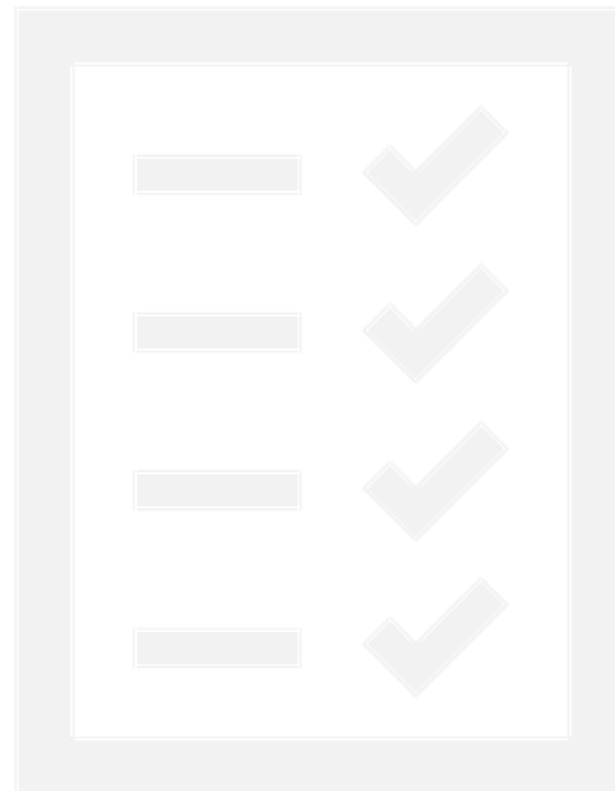


Usklađivanje poslovanja sa odredbama novog Zakona o zaštiti podataka o ličnosti – interni i eksterni akti

Milica Basta
Senior Associate

Sadržaj

1. Zakon o zaštiti podataka o ličnosti (2018) – ZZPL
2. Koraci u procesu usklađivanja
3. Interni akti
4. Obaveštenje o povredi podataka o ličnosti
5. Evidencija radnji obrade
6. Procena uticaja [obrade] na zaštitu podataka o ličnosti
7. Analiza legitimnog interesa kao osnova za obradu
8. Eksterni akti
9. Akti u domenu transfera podataka



Zakon o zaščiti podataka o ličnosti (2018) - ZZPL


1. Zakon o zaštiti podataka o ličnosti (2018) - ZZPL

- Datum stupanja ZZPL -a na snagu: 21. novembar 2018. godine
- Datum početka primene ZZPL -a: 21. avgust 2019. godine

ZZPL-om se u pravni sistem Srbije transponuju Opšta uredba o zaštiti podataka o ličnosti (*General Data Protection Regulation – GDPR*) (2016/679) i Policijska direktiva (*Police Directive*) (2016/680).

ZZPL u najvećoj meri preuzima rešenja iz GDPR-a. Neke od razlika:

- pravni osnov za transfer (iznošenje) podataka iz Srbije;
- stepen verovatnoće nastupanja rizika po prava i slobode lica u vezi sa obaveštavanjem Poverenika i lica o povredi bezbednosti podataka (*data breach*) – verovatnoća nastupanja rizika prema GDPR-u i mogućnost nastupanja rizika prema ZZPL-u; i
- stepen verovatnoće nastupanja rizika i stepena ozbiljnosti rizika u vezi sa izradom evidencija radnji obrade - verovatnoća nastupanja rizika prema GDPR-u i mogućnost nastupanja rizika prema ZZPL; rizik prema GDPR-u i visok rizik prema ZZPL-u.



Koraci u procesu usklađivanja

2. Koraci u procesu usklađivanja

Postoji mogućnost da se postupci usklađivanja (*compliance actions*) koje sprovode multinacionalne kompanije na globalnom nivou primene i na zavisna društva (*subsidiaries*) tih kompanija u Srbiji, uz izvesna prilagođavanja.

Sled koraka:

- Detektovanje konkretnih obrada podataka o ličnosti koje kompanija sprovodi;
- Utvrđivanje svrhe i pravnog osnova za svaku pojedinačnu obradu;
- Ocena srazmernosti svake pojedinačne obrade u odnosu na svrhu koja se tom obradom postiže;
- Donošenje odluke o tome koje obrade treba nastaviti (jer su dozvoljene), a koje modifikovati zbog uočenih nedostataka; i
- Izrada ili revizija akata koji moraju ili treba da prate svaku konkretnu obradu.

