COUNTRY UPDATE-Bulgaria: GDPR one year on

Published 29-May-2019 by
TRRI commissioning team

In May 2018, the European Union's General Data Protection Regulation (GDPR) came into force, imposing wide-reaching new obligations on controllers and processors of personal data. It also contained more than 50 derogations and "opening clauses," giving member states considerable powers to shape its application to their country.

One year after GDPR implementation, this article provides a description of the current position in Bulgaria by Violetta Kunze and Ralitsa Gougleva of Djingov, Gouginski, Kyutchukov & Velichkov.

GDPR highlights

Article 5 general principles:

Personal data must be processed "lawfully, fairly and in a transparent manner." Processing must be limited to a specified, explicit and legitimate purpose; data must be accurate and processed with appropriate security.

An entity controlling personal data is responsible for ensuring and demonstrating compliance with these principles.

Articles 6-11 define "lawfully" and set extra requirements concerning sensitive data.

Examples of derogation powers:

Articles 12-22 describe individuals' rights regarding their personal information but Article 23 permits member states to restrict those rights and Article 5 principles in certain circumstances.

Article 83 sets grounds for imposing administrative fines for GDPR breaches. These can reach 4 percent of an organisation's annual worldwide turnover or euros 20m, whichever is greater. In addition, Article 84 empowers member states to make GDPR infringements not covered by article 83 subject to penalties.

1. Has national legislation come into force that uses GDPR derogation/ opening clause powers?

Bulgarian Law on Personal Data Protection Act (LPDP) dates back to January 2002. At the beginning of March 2019 it was materially amended to implement GDPR in Bulgaria. Most of these latest amendments to LPDP relate namely to GDPR derogations.

Firstly, according to Article 1 of the amended LPDP, where personal data processing is carried out by competent state authorities for the purposes of prevention, investigation, discovery, prosecution and/or punishment of crimes, GDPR does not apply. Instead the special rules of the new Chapter 8 of LPDP shall apply.

These special rules aim to provide data subjects with a level of data protection and with safeguards as those under GDPR to the extent possible in view of the special purposes of the relevant data processing. In principle the lawfulness of such exceptional data processing significantly depends on its purpose and conformity with that purpose. All legitimate purposes for which personal data processing in this case is permissible are set forth in the law.

Secondly, pursuant again to its Article 1, the amended LPDP and GDPR do not apply to personal data processing for the purposes of national security and defence as well as to the processing of personal data of deceased individuals, unless otherwise set out by law. With respect to personal data processing for the purposes of national security and defence, no Bulgarian law sets out that LPDP shall apply.

With respect to deceased individuals Article 25e of LPDP sets out that a controller or processor may process personal data relating to deceased individuals provided only it has legal basis for doing it and has implemented appropriate measures to prevent any negative consequences to occur in respect of (alive) persons, their rights and interests and/or the public interest.

Thirdly, the amended LPDP sets out a number of special provisions to supplement open GDPR clauses. Article 25a provides for a data controller or processor may control personal data that it has received without legal basis for no longer than 1 month of becoming aware of this circumstance and that after that the controller or processor must return the data to the data subject or erase it.

Article 25# supplements Article 8 of GDPR by setting out that any consent-based processing of personal data - including but not limited to processing in relation to the direct offer of information society services – relating to children below 14 years of age may only be done if a valid consent is obtained by the parents or legal guardians of the child.

Personal data processing for journalistic, academic or artistic purposes is lawful, provided that a balance is struck between freedom of expression and right to information, on one the hand, and the right to privacy, on the other hand. Article 25#(2) of LPDP provides guiding criteria to assess whether a balanced approach is present, including the nature of the personal data, the impact that its dissemination might have on the personal life of the data subject, etc.

According to the provisions of Article 25#(3), Article 25#, Article 25# and Article 25# of LPDP data subject's rights to access, correction and/or erasure may - subject to certain conditions - not be respected by a data controller where the personal data processing is for journalistic purposes or for the purposes of academic, artistic or literary expression, for statistical purposes, for the purposes of the National Archives and for humanitarian aid purposes, respectively.

