




**Srpski voz ka EU – (ne)otklonjivi kvar na vozu
ili (s)kretanje u drugom pravcu?**

**Serbian Train to EU – (Ir)reparable Breakdown on the Train
or Turning/Moving in the Other Direction?**

JPM

PARTNERS



```
def save_contacts(contacts):
    with open(FILE_NAME, "wb") as file:
        pickle.dump(contacts, file)

def add_contact(contacts):
    name = input("Enter the contact's name: ")
    phone = input("Enter the contact's phone number: ")
    contacts[name] = phone
    print("Contact added!")

def remove_contact(contacts):
    name = input("Enter the name: ")
    del contacts[name]
    print("Contact removed!")

def list_contacts(contacts):
    for name, phone in contacts.items():
        print(f"{name}: {phone}")

def area_circle():
    radius = float(input("Enter the radius: "))
    area = area_circle(radius)
    print(f"The area of the circle is {area}")

def area_rectangle():
    length = float(input("Enter the length: "))
    width = float(input("Enter the width: "))
    area = area_rectangle(length, width)
    print(f"The area of the rectangle is {area}")

def area_triangle():
    base = float(input("Enter the base of the triangle: "))
    height = float(input("Enter the height of the triangle: "))
    area = area_triangle(base, height)
    print(f"The area of the triangle is {area}")
```

Srpski voz ka EU – (ne)otklonjivi kvar na vozu ili (s)kretanje u drugom pravcu?/
Serbian Train to EU – (Ir)reparable Breakdown on the Train or Turning/Moving in the Other Direction?

Publisher: JPM | Partners
Delta House, 8a Vladimira Popovića street
www.jpm.law
Authors: Ivan Milošević, Partner
Design and prepress: JPM | Partners
Copyright: © JPM | Partners 2026 All rights reserved.

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 & Partners.

Uvidom u dokumente Kancelarije za informacione tehnologije i elektronsku upravu i Ministarstva zdravlja smo utvrdili se Zakon o zaštiti podataka o ličnosti u vezi sa obradom podataka o ličnosti putem softverskih rešenja e-Bolovanje-Poslodavac, Ezdravlje i e-Bolovanje neadekvatno sprovodi ili se uopšte ne sprovodi. Iako je reč masovnoj obradi posebnih kategorija podataka o ličnosti, Poverenik nije sproveo nadzor na obradom od strane ova dva rukovaoca. Nakon sedam godina primene Zakona o zaštiti podataka o ličnosti, imamo sumnju u vezi sa pitanjem u naslovu ovog članka – kakav je uzrok kvara srpskog voza ka EU ili da nije možda reč o kvaru već o (s)kretanju u suprotnom pravcu?

By reviewing the documents of the Office for Information Technology and Electronic Administration and the Ministry of Health, we found that the Law on Protection of Personal Data in connection with the processing of personal data through the software solutions e-Bolovanje-Poslodavac, eZdravlje, and e-Bolovanje is either inadequately implemented or not implemented at all. Although it involves extensive processing of special categories of personal data, the Commissioner did not supervise the processing by these two controllers. After seven years of implementation of the Law on the Protection of Personal Data, we have doubts regarding the question in the title of this article – what is the cause of the failure of the Serbian train to the EU, or is it perhaps not a failure but a turning/movement in the opposite direction?

Kako smo u prošlom članku naveli, uputili smo zahtev za pristup informacijama od javnog značaja kojima se dokazuje usklađenost obrade podataka o ličnosti putem softverskih rešenja e-Bolovanje-Poslodavac, Ezdravlje i e-Bolovanje Kancelariji za informacione tehnologije i elektronsku upravu (Kancelarija), Ministarstvu zdravlja i Povereniku za informacije o javnog značaja i zaštitu podataka o ličnosti (Poverenik).

Kancelarija nam je dostavila Akt o proceni uticaja obrade na zaštitu podataka o ličnosti prilikom korišćenja softverskog rešenja e-Bolovanje-Poslodavac.

