# 20 About Specific Issues of the GDPR of the European Union

*Endre Győző Szabó*[*]

## 20.1 The New Data Protection Regime of the European Union

The European Commission tabled its proposal for a new data protection framework back in 2012. The co-legislators of the European Union approved the package after four years of negotiations in the spring of 2016:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

This paper looks into three specific topics of the GDPR: cooperation between data protection authorities, conditions for imposing administrative fines and the role and responsibility of data protection officers.

## 20.2 Cooperation between Data Protection Authorities, the Administrative Fine[1]

The Regulation is a legal act of the European Union aiming at the highest level of harmonization. Just as the previous data protection directive (96/46/EC, still in force), the new Regulation requires member states to establish independent data protection authorities to protect the rights of private individuals and to ensure the free flow of personal data within the Union. This requirement is not only enshrined in secondary Union law,

* Vice president of the National Authority of Data Protection and Freedom of Information.

1 These matters are regulated by Articles 51-75 of the GDPR and recitals (117)-(152) provide further guidance.

the Regulation, but also in the primary law. In essence, Article 16 of the Treaty on the Functioning of the European Union sets forth the same provision.

Data protection authorities in all member states are entrusted with the same tasks and competencies, including the power to impose sanctions and administrative fines.

According to the Regulation authorities shall play a crucial role in ensuring the consistent application of the Regulation throughout the European Union. To achieve this goal, data protection authorities shall cooperate with each other and the European Commission.

The Regulation expects cooperation between data protection authorities regarding all cross-border data processing operations, when the processing impacts several member states. Under specific circumstances, only one authority will be competent for cross-border operations. In derogation of the one-stop-shop mechanism, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of the Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

Even in these cases the authority seized of the matter shall inform the lead supervisory authority, whose competence is based on the main establishment of the controller.[2] It is up to the lead supervisory authority to decide whether or not handle the case. If the lead supervisory authority decides to handle the case, the one-stop-shop procedure takes place. In this case the supervisory authority seized of the matter may submit to the lead supervisory authority a draft decision. The lead supervisory authority shall take utmost account of that draft when preparing the decision. The lead supervisory authority shall be the sole interlocutor vis-à-vis the data controller.

Should the lead authority decide not to handle the case, the supervisory authority, which informed the lead, shall handle the case. During the procedure the supervisory authority may make use of specific cooperation procedures: mutual assistance[3] and joint operations.[4]

The Regulation provides for requirements regarding the forms of cooperation and includes provisions on cooperation procedures. Meanwhile, supervisory authorities shall follow their national procedural law when handling cross-border cases. Cooperation under the GDPR is built upon the procedural law of the member states. Supervisory authorities carry out intensive talks about the application of the Regulation. One of the questions discussed is the correlation of possibly conflicting provisions of procedural law with the regime set out in the GDPR. What clearly emerged during negotiations was that neither substantial, nor procedural provisions of the member state law may hamper the efficient application of Union law.

2 The paper refers to controllers only, but it should be read as 'controllers and / or processors'.
3 According to Article 61 of the GDPR.
4 According to Article 62 of the GDPR.

### *20.2.1 Cooperation Procedure (One-Stop-Shop)*

During the one-stop-shop procedure, member states endeavor to achieve consensus and exchange all relevant information. The final decision is drafted by the lead supervisory authority and within a period of four weeks may be opined by other supervisory authorities concerned. The lead supervisory authority may revise the draft decision, taking into consideration the relevant and reasoned objection expressed by any of the authorities concerned. Should no consensus emerge in the following two week period, or the lead authority does not intend to revise the draft decision in light of the relevant and reasoned objection, the matter is referred to the consistency mechanism.

If the supervisory authorities concerned do not object to the draft decision, the decision shall be deemed to have been taken by consensus and all authorities will be bound by it. The lead supervisory authority notifies the decision to the main establishment and informs other authorities and the Board about the decision. The authority seized by the matter informs the complainant of the decision. This of course, shall take place in the language of the complainant.

