What the GDPR Requires of and Leaves to the Member States

By IAPP Westin Fellow Müge Fazlioglu, CIPP/US

The shift in the EU's legal instrument to regulate personal data processing from the Directive to the Regulation entails several significant changes in how member state law interacts with legal protections at the Union level. While the Directive required member states to implement the EU's rules and provisions into their legal systems, the General Data Protection Regulation is directly applicable law. However, in multiple areas, member states must take steps in accordance with the GDPR's provisions. The GDPR also allows member states to create derogations or designate exemptions from its rules under certain conditions. Several member states — including Austria, Germany, Slovakia, Belgium, and Ireland — have already enacted and/or published national laws that will give full effect to the GDPR.

This article is divided broadly into two sections: The first explores the legislative actions that the GDPR requires member states to take, while the second examines the optional powers and authority available to them to carve out exceptions for or to clarify the GDPR's rules. This distinction is derived from the division between what the member states "shall" and "may" do within the Articles of the GDPR. These cover such areas as the processing of sensitive data; data processing in the context of employment; conducting DPIAs; appropriate safeguards for data protection for archiving purposes in the public interest, scientific or historical research, or statistical purposes; access rights; automated decision-making and profiling; and data protection officers.

I. ACTIONS REQUIRED BY MEMBER STATES UNDER THE GDPR

Article 36 – Prior consultation

Article 36(4) requires member states to consult the supervisory authority "during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing."

Article 40 – Codes of conduct

Article 40(1) requires member states to "encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation." In so doing, member states should "tak[e] account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises."

Article 42 – Certification

Article 42(1) requires member states to also encourage "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," again while taking into account "[t]he specific needs of micro, small and medium-sized enterprises."

Article 54 – Rules on the establishment of the supervisory authority

Article 54(1) requires member states to "provide by law" for the "establishment of the supervisory authority," including qualifications and eligibility conditions, rules and procedures, duration of and number of eligible terms, and obligations regarding appointment as a member of the supervisory authority.

Also see Recital 117 and Recital 121.

Article 58 - Powers

Article 58(5) requires each member state to "provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation."

Also see Recital 122, Recital 129, and Recital 131.

Article 84 – Penalties

Article 84(1) requires each member state to "lay down the rules on other penalties applicable to infringements of this Regulation," in particular, those infringements not subject to Article 83. Member states must also "take all measures necessary to ensure that they are implemented."

Pursuant to Article 84(2), member states must notify the Commission about legal provisions it implements regarding Article 84(1) and of any subsequent amendments to them.

See also Recital 149, Recital 150, Recital 151, and Recital 152.

Article 85 – Processing and freedom of expression and information

Article 85(1) requires member states by law to "reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression."

Article 85(2) further stipulates that for such processing — i.e., "processing carried out for journalistic purposes or the purpose of academic artistic or literary expression"— member states must "provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information."

Pursuant to Article 84(2), member states must notify the Commission about legal provisions it implements regarding Article 84(1) and of any subsequent amendments to them.

Article 85(3) requires that each member state notify the Commission of any provision it adopts pursuant to Article 85(2) as well as any subsequent amendments affecting them.

Also see Recital 153.

II. ACTIONS MEMBER STATES MAY TAKE UNDER THE GDPR

Article 6 – Lawfulness of processing

To understand the powers that Article 6(2) reserves for member states, two of the legal bases for processing, points (c) and (e) of Article 6(1), must first be considered. Article 6(1)(c) stipulates that processing "shall be lawful only if" it "is necessary for compliance with a legal obligation to which the controller is subject," while Article 6(1)(e) designates processing as lawful "only if" it "is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

In light of these two legal bases for processing, Article 6(2) allows member states to "maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1." Recital 45 clarifies that the obligation to carry out these types of processing "should have a basis in Union or member state law." Moreover, the obligation in question "should be clear and precise and its application should be foreseeable to persons subject to it" (Recital 41). In these respects, member states can "more precisely" determine "specific requirements for the processing and other measures to ensure lawful and fair processing" (Art. 6(2)).

Article 6(2)(e) also gives member states room to interpret the scope of an exception within the GDPR. Given that personal data can be processed for purposes other than those for which it was originally collected "only where the processing is *compatible* with the purposes for which the personal data were initially collected" (Recital 50, emphasis added), Article 6(2)(e) allows member states to partly weigh in on the meaning of this exception. Thus, for processing that "is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller," Article 6(2)(e) carves out space for member states to "determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful" (Recital 50).

Also see Recital 10, Recital 51, and Article 35(10).

Article 8 – Conditions applicable to child's consent in relation to information society services

Article 8(1) requires that parental consent be obtained in order to process the data of a child under the age of 16. However, member states may set the threshold to as young as 13 years old.

Austria, the second country to enact a national law to supplement the GDPR, has lowered the age at which a minor can consent to processing in the absence of parental consent to 14 years old. Germany, meanwhile, did not alter the GDPR's default age of 16 for consent in its new data protection law. Other countries that have changed or proposed to change the age threshold include Ireland (to 13), Finland (to 13 or 15), and the U.K. (to 13).

Article 9 – Processing of special categories of personal data

The GDPR's Article 9(1) prohibits the processing of special categories of personal data (e.g., data that reveals racial or ethnic origin) except under certain conditions.

