DATA PROTECTION · GDPR · DPIA

Procena uticaja bezbednosti obrade i novi model EDPB za procenu uticaja obrade na zaštitu podataka o ličnosti

Security of Processing Impact Assessment and New EDPB Template for Personal Data Protection Impact Assessment

Dve strane iste medalje

Two Sides of the Same Coin

Rizici uticaja bezbednosti obrade za podatke o ličnosti (na zaštitu podataka o ličnosti) su u uskoj vezi sa rizicima koji su predmet procene uticaja obrade na zaštitu podataka o ličnosti. Bezbednost i zaštita su dve strane iste medalje jer se bezbednost postiže zaštitom. Kada su rizici od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti visoki, odnosno kada su identifikovani rizici takvi da mogu da proizvedu značajne posledice po prava i slobode lica čiji se podaci obrađuju, rukovaoci trebalo da razmotre mogućnost sprovođenja procene uticaja obrade na zaštitu podataka o ličnosti. Razmatranje potrebe za procenom uticaja obrade na zaštitu podataka o ličnosti se vrši u kontekstu svrha, prirode, konteksta i obima obrade. Sa druge strane, kada je procena uticaja obrade na zaštitu podataka o ličnosti obavezna prema GDPR ili prema nacionalnom zakonodavstvu, sastavni deo ove procene je i procena uticaja bezbednosti obrade za podatke o ličnosti – ovaj stav se potvrđuje u predloženim EDPB modelu za procenu uticaja obrade na zaštitu podataka o ličnosti.

Risks of impact of security of processing for personal data (protection of personal data) are closely related risks that are the subject of the data protection impact assessment. Security and protection are two flips of the same coin as the security is reached by protection. When the risks of accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data are high, i.e. when the identified risks are such that they can produce significant consequences for the rights and freedoms of data subjects, controllers shall be consider whether data protection impact assessment to be carried out. The need for the data protection impact assessment is considered in the context of the purpose, nature, context, and scope of the processing. On the other hand, when the data protection impact assessment is mandatory according to the GDPR or to national legislation, an integral part of this assessment is security of processing impact assessment – this attitude is confirmed by the EDPB proposed template for data protection impact assessment.

Šta procenjuju rukovaoci i obrađivači

What Controllers & Processors Assess

Da se podsetimo: suština procene uticaja bezbednosti obrade prema GDPR i prema nacionalnim zakonodavstvima država Zapadnog Balkana za koje se godinama pogrešno tvrdi da su usaglašena sa GDPR je u tome da rukovaoci i obrađivači procenjuju:

- verovatnoću stepena ozbiljnosti događaja - pretnji za bezbednost podataka o ličnosti i
- verovatnoću uticaja koji visoko rizične pretnje mogu da imaju za prava i slobode lica čiji se podaci obrađuju.

Let us recall: the essence of the security of processing impact assessment according to the GDPR and according to the national legislations of the Western Balkans countries, which it is for years falsely claimed to be compliant with the GDPR, is that the controllers and processors assess:

- probability of level of severity the events threat to the security of personal data and
- probability of impact that high-risk threats can have on the rights and freedoms of data subjects.

Ilustrativni primer

An Illustrative Example

Na primer: koliki je stepen verovatnoće događaja pretnje da podaci o ličnosti pacijenta dospeju u posed neovlašćenih lica, da ta lica izmene ove podatke o ličnosti ili da zadrže podatke o ličnosti i kakve posledice (verovatnoća uticaja) usled nastupanja neke od ovih pretnji (rizika) mogu da imaju lica čiji se podaci obrađuju.

For example: what is the level of probability of threat to occur that the personal data of the patients will come into the possession of unauthorized persons, that these persons will change this personal data or keep the personal data and what consequences (probability of impact) due to the occurrence of some of these threats (risks) data subjects may have.

Procena poverljivosti, integriteta i raspoloživosti

Assessing the CIA Triad

Stepen verovatnoće povrede CIA - poverljivosti, integriteta i raspoloživosti (ozbiljnosti (intenziteta) rizika, odnosno pretnji) se procenjuje u kontekstu vrste podataka koji se obrađuju, svrhe, prirode okolnosti i obima obrade. Stepen materijalizacije pretnji se procenjuje u kontekstu verovatnoće njenog nastupanja, a imajući u vidu obradu na internetu, mrežnoj infrastrukturi, sistemima i uređajima, procesima i procedurama za upravljanje podacima o ličnosti u kompaniji, zaposlenih i angažovanih trećih lica koja vrše obradu ii radnog okruženja za obradu podataka o ličnosti i obima obrade podataka o ličnosti (aplikativni nivo obrade).