It may be the case that the authorities concerned reject one part of the complaint, while another part of the complaint will be investigated. Authorities concerned will reject the complaint respectively, while the merit of the case will be dealt with under the procedure as described above.

The decision is addressed to the main establishment, however, its scope shall cover the entire European Union. All establishments of the controller shall comply with the decision. The controller shall notify the measures taken for compliance to the lead supervisory authority.

An urgency procedure is launched in case extraordinary circumstances require the supervisory authority to act without delay for the protection of the rights of the individuals. The supervisory authority may adopt provisional measures with validity for a limited period of time (not exceeding three months). Of course, such a decision only produces legal effects in the territory of the member state concerned. Should the circumstances so require, the Board may, upon request of the supervisory authority, adopt a binding decision on the matter.[5]

### *20.2.2 Consistency Mechanism – Dispute Resolution*

The European Data Protection Board will play a role in settling disputes among supervisory authorities by adopting binding decisions. It is fair to say that the full independence of supervisory authorities is eroded in such cases. Under the current data protection Directive supervisory authorities never have to face a situation where they must

5 The urgency procedure is regulated by Article 66 of the GDPR.

accept a standpoint which is contrary to their own position. The Board may act in its role of settling disputes in various cases: where it is debated which supervisory authority is competent; the Board may be requested to settle the dispute if the supervisory authority did not request the opinion of the Board before adopting a specific measure under Article 64 of the Regulation, or the supervisory authority did not take the opinion of the Board into consideration. One-stop-shop related cases may also be resolved by the Board in case supervisory authorities cannot achieve a compromise.

Where no consensus among the supervisory authorities concerned may be forged, the Board adopts a binding decision. The procedure will be similar to the preliminary decision-making procedure of the Court of Justice of the European Union. The Board, set up by representatives of the supervisory authorities in the European Union will give guidance on specific legal issues. The decision of the Board will be binding upon all supervisory authorities concerned. The lead supervisory authority shall adopt a final decision based on the opinion of the Board and communicate it to the main establishment. The communication of the final decision is notified to the supervisory authorities concerned as well as the Board.[6]

### *20.2.3 Administrative Fine*

Supervisory authorities are vested with the same powers to impose administrative fines. The Board may issue guidelines for authorities on the criteria of imposing fines. The Article 29 Working Party carries out consultations on that matter, the result of which will be published.

Member state law determines whether or not data protection supervisory authorities may impose administrative fines on public bodies. When imposing an administrative fine, the procedural law and procedural guarantees of the member state concerned shall be respected. Decisions of the authorities imposing administrative fines will be subject to judicial review.

The exact amount of the fine is not provided for under the Regulation, only the criteria needed to be taken into consideration (Article 83 paragraph (2)). In specific cases the highest amount of the fine is lower (up to 10 million Euros or 2% of the total worldwide annual turnover). This amount shall apply if the Regulation is infringed for example by failing to notify the data breach to the supervisory authority or certain obligations related to the data protection impact assessment are not respected. In other cases the highest amount of the fine shall apply (up to 20 million Euros or 4% of the total worldwide annual turnover), where, for example principles relating to processing of personal data or rights of the data subject are breached.

6 The decision is communicated according to the rules of the member state of the lead supervisory authority.

A novelty in the Regulation is that not only data controllers and processors may be subject to an administrative fine, but also the monitoring body of the code of conduct and certification bodies.

As outlined, supervisory authorities shall endeavor to consistently apply the Regulation throughout the European Union. This is obvious in respect of cross-border cases. But does this expectation apply to cases concerning exclusively one member state? Our answer is in the affirmative, in light of the need for harmonized application of the Regulation. Situations where a specific breach of the Regulation are sanctioned with an administrative fine in member state A and are left unsanctioned in member state B should be prevented. When determining the exact amount of the fine, domestic economic circumstances and all relevant criteria shall be considered. The Board will not issue a binding decision on the amount of the fine. The amount will be determined by the lead supervisory authority with the margin of appreciation provided for under the Regulation.

