



International Data Protection Conference

HOW TO MANAGE GDPR CHALLENGES EFFECTIVELY?

DATA PROTECTION PRINCIPLES

Ivan Milosevic, Partner, JPM Janković Popović Mitić

Belgrade, November 14th, 2019

Introductory Notes

individual's rights

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; **it must be considered in relation to its function in society** and be balanced against other fundamental rights, in accordance with the principle of proportionality (Recital (4) GDPR).

Article 8 of EU Charter of Fundamental Rights:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

legitimate interests

independent authority



Lawfulness, Fairness and Transparency

Lawfulness

After you make decision to achieve certain business goal/s, you have to have to opt for one of six lawful ground for processing of personal data:

- i. Consent of data subject to processing personal data for one or more specific purposes;
- ii. Necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- iii. Necessity for compliance with a legal obligation to which you are subject;
- iv. Necessity in order to protect the vital interests of the data subject or of another natural person;
- v. Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- vi. Necessity for the purposes of the legitimate interests pursued by you or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Serbian Data Protection Act – lawful processing is processing performed in accordance with Data Protection Act or in accordance with the Law governing such processing.

Lawfulness, Fairness and Transparency

Fairness

- fair (Merriam Webster Dictionary) - in a manner that is honest or impartial or that conforms to rules : in a fair manner;
- you cannot process personal data misleading citizens or causing them detriment or against data subjects' reasonable expectations;
- your processing shall not have any unjustified adverse impact on the data subjects;
- The Article 29 Working Party Guidelines on profiling of 2018, providing a concrete example in this regard:

“A data broker sells consumer profiles to financial companies with(out) consumer permission or knowledge of the underlying data. The profiles define consumers into categories (carrying titles such as **“Rural and Barely Making It,” “Ethnic Second-City Strugglers,” “Tough Start: Young Single Parents,”**) or “score” them, focusing on consumers’ financial vulnerability. The financial companies offer these consumers payday loans and other “non-traditional” financial services (high-cost loans and other financially risky products) “.

Lawfulness, Fairness and Transparency

Transparency

- the provision of information to data subjects related to fair processing (Articles 23 and 24 of the LPDP);
- how data controllers communicate with data subjects in relation to their rights (Article 26-37 of the LPDP) and
- how data controllers facilitate data subjects to exercise their rights (Article 21 of the LPDP);
- Being transparent means to gain trust in processes which affect the citizens by enabling them to understand, and if necessary, challenge those processes;
- empowers data subjects to hold data controllers and processors accountable;
- empowers data subjects to exercise control over their personal data;
- applies at the following stages of the data processing cycle:
 - i) before or at the start of the data processing cycle;
 - ii) throughout the whole processing period;
 - iii) at specific points while processing is ongoing.

Lawfulness, Fairness and Transparency

Transparency

- information shall be provided in “concise and transparent” manner (use of a layered privacy statement/ notice);
- intangible information;
- what the scope and consequences of the processing produces;
- particular risks for natural persons;
- easily accessible;
- clear and plain language:

“We may use your personal data to develop new services.” (as it is unclear what the “services” are or how the data will help develop them);

“We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in.”

“We may use your personal data for research purposes” (as it is unclear what kind of “research” this refers to);

“We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive”

Lawfulness, Fairness and Transparency

Transparency

- language qualifiers shall be avoided;
- In writing or by other means;
- the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document;
- the information may be provided orally;
- free of charge;
- appropriate measures will need to be assessed in light of the product/ service user experience;

Exceptions:

- where and insofar as, the data subject already has the information;
- the provision of such information is impossible or would involve a disproportionate effort would make the achievement of the objectives of the processing impossible or seriously impair them;
- - the data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests;
- an obligation of professional secrecy.



LAWFULNESS, FAIRNESS,
TRANSPARENCY



PURPOSE
LIMITATION



DATA
MINIMIZATION



ACCURACY



INTEGRITY,
CONFIDENTIALITY



STORAGE
LIMITATION

Purpose Limitation

- personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

Exception:

further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 92 of the LPDP

- pre-requisite for applying other data protection principles;
- transparency – user control, predictability, adequate safeguards and legal certainty vs. practical approach;
- specified – sufficiently defined - 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' are not specified purposes
- explicit - sufficiently unambiguous and clearly expressed vs. hidden purpose;
- legitimate – lawful;
- the prohibition of incompatible use sets a limitation on further use;

Purpose Limitation

Further processing

- Compatibility is prima facie obvious;
- Compatibility is not obvious and needs further analysis:
 - the relationship between the initial purpose and the purpose of the further processing, and the context in which the data were collected;
- the reasonable expectations of the data subjects as to their further use;
- the nature of the data and the impact of the further processing on the data subjects;
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.



LAWFULNESS, FAIRNESS,
TRANSPARENCY



PURPOSE
LIMITATION



DATA
MINIMIZATION



ACCURACY



INTEGRITY,
CONFIDENTIALITY



STORAGE
LIMITATION



Data Minimization/Accuracy/Storage Limitation

Recital 39 of GDPR: The personal data should be ***adequate, relevant and limited to what is necessary for the purposes for which they are processed***. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

- i) **Adequate:** The data that you are gathering is what you require in order to fulfil your stated purpose;
- ii) **Relevant:** The data that you are gathering has an obvious link to your target and this can be displayed upon review;
- iii) **Limited:** Only the necessary data will be gathered. No additional data that is not required will be gathered and held – you do not hold more than you need for that purpose.

Data Minimization/Accuracy/Storage Limitation

- Personal data shall be accurate and, where necessary, kept up to date;
- Right to rectification;
- Inaccurate personal data, having regard to the purposes for which they are processed, have to be erased or rectified without delay;
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Retention policy.



Integrity and Confidentiality

- Depending on the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, you have to adopt methodology for:
 - i) Security risk assessment;
 - ii) Assessment on impact of processing activities on rights and freedoms of natural persons.
- Once you adopt required methodologies, you have to implement them;
- Risk assessment shall result in recommendation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Integrity and Confidentiality

- Depending on the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, you have to adopt methodology for:
 - i) Security risk assessment;
 - ii) Assessment on impact of processing activities on rights and freedoms of natural persons.
- Once you adopt required methodologies, you have to implement them;
- Risk assessment shall result in recommendation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk.



Accountability

- key building block for effective privacy and data protection regulation;
- you have to implement a comprehensive privacy program governing all aspects of processing of personal data;
- you have to be able to verify and demonstrate the existence and effectiveness of such programs internally and externally;
- “corporate digital responsibility” fit for the 21st century and modern data driven economies:
 - i) ensures effective protection for individuals and their data;
 - ii) enables digital trust and responsible use, sharing and flows of data;
 - iii) facilitates appropriate individual choice and control over such information;
 - iv) translates principles-based legal rules into concrete policies, procedures, controls and governance to deliver compliance.

Accountability

Core elements of accountability:

- i) leadership and oversight;
- ii) risk assessment;
- iii) policies and procedures;
- iv) transparency;
- v. training and awareness;
- vi. monitoring and verification;
- vii. response and enforcement.



JANKOVIĆ POPOVIĆ MITIĆ

a member of **T****L****A** Top-tier Legal Adriatic

THANK YOU FOR YOUR ATTENTION

Vladimira Popovića 6
NBGP Apartments
11070 Belgrade (Serbia)
tel: + 381/11/207-6850
fax: +381/11/207-6899
office@jpm.rs

www.jpm.rs