



**SERBIA: DATA PROTECTION
IMPACT ASSESSMENT – UPDATES**

JPM

JANKOVIĆ POPOVIĆ MITIĆ

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

The Serbian SA provides clear guidance in his opinions on all relevant parts of data protection impact assessment (DPIA) and legitimate interest assessment. It can be concluded that controllers have serious problems to carry out DPIA.

In this article, we analyse all steps to be performed by controllers to carry out DPIA and legitimate interest assessment and, avoid penalties and measures, such as temporary or permanent prohibition to process personal data.


SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

On the occasion of the Data Protection Day, Serbian SA issued the most comprehensive publication insofar and revealed several opinions on DPIAs, including legitimate interest assessment as part of DPIA which have been submitted to him for the purpose of consultation. The general impression from the opinions is that controllers do not understand:

- how to evaluate and justify the legitimate interest as adequate legal ground for processing;
- whether intended processing is proportionate and necessary to the intended purpose of processing and
- how to evaluate risks for rights and freedoms of data subjects and other persons and determine and implement adequate technical and organisational measures (TOMs) and legal measures to mitigate identified risks to acceptable level.

Moreover, it seems that controllers do not understand in which cases they are obliged to consult SA in regard to DPIA.

We are really curious how and whether controllers acted in accordance with recommendations of the Serbian SA in regard to submitted DPIAs for consultation. Especially for the reason that the Serbian SA is authorised to impose penalty up to 10% of the annual controller's revenues gained in the previous business year in case they do not comply with instructions of the Serbian SA.

A black and white photograph showing a hand holding a dark sign with the words 'PRIVACY PLEASE' in white, bold, sans-serif capital letters. The hand is positioned in front of a door, with a silver door handle and keyhole visible above the sign. The background is a light-colored door with vertical paneling.

The Serbian SA provides clear guidance in his opinions on all relevant parts of data protection impact assessment (DPIA) and legitimate interest assessment. It can be concluded that controllers have serious problems to carry out DPIA.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

I When Controller shall carry out DPIA and what is the scope of DPA

Serbian Data Protection Act (“the Act”) prescribes that, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. DPIA shall, in particular, be required in the case of:

1. a systematic and extensive evaluation of personal aspects relating to natural persons which are based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories or of personal data relating to criminal convictions and offences; or
3. systematic monitoring of a publicly accessible area on a large scale.

In June 2019 Serbian SA rendered Decision on List of Types of Processing Operations for Which Data Protection Impact Assessment Must Be Carried Out and the Commissioner for Information of Public Importance and Protection of Personal Data Consulted (“Official Gazette RS” Nos. 45/2019 and 112/2020). This document specifies types of processing operations that are likely to result in high risks for rights and freedoms of data subjects, i.e. when the controller must carry out DPIA and cases when controllers must submit DPIA to Serbian SA for consultation.



The Act further specifies that DPIA shall contain:

1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
3. an assessment of the risks to the rights and freedoms of data subjects; and
4. the measures envisaged addressing the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.



II Key elements of DPIA

Controllers must describe intended processing operations and purposes of the processing.

1. Processing operations

In accordance with Art. 4, a processing means any operation or set of operations that is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Controllers must describe intended processing, i.e., intended set of operations which are likely to result in high risks for rights and freedoms of data subjects – whether they intend to collect personal data and in which manner and from which sources or they are to use personal data which have been already collected. Further, they must explain each further processing operation: for example: if they intend to store personal data – where and how and if they intend to disclose personal data – whom internally and externally and how; how they are to use personal data, etc.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

b) Purposes of processing

Controllers must concisely explain the purposes of the processing. The purposes must be specified, explicit and legitimate.