Ministarstvo zdravlja nam je dostavilo odgovor da je izvršena delimična procena uticaja obrade u okviru portala eZdravlje. Delimična procena nam nije dostavljena. Navodi se i to da je toku javna rasprava o Zakonu o izmenama i dopunama Zakona o zdravstvenoj dokumentaciji i evidencijama u oblasti zdravstva i da je namera Ministarstva zdravlja da pitanje procene uticaja na zaštitu podataka o ličnosti bude obuhvaćeno u postupku donošenja pomenutog propisa.

As we stated in the previous article, we sent a request for access to information of public importance proving compliance of personal data processing through software solutions e-Bolovanje-Poslodavac, Ezdravlje I e-Bolovanje to the Office for Information Technologies and Electronic Administration (Office), the Ministry of Health and the Commissioner for Information of Public Importance and Protection of Personal Data (Commissioner).

The Office submitted to us the Act on data protection impact assessment for the use of the e-Bolovanje-Poslodavac software solution.

The Ministry of Health sent us a response stating that a partial data protection impact assessment was carried out within the Ezdravlje portal. A partial assessment has not been submitted to us. It is also stated that a public debate is underway on the Law on Amendments to the Law on Health Documentation and Records in the Field of Health, and that the Ministry of Health intends to include a data protection impact assessment in the process of passing the aforementioned regulation.

Poverenik nam je dostavio odgovor da Kancelarija nije tražila mišljenje Poverenika na procenu uticaja na zaštitu podataka o ličnosti. Poverenik nije izvršio inspeksijskih nadzor nad obradom podataka o ličnosti putem softverskih rešenja e-Bolovanje-Poslodavac, a imajući u vidu napise u štampi povodom moguće zloupotrebe obrade podataka o ličnosti putem ovog softverskog rešenja.

Dokument Kancelarije

U dokumentu koji nam je dostavila Kancelarija navodi se sledeće:

„Povreda prava na zaštitu podataka o ličnosti lica na koje se podaci odnose može nastupiti zbog povrede bezbednosti prilikom prikupljanja, odnosno prenošenja podataka u okviru Softverskog rešenja e-Bolovanje-Poslodavac (Softversko rešenje), a usled neovlašćenog pristupa tom Softverskom rešenju i opremi koja se koristi u svrhu prikupljanja i prenošenja podataka. Usled navedenog događaja mogla bi nastupiti posledica koja se sastoji u povrede prava na zaštitu ličnih podataka lica na koje se podaci odnose i u odnosu na koje je povređena bezbednost.

The Commissioner provided us with an answer that the Office did not ask for the Commissioner’s opinion on the data protection impact assessment. The Commissioner did not conduct oversight of the processing of personal data through the software solution e-Bolovanje-Poslodavac, given the articles in the press regarding the possible misuse of personal data processed through this software solution.

The Document of the Office

The document provided to us by the Office states the following:

“Violation of the right to the protection of personal data of the person to whom the data refers may occur due to a breach of security during the collection, i.e. data transfer within the Software solution e-Bolovanje-Poslodavac (Software Solution), and due to unauthorised access to that Software solution and the equipment used for the purpose of collecting and transferring data. As a result of the aforementioned event, there may be a consequence consisting of a violation of the right to the protection of personal data of the person to whom the data relate, in relation to which the security is violated.

Ukazujemo da se u okviru Softverskog rešenja može vršiti obrada posebnih vrsta podataka o ličnosti i stoga postoji visok rizik koji je u vezi sa obradom navedene vrste podataka. Procenjujemo da je rizik od nastupanja događaja koji predstavlja opisani rizik nizak, imajući u vidu tehničke, organizacione i kadrovske mere opisane u nastavku ovog akta.“

Ovi navodi se odnose na procenu bezbednosti obrade iz člana 50 Zakona o zaštiti podataka o ličnosti, a ne na procenu uticaja obrade na zaštitu podataka o ličnosti iz člana 54 istog zakona.

Članom 50 stav 1 Zakona o zaštiti podataka o ličnosti propisano je da, u skladu sa nivoom tehnoloških dostignuća i troškovima njihove primene, prirodom, obimom, okolnostima i svrhom obrade, kao i verovatnoćom nastupanja i nivoom rizika za prava i slobode fizičkih lica, rukovalac i obrađivač sprovede odgovarajuće tehničke, organizacione i kadrovske mere kako bi dostigli odgovarajući nivo bezbednosti u odnosu na rizik.