Interni akti

3. Interni akti

Akti koje kompanija treba da usvoji *nezavisno od konkretnih obrada*:

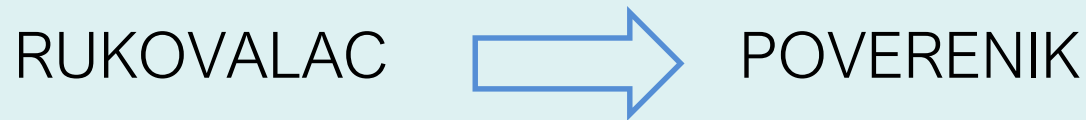
- Procedura postupanja u slučaju povrede podataka (*Data Breach Procedure*); i
- Procedura postupanja po zahtevima lica čiji se podaci obrađuju (*Data Subject Request Procedure*), sa obrascima za dostavljanje odgovora na zahteve.

Akti koje kompanija treba ili mora da usvoji *u vezi sa konkretnim obradama*:

- Politika zadržavanja (čuvanja) podataka (*records retention policy*);
- Evidencije radnji obrade (*records of processing activities*);
- Procena uticaja [obrade] na zaštitu podataka o ličnosti (*data protection impact assessment - DPIA*); i
- Analiza legitimnog interesa rukovaoca ili treće strane kao osnova za obradu (*legitimate interests assessment – LIA*).

Obaveštenje o povredi podataka o ličnosti

4. Obaveštenje o povredi podataka o ličnosti (čl. 52 i 53)



- Ako povreda može da predstavlja rizik za prava lica.
- Bez odlaganja, najkasnije u roku od 72 časa od saznanja za povredu.

Obaveštenje sadrži:

- prirodu povrede, vrste podataka i približan broj lica i podataka obuhvaćenih povredom;
- ime i kontakt lica za zaštitu podataka ili informacije o drugom načinu na koji se mogu dobiti podaci o povredi;
- moguće posledice povrede;
- opis mera koje je rukovalac preduzeo ili čije je preduzimanje predloženo u vezi sa povredom.

Pravilnik o obrascu obaveštenja o povredi podataka o ličnosti i načinu obaveštavanja Poverenika o povredi podataka o ličnosti (2019)

4. Obaveštenje o povredi podataka o ličnosti (nastavak)



Obrađivač obaveštava rukovaoca o povredi bez nepotrebnog odlaganja, po saznanju za povredu.



- Kada povreda može da prouzrokuje visok rizik po prava i slobode lica.
- Obaveza obaveštavanja ne postoji ako:
 - je rukovalac adekvatno zaštitio podatke (naročito kriptozastitom ili sličnom metodom koja onemogućava da podaci budu razumljivi neovlašćenim licima);
 - je rukovalac naknadno preduzeo mere koje onemogućavaju da povreda proizvede posledice po određeno lice; ili
 - bi obaveštavanje predstavljalo nesrazmeran utrošak vremena i sredstava za rukovaoca (umesto toga, javno obaveštavanje ili sličan metod).

Evidencija radnji obrade



5. Evidencija radnji obrade (čl. 47)

Obaveza rukovaoca i obrađivača koji zapošljavaju 250 ili više lica.

Obaveza postoji **bez obzira** na broj zaposlenih ako:

- obrada nije povremena (tj. radi se o kontinuiranoj obradi);
- obrada može da predstavlja visok rizik po prava i slobode lica;
- obrada uključuje posebne vrste podataka o ličnosti; ili
- obrada uključuje podatke u vezi sa krivičnim presudama, kažnjivim delima i merama bezbednosti.

Evidencija se ne registruje.

Dostavljanje Povereniku na zahtev.

Mogućnost korišćenja evidencija koje su rukovaoci formirali prema Zakonu iz 2008. godine.