For example:

- if the controller intends to collect, store and use personal data by introducing access management software – the controller must explain why such processing is to be carried out - improving the protection of persons and property in the controller's premises. The purpose of processing is not the protection of persons and property in the controller's premises as there are many manners to protect people and property;
- if the controller intends to use personal data collected and stored by the access management system to calculate salaries, then the purpose of processing is – an efficient calculation of salaries. The purpose of processing is not improvement of HR management;
- if the controller intends to use software for remarketing, the purpose of processing is efficient adjusted of the products/services to the needs of the customer. The purpose of processing is not profit increase or increase of number of customers.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

B. Legitimate Interest

Last year, the Serbian SA issued legitimate interest guidance and a model for legitimate interest assessment. In its opinions on DPIA, it is clearly noted that it is not sufficient to state legitimate interest in DPIA as the legal ground for intended processing but to assess: i) whether the legitimate interest of controller to process personal data really exists; ii) whether the intended processing is really necessary and iii) whether legitimate interests of the controller or third party are overridden by the interests or fundamental rights and freedoms of the data subject. In case the controllers rely on legitimate interest, they are recommended to use the said model for legitimate interest assessment, in accordance with the accountability principle and take into consideration the following:

- a) Whether the legitimate interest of the controller to process personal data really exists

As a first step, controllers shall evaluate which positive goals are intended to be achieved by processing on the ground of the legitimate interest. The goals which are to be achieved shall be specific, i.e., not too broadly defined. For example: using formulations such as: “profit increase”, “granting benefits to employers or employees” are not acceptable.

The following questions shall be taken into consideration by the controller when they evaluate whether legitimate interest exists:

- why does the controller intend to process certain data;
- which benefits does the controller expect to achieve by intended processing;
- would anyone else benefit from the intended processing;
- would the wider community have benefited from the intended processing;
- are expected benefits that much important for the controller;
- what consequences would occur in case the controller gives up intended processing, etc.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

For example: whether tracking of employees' work by means of having the insight into their correspondence at work would really improve productivity at work, or such processing would create more uncertainty at work and expose employees to fear and cause less productivity.

Is it really necessary to track communication of employees to increase productivity or, it is sufficient to make an arrangement with employees to perform a certain task and instruct the employee to provide reports on work done and part of work that remains to be done? Whether the problem of productivity at work can be increased by granting bonuses to employees?

In cases when the employer intends to track the location data of employees by using GPS application to ensure effective deliverance of goods to its suppliers, whether such processing really helps him to determine the exact location of the employee or, tracking of the employee at best can indicate that company vehicle was in the vicinity of the target location?

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

b) Whether the intended processing is really necessary?

The controllers shall evaluate whether the intended processing based on the legitimate interest is really necessary. In other words, the controllers shall evaluate whether the intended processing really helps them to achieve their goals and whether the intended goals can be achieved by less intrusive measures.

For example: can we check whether the employees really delivered our goods to our suppliers by contacting our suppliers, or do we need permanent GPS location tracking or one-time GPS location tracking?

Do we really have to introduce a time management system to control time spent at work or, we could consider the use of other means, such as increased control by superiors?

Do employees really need to process photos of employees or unique identification numbers of visitors to identify them using an access management system?

Also, whether employers really have to match personal data obtained from the time management system with software for salary calculation or, is there any other less intrusive measure to fulfill the intended purpose?

Controllers shall consider the possibilities to achieve their goals and propose processing by applying technics of pseudo-anonymization or anonymization, if possible.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

c) Whether legitimate interests of the controller or third party are overridden by the interests or fundamental rights and freedoms of the data subject?

When assessing this matter, the controller shall consider the following factors:

1. Processing of special categories of personal data and sensitive data

The controller shall bear in mind that processing of special categories of personal data and other sensitive data (personal data on criminal offenses and convictions, financial data, minors' data, and data of other vulnerable groups) indicates the possibility of greater intrusiveness into privacy and probability that interests or fundamental rights and freedoms of the data subject override legitimate interests of controllers.