We point out that the Software Solution can process special categories of personal data, and therefore, there is a high risk associated with its processing. We estimate that the risk of the occurrence of the event that represents the described risk is low, taking into account the technical, organisational, and personnel measures described in the rest of this act.”

These statements refer to the assessment of the security of processing under Article 50 of the Law on Protection of Personal Data, not to the assessment of the impact on personal data protection under Article 54 of the same law.

Article 50 paragraph 1 of the Law on Protection of Personal Data prescribes that, taking into account 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, organisational and personnel measures to ensure a level of security appropriate to the risk.

Članom 50 stav 3 Zakona o zaštiti podataka o ličnosti propisano je da se prilikom procenjivanja odgovarajućeg nivoa bezbednosti obrade posebno uzimaju u obzir rizici obrade, a naročito rizici od slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneseni, pohranjeni ili obrađivani na drugi način.

Navodi Kancelarije u dokumentu da povreda prava na zaštitu podataka o ličnosti lica na koje se podaci odnose može nastupiti zbog povrede bezbednosti prilikom prikupljanja, odnosno prenošenja podataka u okviru Softverskog rešenja, a usled neovlašćenog pristupa tom Softverskom rešenju i opremi koja se koristi u svrhu prikupljanja i prenošenja podataka nisu utemeljeni na pravilnoj primeni zakona.

Ova tvrdnja nije potkrepljena metodološkim pristupom – nije jasno kako je, odnosno na osnovu kojih merljivih pokazatelja je izvršena procena verovatnoće nastanka događaja odnosno pretnje za bezbednost obrade – da postoji visok rizik od neovlašćenog pristupa podacima o ličnosti, a imajući u vidu prirodu, obim, okolnosti i svrhe obrade podataka o ličnosti.

Article 50 paragraph 3 of the Law on Protection of Personal Data stipulates 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.

The citations of the Office in the document that the violation of the right to the protection of the personal data of the person to whom the data refers may occur due to a breach of security during the collection and transmission of data within the Software solution, and as a result of unauthorized access to that Software solution and the equipment used for data collection and transmission are not based on proper implementation of the law.

A methodological approach does not support this claim - it is not clear how, that is, based on which measurable indicators, the probability of the occurrence of the event, i.e. the threat to the security of the processing, was assessed - that there is a high risk of unauthorized access to personal data, bearing in mind the nature, scope, circumstances and purposes of personal data processing.

Dodatno, u dokumentu nije objašnjeno na osnovu kojih parametra se došlo do procene da neovlašćeni pristup podacima o ličnosti može da proizvede štetne posledice i koje su to štetne posledice po podatke o ličnosti i prava i slobode građana. Prema metodologiji za procenu rizika bezbednosti obrade, verovatnoća nastupanja rizika bezbednosti obrade se procenjuje u odnosu na bezbednost obrade u četiri poslovna segmenta svake organizacije:

1. mreže i tehničkih resursa;
2. procesa i procedura za obradu podataka o ličnosti;
3. strana koje su uključene u obradu podataka o ličnosti i
4. radnog okruženja (aplikativnog nivoa) u kome se vrši obrada podataka o ličnosti.

Na kraju, postavlja se pitanje kako je rukovalac grupisao klase faktora rizika; ni ovaj podatak nije naveden u aktu. Štaviše, nije primenjen osnovni metodološki pristup proceni rizika – da se rizici bezbednosti obrade na podatke o ličnosti procenjuju nezavisno od tehničkih i organizacionih mera koje se trenutno primenjuju.

In addition, the document did not explain on what parameters the assessment was made that unauthorised access to personal data can produce harmful consequences, nor what those consequences are for personal data and the rights and freedoms of citizens. According to the processing security risk assessment methodology, the probability of occurrence of processing security risks is assessed in relation to of security of processing in four business segments of each organization:

1. network and technical resources;
2. processes and procedures for personal data processing;
3. parties involved in personal data processing and
4. working environment in which personal data processing takes place (applicative level).

