Serbia: Chapter 23 - What does it Take to Stay on the Train and reach EU? Part 2

JPM | PARTNERS

SERBIA: CHAPTER 23 - WHAT DOES IT TAKE TO STAY ON THE TRAIN AND REACH EU? Part 2
Publisher: JPM & Partners
Delta House, 8a Vladimira Popovića street
www.jpm.law
Authors: Ivan Milošević, Partner, Prof Gojko Grubor
Design and prepress: JPM & Partners

Accountability is one of the key notions both in GDPR and the Serbian Data Protection Act. As this data protection principle is introduced, controllers cannot keep making excuses claiming they complied their businesses with the GDPR while having pro forma documents and are in lack adequate documents, engaging DPOs who do not understand what it takes to be compliant, and having employees who do not understand their responsibilities.

This principle is closely connected to the integrity and confidentiality principle. The GDPR prescribes a clear obligation for controllers to demonstrate that technical and organisational measures are adequate – measures shall be the result of risk assessment in regard to nature, scope, context, and purposes of processing as well as of varying likelihood and severity for the rights and freedoms of natural persons.

The risk assessment is twofold.

The first part is related to risk assessment of the security of processing (data security) where controllers and processors assess the likelihood of the level of impact of unauthorised disclosure (loss of confidentiality), unauthorized alteration (loss of integrity) and unauthorized destruction or loss (loss of availability) of personal data on natural persons and likelihood and severity of occurrence of events (threats) for personal data.

In parallel, risk assessment in regard to other events which may cause damage to the rights and freedoms of natural persons shall be carried out – GPDR and Serbian Data Protection Act oblige controllers to "assess likelihood and severity of risks for the rights and freedoms of natural persons for rights and freedoms of natural persons".

Discrepancies in terminologies used in GDPR and Serbian Data Protection Act and those used in standard risks assessment methodologies may lead to confusion – in the first phase risks of the likelihood of the level of impact of events on the rights and freedoms are assessed, while, in the second, the likelihood of occurrence and severability of such events.

Data Protection Impact Assessment is carried out in cases where the first assessment shows that certain types of processing are likely to result in a high risk to the rights and freedoms of natural persons or in cases where such assessment is explicitly required by the GDPR and Serbian Data Protection Act.

Requirements for both assessments, sanctions for non-compliance and recommended methodologies for carrying out the assessments shall be subject to forthcoming amendments of the Serbian Data Protection Act.

Our understanding is supported by the Government Working Group for Drafting Data Protection Strategy and it is incorporated in the said strategy.

We have discussed internally and externally the matter of accountability and links of this notion to adequate technical and organisational measures many times.

Robust and neutral formulations in Articles 24, 32 and 35 of GDPR (Articles 41, 50 and 54 of the Serbian Data Protection Act) cause a lot of headaches to all stakeholders.

Our understanding is that GDPR and the Serbian Data Protection Act prescribe a twofold risk-based approach when defining the obligations of controllers to protect the rights and freedoms of the citizens.

A) Scope of responsibility of the controllers

Art. 24 of GDPR (Art. 41 of Serbian Data Protection Act) imposes a general obligation for controllers:

a. to implement adequate technical and organisational measures to
b. ensure and be able to demonstrate

that processing is performed in accordance with GDPR, i.e., Serbian Data Protection Act taking into account:

c. nature, scope, context and purposes of the processing;
d. the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The aim of this Article is to define the scope of responsibility of the controller – to implement adequate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR, i.e., Serbian Data Protection Act. In simple words, technical and organisational measures shall be defined and implemented to comply business of the controller with data protection principles. The controller shall be able to demonstrate i.e. present proofs confirming that its business processes (processing activities) comply with GDPR, i.e., Serbian Data Protection Act.

The notion of “adequate” technical and organisational measures implies that the measures shall be defined and implemented following a risk assessment. This conclusion is based on the formulation in the said Article – “taking into account” which means that the controller shall choose a relevant methodology to assess risks of varying likelihood and severity for the rights and freedoms of natural persons. The risk assessment shall be presented to supervisory authorities in case of possible data breaches to demonstrate the adequacy of defined and implemented measures.

B) Risk Assessment in GDPR and Serbian Data Protection Act

The GDPR and Serbian Data Protection Act do not define the notion of risk. However, the notion of risk can be derived from recital 75 of the GDPR Preamble as: "the existence of a likelihood of occurrence of an event which may cause the damage (including unauthorised limitation of rights and freedoms of natural persons) or the other damage for one or more natural persons. There are two dimensions:

i. the severity of damage;
ii. the likelihood of occurrence of the event which may cause the damage and damage consequences".