## 20.3 Data Protection Officers[7]

The Regulation includes specific provisions on data protection officers, appointed within the organization of the data controller, significantly contributing to the protection of the data subjects.

### *20.3.1 Designation of Data Protection Officer*

The Regulation first lists the organizations where controllers have to designate data protection officers: public authorities and bodies.

The Regulation then lists activities, which require the designation of the officer: core activities of the controller consist of processing operations which require the regular and systematic monitoring of data subjects on a large scale. The text refers not only to activities that are understood as monitoring in general, but also covers activities that log or record users' behavior in detail (for accounting or law enforcement purposes). The latter is only relevant for private sector controllers, since public authorities and bodies must appoint a data protection officer in any case.

Finally, the Regulation lists specific types of personal data, the processing of which takes place on a large scale, and where this is linked to the core activities of the controller, requires the designation of the officer. These include special categories of data (pursuant to Article 9) and personal data relating to criminal convictions and offences (referred to in Article 10).

7 Related provision in the Regulation: Articles 37-39 and recital (97).

As far as Hungary is concerned, it is expected that categories of controllers that are currently obligated to designate an officer will remain the same under the new regime. This is all the more probable, where taking into consideration the complexity of the new rules, controllers will tend to designate data protection officers even if it is not an obligation under the Regulation.

Criteria related to the appointment of data protection officers fit well into the rules on privacy impact assessment. It is therefore logical that in the course of the privacy impact assessment the advice of the officer shall be sought (in case the controller designated one).

### *20.3.2 Legal Status of the Data Protection Officer*

The Hungarian privacy act[8] provides for the specific qualification of the officer (legal, economic, IT or equivalent degree). The Regulation takes another approach: it mentions professional qualities and the ability to fulfil their tasks. A person may be designated or mandated who has an expert knowledge of data protection law and practice.

How may such professional qualities and expert knowledge be evaluated? According to the Regulation the necessary level of expert knowledge should be determined in particular in light of the data processing operations carried out and the protection required for the personal data processed by the controller. The provisions of the Regulation show that the relevant provisions enshrined in the Hungarian privacy act may be repealed.

The Regulation aims at flexibility regarding the form of employment. A group of undertakings may appoint a common officer if they are readily available to work for all undertakings concerned. Specificities of international activities need to be taken into account here, and staff will be needed also locally, since knowledge of local circumstances in indispensable. Correspondence with local data subjects requires the knowledge of the language spoken locally. Being close to data subjects and availability are thus basic requirements.

The Regulation provides for the designation of common data protection officers in the public sector. If a common officer is appointed due regard shall be paid to organizational structure and size. Tasks in such cases shall be defined to make it possible for the single officer to perform them alone.

Associations and other bodies representing categories of controllers or processors may, in the private sector, appoint a common officer. This officer may act for such associations and other bodies representing data controllers. Where required by Union or Member State law, controllers shall designate a data protection officer. This provision of the Regulation leaves room for maneuver for legislators in the member states.

The data protection officer may be a staff member of the controller, or the tasks may be carried out based on a service contract. This provision shall be transposed into the law

8 Act no CXII of 2011 on the informational self-determination and freedom of information.

of the member state concerned accordingly: in Hungary, data protection officers will be employed in accordance with the Labor Code or via the so-called mandate contract. This means that the current practice may be continued under the Regulation.

Publicly available information is closely linked to the legal status of the officer. The Regulation requires controllers to publish the contact details of the officer. These details will be registered by the supervisory authority, therefore, keeping the current register, as a task, will remain with the authority. Publicly available information also guarantee that in case of a complaint the officer will be available to the public at large. In addition, regarding complaints, the data protection officer shall be available to data subjects in case they have any inquiries related to the processing of their personal data or to the exercise of their rights under the Regulation. This does not mean that the officer is the sole correspondent towards data subject, nevertheless, they shall be available in matters related to data protection, particularly in cases of data breaches.