Within Article 9(2), which lists the set of circumstances under which this prohibition

does not apply, paragraph (g) exempts processing that is "necessary for reasons of substantial public interest, on the basis of Union or member state law …," which, in effect, gives each member state "a margin of manoeuvre … to specify its rules" regarding the processing of "sensitive data" (Recital 10). Thus, member states can lay out "the circumstances for specific processing situations" and determine "more precisely the conditions under which the processing of personal data is lawful" (Recital 10).

Furthermore, Article 9(4) permits member states to "maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health." As Recital 53 notes, however, "this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data."

Also see Recital 51 and Recital 102.

Article 10 – Processing of personal data relating to criminal convictions and offences

Article 10 holds that the Article 6(1)-based processing of personal data relating to criminal convictions and offences can only be carried out when it has been authorized by Union or member state law or when it is "under the control of official authority."

Article 22 – Automated individual decision-making, including profiling

Article 22(1) gives data subjects the right "not to be subject to a decision based solely on automated processing." Article 22(2), however, holds that this right does not apply under three conditions, one of which is when the decision "is authorised by Union or member state law to which the controller is subject." Moreover, such a law must include "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." In other words, member state laws that authorize automated decision-making involving special categories of personal data must include "suitable protections for data subjects."[1]

Also see Recital 71.

Article 23 – Restrictions

Article 23 allows member states to create derogations from the GDPR that "restrict by way of a legislative measure the scope of the obligations and rights provided for" in various articles — namely, Articles 12-22, Article 34, and Article 5 "in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22." Restrictions can be put into place to safeguard various interests, including national security, defense, public security, or judicial independence, as long as "such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" (Article 23).

Also see Recital 73.

Article 36 – Prior consultation

Article 36 requires data controllers to consult with the supervisory authority prior to processing when a data protection impact assessment indicates the processing would result in a high risk.

Article 36(5) empowers member states to create laws also requiring controllers to consult with and obtain prior authorization

1 A29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, adopted on October 3, 2017, p. 16.

from the supervisory authority before engaging in processing "for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health."[2]

Also see Recital 93, Recital 94, and Recital 129.

Article 37 – Designation of the data protection officer

Article 37 lists three conditions under which the appointment of a data protection officer is required: when the processing is carried out by a public authority or body, with the exception of courts; when "the core activities of the controller or the processor consist of processing operations which … require regular and systematic monitoring of data subjects on a large scale"; and when these "core activities … consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10."

Article 37(4) allows member states to stipulate additional circumstances under which the appointment of a data protection officer by a controller or processor (or by "associations … of controllers or processors") is required.

Article 38 – Position of the data protection officer

Article 38(5) binds the DPO to "secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or member state law."[3]

Article 49 – Derogations for specific situations

Article 49(5) stipulates that, absent an adequacy decision, member states "may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation." Member states that do so must subsequently notify the Commission of the implemented limitation(s).

Article 58 - Powers

Article 58(6) allows member states to "provide by law that its supervisory authority shall have additional powers" than the investigative, corrective, and authorization and advisory powers of the supervisory authority described in Article 58(1-3).

Article 83 – General conditions for imposing administrative fines

Article 83(7) enables each member state to "lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies" established in it. However, these rules must not interfere with supervisory authorities' corrective powers pursuant to Article 58(2).

Article 87 – Processing of the national identification number

Article 87 allows member states to "further determine the specific conditions for the processing of a national identification number or any other identifier of general application."

2 A29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing is "likely to result in a high risk" for the Purposes of Regulation 2016/679*, adopted on April 4, 2017, as last revised and adopted on October 4, 2017, p. 19.

3 A29 Data Protection Working Party, *Guidelines on Data Protection Officers (DPOs)*, adopted on December 13, 2016, as last revised and adopted on April 5, 2017, p. 18.

Article 88 – Processing in the context of employment

According to Article 88(1), member states may "provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context."

In particular, member states may put such rules in place "for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship" (Article 88(1)).

Furthermore, the rules must include "suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place" (Article 88(2)).

Lastly, member states must notify the Commission by 25 May 2018 of any rules they adopt pursuant to Article 88(1) and of subsequent amendments to them (Article 88(3)).

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 89(2) allows member states to create derogations from the rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object whenever these protections for the processing of personal data "are likely to render impossible or seriously impair the achievement" of scientific, historical research, or statistical purposes. Such a derogation must also be necessary for the fulfilment of these purposes (Article 89(2)). These derogations are subject to the conditions and safeguards laid out in Article 89(1), such as data minimization and pseudonymization (Recital 156).

Furthermore, pursuant to Article 89(3), member states may provide for derogations from the rights enumerated in Articles 15, 16, 18, 19, 20, and 21 insofar as they are "likely to render impossible or seriously impair the achievement of" archiving purposes in the public interest. Any such derogations are also subject to the conditions and safeguards laid out in Article 89(1).

Also see Recital 158.

Article 90 – Obligations of secrecy

Article 90(1) allows member states to "adopt specific rules to set out the powers of the supervisory authorities," contained in Article 58(1)(e-f), "in relation to controllers or processors that are subject, under Union or member state law or rules established by national competent bodies, to an obligation of professional secrecy." Member states must also notify the Commission of any rules made pursuant to this paragraph by 25 May 2018, as well as any subsequent amendments to them (Article 90(2)).

See also Recital 164.