Damage can be expressed as material or immaterial damage or limitations of rights and freedoms of natural persons.

Damage can be expressed as material or immaterial damage or limitations of rights and freedoms of natural persons.

The object of assessment is data protection rights and other rights which are indirectly, through data protection law, protected and which are recognized by EU and national documents.
When assessing the risk to the rights and freedoms of natural persons, controllers shall:

a. identify risks, i.e., determine:

i. which damages for rights and freedoms may occur;
ii. sources of events which may cause the damage and
iii. circumstances under which the events ii) may occur (sources of risks).

Damages are explained in recital 75 of the GDPR Preamble.

The sources are related to breaches of data protection principles and data protection rights.
Circumstances under which the events may occur may be related to excessing authorisations by employees with controllers to handle personal data, hacker attacks, communication with partners and producers of software, etc.

b. evaluate the likelihood of damage occurrence and severity of possible damage to rights and freedoms of natural persons;

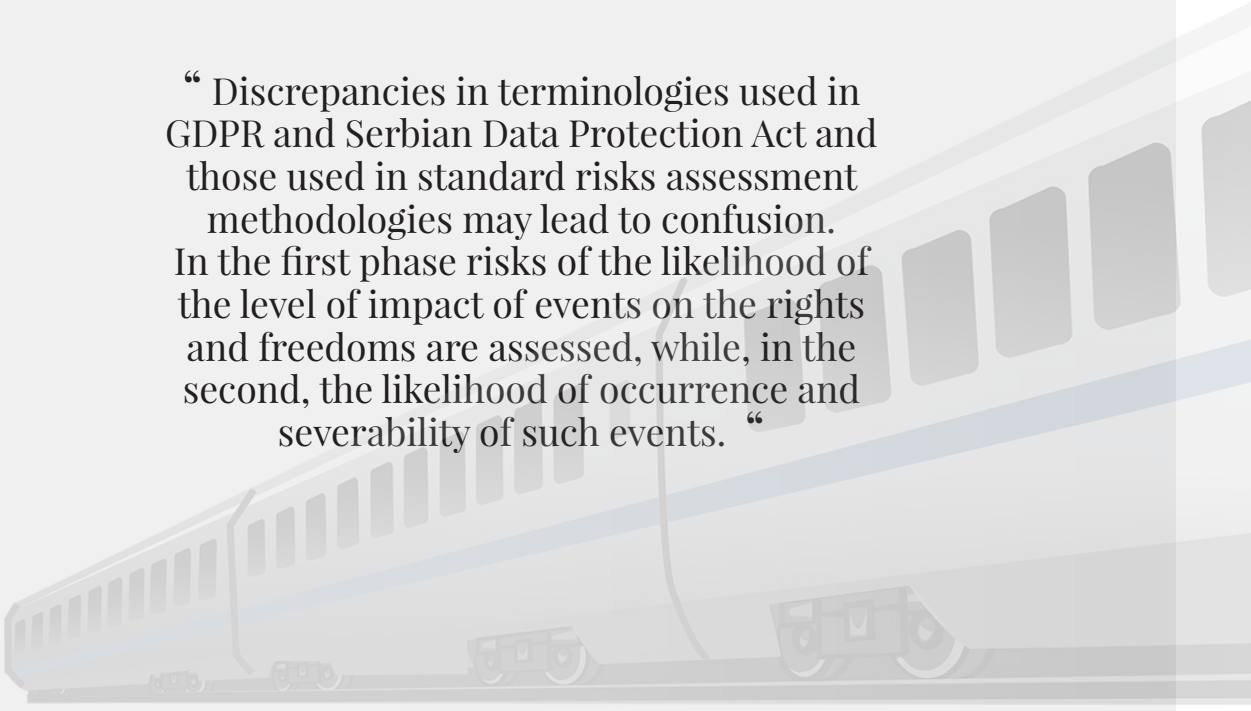
The severity of possible damage to the rights and freedoms of natural persons is evaluated by taking into account the nature, scope, context and purposes of the processing. It is important for controllers, i.e., employees responsible for and work in processing activities to form and discuss the list of scenarios of possible damages for the rights of natural persons.