The level of probability of CIA violation - confidentiality, integrity and availability (severity, i.e. intensity of risk, i.e. threat) is assessed in the context of the type of data being processed, the purpose, nature, context and scope of processing. The level of materialization of the threats is assessed in the context of the probability of its occurrence, taking into account the processing on the internet and network infrastructure, systems and devices, processes and procedures for managing personal data in the company, employees and engagement of third parties processing personal data and the work environment for personal data processing and the scope of personal data processing (applicative level of processing).

ENISA matrica nivoa uticaja

The ENISA Impact Matrix

Prema Uputstvu Evropske agencije za mreže i informacionu bezbednost (ENISA) za mala i srednja pravna lica za bezbednost obrade iz decembra 2016. godine, u proceni rizika za bezbednost obrade procenjuje se stepen verovatnoće nastupanja pretnji (rizika) i verovatnoće uticaja rizika – povrede poverljivosti, integriteta i raspoloživosti na prava i slobode građana prema sledećoj matrici za nivoe uticaja:

According to the Guidelines of the European Network and Information Security Agency (ENISA) for SMEs on the Security of Processing from December 2016, in the risk assessment for processing security, the level of probability of occurrence of threats (risks) and probability of risks impact - violations of confidentiality, integrity and availability to the rights and freedoms of citizens is assessed according to the following matrix for levels of impact:

Nivoi uticaja — nizak i srednji

Impact Levels — Low & Medium

- nizak uticaj - lica čiji se podaci se obrađuju mogu da se suoče sa nekoliko manjih neprijatnosti, koje će prevazići bez ikakvih problema (vreme provedeno u ponovnom unosu informacija, smetnje, iritacije itd.);
- srednji uticaj - lica čiji se podaci se obrađuju mogu da se suoče sa značajnim neprijatnostima, koje će moći da prevaziđu uprkos nekim poteškoćama (dodatni troškovi, uskraćivanje pristupa poslovnim uslugama, strah, nedostatak razumevanja, stres, manje fizičke tegobe itd.);

- low impact – dana subjects may face several minor inconveniences, which they will overcome without any problems (time spent re-entering information, interference, irritation, etc.);
- medium impact - persons whose data are processed may face significant inconveniences, which they will be able to overcome despite some difficulties (additional costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.);

Nivoi uticaja — visok i vrlo visok

Impact Levels — High & Very High

- visok uticaj - lica čiji se podaci se obrađuju mogu da se suoče sa značajnim posledicama koje bi trebalo da budu u stanju da prevaziđu sa ozbiljnim poteškoćama (pronevera sredstava, stavljanje na crnu listu od strane finansijskih institucija, šteta na imovini, gubitak posla, sudski sporovi, pogoršanje zdravlja itd.);
- vrlo visok uticaj - lica čiji se podaci se obrađuju mogu da se suoče sa značajnim ili neotklonjivim posledicama nepovratne posledice koje možda neće moći da prevaziđu (nemogućnost za rad, dugotrajne psihološke ili fizičke tegobe, smrt itd.).

- high impact – dana subjects may face significant consequences that they should be able to overcome with serious difficulties (embezzlement of funds, blacklisting by financial institutions, damage to property, loss of job, lawsuits, deterioration of health, etc.);
- very high impact - persons whose data are processed may face significant or irreversible consequences that they may not be able to overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Fokus procene uticaja (DPIA)

The Focus of a DPIA

Sa druge strane, u proceni uticaja obrade na zaštitu podataka o ličnosti (DPIA) je fokus na proceniverovatnoće nastupanja rizika koje proizilaze iz obrade podataka o ličnosti i proceni uticaja takve obrade na prava i slobode lica čiji se podaci obrađuju. Procenjuju se i rizici koji ne potiču od same planirane obrade podataka o ličnosti već i rizici koji su posledica zaštite (bezbednosti obrade); na primer slučajnih (greške i ranjivosti sredstava za obradu) i nezakonitih događaja, (na primer hakerski maliciozni napadi) tj. rizici van planirane obrade.

On the other hand, in the data protection impact assessment (DPIA), the focus is on the assessment of the probability of the occurrence of risks arising from the processing of personal data and the assessment of the impact of such processing on the rights and freedoms of the person whose data is processed. Risks that do not originate from the planned processing of personal data are also assessed - risks that are a consequence of protection (security of processing); for example of accidental (mistakes and vulnerabilities of means of processing) and illegal events (for example: hacker malicious attacks)., i.e. risks outside of planned processing.

EDPB definicije: Rizik

EDPB Definitions: Risk

Prema EDPB Predlogu objašnjenja modela za DPIA:

Rizik (pretnja) je bilo koja okolnost ili događaj sa potencijalno štetnim uticajem na prava i slobode lica čiji se podaci obrađuju (na primer: povezivanje, identifikacija, netačnost ili otkrivanje podataka) i može da prouzrokuje fizičku, materijalnu ili nematerijalno štetu licima čiji se podaci obrađuju.