Finally, the question arises as to how the controller grouped the risk factor classes, and this information is not specified in the act. Moreover, an essential methodological approach was not applied to assess risks to the security of processing independently of the technical and organisational measures currently in place.

Naprotiv, pošlo se od pretpostavke da su tehničke i organizacione mere a priori dovoljne za zaštitu podataka o ličnosti od neovlašćenog pristupa. Postavlja se pitanje da li su rizici bezbednosti obrade uopšte procenjivani ili se pošlo od pretpostavke da su implementirane tehničke i organizacione mere adekvatne i da nije potrebno da se procenjuju rizici bezbednosti obrade na podatke o ličnosti.

Iz dokumenta koji nam je dostavljen od strane Kancelarije može se zaključiti da uopšte nisu procenjivani rizici u vezi sa skladištenjem podataka o ličnosti na klauđu kao a priori nebezbednom medijumu za skladištenje podataka o ličnosti. Zahtevi za bezbednost podataka o ličnosti na klauđu su propisani u standardu SRPS ISO/IEC 27701:2019.

Na osnovu svega navedenog, zaključujemo da verovatnoća nastanka događaja (realizacije pretnje odnosno rizika i verovatnoća uticaja pretnje, odnosno rizika), nije adekvatno procenjena, a samim tim nije ni ispunjen zahtev iz člana 50 Zakona o zaštiti podataka o ličnosti – da rukovalac sprovodi odgovarajuće tehničke, organizacione i kadrovske mere kako bi dostigli odgovarajući prihvatljiv nivo bezbednosti u odnosu na procenjeni rizik.

On the contrary, it was assumed that technical and organisational measures are a priori sufficient to protect personal data from unauthorised access. The question arises as to whether the risks to the security of processing were assessed at all, or whether it was assumed that the implemented technical and organisational measures are adequate and that it is not necessary to assess the risks to the security of processing of personal data.

From the document submitted to us by the Office, it can be concluded that the risks associated with storing personal data in the cloud, an a priori unsafe medium, were not assessed at all. Requirements for the security of personal data in the cloud are prescribed in the SRPS/IEC ISO 27701:2019 standard.

Based on all of the above, we conclude that the probability of the event (threat, i.e., risk realisation) and the probability of the threat or risk impact have not been adequately assessed. Therefore, the requirement from Article 50 of the Law on Protection of Personal Data has not been met - that the controller implements appropriate technical, organisational, and personnel measures to achieve an appropriate acceptable level of security in relation to the assessed risk.

Sa druge strane, Kancelarija nije sprovela procenu uticaja obrade na zaštitu podataka o ličnosti. Razliku od procene rizika bezbednosti obrade u kojoj je fokus na pitanju kakva je zaštita podataka o ličnosti (kakva je bezbednost obrade) i kako ta ista zaštita može da utiče na prava i slobode građana.

Kod procene rizika za prava i slobode građana je fokus na činjenici kako sama obrada podataka o ličnosti može da utiče na prava i slobode građana i drugih lica. Navodimo primer: kako automatsko obaveštavanje poslodavaca o promenama u vezi sa privremenom sprečenošću za rad zaposlenog može da utiče na pravni položaj građana, koje se tehničke, organizacione i pravne mere primenjuju da bi se smanjio štetan uticaj takve obrade i na koji način se došlo do toga da se baš određene mere primenjuju, a ne neke druge mere.

Da bi čitaocima bilo jasno: Softversko rešenje eZdravlje putem Softverskog rešenja automatski šalje obaveštenja poslodavcu o promenama u vezi sa privremenom sprečenošću za rad zaposlenog i podnetim prigovorima i zahtevima.

On the other hand, the Office did not carry out a data protection risk assessment. In contrast to the risk assessment of the security of processing, in which the focus is on the question of the protection of personal data (what is the security of processing) and how this same protection can affect the rights and freedoms of citizens.

In the data protection risk assessment is focus on the fact that the processing of personal data itself can affect the rights and freedoms of citizens and other persons. Here is an example: how automatic notification of employers about changes related to the temporary incapacity for work of an employee can affect the legal position of citizens, what technical, organisational, and legal measures are applied to reduce the harmful impact of such processing and how it came to be that certain measures are applied, and not some other measures.