Article 25# of LPDP sets out special rules regarding employer's processing of employees' personal data. According to this provision to introduce and use any of the following workplace arrangements: (i) a whistle-blowing system or other system for reporting workplace infringements; (ii) limitations or restrictions on the usage of the organization's resources for private or other work unrelated purposes; and/or (iii) a monitoring or access control system relating to workplace attendance and discipline, an employer, as data controller, must approve and adopt internal company rules and procedures regulating the relevant arrangement and the personal data processing that its implementation involves.

As a minimum the rules and procedure must include information about the scope of application and methods of operation of the relevant arrangement and the employees' and employer's obligations in relation thereto. The arrangement should not in any case restrict or impede the data protection rights of employees' under GDPR and general rules of LPDP. Employees must be notified in a fair and accurate manner by the employer of the adopted rules and procedures prior to their implementation.

2. Has article 84 been used to introduce additional GDPR infringement penalties, administrative or criminal?

According to LPDP there are three groups of infringement administrative fines: (i) fines for infringements and in amounts set out in GDPR; (ii) fines for infringements of the special LPDP provisions supplementing the open GDPR clauses; and (iii) fines for infringement of LPDP that do not fall under any of groups (i) and (ii).

Fines from the first group apply directly to cases where the relevant infringements are duly established under GDPR. As far as the second group of fines is concerned, LPDP provides that the fines set out in Article 83 of GDPR may also be imposed by the Bulgarian Commission for Personal Data Protection (the Commission) for breaches other than those set out in GDPR and relating to some of the specific data protection provisions under LPDP.

For example, processing of child's personal data which is in breach of LPDP may trigger the greater fine under GDPR of 20 million euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher, while the introduction of a whistle-blowing or other internal control system involving processing of employees' personal data by an employer without adoption and due notification to the employees of required internal company rules and procedure, may expose the employer to the risk of being sanctioned by a fine from the lower tier under GDPR of 10 million euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is higher.

The third group of fines serves as a default provision and applies to any breaches of LPDP for which no specific sanction is set out in LPDP. The fine from this group is limited in amount up to BGN 5,000 (approx. 2,500 euros).

The Commission imposes fines by a decision which may be subject to a follow-up administrative court review at two instances.

The amount of the applicable fine will be double if the breach is repetitive, i.e. committed within 1 year from the effective date of a final and enforceable decision of the Commission by which a sanction for the same breach has been imposed to the controller or processor in default.

In respect of any infringement, the Commission may issue a mandatory administrative measure instead of or along with imposing an administrative fine. Under LPDP mandatory administrative measures include the measures under Article 58(2) of GDPR, save for letter "i" thereof.

3. Is any other GDPR derogation/opening clause legislation either in process or proposed?

As of the date hereof, we are not aware of any such legislation being either in process or proposed.

4. Has the national supervisory authority issued any guidance on GDPR operation or its approach to enforcement?

Since May 25, 2018, when GDPR came into effect, the Commission has issued guidance on the operation of GDPR with respect to the following matters:

- Personal data processing by judicial authorities, including courts and prosecution offices, and personal data protection within the judiciary system;
- Controller/processor legal standing of courier and traditional post-mail service providers;
- Controller/processor legal standing of banks and other licensable service providers;
- Lawfulness of voice biometrics processing;
- Evidencing and verification of employee's temporary work incapacity before employers;

- Unambiguous identification of individuals by nonbanking financial institutions in virtual environment for the purposes of distant financial services provision;
- Disclosure of public information;
- CCTV cameras at schools;
- Data processing for the purposes of Multisport cards;
- Controller/processor legal standing of insurers and medical centres with respect to health insurance policies;
- Livestreaming of municipality council meetings by citizens attending the meeting;
- Controller/processor relationship between the National Health Insurance Fund and contracted pharmacies;
- The right "to be forgotten" in the context of personal data processing for the journalistic purposes;
- Personal data processing involved in collection of donations for medical treatment via Facebook groups;
- Codes of conduct; and
- Personal data protection in the context of the Public Procurement Act.

So far the Commission has not issued any official guidance on its approach to enforcement. During the first year of GDPR application the Commission exercised its enforcement and corrective powers in a relatively unaggressive manner. Most of the supervision inspections were undertaken in response to a third-party signal or data subject's claim for a breach. Imposed administrative sanctions were limited in number and amount.

5. Have any issues about GDPR's operation arisen that concern financial services firms?

No material issues have arisen in this respect in Bulgaria.