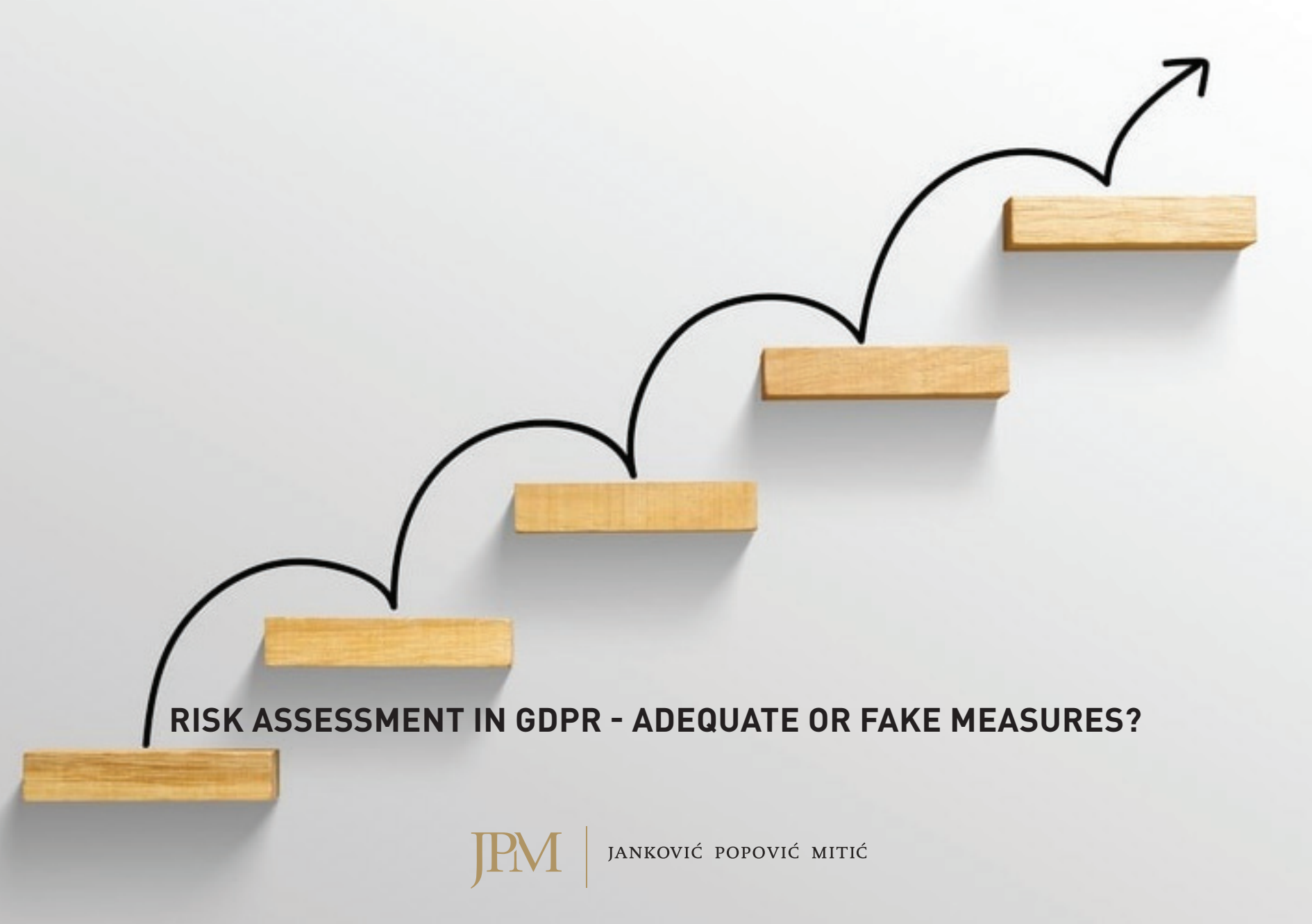

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

JPM | JANKOVIĆ POPOVIĆ MITIĆ

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?
Publisher: JPM Janković Popović Mitić
NBGP Apartmani, Vladimira Popovića 6
www.jpm.rs
Autors: Ivan Milošević, Partner, Andrea Cvetanović, Senior Associate and Prof. Phd. Gojko Grubor

Disclaimer:

The sole purpose of this publication is to provide information about specific topics.
It makes no claims to completeness and does not constitute legal advice.
The information it contains is no substitute for specific legal advice.

If you have any queries regarding the issues raised or other legal topics, please get in touch with your usual contact at JPM Jankovic Popovic Mitic.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

When advising organisations how to comply their businesses with GDPR, i.e., with the Serbian Law on Personal Data Protection, many times we received answers that organisations apply “best information security practices”. What does this formulation mean?

Up to our understanding, such formulation often stands for an excuse for non-compliance with GDPR. Controllers and processors must perform information security risk assessment and assess risks of business activities (processing activities) for personal data (assess security of processing of personal data) to be able to respond to risks for personal data and risks for rights and freedoms of data subjects, i.e., to apply adequate technical, organisational and legal measures to mitigate identified risks to acceptable level.

