New era for personal data protection

On 17 December 2015, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs voted in favour of the proposed Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The draft adopted is the result of several years of legislative work, discussions among stakeholders, and weighing of competing priorities. The proposal is a point of departure for further legislative work and may undergo further modifications. Nonetheless, it gives a clear picture of the General Data Protection Regulation which is soon expected to become law. A major reform of the data protection system throughout the European Union is about to take place.


Sylwia Paszek


Agnieszka Szydlik


Katarzyna Żukowska

When enacted, the General Data Protection Regulation, as it is known, will apply directly in the member states of the European Union, superseding the Data Protection Directive (95/46/EC) and its implementations in national law (in Poland, the Personal Data Protection Act of 29 August 1997).

In this article we highlight selected changes to be introduced when the General Data Protection Regulation is adopted and enters into force.

Scope of application of the regulation

The regulation is to apply to processing of personal data when the processing occurs in the context of the activity of a data controller or data processor based in the EU, regardless of whether the processing occurs in the EU. This means that it will be necessary in each case to analyse the factual circumstances under which the controller processes data.

The regulation will also apply to processing of data of entities from the EU by a data controller or processor based outside the EU, if the processing is connected with offering of goods or services (including free of charge) or observation (monitoring) of the behaviour of data subjects, if the monitoring occurs in the EU.

Data controllers and processors

The draft regulation addresses the requirements for entities processing data more specifically than the current law. For example, the controller is required to select an entity providing adequate guarantees of implementation of appropriate means and technical and organisational procedures so that processing of the data meets the requirements of the regulation. It also specifies the elements that must be established in the agreement between the data controller and the data processor.

According to the draft, a data controller, as well as an entity contracted to process data, may (optionally) appoint a data protection officer. The regulation also provides for situations where it is mandatory to appoint a data protection officer (e.g. in the case of entities processing data concerning criminal convictions). Controllers and processors are also required to ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data. As under current law, the data protection officer is to perform his or her duties independently. The data protection officer should not be given instructions on performance of this function, but should report directly to the management of the data controller or processor.

Notification of data protection breaches

The draft regulation imposes on data controllers an obligation that does not exist under current law to notify the supervisory authority (in Poland, the Inspector General for Personal Data Protection—GIODO) of a breach of personal data protection. The notification must be made without undue delay, but no later than 72 hours after the event. If this deadline is not met, the reasons for the delay must be explained. The notification must include, at least, a description of the nature of the breach, including the categories and number of data subjects potentially affected, the identity and contact details of the data protection officer or other contact point where more information can be obtained, the anticipated consequences of the breach, and the measures proposed or taken to minimise or eliminate the negative consequences of the breach. If complete information cannot be provided immediately, it should be supplemented when possible, along with documentation of remedial measures so that the supervisory authority can verify that they are proper and adequate. Data processors will be subject to a similar notification obligation in the case of a breach, but they should notify the data controller.

The data controller also has to notify the data subject of a breach of data protection, providing an understandable description of the breach, the potential consequences, and the remedial measures. This notice will be required only when the breach carries a high risk of infringement of the rights and freedoms of the data subject. The data controller will be released from the requirement to notify data subjects if it has implemented technological and organisational measures to protect the data affected by the breach, particularly by rendering the data unintelligible to third parties (e.g. through encryption), where the measures taken by the controller have eliminated the risks to the rights and freedoms of the data subjects, and where the notification of data subjects would be disproportionately burdensome to the contractor (in which case the direct notification of data subjects can be replaced by public announcements or other means with similar effect).

The obligation to report data breaches is a major change from current law. Now data controllers and processors do not have to disclose such events. Outside of the public eye, they make their own choice of remedial measures according to their capabilities. Any inadequacies or incompleteness in the solutions they adopt may only be identified in the event of an inspection by GIODO. The proposed model will ensure that in the event of a breach, the data controller will implement remedial measures in close dialogue with GIODO and under GIODO's supervision. This will reduce the risk that measures will be used that are not adequate to the nature of the breach.

Transfer of personal data outside the EU or EEA

The need to ensure an adequate level of protection in the country to which data are transferred is to be maintained.

The transfer of personal data to third countries without obtaining an additional permit from GIODO will still be possible in a situation where the parties have signed standard data protection clauses adopted by the European Commission. However, there is a stress on onward transfers, particularly in light of the clarifications by the Article 29 Working Party excluding the use of clauses for onward transfers when a data controller from the EEA concludes an agreement with a data processor in the EEA and the processor would then subcontract processing to an entity in a third country.

The draft also provides that data may be transferred on the basis of binding corporate rules, approved codes of conduct, and certifications (Art. 38 and 39) without additional permits, but there is also a delegation to establish procedures for the exchange of information among controllers, processors and supervisory authorities.

Under the draft, data may be transferred with the consent of the data subject, after the data subject is informed of the risks of such transfers. This could mean that existing transfers based on consent but without first warning the data subject of the risks cannot be continued.

It is unclear how the Commission will issue decisions on the adequacy of the protection in a third country, processing sector, or international organisation. While the wording of Art. 41 is clear, in light of the holding that the Safe Harbour decision was invalid, the mistrust in data transfer rules based on Commission decisions declared by certain NGOs (and even national data protection authorities) appears justified.

Sanctions for violating data protection regulations

The current law in Poland provides sanctions for violation of data protection regulations (for petty offences and criminal offences), but their application is typically limited to liability for a petty offence (not very severe), while it is exceedingly rare for criminal responsibility to be imposed (because the societal harm of the act is deemed to be low). Thus there is an absence of a proportionally severe sanction to be applied even in the case of small-scale violations.

This gap will be filled by administrative fines imposed by GIODO. The amount of the fines would reflect such factors as the nature, gravity, duration and consequences of the violation, the degree of fault, the infringer's responsibility for implementing proper technical and organisational measures, the remedial actions taken to limit or eliminate the negative consequences of the violation and cooperation with GIODO in this respect, previous violations, and the manner in which GIODO learned of the violation.

The maximum fine, depending on the nature of the violation, would be EUR 10 million or 20 million, or in the case of an enterprise, 2% or 4% of its total annual revenue in the preceding year. The member states are to adopt executive regulations concerning inspection proceedings and procedures for imposing and enforcing penalties, which should be proportionate but severe enough to act as a deterrent.

Data controllers and processors would also be liable (based on fault) for injury caused by unlawful processing of data. Any person who suffers material or non-material damage as a result of unlawful processing of personal data may demand compensation. The data controller's liability is limited to cases where it has violated the regulation, while the data processor's liability is limited to violation of the provisions of the regulation addressed specifically to data processors or for acting contrary to the data controller's instructions. The controller and the processor would bear joint and several liability for the same occurrence, but could assert claims for recourse between one another.

Sylwia Paszek, legal adviser, Personal Data Protection Practice and M&A and Corporate Practice

Agnieszka Szydlik, adwokat, *Personal Data Protection Practice and M&A and Corporate Practice*

Katarzyna Żukowska, Employment Law Practice and Personal Data Protection Practice