According to the EDPB Proposal Explainer of the Template for DPIA:

Risk (threat) is any circumstance or event with a potentially harmful impact on the rights and freedoms of persons whose data is processed (for example: connection, identification, inaccuracy or disclosure of data) and may cause physical, material or non-material damage to dana subjects.

EDPB definicije: Izvor rizika i uticaj

EDPB Definitions: Source & Impact

Izvor rizika je poreklo ili osnovni uzrok iz kojeg pretnja može da se materijalizuje.

Uticaj su posledice koje se mogu očekivati od materijalizacije pretnje, uvek uzimajući u obzir prava i slobode lica čiji se podaci obrađuju (tačka Preambule 75 GDPR).

Source of the risk is the origin or root cause from which the threat can materialize.

Impact is the consequences that can be expected from the materialization of the threat, always taking into account the rights and freedoms of data subjects (recital 75 of the GDPR).

Dve grupe izvora rizika

Two Groups of Risk Sources

Izvori rizika se dele u dve grupe:

- Rizici koji proističu iz same planirane obrade, na primer: iz svrha obrade, podataka koji se obrađuju, neophodnosti i proporcionalnosti obrade, prirode, obima i konteksta obrade, na primer, bezbednosti sredstava za obradu, grešaka u dizajnu i konfigurisanju sredstava za obradu (korišćenje jedinstvenih identifikatora ili dugi periodi čuvanja), izloženost, itd.;
- Rizici koji proističu iz slučajnih, nezakonitih ili abnormalnih događaja – na primer: pretnje koje predstavljaju odstupanja od dizajna i podrazumevanih podešavanja (na primer, dizajna softverskih aplikacija), namerne pretnje za poverljivost, integritet i dostupnost podataka i sl.

Sources of risk are divided into two groups:

- Risks arising from the planned processing itself, for example: from the purposes of the processing, the data being processed, the necessity and proportionality of the processing, the nature, scope and context of the processing, for example: security of means of processing, errors in the design and configuring of the means of processing (use of unique identifiers or long storage periods), exposure, etc.;
- Risks arising from accidental, illegal or abnormal events - for example: threats that represent deviations from design and default settings (for example: design of software applications) threats to confidentiality, integrity and availability of data, etc.

Kada DPIA nije obavezna

When a DPIA Is Not Mandatory

Kada obaveza vršenja DPIA nije predviđena GDPR ili nacionalnim zakonodavstvom i ukoliko procena rizika bezbednosti obrade rezultira visokim rizicima od povrede poverljivosti, integriteta i raspoloživosti podataka o ličnosti, može postojati indikator da je potrebno da se sprovede procena uticaja na zaštitu podataka o ličnosti. Na primer, sama činjenica da postoji visok rizik od neovlašćenog pristupa visoko rizičnim osetljivim podacima pacijenata u slučaju kada nije reč o obradi u velikom obimu ukazuje da je potrebno da se sprovede DPIA.

When obligation to carry out DPIA is not prescribed by GDPR or national legislation and if a security of processing risk assessment results in high risks of breaching the confidentiality, integrity and availability of data, there may be a clear indicator that a personal data protection impact assessment needs to be carried out.
For example, the very fact that there is a high risk of unauthorized access to high risk sensitive patient data in the case where it is not a question of processing on a large scale indicates that it is necessary to carry out the DPIA.

Identifikacija rizika i mere ublažavanja (u slučajevima kada DPIA nije obavezna)

Identifying Risks & Mitigation (in cases when DPIA is not obligatory)

U DPIA se identifikuju rizici i predlažu mere koje bi mogle da ublaže rizik od uticaja bezbednosti obrade na povredu podataka. Na primer: da li bi sprovođenje principa neophodnosti i proporcionalnosti ili principa podrazumevane ili predefinisane zaštite sredstava za obradu moglo da ublaži rizike od povrede poverljivosti, integriteta i raspoloživosti podataka. U slučaju sprovođenja principa podrazumevane i predefinisane zaštite se procenjuje da li su sistemi za obradu dizajnirani i konfigurisani na način da zadovoljavaju zahteve standarda o informacionoj bezbednosti, a imajući u vidu sve parametre obrade podataka o ličnosti.

In DPIA risks are indenfied and measures that could mitigate risks from impact of security of processing to data breaches are proposed. For example: whether the implementation of the principles of necessity and proportionality or the principles of privacy by design and default of means of processing could mitigate the risks of breach of confidentiality, integrity and availability of data. In the case of implementing the principles of privacy by design and defaut, it is assessed whether the processing systems are designed and configured in a manner that meets the requirements of information security standards, taking into account all parameters of personal data processing.