Those who are familiar with application of information security, Data Protection Directive and GDPR understand that information security is predecessor and corner stone of personal data protection. Security of information systems is integral part of GDPR compliance because information security systems are essential means for processing the personal data.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

To protect confidential business information, efforts of business community and information security experts resulted in adoption and implementation of information security standards. Organisations which had and still have business interest to protect confidential business information could and still can apply requirements defined in information security standards to secure their information systems. Efforts of these organisations should result in certification with information security standards, such as ISO/IEC 27001 – information security management standard (ISMS) from 2013. The key matter in certification process is that an independent accredited body verifies the state of art of information security system and approves security measures in practice. Certification means that any organisation and its business partners can rely on such certificate and be confident with level of information security.

However, organisations do not need to have ISMS certificate to protect their information security systems adequately. The pre-conditions for adequate protection of information security are that information security risk assessment based on adequate risk assessment methodology is performed and adequate measures proportional to such risk assessment are implemented. We have advised organisations to apply methodology defined in standard ISO/IEC 27005:2018.

CHECKLIST

When advising organisations how to comply their businesses with GDPR, i.e., with the Serbian Law on Personal Data Protection, many times we received answers that organisations apply “best information security practices”. What does this formulation mean?

.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

When we started receiving information from organisation that they use “best security practices” to protect their security information system, we were a bit confused. We were confused with the meaning of such formulation and how “best security practices”, can be applied to specific business environments where risks for information security vary in each case.

To cope with specific information security level, organisations must apply acceptable risk information methodology, and which measures for information security proportional to assessed risks shall be applied. Without information, security risk assessment, any “best security practices” cannot be verified in practice.

When starting to analyse state of art information security within organisations, we came to a conclusion that everybody was “applying best security practices”. We had an impression that organisations “hide” information security measures, practices and possible security breaches due to market competitiveness.

However, GDPR substantially changes such practice and imposes obligation for organisation to report data breaches to Supervisory Authority. Most organisations have information security policies, but never formally assessed risks for information security. Using “best security practices” without assessing information security risks is the same as when organisations use “know-how” which does not correspond to their real needs.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

For example, when organisation applies technical measures, such as firewalls, computers' and networks' scanners, IDS/IPS systems, real time log file scanners, vulnerability real system scanners and similar, these measures may be unnecessarily too expensive and not adequate to real risks for information.

In addition, organisational, operational and personal measures may be equally effective but much cheaper than technical measures.

On the other side, with rapid development of information technologies and processing of personal data, key stakeholders in Europe came to conclusion that ISMS does not treat protection of personal data sufficiently (primarily treats business data information) and for this reason adopted GDPR. For example, ISMS has nothing to do with processing personal data or profiling or monitoring behaviour of data subjects.

The crucial difference is that ISMS helps organisations implement system to protect security of information, while the focus of GDPR is how to use information security system to protect personal data.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

Such concept is summarised is Article 24 of GDPR:

"Taking into account:

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

the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

Those measures shall be reviewed and updated where necessary.

Where proportionate in relation to processing activities, the measures shall include the implementation of appropriate data protection policies by the controller."

Further, when obliging controllers and processors to ensure security of processing, which means not just security of information itself but security of any form of processing personal data, i.e., how information security system is used to process personal data, GDPR defines that, in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

These provisions shall be interpreted as follows:

Besides information security risk assessment, controllers shall consider additional risks sources for personal data (in GDPR: not just information security risks, but, in addition, security of processing of personal data):

1. Nature of processing – whether it is automated processing, semi-automated or manual processing. Automated processing or profiling may cause high risks for rights and freedoms of natural persons such as discrimination;
2. Scope of processing, meaning whether personal data are processed on a large scale or not;
3. Context of processing, meaning context of organisation which processes personal data, for example, the risk is more significant in organisation which sells goods online that in those which only produce food for animals;
4. Purposes of processing, meaning different purposes of processing may result in different level risks for personal data;
5. Organisation must assess "risk of varying likelihood and severity for the rights and freedoms of natural persons", meaning likelihood and severity of risk impact (breach of confidentiality, integrity and availability of personal data) multiplied by likelihood and severity of risk occurrence (sourced from four main business areas: information technology, processing activities, humans involved in processing and production sector itself). In addition, organisations must assess how breach of confidentiality, integrity and availability of personal data may affect rights and freedoms of data subjects.

RISK ASSESSMENT IN GDPR - ADEQUATE OR FAKE MEASURES?

For assessment of risks for personal data (security of processing), we apply the same risk assessment methodology as for information security risk assessment but with the focus to security of processing.

Example:

1. Nature of processing: automated processing or profiling of the personal data of clients in one part of the processing operation;
2. Context of organisation: a bank;
3. Scope of processing: one of the major players on the market;
4. Purpose of processing: to make decisions on request for granting loans.
5. Whether breach of confidentiality, integrity and availability of personal data of the clients is low, medium, high or very high and how those breaches may affect rights and freedoms of data subjects.

Based on the risks identified in both risk assessments (information security risk assessment and risk assessment for security of processing), we recommend and provide assistance to organisations to implement adequate organisational, technical and legal measures to mitigate risks identified to acceptable level.

Only when organisations implement adequate organisational and technical measures proportional to risks assessed, they can say they are complied with GDPR.

JPM Jankovic Popovic Mitic

6 Vladimira Popovića,
NBGP Apartments
11070 Belgrade, Serbia
T:+ 381/11/207-6850
E: office@jpm.rs

www.jpm.rs