The nature of processing refers to types of processing and categories of personal data. The scope of processing relates to the quantity of personal data processed and of natural persons whose personal data are processed, including natural persons who may suffer the damage indirectly.

The context of processing relates to circumstances under which the processing is carried out – for example, whether personal data are collected from data subjects or from other persons/sources, or whether the processing is taking place in a public or private place.
The purposes of processing are important, for example, in the case when the controller evaluates whether the intended purpose of processing is compatible with the purposes for which personal data are collected.

After completion of risk assessment, risks shall be classified and adequate measures defined and implemented to mitigate the risks to an acceptable level.

“ Discrepancies in terminologies used in GDPR and Serbian Data Protection Act and those used in standard risks assessment methodologies may lead to confusion. In the first phase risks of the likelihood of the level of impact of events on the rights and freedoms are assessed, while, in the second, the likelihood of occurrence and severability of such events. “



C. Discrepancy in terminology

There is a discrepancy between the terminology used in GDPR and Serbian Data Protection Act and the terminology used for standard risk assessment methodologies. The GDPR uses the formulation “risks of varying likelihood and severity for the rights and freedoms of natural persons”.

The terms used in GDPR and Serbian Data Protection Act have been used in a more descriptive manner in standard risks assessment methodologies:

i. risk of likelihood of impact of the event for rights and freedoms of natural persons and

ii. likelihood of occurrence and severity of the event.

The obligation of the controller in Art. 24 of GDPR, i.e., Art. 41 of the Serbian Data Protection Act is expanded in Art. 32 of GDPR, i.e., Art 50 of the Serbian Data Protection Act and Art. 35 of GDPR, i.e., Art. 54 of the Serbian Data Protection Act.

D. Security of processing – risk assessment

Art. 32 of GDPR, i.e., Art. 50 of the Serbian Data Protection Act defines the obligation of the controllers and processors to define and implement adequate data security measures to protect personal data from an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.
“While data protection predominantly lays down requirements related to the autonomy of the individual to protect his personal data, data security has a mission to prevent unauthorised access to personal data as well as to enable integrity and availability of personal data through technical and organisational measures.”

Data protection deals with legal requirements for processing, while data security deals with the technical and organisational framework in which the processing of personal data can be carried out.

According to the methodology recommended by the European Union Agency for Cybersecurity (ENISA), risk assessment of the security of processing is twofold:

a. assessment of the impact of unauthorized disclosure (loss of confidentiality), unauthorized alteration (loss of integrity), and unauthorized destruction or loss (loss of availability) of personal data on the individual;

b. assessment of threats and their likelihood in the following data processing environment (business areas of the controller):

i. network and technical resources (hardware and software);
ii. processes/procedures related to the processing activities;
iii. different parties and people involved in the processing activity; iv) business sector and scale of the processing.

After evaluating the impact of the processing activities and the relevant threat occurrence probability, the final evaluation of risk is possible by multiplying the highest risk levels from both evaluations.

E. Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is carried out in cases when the first assessment shows that certain types of processing are likely to result in a high risk to the rights and freedoms of natural persons or in cases where such assessment is explicitly required by GDPR and Serbian Data Protection Act.

The notion “Data Protection Impact Assessment” itself indicates that the subject of this assessment is an assessment of the existing protection for rights and freedoms of natural persons, i.e., that this assessment is carried out in case the first (existing) assessment and measures determined and implemented cannot mitigate high risks determined. Thus, different methodologies shall be used with the DPIA to assess risks and to define and implement additional measures.

In cases when GDPR and Serbian Data Protection Act obliges controller to carry out Data Protection Impact Assessments (Art, 35 para 3 of GDPR and Art 54 para 4 of Serbian Data Protection and Decision of the Commissioner on Types of Processing for Which Data Protection Impact Assessment Must be Carried Out and the Prior Opinion of the Commissioner Asked (“Official Gazette RS” Nos. 45/2019 and 112/2020), controllers do not carry out risks assessment described above.

When the controllers use artificial intelligence systems (AIS) in processing activities, Data Protection Impact Assessment is more complex, as it includes a risk assessment of AIS which the controller himself is not able to carry out without the provider of AIS (supplier or producer). This topic will be discussed in our next article.

JPM & Partners
8a Vladimira Popovića,
DELTA HOUSE, V Floor
11070 Belgrade, Serbia
T:+ 381/11/207-6850
E: office@jpm.law

www.jpm.law