### *20.3.3 Controllers' Duties in Supporting the Data Protection Officer in Performing Their Tasks*

The data controller (the employer) shall support the data protection officer in performing their tasks by providing the necessary resources. That includes the necessary financial support, the premises and as the case may be, further staff members. It shall be ensured that the officer has access to personal data and processing operations. Furthermore, necessary resources shall be provided by the controller so that the officer may keep their expert knowledge up to date. The relevant list includes rather specific requirements towards the controller in this respect.

The controller shall ensure that the officer carry out his or her tasks in an independent manner. Independence is not equivalent to irresponsibility. Independence means that the officer may not receive any instructions regarding the exercise of their tasks, and this shall be guaranteed by the controller. When acting in their 'supervisory' capacity, evaluating the lawfulness of processing operations, the officer may not be instructed. The officer enjoys protection, namely that they may not be dismissed or penalized by the controller for performing their tasks. Sanctions shall be interpreted broadly, and any perks or benefits shall be covered by this rule if they are not provided to the officer in relation to the performance of their tasks.

The Regulation confirms the Hungarian provision already in force, according to which the data protection officer shall directly report to the highest management level of the controller.

### 20.3.4 Tasks of the Data Protection Officer

The controller shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. This provision cannot be separated from the principle of data protection by design: the officer shall have the opportunity to express their views in due time and at due phase of the process. The Regulation often refers to the risks of processing. The data protection officer is also required to take due account of these risks when performing their duties.

The officer informs and advises the controller and the employees of their obligations pursuant to the Regulation and to other Union or Member State data protection provisions.

The officer monitors compliance with the Regulation and other Union or Member State data protection provisions, furthermore, with the policies of the controller in relation to the protection of personal data, including awareness-raising and training of staff involved in processing operations. The officer is also in charge of monitoring related audits. In addition, the officer provides advice where requested regarding the data protection impact assessment and monitors its performance.

One of the significant tasks of the officer is to cooperate with the supervisory authority. The officer acts as a contact point for the supervisory authority during the prior consultation related to the privacy impact assessment. The officer may consult the authority on any relevant matter.

The Regulation does not provide for regular contact with the supervisory authority or conferences. According to the Hungarian privacy act the conference of data protection officers is convened at least once a year by the supervisory authority. Since this provision is fully in line with the Regulation, the conference will most probably remain an important forum in Hungary also in the future.

### 20.3.5 Future of the Data Protection Register[9]

The Regulation does not mention the data protection register, only one of the recitals provides some guidance, referring to the provisions of Directive (96/46/EC) and the transposing laws of the member states.

According to recital (89) indiscriminate general notification obligations should be abolished, and replaced by effective procedures and mechanisms which instead focus on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. General registration will thus be replaced by the registration of special processing

9 Related provisions in the GDPR: recital (89)

operations. Processing operations may come under the registration which involves the use of new technologies or new types of processing.

The Regulation arrives at the conclusion that the general data protection register produces administrative and financial burdens, meanwhile, it did not in all cases contribute to improving the protection of personal data.

It is therefore to be expected that central data protection registers shall cease to exist in the member states. Another consideration behind this is that within the European Economic Area the free flow of personal data shall be ensured. If the free flow of personal data is not an issue related to specific processing operations (fragmented notifications do not hamper the free flow of data), some room for maneuver may remain with legislators at the member state level. Registration of processing operations carried out by public authorities and bodies may be an exception. Referendums and related collection of citizens' signatures are registered by the supervisory authority in Hungary. This practice may be continued under the GDPR.

The Regulation requires the supervisory authority to carry out registrations at several points. Contact details of the data protection officers will be registered by the authority. Data protection impact assessments and also data breaches will be registered by the authority. In case of certain derogations the authority will register specific data transfers to third countries. The central register, managed by the supervisory authority remains part of the data protection framework, but the role and content of the same will be amended to a significant degree.