5. Evidencija radnji obrade (nastavak)

Evidencija koju vodi rukovalac sadrži:

- ime i kontakt podatke rukovaoca, zajedničkih rukovalaca, predstavnika rukovaoca i lica za zaštitu podataka o ličnosti;
- svrhe obrade;
- vrste lica i vrste podataka o ličnosti;
- vrste primalaca kojima su podaci otkriveni ili će im biti otkriveni, uključujući primaocce u drugim državama ili međunarodnim organizacijama;
- prenos podataka u druge države ili međunarodne organizacije, uz navođenje naziva tih država i međunarodnih organizacija, i dokumenata kojima se obezbeđuju mere zaštite;
- rok za brisanje podataka; i
- tehničke i organizacione bezbednosne mere, ukoliko ih je moguće navesti.

5. Evidencija radnji obrade (nastavak)

Evidencija koju vodi **obrađivač** sadrži:

- ime i kontakt podatke svakog obrađivača i svakog rukovaoca u čije ime se obrada vrši, predstavnika rukovaoca ili obrađivača i lica za zaštitu podataka o ličnosti;
- vrste obrade koje se obavljaju u ime svakog rukovaoca;
- prenos podataka u druge države ili međunarodne organizacije, uz navođenje naziva tih država i međunarodnih organizacija, i dokumenata kojima se obezbeđuju mere zaštite;
- tehničke i organizacione bezbednosne mere, ukoliko ih je moguće navesti.

Procena uticaja [obrade] na zaštitu podataka o ličnosti (čl. 54 i 55)

6. Procena uticaja [obrade] na zaštitu podataka o ličnosti (čl. 54 i 55)

Sprovodi je rukovalac pre početka obrade, ako je verovatno da će vrsta obrade, posebno ako se sprovodi upotrebom novih tehnologija i uzimajući u obzir prirodu, obim, okolnosti i svrhu obrade, predstavljati visok rizik za prava i slobode lica.

Procena se obavezno sprovodi ako obrada podrazumeva:

- sistematske i sveobuhvatne procene stanja i osobina fizičkog lica koje se zasnivaju na automatskoj obradi, kao što je profilisanje, na osnovu kojih se donose odluke koje značajno utiču na pojedinca;
- opsežnu obradu posebnih vrsta podataka, ili podataka u vezi sa krivičnim presudama i kažnjivim delima; ili
- sistematsko i opsežno praćenje javno dostupnih površina.

6. Procena uticaja [obrade] na zaštitu podataka o ličnosti (nastavak)

Kako oceniti stepen rizika? Dokumentovanje odluke rukovaoca da ne radi procenu.

Odluka o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika (2019)

Moguća je jedna procena za više sličnih obrada.

Procena sadrži:

- sveobuhvatan opis predviđenih radnji obrade i svrhe obrade, kao i legitimnog interesa rukovaoca (ako on postoji);
- procenu neophodnosti i srazmernosti obrade u odnosu na svrhe;
- procenu rizika po prava i slobode lica; i
- mere za rešavanje problema rizika, što uključuje mere bezbednosti.

6. Procena uticaja [obrade] na zaštitu podataka o ličnosti (nastavak)

Prema ZZPL-u, ako procena uticaja ukazuje na visok rizik u slučaju nepreduzimanja mera za umanjeње rizika, rukovalac je dužan da pre započinjanja obrade traži mišljenje Poverenika.

Logično: traženje mišljenja obavezno kada procena ukazuje na visok rezidualni rizik.

Smernice Radne grupe 29 o proceni uticaja obrade na zaštitu podataka o ličnosti, 4. april 2017.

Prema Odluci Poverenika, kod svih obrada kod kojih se procena obavezno sprovodi, takođe je obavezno da se traži mišljenje.