2. Reasonable expectations of data subjects

Controllers must evaluate whether data subjects, whose personal data are to be processed on the ground of legitimate interest, can expect that their personal data are to be processed. The logic is simple: if data subjects do not expect that their personal data will be processed, the possibility to lose control over their data is more significant. The following factors shall be taken into account:

- Whether the controller already processes personal data of particular data subject and on which legal basis;
- whether the controller and data subject are in a certain relationship and, whether such relationship implies a higher degree of confidentiality (for example doctor-patient);
- whether personal data are collected directly from the data subject or another source;
- which information regarding processing has been provided by the controller to a data subject when collecting data, or subsequently if the data was not collected from the persons involved;
- how much time has passed since the data collection;

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

3. Evaluation on possible consequences on rights and freedoms of data subjects

The controller shall evaluate risks of the possible impact of intended processing on right to protection of personal data, right to privacy, and on other rights such as: right to freedom of expression, right to freedom of thought, consciousness and religion, freedom of movement, forbiddance of discrimination and other human rights, as well as possible material and/or immaterial loss, loss of control over personal data and similar.

As a first step, controllers must analyse sources of possible consequences – risks for rights and freedoms of data subjects, i.e.:

- level of probability of impact to rights and freedoms and
- level of probability of threats occurrence for rights and freedoms.

Sources of threats shall be analysed in the context of equipment intended to be used for processing, manner of processing (manual, semi-automated or automated processing), persons having access to personal data, the lawfulness of processing, social values, etc.

Based on the probability of possible threats to occur and the probability and severability of potential consequences, the controller must assess the level of risks for data subjects to exercise the right to data protection and other rights mentioned above and define adequate TOMs and legal measures to mitigate risks identified to an acceptable level.

For example: if personal data from access management software are transferred to software for calculation of salaries and used for calculation of salaries, the controller shall evaluate the risk of such automated processing to possible discrimination of employees – whether and to what extent the human intervention is involved in such automated processing.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

Or, if the controller uses software for remarketing operated by the processor, the controller shall evaluate whether data subjects are provided with the possibility to provide granular consent for such processing, which TOMs are applied by the processor, and whether personal data are transferred to the processor which is located in the third country and if the controller has carried out a transfer impact assessment, etc.

B Proportionality and necessity of the intended processing in relation to the intended purpose of processing

In this part, the controller must justify the proportionality and necessity of the intended processing in relation to the intended purpose of processing. In practice, this means that controllers shall provide arguments and documents that they complied in their businesses with data protection principles and that intended processing is necessary to fulfill the intended purpose.

For example, the controller must act in accordance with data minimisation principle. In relation to the intended purposes, this means that personal data, that the controller collects or has already collected and intended to use for other purposes, is:

- adequate – personal data which help him to implement the intended purpose (sufficient to fulfill the intended purpose properly);
- relevant – personal data which are in logical connection to the intended purpose (personal data really needed to fulfill the intended purpose);
- limited to what is necessary in relation to the intended purpose – personal data are reviewed periodically and deleted if not needed to fulfill the intended purpose.

For example, a photo of an employee is adequate for access management control as it helps the controller to identify the person. On the other side, this personal data may not be relevant as the person may be identified with other personal data, such as name and surname and a number of an identity document.

SERBIA: DATA PROTECTION IMPACT ASSESSMENT – UPDATES

As a further example, the controller must comply with the lawfulness and transparency principle which means to apply adequate legal ground for processing and that processing is not contrary to applicable regulations, as well as that data subjects are informed on processing and enabled to exercise their rights.

In addition to this, the controller must justify that intended processing is necessary to fulfill the intended purposes. For example – why are tracking of location data by GPS systems, processing personal data by access management software, monitoring of computers or correspondence of employees or, processing personal data of potential customers at social networks, as well as matching personal data from access management software with software for calculation salaries, necessary to achieve the intended purposes and why there are no less intrusive measures to the fulfill these purposes.

C. Evaluation of risks and implementation of adequate TOMs

It can be concluded from the opinions of the Serbian SA that controllers are free to choose any adequate methodology to assess the risks for rights and freedoms of data subjects and accordingly, to implement the adequate TOMs and legal measures to mitigate identified risks to the acceptable level.

We have successfully evaluated risks and implemented adequate TOMs applying the ENISA Model for evaluation of risks for the security of processing – in regard to DPIA, the focus is on risks for rights and freedoms of the data subject.



JPM Jankovic Popovic Mitic

8a Vladimira Popovića,
DELTA HOUSE
11070 Belgrade, Serbia
T:+ 381/11/207-6850
E: office@jpm.rs

www.jpm.rs