To make it clear to the readers: The eZdravlje software solution automatically sends notifications to the employer about changes related to the employee's temporary incapacity for work, as well as submitted complaints and requests, through the Software Solution.

U situacijama kada izabrani lekar ne produži datum očekivanog trajanja privremene sprečenosti za rad, a osiguranik se ne pojavi na pregledu, zatim na kraju meseca tokom trajanja privremene sprečenosti za rad, kao i kada se promeni isplatilac naknade zarade tokom trajanja privremene sprečenosti za rad, izveštaj se izdaje u formi elektronskog dokumenta na automatizovan način.

Automatska obrada uključuje sledeće podatke o ličnosti status privremene sprečenosti i podatke o ličnosti podatke zaposlenog, i to: ime i prezime, jedinstveni matični broj građanina (JMBG), odnosno evidencijski broj za strance (EBS).

In situations where the selected doctor does not extend the expected duration of temporary incapacity for work, and the insured does not appear for the examination, then at the end of the month during the period of temporary incapacity for work, as well as when the payer of the wage compensation changes during the period of temporary incapacity for work, the report is issued in the form of an electronic document in an automated manner.

Automatic processing includes the following personal data: the status of temporary disability and the employee's personal data, namely: first and last name, unique citizen identification number (JMBG), or registration number for foreigners (EBS).

Dokument Ministarstva zdravlja

Činjenica da Ministarstvo zdravlja već godinama obrađuje podatke o ličnosti u okviru softverskih rešenja eZdravlje i e-Bolovanje i da još uvek nije sprovedena procena uticaja obrade na prava i slobode građana je sama po sebi upitna. Reč je o softverskim rešenjima koja obrađuju posebne kategorije podataka o ličnosti više miliona građana, a sama činjenica da je reč o najosetljivijim podacima o ličnosti građanstva ukazuje na to da bi Poverenik morao hitno da reaguje i da preduzme odgovarajuće mere.

Za sedam godina primene Zakona o zaštiti podataka o ličnosti, Poverenik nije našao da je potrebno da objasni razliku između procene rizika informacione bezbednosti, procene rizika bezbednosti obrade i procene uticaja obrade na zaštitu podataka o ličnosti, niti da u nadzoru nad sprovođenjem ovog zakona zahteva od rukovodstva da dostave ove procene.

The document of the Ministry of Health

The fact that the Ministry of Health has been processing personal data for years through the software solutions eZdravlje and e-Bolovanje, and that a data protection risk assessment has not yet been carried out, is questionable in itself. It concerns software solutions that process special categories of personal data for several million citizens, and the very nature of this data indicates that the Commissioner must act urgently and take appropriate measures.

In seven years of implementing the Personal Data Protection Act, the Commissioner did not find it necessary to explain the differences between information security risk assessment, risk for the security of processing, and data protection risk assessment, nor to require controllers to submit these assessments during the supervision of the implementation of this law.

Zaključak

Naš je utisak da ne postoji konsenzus o tome da su adekvatne procene bezbednosti obrade i uticaja o obrade na zaštitu podataka o ličnosti od suštinske važnosti za bezbednost podataka i da direktno utiče na stepen uživanja prava svih građana na zaštitu podataka o ličnosti. Nakon sedam godina primene Zakona o zaštiti podataka o ličnosti, postoje ozbiljni problemi u razumevanju osnovnih termina u Zakonu o zaštiti podataka o ličnosti i u njihovoj primeni.

Conclusion

It is our impression that there is no consensus that adequate assessment of the security of processing and the data processing impact assessment are essential for data security and that they directly affect the degree of enjoyment of the right to protection of personal data by all citizens. After seven years of implementing the Law on Protection of Personal Data, there are serious problems with understanding its basic terms and their application.

Autor/Author



Ivan Milošević

Partner

E: ivan.milosevic@jpm.law

JPM | PARTNERS

8a Vladimira Popovića,

DELTA HOUSE, V Floor

11070 Belgrade, Serbia

T: + 381/11/207-6850

E: office@jpm.law

www.jpm.law