Urszula Goral[1]

The Challenges of GDPR compliance in Poland – the point of view of the national Supervisory Authority

In Poland, the issue of the personal data protection was settled for the first time in 1997 – in Article 51 and 47 of the Constitution of the Republic of Poland of April 2, 1997 – and comprehensively – in the Act of August 29, 1997 on personal data protection, supplemented by legal acts, so called implementing regulations. In the Polish legal system, GIODO was the authority responsible for guarding the observance of data protection rights in the past twenty years.

On 25 of May, the old Data Protection Act was replaced by the New Act implementing the GDPR. Of course, we all know that according to European law the GDPR applies directly, but some aspects had to be regulated at the national level in the form of the national Data Protection Act.

The European data protection reform involved two legal acts (as a package): the GDPR and the less popular Directive 2016/680, the so-called Police Directive. These two pieces of legislation should have been implemented by May 2018; however, Poland is still one of the ten Member States that did not meet the deadline for the implementation of the latter Directive. That is why, to regulate data protection issues related to the so-called third pillar matters, the Polish legislator

1 Polish Personal Data Protection Office; Director of the International Cooperation and Education Department, Cardinal Stefan Wyszyński University, Warsaw

upheld some of the provisions of the previous Data Protection Act. The draft law implementing the Police Directive was approved by the Polish government in August (2018), but is still not subject to the parliamentary procedure and this stage of the legislative procedure has not been started yet. It means that in Poland we have mixed the previous and the current legislation in the field where the Directive should be implemented. It also means that there are several institutions in Poland, especially in the context of law enforcement, which should apply both frameworks while performing their tasks.

As regards the new Data Protection Act, it should be mentioned that the draft was presented by the Polish government in March 2018, adopted by the Parliament in May – the date when the Polish Data Protection Act entered into force is very significant – 25 May 2018. It means that the parliamentary procedure was very fast, sometimes without deeper discussions, but the Act was adopted on time.

As far as another element of the legislative package in Poland is concerned, to implement the GDPR the government decided to propose a draft of the huge act that introduced amendments to sectoral legislations. They just started to propose changes in September 2017, and the scope of these changes is getting wider and wider. This is probably then reason why this act has not yet been adopted. It is not difficult to find out that the main aim of law is to limit the application of the GDPR in Poland. Numerous ideas appeared and one of the examples was the exemption of the information obligation in the context of SMEs. The position presented by our data protection authority was that such proposal is not in line with the GDPR. A consultation was also held between the Polish government and the European Commission and finally this proposal was not introduced.

As for the sectoral legislation, there are major changes regarding labor law, banking law and insurance law. It is difficult to foresee when this draft legislation will be adopted. The lack of existence of this law is not such a big problem, as the GDPR applies directly in all these fields. In terms of principles, obligations, all seems to be clear. However, there

seems to be some misunderstanding by some of the data controllers in certain sectors. It looks like the GDPR left an impression that data protection is a completely new phenomenon. However, it is not. Data protection legislation has existed since 1997 in Poland and remains largely the same in terms of general principles or data controllers' obligations. The biggest challenge in this whole discussion is that the GDPR should be considered as evolution rather than revolution. Many obligations are similar to the former ones under the previous Directive 95/46.

As regards the Polish Data Protection Act adopted in May 2018, it mainly focuses on the status and powers of the data protection authority. One of the changes introduced by the Act is the change of the name of the authority. We are now called – as a supervisory authority – the Personal Data Protection Office, the name GIODO (Inspector General for Personal Data Protection) no longer exists. In addition, this Act provides for specific rules for procedures before the supervisory authority in line with the general powers foreseen by the GDPR.

The effect of the General Data Protection Regulation required the adaptation of local law to the new requirements. The Act includes, *inter alia*, details on appointing and notifying a Data Protection Officer (DPO), who shall be appointed by a controller or a processor on a mandatory or voluntary basis. The appointment of the DPO should be followed by notification of the appointment to the competent supervisory authority. Provisions also regulate issues concerning DPOs, e.g. the rules for providing their contact details. We also modified the scope of information provided, adopted to the general requirements.