Pravni osnov: Odluka Poverenika

Legal Basis: The Commissioner's Decision

U prilog navedenoj tvrdnji, navodimo sledeće:

Tačkom 3 Odluke Poverenika o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti DPIA i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti ("Sl. glasnik RS", br. 45/2019 i 112/2020) propisano je da je, osim u slučajevima iz tačke 2. ove odluke (slučajevi kada je odlukom propisano da je rukovalac dužan da sprovede DPIA), rukovalac obavezan da DPIA i u drugim slučajevima ako je verovatno da će neka vrsta obrade, posebno upotrebom novih tehnologija (na primer: rešenja AI za automatizovanu obradu) uzimajući u obzir prirodu, obim, okolnosti i svrhu obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica.

In support of this claim, we state the following:

Point 3 of the Commissioner's Decision on the list of types of processing of personal data for which DPIA must be carried out and the opinion of the Commissioner for Information of Public Importance and Protection of Personal Data asked ("Official Gazette of RS", no. 45/2019 and 112/2020) is stipulated that, except for the cases from point 2 of this decision (cases when the decision stipulates that the controller is obliged to carry out the DPIA), the controller is obliged to carry out DPIA and in other cases if it is likely that some type of processing, especially with the use of new technologies (for example: AI solutions for automated processing) and taking into account the nature, scope, circumstances and purpose of the processing, will cause a high risk to the rights and freedoms of natural persons.

Pravni osnov: član 50

Legal Basis: Article 50

Smatramo je da upravo reč o tome da je rukovalac u svakom slučaju, u skladu sa članom 50 Zakona o zaštiti podataka o ličnosti, u obavezi da izvrši procenu rizika bezbednosti obrade. Ovu tvrdnju zasnivamo na činjenici da članom 50 Zakona o zaštiti podataka o ličnosti propisano da, u skladu sa nivoom tehnoloških dostignuća i troškovima njihove primene, prirodom, obimom, okolnostima i svrhom obrade, kao i verovatnoćom nastupanja rizika i nivoom rizika za prava i slobode fizičkih lica, rukovalac i obrađivač sprovode odgovarajuće tehničke, organizacione i kadrovske mere kako bi dostigli odgovarajući nivo bezbednosti u odnosu na rizik.

Ukoliko procena pokazala da postoji visok rizik od povrede CIA i imajući u vidu prirodu, obim, okolnosti i svrhu obrade, rukovalac bi trebalo da razmotri opciju da li bi sprovođenje DPIA moglo da identifikuje rizike i rezultira merama koje bi mogle da oblaže rizike za povredu CIA.

We believe that it is precisely the fact that the controller is in any case, in accordance with Article 50 of the Law on Protection of Personal Data obliged to carry out a security of processing risk assessment. We base this claim on the fact that Article 50 of the Law on Protection of Personal Data prescribes that, according to 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

If this assessment showed that there is a high risk of a CIA breach, and considering the nature, scope, circumstances, and purpose of the processing, the controller should consider whether carrying out a DPIA could identify risks and result in measures that could mitigate the risks of a CIA breach.

Zaključak

Conclusion

Rizici za prava i slobode lica čiji se podaci obrađuju u velikom broju slučajeva nastupaju upravo usled visokog rizika od nastupanja povrede (gubitka) poverljivosti, integriteta i raspoloživosti podataka o ličnosti. Za ublažavanje ovih rizika potrebno da se razmotri mogućnost da li bi sprovođenje DPIA moglo da ublaži identifikovane bezbednosne rizike (bez obzira na to što u konkretnom slučaju GDPR ili nacionalno zakonodavstvo ne propisuje DPIA kao obaveznu).

U slučajevima kada je DPIA GDPR ili nacionalnim zakonodavstvom propisana kao obavezna, procena bezbednosti obrade je sastavni deo DPIA, a što se potvrđuje predloženim EDPB modelom DPIA.

Risks for the rights and freedoms of data subjects in a large number of cases occur precisely because of the high risk of breach (loss) of confidentiality, integrity and availability of personal data. To mitigate these risks, it is necessary to consider whether carrying out of DPIA may mitigate identified security risks, regardless the fact that DPIA is not prescribed by GDPR or national legislation as obligatory.

In the cases when DPIA is prescribed by the GDPR or national legislation as obligatory, the assessment of the security of processing is an integral part of the DPIA, which is confirmed by the proposed EDPB DPIA template.

AUTOR TEKSTA · AUTHOR OF THE ARTICLE

Ivan Milošević

Partner · JPM Partners