ensure decisions are enforceable, the GDPR sets out in Article 51(1) that each controller or processor will be subject primarily to the authority of a single "lead supervisory authority." The lead supervisory authority is the DPA of the Member State where the controller or processor has its "main establishment" (Article 56). If the controller or processor has offices in multiple jurisdictions, the main establishment is "the place of its central administration in the Union" (i.e., its headquarters, in most cases). For controllers or processors located in only one Member State, that State's DPA will serve as the lead.

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. The lead DPA has three weeks to decide whether to keep the case or delegate it back to the first DPA. In making its decision,

it should consider whether the controller or processor has an establishment in the Member State where the action was initiated.

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. These provisions mandate cooperation among the DPAs in pursuit of the case and set out specific rules for joint investigations and enforcement actions. If the lead DPA decides to pursue the case, Article 60 (cooperation and consistency) procedures apply. The original supervisory authority is invited to submit a draft decision to the lead, who "shall take utmost account" of the draft.

Article 60: "One-stop-shop" cooperation

Assuming an infringement proceeding involves a controller or processor with establishments in multiple Member States, the lead supervisory authority must cooperate with the other "concerned" supervisory authorities in preparing a decision, incorporating appropriate suggested changes or objections. Article 65 creates a mechanism by which the European Data Protection Board may resolve any disputes among the DPAs. Decisions of the Board and decisions jointly agreed upon by lead and concerned supervisory authorities become binding.

In any case, the lead DPA must notify the accused controller or processor of any final decision, whereas the DPA where the complaint was originally lodged must notify the complainant. The complainant retains its right to an effective judicial remedy against a legally binding decision of a supervisory authority or where the supervisory authority fails to deal with a complaint or inform a data subject about the outcome of a case within three months. Additionally, under Article 83(8), the "exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union law and Member State law, including effective judicial remedy and due process."

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. Individual causes of action are independent from and without prejudice to an action by a supervisory authority to impose administrative fines.

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.

Any non-compliant controller involved in data processing faces liability for damages under Article 82. Processors, however, face liability only when they have not complied with processor-specific regulations or with the controller's lawful instructions. Both are immune from liability if they can prove they are "not in any way responsible for the event giving rise to the damage." In other words, after a data subject demonstrates an infringement, the burden shifts to the controller or processor to prove they are not personally responsible.

Simply put, the GDPR empowers data subjects to seek judicial relief for damages and file administrative complaints with supervisory authorities.

When the controller and processor are joined in the same judicial proceedings, or when more than one controller is concerned, the data subject is entitled to receive full compensation from any one of the parties. Liability for damages subsequently may be apportioned among them according to their respective responsibility for the harm. When those controllers and processors are also involved in the same processing, each is liable for the entire harm.

Article 26 provides specific provisions for when "two or more controllers jointly determine the purposes and means of processing," termed joint controllers. Joint controllers are required to create an agreement determining their respective duties to comply with the Regulation. The agreement must be available for data subjects, who may enforce their rights against each of the controllers irrespective of the terms of the agreement. In other words, joint controllers remain jointly and severally liable to data subjects harmed by GDPR non-compliance even if they allocate liability among themselves by agreement.

Simply put, the GDPR empowers data subjects to seek judicial relief for damages and file administrative complaints with supervisory authorities. The Regulation's guidance on imposing fines replaces the patchwork enforcement structure of the Directive, while establishing accountability and consistency mechanisms also lacking under the Directive. The hefty fines and penalties for infringement not only encourage accountability, they may be the single most eye-catching feature of the Regulation, causing multinationals and local companies to invest more in compliance.