The new Act provides the procedural rules for the adoption and approval of codes of conduct. I would like to stress that we have high hopes for the development of such norms. This is a new tool in our national system. We had some experience in this field, because under previous legislation we used to promote this concept in the form of codes of good practices. However, this solution was not legally binding. Now, under the GDPR, codes of conduct can be very crucial enforcement mechanisms.

The Act also implements the general rules for the certification mechanisms on the national level. The Polish legislator decided that certification shall be carried out by the competent certification bodies accredited by the national accreditation agency and at the same time by the data protection authority. As you can see, in Poland we have a mixed model, not only dedicated to certification bodies. The Act furthermore sets forth general rules for the obligation to notify data breaches or procedural rules for prior consultations.

As regards the activities of the Polish Data Protection Authority, one of our responsibilities was the publication of the list of the processing operations which require data protection impact assessment (DPIA). The Polish Data Protection Authority prepared and published a draft list of processing operations which are subject to mandatory DPIA. We published the first draft of the list in March for public consultation with the official list of the national (not transborder) operations being published (by law) within three months from 25 May.

We are also subject to review within the European Data Protection Board (EDPB) under the consistency mechanism. The Polish authority has already received the opinion from the EDPB and we have introduced some amendments to the initial list. After the completion of the procedure both national and transborder lists are ready to be finally published.

The Personal Data Protection Office of Poland has issued a series of guidelines to help ensuring compliance with the GDPR, including:

1. *"Personal Data Protection at Work. A Guide for Employers"*. The Guide explains how employers shall process personal data of job applicants and employees during the recruitment process and the entire employment period in compliance with the GDPR and indicates how they should approach certain problems. It includes, e.g., the following guidelines:

- The employer can request from a job applicant only the data to the collection of which it is authorized by law and which are necessary for making the decision on their employment;
- Excessive or 'just in case' data may not be collected in the recruitment process;
- It is not permitted to collect the data on potential applicants from social networks nor to draw up blacklists of job applicants;
- The employer shall not make nor store copies of employee's ID cards;
- Monitoring of phone calls or tracking private e-mails of employees is not allowed;
- The employer can monitor official e-mail correspondence of employees, but they must be informed thereof.

2. "*Personal Data Protection at Schools and Educational Institutions: A Guide*". The Guide addressed to school principals and directors of educational institutions contains updated advice on the processing of personal data of children, their parents and guardians, teachers. It describes how to use the GDPR provisions and sectoral legal acts in specific situations. The Guide includes for example the following advice:
   - Schools and educational institutions can publish the lists of admitted or non-admitted applicants only at their seat (publication on the school's website is prohibited);
   - Posting information containing personal data of students for the purpose of distinguishing them for special educational achievements on boards at the premises of school is allowed and does not require previous consent of student's guardian.

3. *The Guide* "*Personal Data Protection in Electoral Campaign*". It is addressed to all entities involved in the election process – not only candidates and their committees, but also institutions carrying out

elections and the voters. It indicates *inter alia* the main principles of personal data processing, the notions and definitions provided in the GDPR. It stresses the importance of the role of data controllers and indicates that at various stages of the electoral campaign different controllers are processing the data. A separate part of the Guide includes answers to FAQs on practical problems related to personal data processing for the purposes of the election.

4. *"Guidelines of the President of the Personal Data Protection Office on the Use of Video Surveillance"*. In these Guidelines, the permitted purposes for which video surveillance can be used, the rights of the persons subject to surveillance, and the controllers' obligations are discussed in a comprehensive manner. The Guidelines include also answers to FAQs and were subject to public consultation. Currently, the information received during the consultation is being analyzed, and following analysis the updated version of the Guidelines will be published to inform video surveillance operators in adapting to the applicable legal provisions, including the GDPR and national regulations.