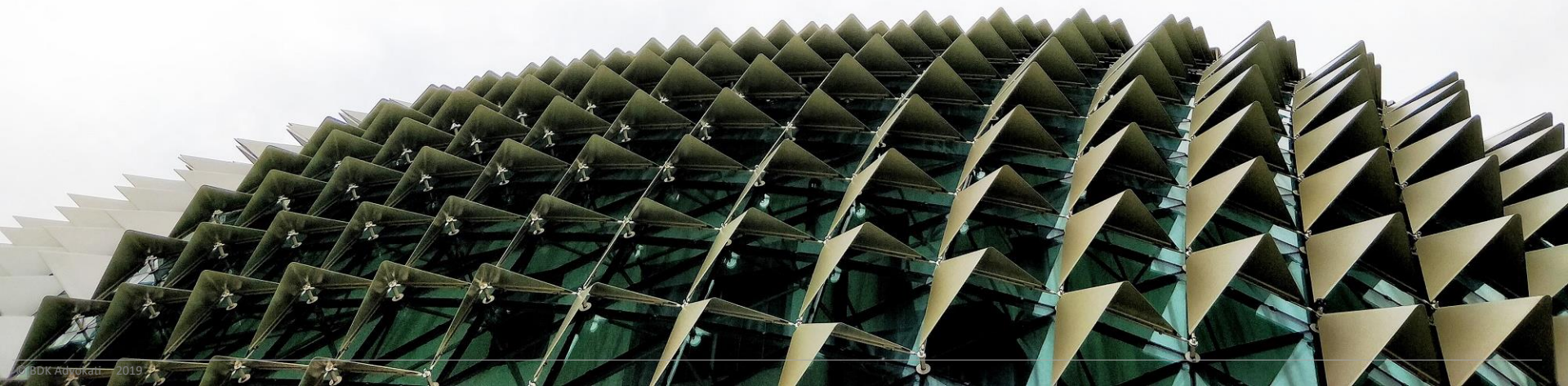
Analiza legitimnog interesa kao osnova za obradu

7. Analiza legitimnog interesa kao osnova za obradu

- Ne spada u kategoriju akata čije je donošenje obavezno.
- Od značaja je za dokumentovanje (ovo se posebno odnosi na situacije kada legitimni interes ili njegova prevalentnost nisu očigledni).



Eksterni akti – akti koje kompanija predaje ili zaključuje sa drugim licima, koje pribavlja ili kojima pristupa



8. Eksterni akti – akti koje kompanija predaje ili zaključuje sa drugim licima, koje pribavlja ili kojima pristupa

- obaveštenja kojima se lica upoznaju sa obradom njihovih podataka o ličnosti (*notices to data subjects*) – članovi 23 i 24 ZZPL;
- akt kojim se Poverenik obaveštava o licu za zaštitu podataka o ličnosti i njegovim kontakt podacima;
- ugovori sa obrađivačima podataka (*data processing agreements*) – čl. 45 ZZPL;
- politika upotrebe "kolačića" na sajtu kompanije (*cookie policy*);
- saglasnost lica za obradu podataka o ličnosti (*data subjects's consents*) – ograničena mogućnost oslanjanja (zaposleni);
- ugovori o radu;
- kontrolna lista pomoću koje se utvrđuje stepen usklađenosti sa ZZPL-om; i
- akti u domenu transfera (iznošenja) podataka.

Akti u domenu transfera podataka



9. Akti u domenu transfera podataka

Potrebni su kod transfera u države koje ne obezbeđuju primereni nivo zaštite podataka.

Države koje obezbeđuju primereni nivo zaštite:

- Članice Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu ličnih podataka;
- Države za koje je EU svojim odlukama (*adequacy decisions*) utvrdila da obezbeđuju primereni nivo zaštite;
- Države sa kojima Srbija zaključi međunarodni sporazum o prenosu podataka o ličnosti.

Lista država koje obezbeđuju primereni nivo zaštite - Odluka Vlade iz avgusta 2019. godine

9. Akti u domenu transfera podataka

Vrste akata:

- Standardne ugovorne klauzule koje izrađuje Poverenik (ovlašćenje, ali ne i obaveza);
- Obavezujuća poslovna pravila (Binding Corporate Rules – BCRs) koje odobrava Poverenik;
- Kodeksi postupanja – izrađuju ih udruženja i drugi subjekti koji predstavljaju grupe rukovalaca i obrađivača, a registruje i javno objavljuje Poverenik;
- Sertifikati – izdaju ih sertifikaciona tela ili Poverenik;
- Saglasnost lica; i
- Dozvola Poverenika.



Advokati

BDK Srbija

Bulevar kralja Aleksandra 28
11000 Beograd
Tel: +381 11 3284 212
Fax: +381 11 3284 213
office@bdkadvokati.com

BDK Crna Gora

Cetinjska 11, The Capital Plaza
81000 Podgorica
Tel: +382 20 230 396
Fax: +382 20 230 396
office.cg@bdkadvokati.com

BDK Bosna i Hercegovina

Gundulićeva 6
78000 Banja Luka
Tel: +387 51 250 641
Fax: +387 51 250 642
office.banjaluka@bdkadvokati.com

www.bdkadvokati.com

